ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ-ΔΙΟΙΚΗΣΗ ΟΛΙΚΗΣ ΠΟΙΟΤΗΤΑΣ (MBA-TQM)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Διαχείριση Παραβατικότητας μέσω Τεχνικών Ασφαλείας στο Διαδίκτυο

Χαραλαμπία Ν. Φλώρου

Τριμελής Επιτροπή

Επιβλέπων Καθηγητής: Σφακιανάκης Μιχαήλ
Αναπληρωτής Καθηγητής: Μακρής Αριστομένης
Λέκτορας: Μαραβελάκης Πέτρος

Πειραιάς

Οκτώβριος 2013

Περίληψη.

Η παρούσα εργασία έχει ως στόχο να παρουσιάσει τις ποικίλες μορφές παραβατικότητας που εκτελούνται μέσω ηλεκτρονικού υπολογιστή και διαδικτύου, ξεκινώντας από τα γνήσια ηλεκτρονικά εγκλήματα στα οποία ο υπολογιστής αποτελεί αποκλειστικό μέσο τέλεσής τους έως τα συμβατικά εγκλήματα τα οποία πραγματοποιούνται και χωρίς τη χρήση ηλεκτρονικού υπολογιστή. Αναμφίβολα το διαδίκτυο αποτελεί ένα από τα πιο καινοτόμα επιτεύγματα της τεχνολογίας και συνιστά ένα πανίσχυρο εργαλείο όχι μόνο πληροφόρησης, επικοινωνίας, κοινωνικοποίησης, συναλλαγών και λοιπών δραστηριοτήτων αλλά και εκμετάλλευσης όλων των δυνατοτήτων που μπορεί να προσφέρει στους χρήστες του για ίδιον όφελος, ανεξαρτήτως γεωγραφικών συνόρων.

Στο σημείο αυτό ελλοχεύει πλήθος κινδύνων που μπορεί να προκαλέσει μείζονος ή ήσσονος σημασίας προβλήματα, ανάλογα με τη μορφή παραβατικότητας. Αξίζει να σημειωθεί ότι κάθε ευκαιρία που παρουσιάζεται, ακολουθείται από μία πρόθεση κακόβουλης εκμετάλλευσής της. Συνεπώς, στη συνέχεια θα περιγραφούν τα μέτρα για τη διαχείριση της παραβατικότητας που κρίνονται απολύτως αναγκαία, καθώς εξασφαλίζουν την ασφαλέστερη χρήση του διαδικτύου.

Τέλος, αφού παρουσιαστούν και αναλυθούν οι βασικές έννοιες για την κατανόηση της παρούσας εργασίας όπως ο ηλεκτρονικός υπολογιστής, το διαδίκτυο, τα μέσα κοινωνικής δικτύωσης, αλλά και οι ορισμοί εγκλήματος και ηλεκτρονικού εγκλήματος,στη συνέχεια παρατίθεται το εγχώριο αλλά και διεθνές νομοθετικό πλαίσιο που διέπει το ηλεκτρονικό έγκλημα καθώς και οι προτεινόμενοι τρόποι με τους οποίους οι χρήστες μπορούν να προστατευτούν από κάθε είδους παραβατικότητα στο διαδίκτυο.

Λέξεις Κλειδιά: Διαδίκτυο, Παραβατικότητα, Κοινωνική δικτύωση, Ηλεκτρονικό έγκλημα, Τεχνικές ασφαλείας

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον Καθηγητή κ. Μ. Σφακιανάκη για την παροχή των πολύτιμων επιστημονικών του συμβουλών και επισημάνσεων κατά την επίβλεψη της εργασίας μου.

Ευχαριστώ όλους τους καθηγητές του μεταπτυχιακού προγράμματος για τη συμβολή τους στην απόκτηση πολύ σημαντικών γνώσεων.

Επίσης μέσα από την καρδιά μου ευχαριστώ την οικογένεια μου για την αμέριστη συμπαράσταση και ενθάρρυνση που μου προσφέρει όλα αυτά τα χρόνια για την επιτυχή ολοκλήρωση των σπουδών μου.

Τέλος θα ήθελα να ευχαριστήσω όλους όσους με στήριξαν κατά τη διάρκεια του απαιτητικού αυτού μεταπτυχιακού προγράμματος.

Εισαγωγή

Αντικείμενο της παρούσας εργασίας αποτελεί η μελέτη του σύγχρονου και συνεχώς αυξανόμενου φαινομένου του ηλεκτρονικού εγκλήματος, των χαρακτηριστικών του, των μορφών με τις οποίες αυτό παρουσιάζεται καθώς και ο τρόπος διαχείρισης του μέσω τεχνικών ασφαλείας.

Στόχος της εργασίας είναι μέσω της περιγραφής της σύγχρονης μορφής παραβατικότητας στο διαδίκτυο (ηλεκτρονικό έγκλημα) να προταθούν τεχνικές ασφαλείας, οι οποίες δύναται να υιοθετηθούν από χρήστες κάθε ηλικίας προκειμένου να προστατευτούν και να αντιμετωπίσουν κάθε είδους εγκληματική διαδικτυακή δραστηριότητα.

Το περιεχόμενο της συγκεκριμένης εργασίας βασίστηκε τόσο σε διεθνείς και ελληνικές βιβλιογραφικές αναφορές ηλεκτρονικής και έντυπης μορφής όσο και σε πραγματικά στοιχεία τα οποία αντλήθηκαν από τους διαδικτυακούς τόπους της Ελληνικής Αστυνομίας, της Eurostat και του Internet World Statistics. Τέλος, έγινε χρήση του υπάρχοντος εγχώριου και διεθνούς νομοθετικού πλαισίου που διέπει το ηλεκτρονικό έγκλημα.

Συγκεκριμένα, με το μείζον ζήτημα της παραβατικότητας στο διαδίκτυο έχει ασχοληθεί στο βιβλίο του ο Steve Furnell «Κυβερνοέγκλημα. Καταστρέφοντας την κοινωνία της πληροφορίας». Στο βιβλίο αυτό περιγράφεται η εξάρτηση της κοινωνίας από το διαδίκτυο, επισημαίνονται οι κίνδυνοι που ελλοχεύουν από τη χρήση του και δίνεται έμφαση στην πρόληψη και ασφάλεια των δραστηριοτήτων των χρηστών στο διαδίκτυο. Ο ίδιος ο Furnell ορίζοντας το κυβερνοέγκλημα (cyber-crime) και εκτιμώντας το μέγεθος του προβλήματος αυτού προσπαθεί να σκιαγραφήσει το προφίλ των διαδικτυακών εγκληματιών και τις ζημιές που μπορούν να προκαλέσουν σε χρήστες του Ίντερνετ μεμονωμένα αλλά και συνολικά στην κοινωνία.

Το ηλεκτρονικό έγκλημα, οι μορφές, τα μέσα τέλεσης αυτού αλλά και γενικότερα η παραβατικότητα στο διαδίκτυο έχει αποτελέσει τον πυρήνα της διπλωματικής εργασίας αρκετών φοιτητών κυρίως στα Τμήματα Πληροφορικής και Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Αντλώντας πληροφορίες από όλες τις ανωτέρω πηγές η δομή της παρούσας εργασίας συνίσταται στα παρακάτω.

Στο πρώτο κεφάλαιο παρουσιάζεται η ιστορική εξέλιξη των υπολογιστών καθώς και ο διαχωρισμός τους σε εποχές ανάλογες με το εξελικτικό στάδιο φτάνοντας ως το σήμερα.

Στο δεύτερο κεφάλαιο δίνονται οι ορισμοί του ηλεκτρονικού εγκλήματος και του διαδικτύου καθώς είναι οι δύο έννοιες που συναποτελούν το σύγχρονο ηλεκτρονικό έγκλημα και στη συνέχεια παρατίθενται τα κυριότερα χαρακτηριστικά του.

Στο τρίτο κεφάλαιο περιγράφονται οι κατηγορίες του ηλεκτρονικού εγκλήματος καθώς και οι μορφές με τις οποίες εμφανίζεται.

Στο τέταρτο κεφάλαιο περιγράφεται η σύγχρονη έννοια της κοινωνικής δικτύωσης, τα μέσα κοινωνικής δικτύωσης κάνοντας ξεχωριστή μνεία σε Facebook και Twitter.

Στο πέμπτο κεφάλαιο αναλύουμε το νομοθετικό πλαίσιο που διέπει το ηλεκτρονικό έγκλημα σε Ελλάδα και εξωτερικό .

Τέλος, το κεφάλαιο έξι αφορά τη διαχείριση παραβατικότητας μέσω τεχνικών ασφαλείας σε όλο το φάσμα του διαδικτύου, και συνοψίζοντας στο κεφάλαιο επτά τα όσα καταγράφονται στην παρούσα εργασία προτείνονται κάποιες συμβουλές προστασίας για ασφαλείς διαδικτυακές δραστηριότητες.

ΚΕΦΑΛΑΙΟ 1^{ο}

Ιστορική Εξέλιξη των Υπολογιστών

1.1 Η «προϊστορική εποχή»

Είναι σημαντικό να γίνει μία μικρή αναφορά σε εκείνους τους ανθρώπους αλλά και επιστήμονες που συνέβαλαν στην ανάπτυξη και εξέλιξη των ηλεκτρονικών υπολογιστών χωρίς την ύπαρξη των οποίων δεν θα εμφανιζόταν το ηλεκτρονικό έγκλημα.

Η ιστορία των υπολογιστικών μηχανών ξεκινάει από την αρχαιότητα. Κοντά στο 4.000 π.Χ. εμφανίζεται ο άβακας, αρχικά μάλλον στην Κίνα. Οι πρώτοι μηχανισμοί όμως που, τηρουμένων των αναλογιών μπορούν να θεωρηθούν ότι προσιδιάζουν με τους σύγχρονους αναλογικούς υπολογιστές είναι οι αστρολάβοι. Οι αστρολάβοι χρησιμοποιήθηκαν για την παρατήρηση των αστέρων και τον προσδιορισμό του ύψους τους από το ορίζοντα. Ένας τέτοιος μηχανισμός, που η έμπνευση του αποδίδεται στον Ίππαρχο είναι γνωστός ως «Αστρολάβος των Αντικυθήρων».

Είναι ο αρχαιότερος, πολυσύνθετος αστρονομικός φορητός υπολογιστής, με τον οποίον προσδιορίζονταν οι θέσεις του Ήλιου, της Σελήνης και, πιθανότατα, των πέντε γνωστών κατά την αρχαιότητα πλανητών του Ερμή, της Αφροδίτης, του Άρη, του Δία και του Κρόνου. Επίσης, χρησιμοποιούνταν για την πρόβλεψη των εκλείψεων του Ήλιου και της Σελήνης, για την τήρηση ενός πολυετούς ημερολογίου με μεγάλη ακρίβεια, καθώς και για τον προσδιορισμό του χρόνου τέλεσης των Πανελλήνιων Αγώνων που πραγματοποιούνταν στην Ολυμπία, στους Δελφούς, στη Νεμέα, στην Ισθμία και στη Δωδώνη.

Η κατασκευή του ανάγεται στο β΄ μισό του 2ου αι. π.Χ.. Η τεχνολογία του, η οποία παραπέμπει στους διαδόχους του Αρχιμήδη και τη Σχολή του Ποσειδωνίου στη Ρόδο, είναι αποτέλεσμα της ανάπτυξης της φιλοσοφίας και των θετικών επιστημών, που είχε συντελεστεί στον ελλαδικό χώρο μέχρι εκείνη την εποχή, και στηρίχθηκε σε γνώσεις της Ελληνιστικής Εποχής (αστρονομικές σταθερές, μηχανικό σχεδιασμό και χρήση των επικυκλικών οδοντωτών τροχών). Ο Μηχανισμός αποτελεί μαρτυρία για την

αστρονομική, μαθηματική και μηχανική ιδιοφυΐα των αρχαίων Ελλήνων στα μέσα του 2ου αι. π.Χ.

Η εύρεση του Μηχανισμού ανάμεσα στα άλλα αντικείμενα του φορτίου του πλοίου που ναυάγησε στα Αντικύθηρα προσδίδει στο ναυάγιο μοναδικότητα και απαράμιλλη σπουδαιότητα. Σώζονται 7 μεγάλα θραύσματα (A-G) και 75 μικρότερα σπαράγματα (1-75). Η ακριβής θέση τους και η αρχική δομή του Μηχανισμού αποτελεί αντικείμενο συνεχούς έρευνας. Περιελάμβανε τουλάχιστον 30 οδοντωτούς τροχούς καθώς επίσης κλίμακες, άξονες και δείκτες. Οι ελληνικές, αστρονομικού περιεχομένου επιγραφές στην επιφάνεια του Μηχανισμού αναφέρονται σε αστρονομικούς και ημερολογιακούς υπολογισμούς, ενώ οι επιγραφές στις μεταλλικές πλάκες, που τον προστάτευαν, αφορούν στις οδηγίες χρήσεις του οργάνου. Ο Μηχανισμός προστατευόταν από ξύλινο πλαίσιο, που έφερε από μια ορειχάλκινη πλάκα στην πρόσθια και στην οπίσθια όψη.

Στη συνέχεια έπεται η περίοδος από το 17^{ο} μέχρι το 19^{ο} αιώνα, η οποία σηματοδοτεί πλήθος ανακαλύψεων σε όλους τους τομείς των επιστημών. Ορισμένοι από τους πιο διακεκριμένους μαθηματικούς της εποχής απασχολήθηκαν κάποια στιγμή της ζωής τους με το πρόβλημα του «μηχανικού υπολογιστή». Το 1614 ο John Napier επινόησε του λογαρίθμους ως έναν τρόπο για να απλοποιήσει δύσκολους μαθηματικούς υπολογισμούς, και τρία χρόνια αργότερα κατασκεύασε μια πρωτόγονη συσκευή που μπορούσε να κάνει απλούς υπολογισμούς και ονομάστηκε ράβδοι του Napier. Η πρώτη προσπάθεια στον τομέα του μηχανικού υπολογισμού είναι του Γερμανού καθηγητή μαθηματικών και αστρονομίας Wilhelm Schickard. Το «υπολογιστικό ρολόι» του Schickard στηριζόταν σε απλά συστήματα τροχών και είχε τη δυνατότητα να εκτελεί και τις τέσσερις πράξεις της αριθμητικής. Τα σχέδιά του όμως δεν έγιναν ποτέ πραγματικότητα.

Το 1630 ο Oughtred κατασκεύασε το λογαριθμικό κανόνα, που θεωρείται ο πρώτος αναλογικός υπολογιστής. Χρησιμοποιούσε αποστάσεις (μήκη) ανάλογες με τους αριθμούς που έπαιρναν μέρος στην επεξεργασία (και όχι αριθμούς όπως ο άβακας) και είχε τη δυνατότητα να εκτελεί αριθμητικές πράξεις.

Έπειτα εμφανίστηκε ο μεγάλος μαθηματικός και φιλόσοφος Blaise Pascal. Ο Pascal το 1642, σε ηλικία 17 ετών, σχεδίασε και κατασκεύασε έναν από τους πρώτους μηχανικούς υπολογιστές, την πασκαλίνα, η οποία στηριζόταν στις ίδιες αρχές με αυτές

του Schickard. Συστήματα γραναζιών εκτελούσαν προσθέσεις και αφαιρέσεις. Κατασκευάστηκαν και πουλήθηκαν συνολικά 37 τέτοιες μηχανές (Κάβουρας, 1990).

Τη συνέχεια της προσπάθειας αυτής ανέλαβε ο Γερμανός μαθηματικός Gotifried Leibnitz ο οποίος αφού πρώτα μελέτησε το έργο του Pascal, το 1964 κατασκεύασε ένα μηχανικό υπολογιστή, τον τροχό του Leibnitz. Η μηχανή που κατασκεύασε μπορούσε να κάνει όχι μόνο πρόσθεση και αφαίρεση αλλά και πολλαπλασιασμό και διαίρεση. Οι δύο παραπάνω υπολογιστικές συσκευές, αν και αρκετά εντυπωσιακές για την εποχή τους, είχαν έλλειψη δύο θεμελιωδών χαρακτηριστικών για να θεωρηθούν υπολογιστές:

- Δεν είχαν μνήμη ώστε να είναι δυνατή η αποθήκευση στοιχείων σε μορφή που να μπορεί να «διαβάσει» η μηχανή
- Δεν ήταν προγραμματίσιμοι. Δηλαδή, ένα άτομο δεν θα μπορούσε να παράσχει εκ των προτέρων μια σειρά εντολών που να εκτελούνται από τη συσκευή χωρίς ανθρώπινη παρέμβαση.

Η πρώτη πραγματική υπολογιστική συσκευή που περιλαμβάνει αυτά τα δύο χαρακτηριστικά, κατασκευάστηκε το 1801 από τον Γάλλο Joseph Jacquard και δε δημιουργήθηκε για σκοπούς μαθηματικών υπολογισμών αλλά ήταν ένας αργαλειός που κύριο σκοπό είχε την κατασκευή χαλιών και ρούχων. Ο αργαλειός του Jacquard αντιπροσωπεύει ένα πολύ σημαντικό στάδιο στην εξέλιξη των υπολογιστών, αφού δεν αποτέλεσε μόνο την πρώτη προγραμματιζόμενη υπολογιστική μηχανή αλλά έδειχνε και πως η γνώση ενός ειδικευμένου ατόμου θα μπορούσε να αποθηκευτεί σε μορφή που είναι δυνατόν να διαβαστεί από τη μηχανή και να πραγματοποιήσει αυτή την ίδια εργασία αυτόματα.

Ένα άτομο αρκετά επηρεασμένο από τις προηγούμενες εργασίες πάνω στα υπολογιστικά συστήματα ήταν καθηγητής μαθηματικών στο πανεπιστήμιο του Cambridge, Charles Babbage. Ο Babbage ασχολήθηκε αρκετά με τον αυτοματοποιημένο υπολογισμό. Το 1822 κατασκεύασε τη Διαφορική Μηχανή που μπορούσε να κάνει πρόσθεση, αφαίρεση, πολλαπλασιασμό και διαίρεση με ακρίβεια 6 δεκαδικών ψηφίων και να λύνει πολυωνυμικές εξισώσεις και άλλα πολύπλοκα μαθηματικά προβλήματα εξίσου καλά. Το 1830 σχεδίασε την Αναλυτική Μηχανή.

Παρόλο που θα περάσουν 110 χρόνια πριν από την κατασκευή ενός πραγματικού υπολογιστή, η προτεινόμενη μηχανή του Babbage είναι πραγματικά σχεδόν όμοια σε σχεδιασμό με το σύγχρονο υπολογιστή (Σφακιανάκης, 2003 & 2006).

1.2 Η γέννηση των υπολογιστών: 1940-1950

Οι ανάγκες του πολέμου για πολύπλοκους υπολογισμούς σε προβλήματα βαλλιστικής, μεταφοράς, διοίκησης και άλλα, κάνουν πιο επιτακτική την ανάγκη κατασκευής μιας ικανής υπολογιστικής μηχανής. Το 1939 ο καθηγητής John Atanasoff μαζί με τον μεταπτυχιακό σπουδαστή Clifford Berry, ανέπτυξαν τον πρώτο ηλεκτρονικό ψηφιακό υπολογιστή με την ονομασία Atanasoff-Berry computer. Αν και δεν αναγνωρίστηκε ποτέ επίσημα, ήταν ο πρώτος ηλεκτρονικός υπολογιστής.

Την ίδια χρονιά, ένας νεαρός Γερμανός μηχανικός που ονομαζόταν Konrad Zuse ολοκλήρωσε τον πρώτο προγραμματιζόμενο ψηφιακό υπολογιστή γενικού σκοπού, μία μηχανή που δημιουργήθηκε από ηλεκτρικά ρελέ για την αυτοματοποίηση της διαδικασίας των μηχανικών υπολογισμών. Το 1941 κατασκεύασε για το γερμανικό στρατό μια γενικού σκοπού προγραμματίσιμη ηλεκτρονική υπολογιστική συσκευή, με το κωδικό όνομα Z1. Στην Αγγλία την ίδια χρονική περίοδο μια ομάδα που καθοδηγούνταν από τον διάσημο μαθηματικό Alan Turing, κατασκεύασε τον Colossus, έναν γενικό ηλεκτρονικό υπολογιστή που κατάφερε να σπάσει κωδικούς με επιτυχία. Το 1941, το Αμερικανικό Ναυτικό και η IBM χρηματοδότησε ένα πρόγραμμα στο Πανεπιστήμιο του Harvard με επικεφαλής τον καθηγητή Howard Aiken, για την κατασκευή μια υπολογιστικής συσκευής με την ονομασία Mark I (Αναστασόπουλος & Σκόρδας, 2001).

Μια πολύ ισχυρότερη μηχανή άρχιζε να κατασκευάζεται στο πανεπιστήμιο της Pennsylvania σε συνεργασία με τον Αμερικάνικο Στρατό, με υπεύθυνο τους J.Presper Eckert και John Mauchly, η οποία ονομάστηκε ENIAC. Το 1946 ο Von Neumann προτείνει ένα διαφορετικού σχεδιασμού υπολογιστή βασισμένο σε ένα μοντέλο υπολογιστών που ονομάζεται υπολογιστής αποθηκευμένου προγράμματος. Έτσι, έθεσε τις βάσεις ενός νέου ηλεκτρονικού υπολογιστή, του EDVAC, που ήταν οι εξής:

- Χρήση μόνο δυαδικής αριθμητικής
- Στη μνήμη αποθηκεύονται τα δεδομένα αλλά και το πρόγραμμα που εκτελείται

1.3 Η σύγχρονη εποχή: 1950 έως σήμερα

Τα επόμενα 50 χρόνια ανάπτυξης των υπολογιστών έχουν σχέση με την υλοποίηση του μοντέλου που πρότεινε ο Von Neumann, και η βελτίωσή του και ως προς το λογισμικό (software) και ως προς το υλικό (hardware). Από το 1950 η οργάνωση των υπολογιστών έχει μια εξελικτική πορεία, αφού οι ηλεκτρονικοί υπολογιστές έχουν γίνει πιο φθηνοί, πιο αξιόπιστοι, πιο εύχρηστοι χωρίς να έχουν συμβεί δραστικές αλλαγές στις βασικές ιδέες και αρχιτεκτονική του Von Neumann. Κάποιες πρόσφατες εξελίξεις στην πληροφορική περιλαμβάνουν τις εξής:

- Μαζική παράλληλη επεξεργασία ικανή για τρισεκατομμύρια υπολογισμούς ανά δευτερόλεπτο
- Τεχνητή νοημοσύνη και ρομποτική
- Μικροσκοπικοί φορητοί υπολογιστές και υπολογιστές παλάμης
- Υψηλής ανάλυσης προσομοιώσεις μέσω γραφικών που ονομάζονται εικονική πραγματικότητα
- Ολοκληρωμένες παγκόσμιες τηλεπικοινωνίες που έχουν σχέση με πληροφορίες, τηλεόραση, τηλέφωνο, φαξ, το διαδίκτυο και τον παγκόσμιο πληροφοριακό ιστό
- Ασύρματες επικοινωνίες
- Μαζικές αποθηκευτικές συσκευές ικανές για την αποθήκευση και την ανάκτηση terabyte πληροφοριών
- Συνεργασία της IBM και της Microsoft με στόχο την «αυτοθεραπεία» των υπολογιστών ως αποτέλεσμα τεχνολογίας που θα λειτουργεί με πρότυπο την ανάλογη λειτουργία του ανθρώπινου σώματος. Οι υπολογιστές και τα δίκτυα όχι μόνο θα διακρίνουν τα συμπτώματα που ενδέχεται να τους οδηγήσουν σε «ασθένεια» αλλά ταυτόχρονα θα

μπορούν να ενεργοποιούν εφεδρικά συστήματα ασφαλείας, να παραγγέλνουν εξαρτήματα κτλ (Σφακιανάκης, 2003 & 2006).

Θα ήταν παράλειψη να κλείσουμε την ιστορική αναδρομή στη σύγχρονη εποχή χωρίς αναφορά στον Alan Key. Είναι αυτός που δημιούργησε τον υπολογιστή του μέλλοντος και συγχρόνως δημιούργησε το πρώτο πρόγραμμα ζωγραφικής και τη Smalltalk την αντικειμενοστρεφή γλώσσα προγραμματισμού. Συγχρόνως ανέπτυξε με τους συνεργάτες του τον πρώτο προσωπικό υπολογιστή σχεδιασμένο για αλληλεπιδραστική χρήση. Είναι χαρακτηριστικό ότι για πρώτη φορά οι προσωπικοί υπολογιστές στις Η.Π.Α. ξεπέρασαν τις πωλήσεις τηλεοράσεων και το 1999 το ηλεκτρονικό ταχυδρομείο του διαδικτύου ξεπερνά το κοινό ταχυδρομείο (Γιαννακουδάκης, 1998).

ΚΕΦΑΛΑΙΟ 2°

Ηλεκτρονικό Έγκλημα-Παραβατικότητα

2.1 Τι είναι το έγκλημα

Το έγκλημα είναι μία σύνθετη έννοια, καθώς σε αυτή συνυπάρχουν από τη μία η κοινωνική, βιολογική και ψυχολογική πραγματικότητα του ανθρώπου και από την άλλη η δεοντολογία που διέπει στο πλαίσιο ορισμένης κοινωνίας την κοινωνική συμπεριφορά του. Το έγκλημα αποτελεί αναμφίβολα αναπόσπαστο κομμάτι της εκάστοτε κοινωνίας και λειτουργεί ως ένας οργανισμός μέσα στον οποίο μεταβάλλονται οι εκφάνσεις, τα μέσα τέλεσης και το νομικό πλαίσιο που το διέπει (Μαγκάκης, 1984).

Με διαφορετικό περιτύλιγμα αλλά και περιεχόμενο, ποικίλλει ανάλογα με τις κοινωνικοπολιτικές και ηθικές τάσεις της εκάστοτε εποχής. Παραμένει πάντα όμως παρόν κινούμενο σε τρεις βασικούς άξονες.

Δογματικό ορισμό του εγκλήματος μας δίνει ο ίδιος ο Ποινικός Κώδικας μας στην διάταξη του άρθρου 14. Σύμφωνα με το άρθρο 14 Π.Κ. «έγκλημα είναι πράξη άδικος και καταλογιστή εις τον πράξαντα, τιμωρούμενη υπό του νόμου».

Το νόημα του περιεχομένου του εγκλήματος συνίσταται στο ότι αποτελεί μία πράξη η οποία θίγει τις αξίες της κοινωνική ζωής, και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά αναγκαία (Μαγκάκης, 1984).

Το φαινόμενο του εγκλήματος διέπεται από διαχρονικότητα, καθώς ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Καμιά κοινωνία δεν έχει απαλλαχθεί από αυτό, και σε κάθε έγκλημα (προσβολή), υπήρχε, υπάρχει και θα υπάρχει ποινή (αντίδραση). Αντίθετα αυτό που παρατηρείται είναι μια αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς (Μαγκάκης, 1984).

Σε κάθε κοινωνία υπάρχουν κανόνες οι οποίοι θεσπίστηκαν τυπικά ή άτυπα (έθιμα) προκειμένου να προστατευτούν κοινωνικά αγαθά σε κάθε όμως κοινωνία υπάρχουν άνθρωποι οι οποίοι παραβαίνουν τους κανόνες αυτούς. Αποτέλεσμα της προσβολής αυτών των αγαθών είναι η επιβολή διαφόρων κυρώσεων (ποινών) στους

παραβάτες, οι οποίες αποτελούν τον τρόπο αντίδρασης της κοινωνίας στο έγκλημα. Η αντίδραση, καθώς και το είδος της ποινής, βρίσκονται πάντα σε άμεση εξάρτηση με την εκάστοτε εποχή και πολιτισμό.

Τα βασικά στοιχεία του εγκληματικού φαινομένου, κανόνας, έγκλημα, κύρωση (ποινή), συναποτελούν έναν αδιάσπαστο κύκλο. Εδώ είναι έκδηλη η αλληλεξάρτηση των στοιχείων. Αν δεν υπήρχε έγκλημα δεν θα υφίστατο η κύρωση. Η μη ύπαρξη κανόνα δεν καθιστά δυνατή την παράβασή του. Ο κανόνας δημιουργήθηκε για να οργανώσει και να περιφρουρήσει τα κοινωνικά αγαθά (υλικά και άυλα) από κάθε δυνητική προσβολή τους στα πλαίσια της κοινωνικής συμβίωσης. Στη συνέχεια, και αφού επέλθει η προσβολή του έννομου αγαθού (αυτό που προστατεύεται από τον κανόνα-νόμο), έρχεται η κύρωση (ποινή). Εν συντομία η κύρωση (ποινή) αποτελεί συνέπεια της παράβασης του κανόνα και δηλώνει προς αυτόν που επιβάλλεται ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Θα λέγαμε ότι η ποινή αποτελεί την εκτόνωση της κοινωνικής αντίδρασης στο έγκλημα.

2.2 Τι είναι το διαδίκτυο

Το διαδίκτυο αποτελεί αδιαμφισβήτητα τα θεμέλια αλλά και την κινητήριο δύναμη της σύγχρονης και τεχνολογικά ανεπτυγμένης σημερινής κοινωνίας. Με την πάροδο του χρόνου έχει αλλάξει τον τρόπο που ο κόσμος επικοινωνεί, ενημερώνεται, μαθαίνει ,εργάζεται, διασκεδάζει και ζει. Θα μπορούσε να περιγραφεί ως ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί εκατομμύρια χρηστών καθημερινά σε ολόκληρο τον κόσμο (Ζάννη, 2005).

Το διαδίκτυο και κατ' επέκταση οι ηλεκτρονικοί υπολογιστές (Η/Υ), έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητας μας, είτε ως μέσα ψυχαγωγίας-ενημέρωσης, είτε ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων.

Η πληροφορία στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά

μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε όγκο αλλά και σε αριθμό. Στις μέρες μας, γίνεται σε μεγάλο βαθμό και η χρήση εφαρμογών κοινωνικής δικτύωσης-facebook, twitter, chat rooms (Ζάννη, 2005).

2.3 Η Έννοια του ηλεκτρονικού εγκλήματος

Κατά καιρούς έχουν γίνει πολλές προσπάθειες να οριστεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester and Morrison 1994 προσδιόρισε το ηλεκτρονικό έγκλημα ως «μία εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσης της»

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), τα οποία τελούνται μέσω του Διαδικτύου (Ελληνική Αστυνομία).

Το ιντερνέτ και οι Η/Υ παρέχουν στους χρήστες άπειρες και ποικίλες δυνατότητες, ταυτοχρόνως όμως εισαγάγουν νέες μορφές παραβατικής συμπεριφοράς. Έτσι, παραδοσιακές εγκληματικές πράξεις όπως εξύβριση ή δυσφήμιση, μέσω μιας ιστοσελίδας (web site) ή ηλεκτρονικού ταχυδρομείου, διαπράττονται πλέον ταχύτερα και ευκολότερα, με το διαδίκτυο να αποτελεί το κυριότερο μέσο τέλεσης τους. Το πέπλο της ανωνυμίας που καλύπτει τους δράστες, η δυσκολία των αρχών στην διαλεύκανση της ηλεκτρονικής εγκληματικότητας έχουν ως απόρροια την ελαχιστοποίηση της τιμωρίας του δράστη και αποτελούν εκείνα τα στοιχεία που ωθούν πολλούς χρήστες στην τέλεση αξιόποινων πράξεων μέσω Διαδικτύου.

Είναι μείζονος όμως σημασίας να επισημάνουμε την ειδοποιό διαφορά μεταξύ διαδικτυακού και ηλεκτρονικού εγκλήματος. Έτσι το διαδικτυακό έγκλημα εμπεριέχεται στο ηλεκτρονικό καθώς αποτελεί μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος

και δεν πρέπει να ταυτίζεται με αυτό. Σύμφωνα με τον ορισμό του Donn Parker «Το διαδικτυακό έγκλημα ή αλλιώς το κυβερνοέγκλημα (cyber-crime) είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος, για την τέλεση του οποίου ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο. Σχετίζεται με την οποιαδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το διαδίκτυο» (Furnell, 2006).

Αν λοιπόν θέλουμε να κατηγοριοποιήσουμε τα ηλεκτρονικά εγκλήματα, διακρίνουμε τα παρακάτω:

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.
- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Τέτοιο έγκλημα θεωρείται η παράνομη αντιγραφή λογισμικού.
- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η χρήση του διαδικτύου είναι απαραίτητο στοιχείο για την εγκληματική συμπεριφορά του δράστη. Εδώ εντάσσουμε τη διασπορά κακόβουλου λογισμικού.

Σύμφωνα με τον Neil Barrett (1997) τα ηλεκτρονικά εγκλήματα διακρίνονται σε δύο κατηγορίες:

α) σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ , η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών.

β) σε εκείνα που υποστηρίζονται από Η/Υ και οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα μαύρου χρήματος που γίνονται ηλεκτρονικά.

Μια άλλη οπτική είναι η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων που προτάθηκε από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα που από την ίδρυση του στις αρχές της δεκαετία του 1980, διενήργησε έρευνες με στόχο να εξακριβώσει την έκταση του εγκλήματος μέσω Η/Υ σε δημόσιο και ιδιωτικό τομέα.

Οι κατηγορίες είναι (Furnell, 2006):

1. **Απάτη:** Για προσωπική ωφέλεια (αλλοίωση των εισαγόμενων με νόμιμο τρόπο, καταστροφή/ συμπίεση/ ακαταλληλότητα εκροών, αλλοίωση των δεδομένων του Η/Υ, αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρούμενων των προσβολών από τους ιούς)
2. **Κλοπή:** των δεδομένων, του λογισμικού
3. **Χρήση λογισμικού χωρίς άδεια:** χρήση παράνομων αντιγράφων λογισμικού
4. **Ιδιωτική εργασία:** μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος
5. **Χάκινγκ:** ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας
6. **Σαμποτάζ:** η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό
7. **Εισαγωγή πορνογραφικού υλικού**
8. **Ιοί:** διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής

2.4 Χαρακτηριστικά του ηλεκτρονικού εγκλήματος

Παρατηρώντας κανείς την φύση των ηλεκτρονικών εγκλημάτων, μπορεί να καταλήξει στα παρακάτω χαρακτηριστικά γνωρίσματα:

1. Το διαδικτυακό έγκλημα διαπράττεται σε χρόνο ελάχιστων δευτερολέπτων. Η αμεσότητα αυτή έχει αποτέλεσμα τη μεγάλη ταχύτητα τέλεσης του που πολλές φορές δεν γίνεται αντιληπτό ούτε το ίδιο το θύμα. Ο δράστης, κάνοντας χρήση του Η/Υ που είναι συνδεδεμένος στο διαδίκτυο, επιτίθεται και μπορεί να

εισβάλλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του πλανήτη. Επομένως γίνεται εύκολα αντιληπτό, ότι δεν απαιτείται η φυσική παρουσία του δράστη στον τόπο τέλεσης του εγκλήματος, καθώς με το πάτημα ορισμένων πλήκτρων του υπολογιστή του δύναται να τελέσει το έγκλημα από το σπίτι ή το γραφείο του.

2. Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία που περιέχουν τα ηλεκτρονικά δεδομένα. Βλάβες, φθορές καθώς και αλλοιώσεις που προκαλούνται σε ενσώματα αντικείμενα όπως σκληρούς δίσκους, μνήμες κ.λπ., αποτελούν δευτερεύουσες συνέπειες της κύριας προσβολής που αφορά τα δεδομένα.

3. Η εισβολή σε ένα υπολογιστικό σύστημα διευκολύνεται από το ίδιο το διαδίκτυο και αυτό γιατί διατίθεται σε αυτό ελεύθερα εφαρμογές λογισμικού με τις οποίες οι χάκερς μπορούν να εισβάλλουν εύκολα σε δίκτυα και υπολογιστικά συστήματα και να πραγματοποιήσουν πλήθος ηλεκτρονικών επιθέσεων.

4. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (του κράτους στο οποίο γίνεται αντιληπτή η διάπραξη του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Αυτός ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος οδηγεί σε πολλές περιπτώσεις σε διαφορετική αξιολόγηση του περιεχομένου, αφού αυτό μπορεί να είναι νόμιμο στο κράτος που βρίσκεται ο δράστης ή που υπάρχουν αποθηκευμένα τα δεδομένα και να είναι παράνομο στο κράτος που τα δεδομένα λαμβάνονται ή βρίσκεται ο αποδέκτης τους.

5. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες γνώσεις σε θέματα πληροφορικής τεχνολογίας και διαδικτύου καθώς και συνεχή εκπαίδευση όσων είναι αρμόδιοι για τη δίωξή του (αστυνομικές και δικαστικές αρχές).

6. Το ηλεκτρονικό έγκλημα έχει εισάγει νέους περιορισμούς: α) αρκετές φορές είναι ιδιαίτερα πολύπλοκο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος και αυτό γιατί με τη χρήση ενός μόνο δικτυωμένου ηλεκτρονικού υπολογιστή ο εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου

και β) ο ακριβής χρόνος τέλεσης του εγκλήματος και αυτό γιατί τα θύματα κατά κανόνα αντιλαμβάνονται την επίθεση και τη ζημιά που προκλήθηκε πολύ αργότερα από τον χρόνο πραγματοποίησης.

7. Τα στατιστικά στοιχεία που υπάρχουν τόσο στο διεθνή όσο και στον ελληνικό χώρο δεν είναι επαρκή. Τα διαδικτυακά εγκλήματα που καταγγέλλονται είναι σχετικά ολιγάριθμα καθώς το θύμα ακόμα και όταν αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, δεν ενημερώνει τις αρμόδιες αρχές. Ένας από τους σημαντικότερους λόγους για τον δισταγμό αναφοράς του εγκλήματος σε επιχειρηματικό επίπεδο είναι ο φόβος της εταιρίας που δέχτηκε την επίθεση ότι η αποκάλυψη του γεγονότος θα επέφερε μεγάλο πλήγμα στο κύρος, την αξιοπιστία και την εικόνα της προς τους πελάτες.

2.5 Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα.

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία.

Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών, πληθαίνουν τα περιστατικά παραβατικής συμπεριφοράς.

ΚΕΦΑΛΑΙΟ 3°

Κατηγορίες Ηλεκτρονικού Εγκλήματος-Παραβατικότητας

3.1 Γνήσια ηλεκτρονικά εγκλήματα

Τα κυριότερα και πιο διαδεδομένα εγκλήματα που περιλαμβάνονται σε αυτήν την κατηγορία είναι:

- Κακόβουλες εισβολές σε δίκτυα (hacking, cracking)
- Ανεπιθύμητη αλληλογραφία (spamming)
- Ηλεκτρονικό «Ψάρεμα» (phising - pharming)
- Διασπορά κακόβουλου λογισμικού (ιοί- viruses, σκουλήκια- worms, δούρειοι ίπποι- trojan horses)
- Πειρατεία ονομάτων χώρου (domain names piracy)
- Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)

3.1.1 Κακόβουλες εισβολές σε δίκτυα.

Α. **Hacking**

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα. Η εισβολή στο δίκτυο ακόμα και αν δεν είναι κακόβουλη, θα λέγαμε ότι ενέχει κακόβουλο χαρακτήρα. Αυτό συμβαίνει διότι ο επιτιθέμενος ή αλλιώς hacker (χάκερ), εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του, εντοπίζει πιθανά αδύνατα σημεία του και έτσι μπορεί στη συνέχεια αν θέλει να διαπράξει κακόβουλη επίθεση ή ακόμα και να διαθέσει τις πληροφορίες που

έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει στην επίθεση. Η δράση των hackers (χάκερ) δεν είναι πάντα καταστροφική και συνδεδεμένη με εγκληματικές πράξεις, αλλά μια πτυχή των παραβιάσεων σχετίζεται με την ανάγκη επίδειξης των τεχνικών δυνατοτήτων τους. Όπως σε μια πραγματική μάχη, έτσι και στο ιντερνέτ το βασικότερο πριν από μια επίθεση είναι η συλλογή πληροφοριών για τον αντίπαλο.

Συνοπτικά ως χάκερ (hacker) μπορεί να χαρακτηρισθεί το άτομο εκείνο το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών. Γενικά υπάρχουν τρεις (3) κατηγορίες hacker (χάκερ):

1. **White hat-hackers:** Στόχος τους είναι να καταπολεμούν το ηλεκτρονικό έγκλημα και τους black hat-hackers. Οι grey hats τους ταυτίζουν με τους ειδικούς ασφαλείας και διαχειριστές συστημάτων. Οι ηλικία τους κυμαίνεται από 25 έως και 40 έτη, Μερικές φορές οι grey hats μετατρέπονται σε white hats όταν μεγαλώσουν.

2 .**Black hat- hackers**: Είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα. Χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνοντας παράνομα προγράμματα, όπως ηλεκτρονικούς ιούς και κατασκοπευτικά προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν , σπάνε κωδικούς από ιστοσελίδες και τις καταστρέφουν. Το κίνητρο τους είναι χρηματικό τις περισσότερες φορές και όχι ιδεολογικό.

3. **Grey hat-Hackers** Εδώ μπαίνουμε στην γκρίζα ζώνη του ιντερνέτ. Σε αυτή την κατηγορία ανήκουν χάκερ που παραβιάζουν τον νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Μπορεί να ανακαλύψουν κενά ασφαλείας ξένων δικτύων ή προγραμμάτων και να τα σπάσουν για να αποδείξουν την αδυναμία τους. Αυτοί οι χάκερς είναι ως επί των πλείστων μικρής ηλικίας, ξεκινούν σε ηλικία 15 χρονών και φτάνουν στο ζενίθ των γνώσεων τους ως φοιτητές. Οι ίδιοι δεν θεωρούν τον εαυτό τους εγκληματία ακόμα και αν παραβιάζουν νόμους γιατί δεν καταστρέφουν ούτε δημιουργούν ζημία στα συστήματα που εισβάλουν. Θεωρούν τον εαυτό τους ερευνητές της τεχνολογίας και σε κάποιες περιπτώσεις ενημερώνουν ακόμα και το κοινό ή τους διαχειριστές συστημάτων για τυχόν προβλήματα ασφάλειας.

B. Cracking (κράκινγκ)

Το Cracking (κράκινγκ) αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, η αλλαγή των σχετικών κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους. Βασικός σκοπός είναι η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς.

3.1.2 Ανεπιθύμητη αλληλογραφία (spamming)

Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα. Παρά το γεγονός ότι ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλου όγκου μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για αυτόν που το λαμβάνει.

Η αλληλογραφία αυτή θα μπορούσε να χαρακτηριστεί «απρόκλητη» καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας (Λάζος, 2001).

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του spamming:

- **Απρόκλητο:** Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα η οποία θα δικαιολογούσε ή θα προκαλούσε τη σχέση αυτή.
- **Εμπορικό:** Το spamming αφορά την αποστολή μηνυμάτων με εμπορικό σκοπό κατά κύριο λόγο, σκοπεύοντας την προβολή και διαφήμιση προϊόντων και υπηρεσιών και εν συνεχεία διεύρυνση πελατολογίου και πραγματοποίηση πωλήσεων.
- **Μαζικό:** Το spamming συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών.

3.1.3 Ηλεκτρονικό «Ψάρεμα» (phishing - pharming).

α) Phishing

Στην περίπτωση αυτή ο επιτήδειος προσπαθεί μέσω των μηνυμάτων που στέλνει να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα email, αποστολέας του οποίου φαίνεται να είναι η τράπεζα του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρεται σε προβλήματα σε Η.Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί. Το email αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας,ο οποίος όμως δεν είναι πραγματικός και έτσι το θύμα αποστέλλει τα στοιχεία που του έχουν ζητηθεί κατευθείαν σε κάποιον απατεώνα (Τσουραμάνης, 2005).

β) Vishing

Vishing είναι η προσαρμογή του ηλεκτρονικού ψαρέματος (phishing) σε αυτούς που χρησιμοποιούν το τηλέφωνο ή το VoIP (Voice over IP tools). Ο χρήστης λαμβάνει e-mail ή SMS με το οποίο του ζητείται να καλέσει έναν αριθμό χωρίς χρέωση με στόχο να επιβεβαιώσει τα στοιχεία του. Μπορεί ακόμα να λάβει ένα τηλέφωνο με μαγνητοφωνημένο μήνυμα που να του ζητά να εισάγει τα προσωπικά του στοιχεία.

γ) Pharming

Pharming είναι η εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name), που επιτρέπει σε έναν hacker να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Οι δράστες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Οι δράστες δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν προγράμματα που στην πραγματικότητα επαναδρομολογούν την κυκλοφορία των δεδομένων. Με παρεμβάσεις

στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα που είναι αντίγραφο της γνήσιας. Έτσι, ο χρήστης καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα, ενώ στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, οι δράστες αποστέλλουν μέσω e-mail προγράμματα, τα οποία μετά την εγκατάστασή τους στον υπολογιστή του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία τους ενδιαφέρουν. Κατόπιν τα χρησιμοποιούν προκαλώντας περιουσιακή ζημία στο θύμα.

3.1.4 Διασπορά κακόβουλου λογισμικού (ιοί- viruses, σκουλήκια- worms, δούρειοι ίππο - trojan horses)

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται σε προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν προσωπικά στοιχεία. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms) καθώς και οι δούρειοι ίπποι-Trojan horses.

α) Ιοί (Viruses)

Ο ιός είναι ένα πρόγραμμα Η/Υ που έχει σχεδιαστεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφά του. Επειδή δε έχει την δυνατότητα να αναπαράγεται συνεχώς μπορεί να μεταδοθεί από ένα σύστημα σε άλλο , με σκοπό να εκτελέσει την αποστολή του η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων, την διαγραφή αρχείων ή το σβήσιμο του συνόλου των σκληρών δίσκων.

Ουσιαστικά είναι ένας βλαβερός εκτελέσιμος κώδικας, ο οποίος επιζεί με το να «κολλάει» ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα. Έχουν παρασιτική συμπεριφορά, καθώς επιζούν με το να «μολύνουν» άλλα αρχεία, ακολουθώντας έτσι πιστά την ανάλογη

συμπεριφορά (ο τρόπος που ζουν και πολλαπλασιάζονται) των οργανικών ιών. Σήμερα ο συνηθέστερος τρόπος μετάδοσης των ιών είναι η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Σύμφωνα με τον Kyas (1997) και με βασικά κριτήρια το προσβαλλόμενο μέρος του Η/Υ καθώς επίσης και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί, έχουμε τον παρακάτω διαχωρισμό (Τσουραμάνης, 2005):

1. Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή (Boot Viruses).

2. Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (System Cluster Viruses).

3. Ιοί που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (Software Viruses).

4. Ιοί που μπορούν και αναπαράγονται με πολλούς και διάφορους τρόπους με σκοπό να εξασφαλίζουν έτσι την ανθεκτικότητα τους έναντι των διαφόρων προγραμμάτων Anti-Virus (Polymorphous Viruses).

5. Ιοί που «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (Stealth Viruses).

6. Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (Retroviruses).

7. Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses).

β) Δούρειοι ίπποι (Trojan Horses).

Ένας δούρειος ίππος αποτελείται από δύο μέρη, το server και το client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτό το μέρος του server. Στη συνέχεια, αφού εκτελεστεί το μέρος client στον υπολογιστή του επιτιθέμενου και δοθεί

η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή λέγονται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω διαφόρων θυρών (ports) του υπολογιστή τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας-firewall (Λάζος, 2001).

Οι Δούρειοι Ίπποι είναι προγράμματα που ενώ φαίνονται να λειτουργούν κανονικά παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. Έτσι ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού, αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδικτύου. Στις περισσότερες των περιπτώσεων, ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Κερκόπορτα (trapdoor) είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης.

γ) Σκουλήκια (worms).

Τα σκουλήκια είναι και αυτά προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για τον λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα δηλαδή έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Η διαφορά τους από τους ιούς έγκειται ότι δεν χρειάζεται ανθρώπινη παρεμβολή για την ενεργοποίηση τους (Λάζος, 2001).

δ) Άλλα είδη κακόβουλου λογισμικού.

1. Dialers

Οι dialers είναι μια υποκατηγορία των κακόβουλων προγραμμάτων spyware που είναι σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες (κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, στοιχεία λογαριασμών κλπ) για τον χρήστη, εν αγνοία του ή χωρίς την έγκρισή του. Σκοπός των δημιουργών προγραμμάτων spyware είναι η προσκόμιση πολλών χρημάτων εύκολα και γρήγορα. Οι dialers

αλλάζουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (dial up networking) ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο σε αυτόν αριθμό που είθισται να είναι διεθνής κλήση με υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του παρόχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου.

2. Λογική βόμβα

Οι λογικές βόμβες είναι μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή τροποποιούν κάποιον υπάρχοντα κώδικα. Ονομάζονται έτσι λόγω του γεγονότος ότι είναι προγραμματισμένες να «εκραγούν» ηλεκτρονικά κάτω από ορισμένες προϋποθέσεις. Η λογική βόμβα προστίθεται στο πρόγραμμα από χρήστη ο οποίος έχει πρόσβαση στο σύστημα και φυσικά την απαιτούμενη γνώση για την εγκατάσταση της. Είναι περισσότερο επικίνδυνες από τα σκουλήκια και τους δούρειους ίππους γιατί κατασκευάζονται ευκολότερα και έχουν δυνατότητα να προκαλέσουν σοβαρές ζημιές ακόμα και καταστροφές σε σωσμένα αρχεία αλλά και σε ολόκληρο το λογισμικό ενός ηλεκτρονικού υπολογιστή.

3. Rootkits

Τα rootkits είναι ένα σύνολο εργαλείων και υπηρεσιών που ο χάκερ μπορεί να χρησιμοποιήσει για να διατηρήσει την πρόσβαση του στο σύστημα που έχει χακάρει από τη στιγμή που θα εισβάλει σε αυτό. Τα εργαλεία του rootkit θα του επιτρέψουν να αναζητήσει ονόματα χρηστών και κωδικούς πρόσβασης, να εξαπολύσει επιθέσεις κατά συστημάτων από απόσταση και να αποκρύψει τις δράσεις του με την απόκρυψη αρχείων και την διαγραφή κάθε δραστηριότητας από τα αρχεία καταγραφής του συστήματος. Το rootkit αποκτά πρόσβαση, μπορεί να κάνει σχεδόν ότι θέλει, έχοντας δικαιώματα διαχειριστή, παραδείγματος χάριν, να ελέγξει την κίνηση, την πληκτρολόγηση, να επιτίθεται σε άλλους υπολογιστές στο δίκτυο, ή να δημιουργήσει κερκόπορτες συστήματος για την εξυπηρέτηση των εισβολέων.

4. Ransomware

Είναι μια κατηγορία κακόβουλου λογισμικού που ουσιαστικά είτε αποτρέπει τη χρήση του υπολογιστή από τον κάτοχο του,είτε δε δίνει τη δυνατότητα στο χρήστη να έχει πρόσβαση στα δεδομένα του αν δεν πληρώσει κάποιο συγκεκριμένο ποσό (λύτρα).Υπάρχουν δύο είδη ransomware:

- Κλειδωμένη οθόνη ransomware, η οποία εμφανίζει μία εικόνα πλήρους οθόνης ή ιστοσελίδα η οποία αποτρέπει κάθε είδους πρόσβαση στον κάτοχο του υπολογιστή.
- Ransomware κρυπτογράφησης, το οποίο αποκρυπτογραφεί τα αρχεία του χρήστη με κωδικό πρόσβασης και τον εμποδίζει να τα ανοίξει.

5. Bots-zombies

Μία «bot» είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο πάνω στον «πληγέντα» υπολογιστή. Οι υπολογιστές που έχουν μολυνθεί με bot γενικά αναφέρονται ως ζόμπι. Υπάρχουν κυριολεκτικά χιλιάδες υπολογιστές στο Ιντερνέτ που έχουν μολυνθεί με κάποιο είδος bot και δεν το συνειδητοποιούν ακόμα. Συχνά ο ιδιοκτήτης δεν γνωρίζει ότι έχει εξαπολύσει έναν ιό ή έχει εγκαταστήσει έναν δούρειο ίππο ο οποίος ενεργοποιεί τον υπολογιστή να λειτουργήσει σαν ένα Zombie. Ο εισβολέας μπορεί να χρησιμοποιήσει το μολυσμένο υπολογιστή για να επιτεθεί ή να στείλει spam σε άλλους υπολογιστές χωρίς να το ξέρουν οι ιδιοκτήτες τους.

6. Scareware

Το scare ware είναι προγράμματα εξαπάτησης. Γνωστά και ως fraud ware, τα οποία τις περισσότερες φορές εμφανίζονται με τη μορφή pop-up παραθύρων, με σκοπό να εκφοβίσουν τους χρήστες του διαδικτύου (π.χ. προειδοποιώντας τους ότι ο υπολογιστής τους έχει μολυνθεί με κακόβουλο λογισμικό) και να τους πείσουν να προβούν στην αγορά ή/και εγκατάσταση συγκεκριμένου λογισμικού που υποτίθεται πως θα τους προστατέψει από επιθέσεις και απειλές.

7. Βακτήρια (bacteria)

Τα βακτήρια (bacteria) είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα πολυπρογραμματιζόμενο σύστημα ή πιθανόν να δημιουργεί δύο νέα αρχεία, καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές κ.ο.κ. Τα βακτήρια αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες.

3.1.5 Πειρατεία ονομάτων χώρου (domain names piracy)

Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Μέσο (εισιτήριο) για την είσοδο στο διαδίκτυο αποτελεί το «domain name» (όνομα πεδίου ή όνομα χώρου), το οποίο κατ' ουσίαν επιτελεί ρόλο ηλεκτρονικής διευθύνσεως ή «κυβερνοδιευθύνσεως», επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως. Το «domain name» αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το πρώτο μέρος είναι κοινό για όλα τα «domain names» και αποτελείται από τα αρκτικόλεξα «http://www» (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο). Το δεύτερο μέρος (second level domain – SLD) ή Μεταβλητό Πεδίο αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το κατ' εξοχήν όνομα, την κατ' εξοχήν διαδικτυακή διεύθυνση. Το τρίτο μέρος αποτελεί το επονομαζόμενο top level domain (TLD), που δηλώνει το είδος της τοποθεσίας (ιστοθέσης) ή τη γεωγραφική

προέλευση, όπως «.com» για όσους ασκούν εμπορική δραστηριότητα, «.edu» για εκπαιδευτικούς οργανισμούς, «.org» για οργανισμούς, «.net» για παροχές υπηρεσιών διαδικτύου, «.gov» για κυβερνητικούς οργανισμούς, «.int» για διεθνείς οργανισμούς, «.gr» για τη χώρα αρχειακής καταχωρίσεως του «domain name» του χρήστη, εν προκειμένω για την Ελλάδα.

3.1.6 Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)

Οι επιθέσεις άρνησης εξυπηρέτησης (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου, για παράδειγμα ενός διακομιστή ιστοσελίδας (web server) ή ενός διακομιστή αρχείων (file server). Ο υπολογιστής- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου πλήθους των «ψεύτικων» αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου (κάνοντας τες 37 σαφώς χαμηλότερες έως και μηδενικές) καθώς επίσης την ακεραιότητα των δεδομένων και τη γενικότερη λειτουργία του συστήματος.

Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι:

- Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο.
- Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες.
- Υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες.

3.2 Συμβατικά εγκλήματα (πραγματοποίηση και χωρίς χρήση Η/Υ)

3.2.1 Ξέπλυμα χρήματος

Ο όρος «ξέπλυμα χρήματος» χρησιμοποιείται για να περιγράψει τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων (βρώμικο χρήμα) υπόκεινται σε μία σειρά διαδικασιών οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα) (Λάζος, 2001).

Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια (Χλούπη, 2000/369):

1. **Τοποθέτηση:** Ο δράστης τοποθετεί τα χρήματα που προέρχονται από παράνομη δραστηριότητα ως επένδυση στο γενικότερο οικονομικό σύστημα, σε παραδοσιακό ή μη χρηματοοικονομικό οργανισμό, όπως τράπεζα με κατάθεση σε λογαριασμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο και άλλες συναφείς επενδύσεις.
2. **Στρωματοποίηση:** Ο δράστης επιχειρεί μία σειρά κινήσεων και συναλλαγών με αποκλειστικό σκοπό να απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση και έτσι να μεταμφιέσει τις αληθινές πηγές κεφαλαίων, εμποδίζοντας τον εντοπισμό τους από τα ελεγκτικά όργανα του φορέα στον οποίο επενδύθηκαν τελικά.
3. **Ενσωμάτωση:** Ο δράστης επανατοποθετεί τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριότητας όπως για παράδειγμα σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κλπ, έτσι ώστε τα εν λόγω κεφάλαια να επιστρέφουν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια.

Έτσι λοιπόν, βλέπει κανείς ένα παραδοσιακό έγκλημα του ποινικού κώδικα να διαπράττεται με τη βοήθεια πλέον της τεχνολογίας και των νέων μέσων που αυτή

προσφέρει, με σύγχρονους τρόπους και μεθόδους πάντα όμως με τον ίδιο επιδιωκόμενο σκοπό.

Το βασικό πλεονέκτημα του ξεπλύματος χρήματος μέσω ιντερνέτ είναι ότι δεν υπάρχει προσωπική επαφή μεταξύ των συναλλασσόμενων μερών με άμεσο επακόλουθο, οι δράστες να νιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από την ανωνυμία τους να νομιμοποιούν έσοδα παράνομων δραστηριοτήτων.

3.2.2 Πειρατεία λογισμικού

Ο όρος πειρατεία λογισμικού αναφέρεται στην αναπαραγωγή ή/και διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους (Βλαχόπουλος, 2007).

Α) Μορφές πειρατείας λογισμικού

Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι εξής:

1) Χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση της αδείας χρήσης: Είναι η πιο συνηθισμένη μορφή παράνομης χρήσης εφόσον απαιτείται ξεχωριστή άδεια για κάθε υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα εκδηλώνεται δε ως εξής:

α. Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες.

β. Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια εταιρεία που διαθέτει άδειες για έναν συγκεκριμένο αριθμό χρηστών υπολογιστών (η άδεια χρήσης παραδίδεται μαζί με το λογισμικό καθώς ορίζεται πως αφορούν σε ένα και μοναδικό εμπόρευμα).

γ. Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών .

δ. Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους.

Συχνά οι πωλητές υπολογιστών προκειμένου να κάνουν την αγορά ενός υπολογιστή πιο ελκυστική προσφέρουν προγράμματα χωρίς τις άδειες. Έτσι χρειάζεται μεγάλη προσοχή και έλεγχος των αδειών κατά την αγορά υπολογιστή που διαθέτει προεγκατεστημένα προγράμματα. Το λογισμικό αυτό δεν συνοδεύεται από οδηγίες χρήσης ή βοηθητικές δισκέτες για προγράμματα.

2) Πλαστογράφηση ή αλλιώς πλήρης απομίμηση του προϊόντος: Η παράνομη αναπαραγωγή και πώληση λογισμικού με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, επαναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Η αυξανόμενη επιλογή του εμπορίου μέσω ιντερνέτ έχει αυξήσει και τις πιθανότητες να βρεθούν οι καταναλωτές αντιμέτωποι με το πρόβλημα της χρήσης πλαστών προϊόντων. Η όλο και περισσότερο εξελιγμένη τεχνολογία που χρησιμοποιούν οι πλαστογράφοι, καθιστούν ακόμα και τους πιο απαιτητικούς καταναλωτές συχνά ανήμπορους να διακρίνουν το νόμιμο λογισμικό από το πλαστό. Το πλαστό λογισμικό συνήθως κατασκευάζεται και προωθείται με τρόπο ώστε να μοιάζει και να ανταγωνίζεται το αυθεντικό προϊόν.

3.2.3 Παιδική Πορνογραφία

Σύμφωνα με το προαιρετικό πρωτόκολλο της σύμβασης για τα δικαιώματα των παιδιών και συγκεκριμένα στο άρθρο 2 «Παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές η προσομοιωμένες, ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς.

Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η μεγέθυνση του κυβερνοχώρου παρέχει στους παραγωγούς και διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προϊόντος τους. Οι εγκληματίες διακίνησης πορνογραφικού υλικού ανηλίκων μέσα στον αχανή χώρο του διαδικτύου

εξασφαλίζουν την ανωνυμία τους και δρουν ανενόχλητα εκμεταλλευόμενοι την παιδική αθωότητα (A textbook of cybercrimes and penalties)

Με τη χρήση του διαδικτύου:

- Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτότητά του.
- Υπάρχει προσβασιμότητα του επίμαχου υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με σχετικά μικρό κόστος.
- Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων.
- Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κ.λπ.) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.

3.2.3.1 Τρόποι εγκληματικής δράσης

Με βάση το άρθρο 348Α του Ποινικού Κώδικα, οι τρόποι εγκληματικής δράσης είναι:

- Κατασκευή υλικού πορνογραφίας (κινηματογραφική λήψη, μοντάζ, επεξεργασία εικόνων κ.λπ.).
- Κατοχή πορνογραφικού υλικού δηλαδή φυσική εξουσίαση επί του υλικού.
- Προμήθεια και αγορά υλικού (πραγματική μετακίνηση του πορνογραφικού υλικού στην κατοχή του δράστη).
- Μεταφορά πορνογραφικού υλικού.
- Κυκλοφορία πορνογραφικού υλικού (διακίνηση, διάθεση, πώληση) (Συμεωνίδου-Καστανίδου, 2006).

Έχουμε λοιπόν δύο εκφάνσεις της παιδικής πορνογραφίας στο διαδίκτυο: από τη μία τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο την πραγματοποίηση κέρδους και από την άλλη την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.

3.2.4 Διαδικτυακή Τρομοκρατία

Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποθετικές ομάδες και μυστικούς πράκτορες».

Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

1. Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.
2. Οι ενέργειες τους δύσκολα εντοπίζονται.
3. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
4. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρώντας την ανωνυμία του. Με τη χρήση λοιπόν του Διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων.

3.2.5 Τυχερά παιχνίδια-Τζόγος

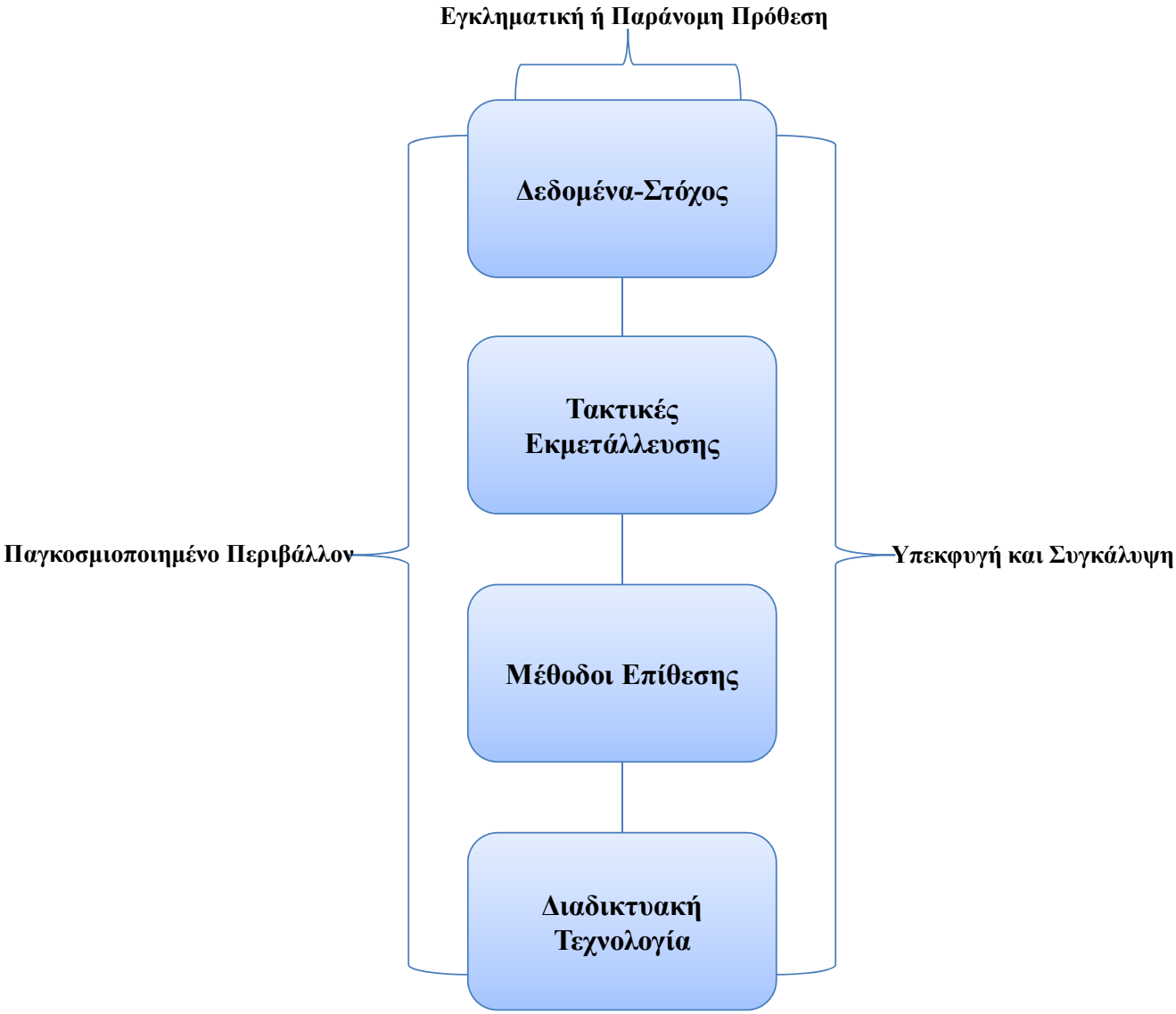
Ανεξέλεγκτες διαστάσεις στις μέρες μας λαμβάνει ο διαδικτυακός τζόγος. Πόκερ, «φρουτάκια», πλήρως εξοπλισμένα καζίνο και πάσης φύσεως τυχερά παιχνίδια είναι διαθέσιμα σε όποιον επιθυμήσει να δοκιμάσει την τύχη του μέσω του διαδικτύου. Το ανησυχητικό της υπόθεσης είναι ότι πέρα από τους ενήλικες όλο και περισσότερα παιδιά - στην προσπάθειά τους να ανακαλύψουν κάποιο παιχνίδι στο internet, καταλήγουν, όχι σε ένα συνηθισμένο παιχνίδι της ηλικίας τους, αλλά σε ηλεκτρονικά στοιχήματα. Σε αυτά, μπορούν να συμμετέχουν ανώνυμα, δίνοντας μόνον τα στοιχεία

κάποιας πιστωτικής κάρτας. Κάποιον αριθμό δηλαδή, σε συνδυασμό με την αντίστοιχη ημερομηνία λήξεως. Και επειδή όπως είναι φυσικό το ίδιο το παιδί δε διαθέτει πιστωτική κάρτα, ο κίνδυνος να αρπάξει την κάρτα του μπαμπά ή της μαμάς κρυφά, είναι κάτι παραπάνω από ορατός. Είναι σημαντικό να διαχωρίσουμε τους όρους ηλεκτρονικά παιχνίδια και τζόγος καθώς είναι δύο εντελώς διαφορετικοί όροι και δεν πρέπει να συγχέονται. Ενώ το παιχνίδι έχει μια μη πραγματική προσέγγιση με μόνο φανταστικούς δεσμούς με τον φυσικό κόσμο, ο τζόγος περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους**.**

Ο παράνομος ηλεκτρονικός τζόγος – τυχερά παιχνίδια έχει ως άμεση συνέπεια την μεγάλη εκροή συναλλάγματος, προς τις έδρες των ξένων εταιρειών που διακινούν παράνομα το παιχνίδι στη Χώρα μας, την φοροδιαφυγή, παρανομία και παράνομο πλουτισμό, λόγω της μη είσπραξης φόρων από τα κέρδη που καταβάλλουν οι εταιρείες στους παίκτες καθώς και την μείωση των εσόδων του κράτους από τα παιχνίδια που διαχειρίζεται η Ο.Π.Α.Π. Α.Ε.

Σχήμα 1

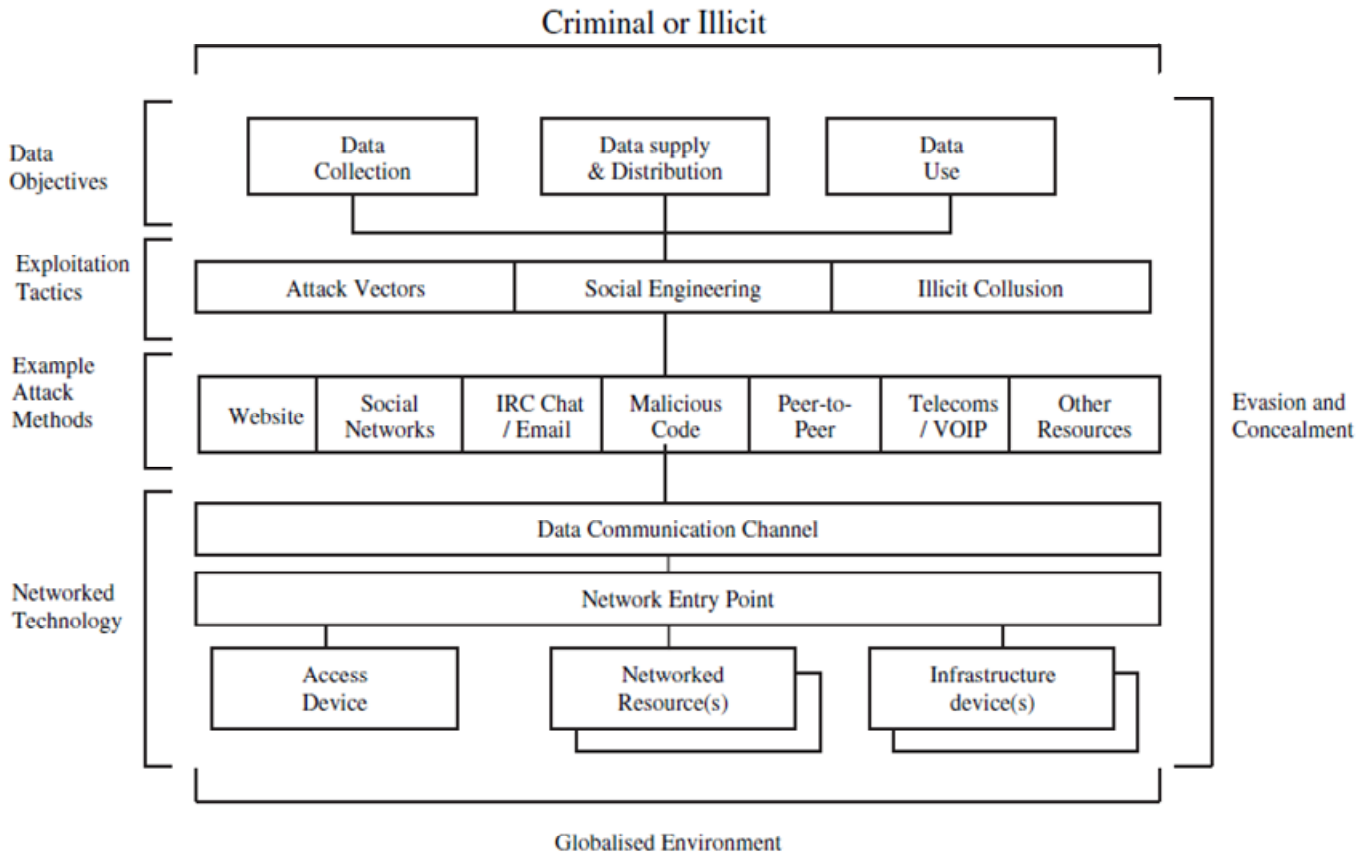
Στάδια Εκτέλεσης Κυβερνοεγκλήματος



Πηγή: Hunton, P., 2009. "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model", Computer Law & Security Review, 25(6), 528-535.

Σχήμα 2

Διερεύνηση Κυβερνοεγκλήματος και Ανάλυση Πλαισίου



Πηγή: Hunton, P., 2009. "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model", Computer Law & Security Review, 25(6), 528-535.

ΚΕΦΑΛΑΙΟ 4°

Η έννοια της Κοινωνική Δικτύωσης

4.1. Τι είναι τα κοινωνικά μέσα δικτύωσης

Κοινωνικά μέσα δικτύωσης είναι οι υπηρεσίες που έχουν ως βάση το διαδίκτυο και επιτρέπουν στους χρήστες τους να δημιουργήσουν ένα δημόσιο προσωπικό προφίλ, το οποίο θα δύναται να επηρεάσει τις αποφάσεις των άλλων μελών αλληλεπιδρώντας μεταξύ τους για την επίτευξη προσωπικών ή κοινών στόχων της ομάδας τους .Ιδιαίτερο χαρακτηριστικό των κοινωνικών δικτύων αποτελεί το γεγονός ότι η ανάπτυξη τους ξεκίνησε από τους ίδιους τους χρήστες που σκέφτηκαν να δημιουργήσουν κάποιες κοινότητες ανθρώπων με κοινά στοιχεία ώστε να μπορούν να εκμεταλλευτούν χαρακτηριστικά του διαδικτύου προς όφελος τους.

Άλλος ένας ορισμός των κοινωνικών μέσων δικτύωσης είναι ο χαρακτηρισμός τους ως κοινός τόπος συνάντησης των μελών της στον ηλεκτρονικό χώρο όπου δεν υπάρχουν γεωγραφικοί και χρονικοί περιορισμοί και υπάρχει απεριόριστη δυνατότητα κοινωνικής αλληλεπίδρασης. Μεταξύ των χρηστών κυριαρχεί η αίσθηση ότι συγκεντρώνονται όλοι στον ίδιο χώρο ανεξάρτητα το που βρίσκονται στην πραγματικότητα.

Αρχικός σκοπός δημιουργίας τους ήταν η ανάπτυξη των ανθρώπινων ικανοτήτων για δικτύωση και επικοινωνία, για διοχέτευση μηνυμάτων ,απόψεων και ανατροφοδότηση συζητήσεων. Η επικράτηση τους βέβαια ήταν αποτέλεσμα της τεχνολογικής ανάπτυξης του Διαδικτύου αλλά και λόγω της συνεχούς αυξημένης χρήσης φορητών συσκευών (smart phones, tablets, netbooks, pads) που γίνονται εργαλεία δικτύωσης (The Economist, 2012). Τα κοινωνικά δίκτυα αποτελούν σημεία συνάντησης μεταξύ των ανθρώπων και συμβάλλουν ιδιαίτερα στην ανταλλαγή πληροφοριών οποιαδήποτε στιγμή αυτοί το επιλέξουν, εκμηδενίζοντας χρόνο και αποστάσεις.

Κοινωνικά δίκτυα είναι ένα είδος on line μέσο ενημέρωσης που διευκολύνει την συνομιλία .Σε αντίθεση με τα παραδοσιακά μέσα τα οποία προσφέρουν το περιεχόμενο

αλλά δεν επιτρέπουν στους αναγνώστες να συμβάλλουν στη δημιουργία ή στην ανάπτυξη του.

Τα μέσα κοινωνικής δικτύωσης συνιστούν υπηρεσίες που επιτρέπουν σε κάθε άτομο να δημιουργήσει το δικό του προσωπικό προφίλ ,να επικοινωνεί με άλλους χρήστες με τους οποίους μπορεί να ανταλλάζει δεδομένα και να παρακολουθεί τις δραστηριότητες τους (Ellison, et al., 2011) Γενικά μέσω των σελίδων κοινωνικής δικτύωσης και της ελεύθερης πλοήγησης στα προφίλ των άλλων χρηστών δημιουργούνται οι διαδικτυακές σχέσεις. Επιπλέον τα συγκεκριμένα μέσα αποτελούν μέσο έκφρασης της δημοκρατίας καθώς ενεργοποιείται η συμμετοχή των πολιτών και η ελεύθερη έκφραση της γνώμης τους. Μέσω του διαδικτυακού χώρου διεξάγονται συζητήσεις για όλα τα θέματα της επικαιρότητας και της πολιτικής ζωής.

Μέσω της άμεσης αλληλεπίδρασης που προσφέρει η κοινωνική δικτύωση τα άτομα μπορούν να βρίσκονται σε επαφή όχι μόνο κατά την διάρκεια του ελεύθερου τους χρόνου αλλά και όταν βρίσκονται στον χώρο εργασίας τους και γενικά σε όλες τις φάσεις της καθημερινότητας τους (Antoci et al., 2012).

Οι ιστοσελίδες κοινωνικής δικτύωσης επιτρέπουν στο χρήστη να δημιουργήσει και να σχεδιάσει την προσωπική του ιστοσελίδα,blog ή ημερολόγιο δίνοντας το δικό του ξεχωριστό χαρακτήρα και χρώμα Αυτός είναι και ο λόγος που η συμμετοχή στους τόπους κοινωνικής δικτύωσης αυξάνεται με ιλιγγιώδη ταχύτητα καθώς κάθε άνθρωπος αναζητά ένα τρόπο κοινωνικοποίησης, επικοινωνίας, δημιουργίας μέσα από τον οποίο να σκιαγραφείται η δική του μοναδική προσωπικότητα. Ο πίνακας που ακολουθεί παρουσιάζει τις δημοφιλέστερες πλατφόρμες κοινωνικής δικτύωσης

Πίνακας 1

Δημοφιλέστερες πλατφόρμες κοινωνικής δικτύωσης παγκοσμίως

Facebook	***Linkedin***
Fotolog	***Google+***
Foursquare	***Open Diary***
Friendster	***Youtube***
Myspace	***Blogger***
Netlog	**Flickr**
LibraryThing	**Wordpress**

Γενικά τα μέσα δικτύωσης έχουν επιφέρει γιγάντιες αλλαγές στον τρόπο επικοινωνίας και στις διαπροσωπικές σχέσεις. Η κλασσική σχέση μέχρι τώρα πομπού-μήνυμα-μέσο-δέκτης ανατρέπεται και στην ουσία ο πομπός γίνεται δέκτης και αντίστροφα. Διευκολύνεται η κοινωνική μάθηση, προωθούνται κοινωνικές δράσεις, διευρύνονται οι ορίζοντες. Μέσω των δικτύων αυτών τα άτομα μπορούν πλέον να επικοινωνήσουν με ανθρώπους που θα ήθελαν να γνωρίσουν που είτε ανήκουν στο χώρο του θεάματος, είτε στο χώρο των τεχνών και των γραμμάτων είτε στον πολιτικό χώρο. Επιπλέον πολλοί φοιτητές μπορούν να προσεγγίσουν πιο εύκολα τους καθηγητές τους ,και πολλοί από τον ερευνητικό τομέα μπορούν να ανταλλάξουν απόψεις και θεωρίες (Antoci et al ., 2012).

Σίγουρα όμως η συνεχής μείωση του ελεύθερου χρόνου στην σημερινή εποχή λόγω αυξημένων υποχρεώσεων έχει καταστήσει τα κοινωνικά μέσα δικτύωσης ως ένα απαραίτητο περιβάλλον για την ανάπτυξη διαπροσωπικών σχέσεων (Antoci et al ., 2012).Ο παρακάτω πίνακας παρουσιάζει τα ποσοστά χρήσης του Ίντερνετ και του Facebook σε όλη την Ευρώπη.

Χρήση Internet & Facebook στην Ευρώπη					
ΕΥΡΩΠΗ	**Πληθυσμός (Εκτίμηση 2012)**	**Χρήστες Ίντερνετ (30/6/2012)**	**Διείσδυση (% Πληθυσμού)**	**Χρήστες % (Στην Ευρώπη)**	**Facebook (31/12/2012)**
Αλβανία	3,002,859	**1,471,400**	49.0 %	0.3 %	1,097,800
Ανδόρα	85,082	**68,916**	81.0 %	0.0 %	34,54
Αυστρία	8,219,743	**6,559,355**	79.8 %	1.3 %	2,915,240
Λευκορωσία	9,643,566	**4,436,800**	46.0 %	0.9 %	533,36
Βέλγιο	10,438,353	**8,489,901**	81.3 %	1.6 %	4,922,260
Βοσνία-Ερζεγοβίνη	3,879,296	**2,327,578**	60.0 %	0.4 %	1,345,020
Βουλγαρία	7,037,935	**3,589,347**	51.0 %	0.7 %	2,522,120
Κροατία	4,480,043	**3,167,838**	70.7 %	0.6 %	1,595,760
Κύπρος	1,138,071	**656,439**	57.7%	0.1 %	582,6
Δημοκρατία της Τσεχίας	10,177,300	**7,426,376**	73.0 %	1.4 %	3,834,620
Δανία	5,543,453	**4,989,108**	90.0 %	1.0 %	3,037,700
Εσθονία	1,274,709	**993,785**	78.0 %	0.2 %	501,68
Νησιά Φερόες	49,483	**39,948**	80.7 %	0.0 %	31,82
Φιλανδία	5,262,930	**4,703,480**	89.4 %	0.9 %	2,287,960
Γαλλία	65,630,692	**52,228,905**	79.6 %	10.1 %	25,624,760
Γερμανία	81,305,856	**67,483,860**	83.0 %	13.0 %	25,332,440
Γιβραλτάρ	29,034	**20,66**	71.2 %	0.0 %	21,7
Ελλάδα	10,767,827	**5,706,948**	53.0 %	1.1 %	3,845,820
Γκρένσεϊ & Άλντερνεϊ	65,345	**48,3**	73.9 %	0.0 %	2,62
Ουγγαρία	9,958,453	**6,516,627**	65.4 %	1.3 %	4,265,960
Ισλανδία	313,183	**304,129**	97.1 %	0.1 %	227
Ιρλανδία	4,722,028	**3,627,462**	76.8 %	0.7 %	2,183,760
Ιταλία	61,261,254	**35,800,000**	58.4 %	6.9 %	23,202,640
Τζέρσεϊ	94,949	**45,8**	48.2 %	0.0 %	32,76
Κόσσοβο	1,836,529	**377**	20.5 %	0.1 %	n/a
Λετονία	2,191,580	**1,570,925**	71.7 %	0.3 %	414,52
Λιχτενστάιν	36,713	**31,206**	85.0 %	0.0 %	12,78
Λιθουανία	3,525,761	**2,293,508**	65.1 %	0.4 %	1,118,500
Λουξεμβούργο	509,074	**462,697**	90.9 %	0.1 %	227,52

Μακεδονία	2,082,370	**1,180,704**	56.7 %	0.2 %	962,78
Μάλτα	409,836	**282,648**	69.0 %	0.1 %	217,04
Νήσος του Μαν	85,421	**39,46**	46.2 %	0.0 %	39,38
Μολδαβία	3,656,843	**1,639,463**	44.8 %	0.3 %	285,64
Μονακό	30,51	**30,7**	100.6 %	0.0 %	36,22
Μαυροβούνιο	657,394	**328,375**	50.0 %	0.1 %	306,26
Ολλανδία	16,730,632	**15,549,787**	92.9 %	3.0 %	7,554,940
Νορβηγία	4,707,270	**4,560,572**	96.9 %	0.9 %	2,771,480
Πολωνία	38,415,284	**24,940,902**	64.9 %	4.8 %	9,863,380
Πορτογαλία	10,781,459	**5,950,449**	55.2 %	1.1 %	4,663,060
Ρουμανία	21,848,504	**9,642,383**	44.1 %	1.9 %	5,374,980
Ρωσία	142,517,670	**67,982,547**	47.7 %	13.1 %	7,963,400
Σαν Μαρίνο	32,14	**17**	52.9 %	0.0 %	9,42
Σερβία	7,276,604	**4,107,000**	56.4 %	0.8 %	3,377,340
Σλοβακία	5,483,088	**4,337,868**	79.1 %	0.8 %	2,032,200
Σλοβενία	1,996,617	**1,440,066**	72.1 %	0.3 %	730,16
Ισπανία	47,042,984	**31,606,233**	67.2 %	6.1 %	17,590,500
Svalbard & Jan Mayen	2,191	n/a	n/a	n/a	n/a
Σουηδία	9,103,788	**8,441,718**	92.7 %	1.6 %	4,950,160
Ελβετία	7,925,517	**6,509,247**	82.1 %	1.3 %	3,055,800
Τουρκία	79,749,461	**36,455,000**	45.7 %	7.0 %	32,131,260
Ουκρανία	44,854,065	**15,300,000**	34.1 %	3.0 %	2,312,920
Ην. Βασίλειο	63,047,162	**52,731,209**	83.6 %	10.2 %	32,950,400
Πόλη του Βατικανό	535	**480**	89.7 %	0.0 %	20
Σύνολο Ευρώπης	**820,918,446**	**518,512,109**	**63.2 %**	**100.0 %**	**250,934,000**

Σημειώσεις: (1) Τα Ευρωπαϊκά στατιστικά στοιχεία (τα προκαταρτικά) ενημερώθηκαν για τις 30 Ιουνίου το 2012. (2) Τα δεδομένα χρηστών Face book αφορούν τις 31του Δεκέμβρη του 2012. (3) Οι αριθμοί πληθυσμού αφορούν τα μέσα του έτους 2012 με βάση κυρίως τα στοιχεία που περιέχονται στις Η.Π.Α Υπηρεσία Απογραφής. (4) Η χρήση αριθμών προέρχεται από ποικίλες πηγές ,βασισμένες κυρίως στα στατιστικά στοιχεία δημοσιευμένα από Nielsen Online,ITU,Face book, GfK και άλλες αξιόπιστες πηγές.

Πηγή: Internet World Statistics

4.2 Κοινωνική δικτύωση

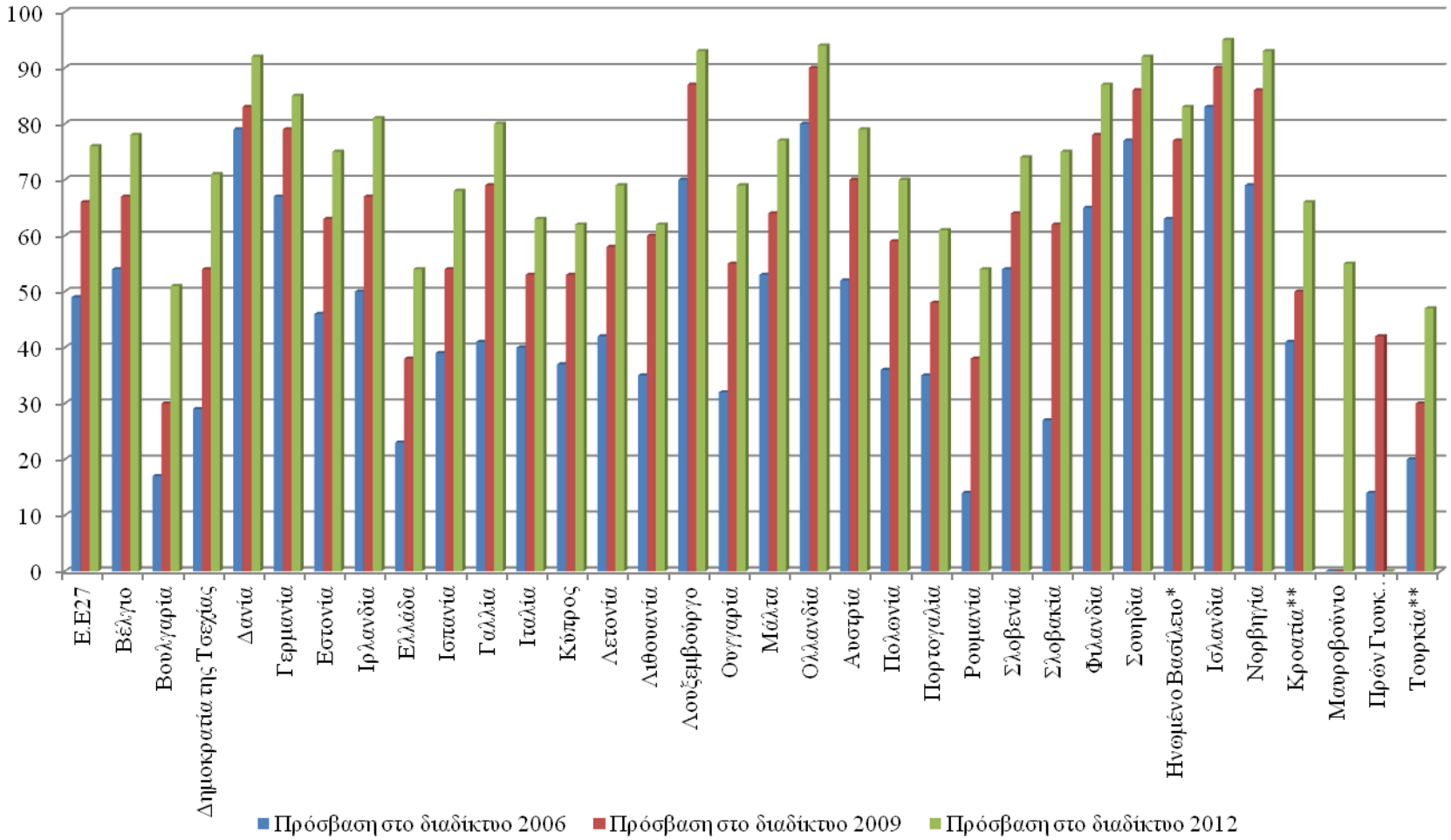
Τα τελευταία χρόνια το φαινόμενο της κοινωνικής δικτύωσης είναι εντονότερο καθώς η εξέλιξη της τεχνολογίας και οι γρήγοροι ρυθμοί ζωής επιβάλλουν τη διαδικτυακή δραστηριότητα.

Στο διάγραμμα 1 που ακολουθεί απεικονίζεται το ποσοστό νοικοκυριών με πρόσβαση στο διαδίκτυο τα έτη 2006-2009-2012.

Στο διάγραμμα 2 απεικονίζεται το ποσοστό νοικοκυριών με Ευρυζωνική σύνδεση τα έτη 2006-2009-2012.

Διάγραμμα 1

Νοικοκυριά με Πρόσβαση στον Ίντερνετ % (τα έτη 2006-2009-2012)

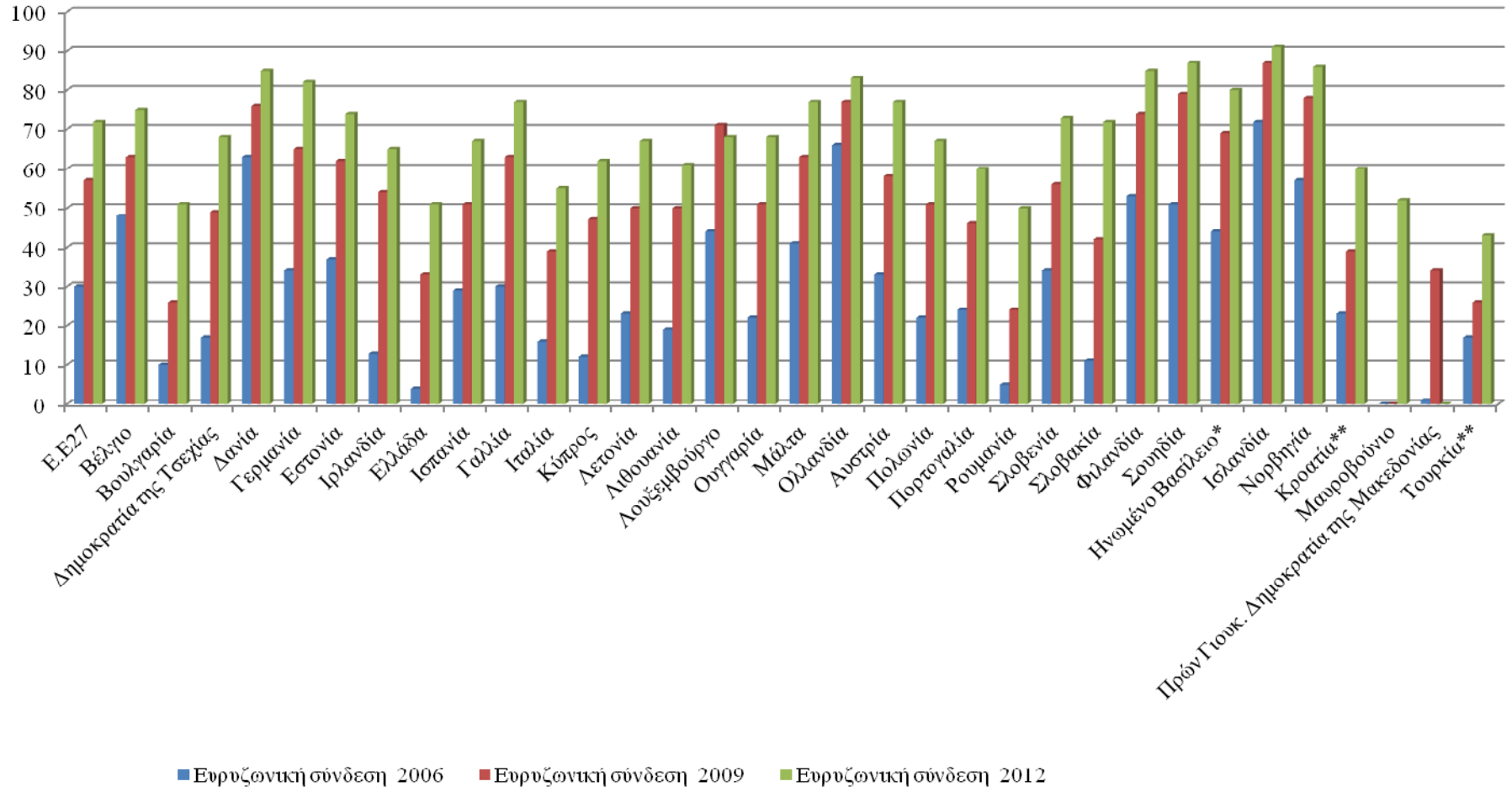


Πηγή: Eurostat, Reference: STAT/12/185/18-12-2012

(Τα δεδομένα δεν είναι διαθέσιμα* Τα δεδομένα του Ην. Βασιλείου ξεκινούν το 2011; Στην ΕΕ27 για το 2012 τα δεδομένα που χρησιμοποιούνται για το Ην. Βασίλειο είναι του 2011, Τα δεδομένα της Κροατίας και της Τουρκίας ξεκινούν από το 2007)

Διάγραμμα 2

Νοικοκυριά με Ευρυζωνική σύνδεση % (τα έτη 2006-2009-2012)



Πηγή: Eurostat, Reference: STAT/12/185/18-12-2012

(Τα δεδομένα δεν είναι διαθέσιμα* Τα δεδομένα του Ην. Βασιλείου ξεκινούν το 2011; Στην ΕΕ27 για το 2012 τα δεδομένα που χρησιμοποιούνται για το Ην. Βασίλειο είναι του 2011, Τα δεδομένα της Κροατίας και της Τουρκίας ξεκινούν από το 2007)

Η κοινωνική δικτύωση έχει διάφορους ορισμούς ανάλογα την οπτική γωνία που τη βλέπουν όσοι τη χρησιμοποιούν ως μέσο ενημέρωσης, πληροφόρησης επικοινωνίας, διαφήμισης,. Για παράδειγμα άτομα του μάρκετινγκ όταν αναφέρονται στην κοινωνική δικτύωση αναφέρονται στην δημιουργική προώθηση ενός προϊόντος και την σχέση του πελάτη με την εταιρεία (Steinfield, et al., 2008).

Η κοινωνική δικτύωση είναι μια αμφίδρομη σχέση και μορφή επικοινωνίας που επιτρέπει σε ομάδες να υποστηρίζουν τα συμφέροντα τους. Τα κοινωνικά μέσα δικτύωσης δεν έχουν προκαθορισμένα όρια. Οποιοσδήποτε μπορεί να συμμετάσχει σε αυτά. Όλα τα κοινωνικά δίκτυα έχουν τα δικά τους χαρακτηριστικά που τα διαχωρίζουν από τα υπόλοιπα. Αυτό το γεγονός δίνει στους χρήστες την αίσθηση ότι ανήκουν σε μία κοινότητα, σε έναν «κόσμο» χωρίς διακρίσεις με κοινή γλώσσα επικοινωνίας και κοινά ενδιαφέροντα (Lampe, et al., 2008).

Τα κοινωνικά δίκτυα χωρίζονται κυρίως σε 3 κατηγορίες ανάλογα με την χρήση τους από τα μέλη τους:

α) επαγγελματικού ενδιαφέροντος (επιχειρηματικού προσανατολισμού)

β) γενικού ενδιαφέροντος (κοινωνικού χαρακτήρα και δίκτυα αλληλεπίδρασης)

γ) ειδικού ενδιαφέροντος (συγκεκριμένη κοινωνική ή οικονομική δραστηριότητα)

Άλλος διαχωρισμός των κοινωνικών δικτύων είναι:

α) άμεσα δίκτυα (δυνατότητα πρόσβασης στο προφίλ ενός χρήστη χωρίς την έγκριση του)

β) έμμεσα δίκτυα (απαραίτητη άδεια έγκρισης για την σύνδεση στο προφίλ ενός άλλου χρήστη) (Goldbaum, 2008)

Τα άμεσα δίκτυα χρησιμοποιούνται κυρίως για διαφήμιση και μάρκετινγκ ενώ τα έμμεσα για την διαμόρφωση μιας συμπεριφοράς καταναλωτών.

Άλλος ένας διαχωρισμός μπορεί να γίνει βάση του μεγέθους των αριθμών χρηστών των δικτύων και αυτοί που επηρεάζουν πιο πολύ τις διαδράσεις του δικτύου

είναι οι συχνοί χρήστες και από την πυκνότητα δηλαδή ανάλογα με το είδος των σχέσεων που δημιουργούνται μεταξύ των χρηστών. (Chuhay, 2010, Hamill & Gilbert, 2009)

Τα κοινωνικά μέσα δικτύωσης στην ουσία προσιδιάζουν μεταξύ τους καθώς έχουν την τάση να μιμούνται τα χαρακτηριστικά των άλλων μέσων του Διαδικτύου. Γι' αυτό, αυτό που στην ουσία διαφέρει μεταξύ τους είναι οι χρήστες που το χρησιμοποιούν και όχι οι υπηρεσίες που προσφέρουν και αυτός είναι ο κύριος παράγοντας που λαμβάνουν υπόψη οι χρήστες για να γίνουν μέλη τους.

Κάθε χρήστης μπορεί ταυτόχρονα να έχει την δικιά του επαγγελματική, κοινωνική, δημόσια ταυτότητα του και να συμμετέχει στα κοινά με το να είναι ακροατής σχολιαστής, πελάτης και θεατής. Αυτό αναφέρεται σαν «γενετικός κώδικας» των κοινωνικών δικτύων.

Ένα σημαντικό χαρακτηριστικό των κοινωνικών μέσων δικτύωσης είναι η ιδιαίτερη αξία που δίνουν στους χρήστες τους και αυτό φαίνεται από τη χρήση του Web 2.0. Οι χρήστες είναι το επίκεντρο και έχουν μεγάλη επιρροή καθώς χωρίς την εμπλοκή τους δεν θα υπήρχε ροή πληροφοριών. Με την χρήση του Web 2.0 νοείται ότι οι χρήστες επιτρέπεται να αλλάξουν το περιβάλλον της σελίδας τους και να κάνουν όποια τροποποίηση θελήσουν όπως είναι τα links και τα tag.

Οι λόγοι που πολλοί άνθρωποι συμμετέχουν στα μέσα κοινωνικής δικτύωσης είναι πολλοί και διαφορετικοί μερικοί εκ των οποίων είναι :

α)δημιουργία κοινότητας

β)συμμετοχή σε ομάδες με κοινά συμφέροντα

γ)ανταλλαγή πληροφοριών ,απόψεων ,σκέψεων

δ)προώθηση φωτογραφιών ,τραγουδιών ,εμπειριών

ε)εύρεση καινούργιων φίλων

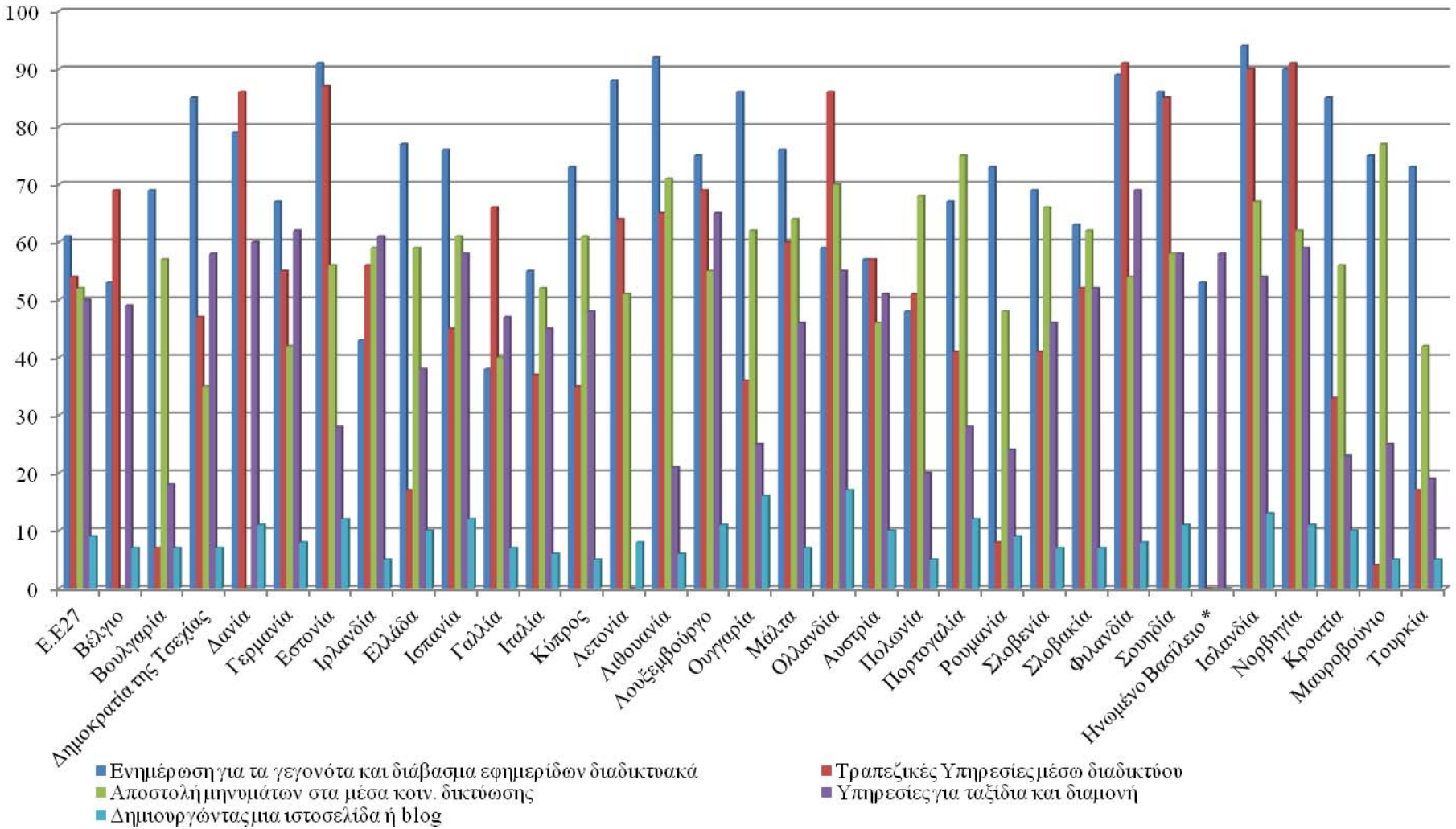
στ)διατήρηση επαφής με συγγενείς ,φίλους

ζ) ψυχαγωγία

Το παρακάτω διάγραμμα απεικονίζει το ποσοστό % των επιλεγμένων δραστηριοτήτων των χρηστών του διαδικτύου.

Διάγραμμα 3

Ποσοστό % των επιλεγμένων δραστηριοτήτων των χρηστών του διαδικτύου τους 3 τελευταίους μήνες (2012)



Πηγή: Eurostat, Reference: STAT/12/185/18-12-2012

(Τα δεδομένα δεν είναι αξιόπιστα* Τα δεδομένα του Ην. Βασιλείου ξεκινούν το 2011; Στην ΕΕ27 για το 2012 τα δεδομένα που χρησιμοποιούνται για το Ην. Βασίλειο είναι του 2011)

4.3 Οι πιο διαδεδομένοι κοινωνικά Ιστότοποι - Facebook &Twitter

Η δημοτικότητα των κοινωνικών δικτύων στη σύγχρονη εποχή είναι ιδιαίτερα υψηλή τόσο σε εγχώριο όσο και σε διεθνές επίπεδο. Η έμφυτη ανάγκη του ανθρώπου για επικοινωνία έχει οδηγήσει στη δημιουργία μιας σύγχρονης ηλεκτρονικής κοινωνίας διαμορφωμένη μέσα από τα κοινωνικά δίκτυα.

Το Facebook αποτελεί έναν από τους διασημότερους ιστότοπους διεθνώς και εμφανίστηκε για πρώτη φορά στις 4 Φεβρουαρίου το 2004.Οι χρήστες έχουν τη δυνατότητα μέσω facebook να ανταλλάσσουν πληροφορίες, τα νέα τους, να ανεβάζουν βίντεο και φωτογραφίες και να αλληλεπιδρούν με τους φίλους τους. Στο facebook μπορεί ο οποιοσδήποτε χρήστης να δημιουργήσει ένα ολοκληρωμένο προφίλ συμπληρώνοντας διάφορα προσωπικά στοιχεία εφόσον το επιθυμεί φυσικά. Σε αυτά τα στοιχεία συγκαταλέγονται το όνομα του, η ημερομηνία γέννησης του, τα στοιχεία επικοινωνίας του όπως προσωπικός αριθμός τηλεφώνου, οι πολιτικές και θρησκευτικές του πεποιθήσεις,τα βιβλία και οι ταινίες ποτ του αρέσουν σκιαγραφώντας έτσι τον χαρακτήρα του και γνωστοποιώντας τον στους φίλους που έχει στο facebook. Ο συγκεκριμένος ιστότοπος αποτελεί ένα δωρεάν μέσο επικοινωνίας και αλληλεπίδρασης που συνεχώς εξελίσσεται προσφέροντας όλο και περισσότερες δυνατότητες στους χρήστες του.

Το Twitter συνιστά έναν επίσης δωρεάν τρόπο κοινωνικής δικτύωσης, με τον οποίο οι χρήστες μπορούν να γράφουν σύντομα μηνύματα και να διαβάζουν τα μηνύματα άλλων χρηστών της συγκεκριμένης υπηρεσίας (τα λεγόμενα tweets).Το Twitter αποτελεί και αυτό ένα μέσο συνεχούς εξέλιξης, το οποίο προσφέρει τη δυνατότητα συνεχούς επικοινωνίας των χρηστών μεταξύ τους Συνιστά επίσης ένα εργαλείο για να ανακοινώνει κανείς ότι εκείνος επιθυμεί και να το μοιραστεί με τους υπόλοιπους χρήστες.

4.4 Ασφάλεια και Ιδιωτικότητα στο Facebook

Η ασφάλεια των χρηστών και των δεδομένων τους στο Facebook υπονομεύεται κυρίως από τρεις παράγοντες.

- Από τους ίδιους τους χρήστες που κατά τεκμήριο κάνουν κακή χρήση των δυνατοτήτων και των επιλογών που τους προσφέρονται από τα κοινωνικά δίκτυα.
- Από τα ίδια τα κοινωνικά δίκτυα που δεν έχουν ως κύριο μέλημα την ασφάλεια των χρηστών τους και
- Από τους κακόβουλους χρήστες οι οποίοι εκμεταλλευόμενοι αυτή την αδυναμία των δικτύων στοχεύουν τους απλούς χρήστες με σκοπό να τους αποσπάσουν πληροφορίες που μπορούν να χρησιμοποιήσουν προς όφελος τους.

Η περιοχή "About me" παρουσιάζει μεγάλο ενδιαφέρον καθότι είναι η περιοχή στην οποία ο χρήστης δίνει πληροφορίες για τον εαυτό του με σκοπό να συστηθεί στους άλλους. Πληροφορίες που καλύπτουν ένα πολύ μεγάλο εύρος της ζωής του και μπορεί να αφορούν από ονοματεπώνυμα δικά του ή και μελών της οικογένειας του μέχρι και μέρη που έχει ζήσει η επισκεφτεί . Επίσης κανείς μπορεί να βρει πληροφορίες σχετικά με το που έχει εργαστεί η έχει σπουδάσει κάποιος αλλά και τρόπους επικοινωνίας όπως διευθύνσεις και κινητά τηλέφωνα. Σε μερικές ακραίες περιπτώσεις κυρίως στην Αμερική, έχει παρατηρηθεί χρήστες να δίνουν αριθμούς κοινωνικής ασφάλισης αλλά και πιστωτικών καρτών (Gentile, 2010).

Αξιοσημείωτο σε αυτήν την ενότητα που αποτελεί και μεγάλο κενό ασφάλειας, είναι ότι ζητούνται πληροφορίες όπως το σχολείο η ο καλύτερος φίλος η το όνομα της μητέρας οι οποίες χρησιμοποιούνται σαν ερωτήσεις ασφάλειας στη περίπτωση ανάκτησης χαμένων κωδικών πρόσβασης.

Επιπλέον χρήστες πολλές φορές έχουν κοινοποιήσει ότι βρίσκονται μακριά από τον τόπο κατοικίας τους με αποτέλεσμα να έχουν πέσει θύματα κλοπής. Σύμφωνα με το τελευταίο update (Facebook Timeline) σημαντικά γεγονότα της ζωής του χρήστη, τα οποία περιλαμβάνουν από ιατρικά στοιχεία μέχρι απώλειες οικείων του προσώπων είναι διαθέσιμα στο κοινό by default. Σημαντικές πληροφορίες μπορεί

να αντλήσει κανείς και από τις φωτογραφίες στις οποίες ο χρήστης ενθαρρύνεται να δηλώσει ακριβές μέρος και ημερομηνία. Συνήθως η φωτογραφία προφίλ είναι δημόσια και έτσι διευκολύνεται το profile cloning. Τέλος στην ενότητα "Map" υπάρχουν συνοψισμένα όλα τα μέρη τα οποία ο χρήστης έχει επισκεφτεί.

Το Facebook προσφέρει παρά πολλές εφαρμογές οι οποίες, προκειμένου να τις χρησιμοποιήσει κανείς, ζητούν πρόσβαση στα δεδομένα των χρηστών (Murphy, 2012).

Έπειτα το Facebook χρησιμοποιεί ένα λογισμικό αναγνώρισης προσώπου προκειμένου να ξεχωρίζει χρήστες σε φωτογραφίες και να προτείνει στους φίλους τους να τους «επισημάνουν» με άγνωστες προς το παρόν προεκτάσεις.

Όπως γίνεται εύκολα αντιληπτό οι κίνδυνοι που ελλοχεύουν είναι αρκετοί και δεν περιορίζονται μόνο στην απώλεια των κωδικών πρόσβασης ή ακόμα και των πιστωτικών καρτών (με τις όποιες συνέπειες) αλλά μπορούν να έχουν ακόμα σοβαρότερες προεκτάσεις και επιπτώσεις όχι μόνο στην ψηφιακή ζωή, με περιπτώσεις identity theft και διαδικτυακής παρενόχλησης (cyber bullying) αλλά και στη κανονική ζωή με τα περιστατικά απολύσεων, αποβολών και εκβιασμών συνεχώς να αυξάνονται (Monkovic, 2009).

4.5 Ασφάλεια και Ιδιωτικότητα στο Twitter

Στο Twitter τα πράγματα μοιάζουν να είναι πιο απλά κυρίως λόγο του ότι οι χρήστες δεν συνηθίζουν (και αυτό γιατί δεν ενθαρρύνονται από το ίδιο το δίκτυο) να κοινοποιούν πολλά δεδομένα μιας και το twitter στηρίζει την λειτουργία του στα «τιτιβίσματα» (tweets αντίστοιχο του status update στο Facebook μεγέθους 140 χαρακτήρων). Εδώ η ασφάλεια και η ιδιωτικότητα μπορούμε να πούμε πως υπονομεύονται κατά κύριο λόγο από κακόβουλους χρήστες αλλά και η απερίσκεπτη χρήση έχει και εδώ πρωτεύοντα ρόλο. Παρακάτω θα αναφερθούμε στους κινδύνους που υπάρχουν και θα δούμε πως μπορεί κάποιος να προφυλαχθεί.

Βασική λειτουργία του Twitter αποτελεί όπως είπαμε το tweet με το οποίο οι χρήστες εκφράζουν τις απόψεις τους, σχολιάζουν γεγονότα, ή μοιράζονται links και φωτογραφίες με άλλους χρήστες. Στο Twitter όμως υπάρχει μία σημαντική διαφορά. Οι συνδέσεις μεταξύ των χρηστών του είναι μονόδρομες που σημαίνει ότι ένας χρήστης μπορεί να δει τα σχόλια ενός άλλου χωρίς να του ζητήσει την άδεια. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση ενός υποψήφιου εργαζομένου στη Cisco ο οποίος μετά την συνέντευξη έσπευσε να σχολιάσει στο λογαριασμό του «*η Cisco μου προσέφερε δουλειά! Τώρα θα πρέπει να αποφασίσω μεταξύ ενός παχυλού μισθού και του να πηγαίνω κάθε μέρα μέχρι το San Jose και να μισώ τη δουλεία*» με αποτέλεσμα να λάβει την απάντηση με ειρωνικό τρόπο «*Είμαι σίγουρος ότι ο υπεύθυνος προσλήψεων θα χαρεί πολύ να μάθει ότι μισείς τη δουλειά. Εμείς στη Cisco χρησιμοποιούμε πολύ το διαδίκτυο*» και φυσικά να μην πάρει την θέση.

Από την άλλη μεριά, τα tweets και οι φωτογραφίες συνοδεύονται από προσδιορισμό θέσης με τις επιπτώσεις στην ιδιωτικότητα των χρηστών να είναι σαφής. Εκτός από τα κλασσικά προβλήματα που δημιουργούνται από τους ίδιους τους χρήστες και συναντώνται σχεδόν σε όλα τα κοινωνικά δίκτυα το twitter ευνοεί και τη δράση των spammers και αυτό γιατί οι πλαστοί λογαριασμοί είναι πολύ εύκολο να δημιουργηθούν.

Αυτοί μέσω πλαστών (hoax) emails στοχεύουν σε phishing attacks σε χρήστες για να τους αποσπάσουν τα συνθηματικά. Επίσης προσθέτουν και κακόβουλο λογισμικό σε αυτά που συνήθως είναι κάποιο worm (Koobface) ή twitter worm τα οποία εξαπλώνονται σε όλες τις επαφές των θυμάτων αποκτώντας δεδομένα. Άλλος

γνωστός τρόπος spam είναι το click jacking όπου οι επιτιθέμενοι «χακάρουν» έναν λογαριασμό ο οποίος είναι δημοφιλής και θεωρείται αξιόπιστος και μέσω URL shortening δημοσιεύουν ένα link και καλούν όλες τις επαφές αυτό του λογαριασμού να το ακολουθήσουν. Συνοψίζοντας, μπορεί το Twitter να φαίνεται εκ πρώτης όψεως ότι δεν αντιμετωπίζει πολλά προβλήματα λόγο του ότι διαχειρίζεται λιγότερες πληροφορίες σε σχέση με το Facebook αλλά δεν παύει να αποτελεί πηγή κινδύνων για τους απερίσκεπτους χρήστες και πόλο έλξης για τους επιτιθέμενους.

ΚΕΦΑΛΑΙΟ 5°

Νομοθεσία για το Ηλεκτρονικό Έγκλημα

Στην Ελλάδα αλλά και σε άλλες χώρες, η νομοθεσία που διέπει τα ηλεκτρονικά εγκλήματα παρουσιάζει αδυναμίες. Οι νομοθέτες οφείλουν να ενημερώνονται συνεχώς για τις εξελίξεις που προκύπτουν στον τομέα της τεχνολογίας των υπολογιστών, ώστε να μπορούν να ανιχνεύουν και να εντοπίζουν τη διάπραξη των σχετικών αξιόποινων πράξεων και να επιβάλλουν την αντίστοιχη ποινή. Η ψηφιακή εγκληματικότητα συνιστά μια δραστηριότητα ιδιαίτερα εξειδικευμένη αλλά και ανεπτυγμένη τεχνολογικά, με απόρροια την εμφάνιση ποικίλων προβλημάτων στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά.

Ο διεθνής χαρακτήρας που αποδίδεται στα συγκεκριμένα εγκλήματα δίνει τη δυνατότητα στους δράστες να έχουν αφενός γρήγορη πρόσβαση και αφετέρου εύκολη προσβολή των δεδομένων στα συστήματα Η/Υ παγκοσμίως. Τα ψηφιακά εγκλήματα διακρίνονται επίσης για την πληθώρα δεδομένων τους, τον μη οπτικό χαρακτήρα των πιθανών αποδείξεων, τη δυνατότητα «μεταμφίεσης» τους καθώς και την ταχεία εξαφάνιση των οποιωνδήποτε στοιχείων από τη μεριά των δραστών-εγκληματιών.

Το ηλεκτρονικό έγκλημα στην εποχή μας παρουσιάζει, δυστυχώς, αλματώδη αύξηση και εμφανίζεται σε ποικίλες μορφές. Για την αντιμετώπιση αυτού κρίθηκε απαραίτητη η συνεργασία μεταξύ των κρατών για τη χάραξη μιας αναλυτικής και αποτελεσματικής στρατηγικής για την καταπολέμηση αυτού του φαινομένου. Ο σκοπός αυτός επετεύχθη με το Συνέδριο για το Ηλεκτρονικό έγκλημα (Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφηκε στην Βουδαπέστη στις 23.11.2001.

Στη συνθήκη της Βουδαπέστη, μεταξύ πολλών άλλων χωρών υπέγραψε και η Ελλάδα, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα είδη ηλεκτρονικών εγκλημάτων:

- Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ. Τέτοια αδικήματα

είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.

- Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικούς υπολογιστές και πλαστογραφία.
- Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.
- Για τα αδικήματα που αφορούν την καταπάτηση πνευματικής ιδιοκτησίας. Επιπλέον η συνθήκη περιέχει ρυθμίσεις για την συνέργεια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων.

Επίσης επισημαίνεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή συνιστά το πιο άρτιο κείμενο αναφορικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση. Σαφώς υπάρχουν και άλλα γενικά νομοθετήματα που βοηθούν στην αντιμετώπιση του Ηλεκτρονικού εγκλήματος και τα οποία θα αναφερθούν παρακάτω με ενδελέχεια.

Ένα ακόμα σημαντικό βήμα αποτελεί η ίδρυση, το 2002, ενός νέου ευρωπαϊκού οργάνου, της Eurojust, με γνώμονα τη δημιουργία ενός ενιαίου ευρωπαϊκού χώρου Δικαιοσύνης, που θα έχει ως σκοπό την ισχυροποίηση του αγώνα κατά των πιο βασικών μορφών εγκληματικότητας και της εποικοδομητικότερης συνεργασίας σε ποινικές υποθέσεις. Ωστόσο και το έγκλημα στον κυβερνοχώρο, με τις ποσοτικές και ποιοτικές διαστάσεις του, αποτελεί, σε κάθε περίπτωση, έναν από τους «ευαίσθητους τομείς» για την προώθηση αυτής της συνεργασίας υπό την αιγίδα και το κύρος της Eurojust.

Στην Ελλάδα ισχύουν οι νόμοι 2928/2001 για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων και 3251/2004 αναφορικά με το Ευρωπαϊκό ένταλμα σύλληψης .Είναι σημαντικό να τονιστεί ότι οι ποικίλες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα νομοθετήματα τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση γενικότερα.

5.1 Το πρόβλημα της δικαιοδοσίας στο διαδίκτυο

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο διαδίκτυο είναι ιδιαίτερα περίπλοκο εξαιτίας της παγκοσμιότητας του. Δικαιοδοσία είναι η αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση αλλά συγχρόνως και η αντίστοιχη αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά.

Η ανεύρεση της αρμοδιότητας του δικαστηρίου είναι συνυφασμένη με τον καθορισμό του τόπου τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες (Mali, 2008):

1. **Η θεωρία του τόπου του αποτελέσματος**. Τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
2. **Η θεωρία του τόπου ενέργειας**. Ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου έχει τελεστεί η ενέργεια που έτεινε στο άδικο αποτέλεσμα. Εφόσον η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος ενέργειας είναι αυτός όπου ολοκληρώθηκε η ενέργεια.
3. **Η μικτή θεωρία**. Τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.
4. **Η θεωρία του βαρύνοντος τόπου**. Σύμφωνα με την αυτήν την θεωρία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Όμως υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας καθώς είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.

5.1.1 Ελληνική Νομοθεσία

Η Ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, διαθέτει έναν συνδυασμό διεθνών

συνθηκών, συνταγματικών διατάξεων, διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάσει κοινοτικών οδηγιών.

Στο Σύνταγμα της Ελλάδος, περιλαμβάνονται μια σειρά από διατάξεις, για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας». Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9, αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της.

5.2 Νόμοι ανάλογοι των παραβιάσεων

5.2.1 Ποινική προστασία των προσωπικών δεδομένων

Οι διατάξεις του Ν. 2472/97 αποσκοπούν στην προστασία της ιδιωτικότητας και των προσωπικών δεδομένων και προβλέπει ποινές για όσους δεν τηρούν τις υποχρεώσεις τους ως προς τον νόμο. (π.χ. διατήρηση αρχείου με ευαίσθητα δεδομένα χωρίς άδεια, διασύνδεση αρχείων χωρίς γνωστοποίηση και άδεια) .

Συγκεκριμένα στην παράγραφο 4 όποιος αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει , επεξεργάζεται, μεταδίδει, ανακοινώνει δεδομένα άλλων κινδυνεύει να τιμωρηθεί με φυλάκιση τουλάχιστον 1 έτους και χρηματική ποινή τουλάχιστον 2.900 ευρώ έως 29.000 ευρώ, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις

5.2.2 Οικονομικό ηλεκτρονικό εμπόριο και έγκλημα

Το ηλεκτρονικό εμπόριο γνωρίζει ιδιαίτερη ανάπτυξη κι αποτελεί ανασταλτικός παράγοντας από πλευράς χρηστών-πελατών αλλά και των

επιχειρήσεων αυτής της μορφής αλλά παράλληλα αποτελεί κατασταλτικό παράγοντα για το συμβατικό εμπόριο.

Η Ευρωπαϊκή Κοινότητα έχει εκδώσει μια σειρά από οδηγίες που ρυθμίζουν τα θέματα του ηλεκτρονικού εμπορίου με σκοπό την ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ κρατών-μελών και την ανθρώπινη αξιοπρέπεια, την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας και την προστασία του καταναλωτή και της δημόσιας υγείας.

Όσον αφόρα στο ηλεκτρονικό εμπόριο ρυθμίζεται στο Ελληνικό δίκαιο με το Ποινικό Δίκαιο 131/2003 στο όποιο ενσωματώθηκε η οδηγία 2000/31/ΕΚ. Οι πιο σημαντικές διατάξεις περιλαμβάνονται:

- **άρθρο 6**, το όποιο ρυθμίζει το ζήτημα της μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου, βάσει του όποιου, οι πάροχοι των υπηρεσιών αυτών υποχρεούνται να τηρούν και να συμβουλεύονται τακτικά μητρώα επιλογών, όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες.
- **άρθρα 8-10**, που αναφέρονται στις ηλεκτρονικές συμβάσεις και τους τρόπους ηλεκτρονικής παραγγελίας. Γενικά, επιτρέπεται η κατάρτιση ηλεκτρονικών συμβάσεων, εξαιρούμενων περιπτώσεων που αφορούν θεμελίωση ή μεταβίβαση εμπράγματων δικαιωμάτων επί ακινήτων, που εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο και όσες, εκ του νομού, απαιτείται προσφυγή σε δημοσιές αρχές, δικαστήρια ή επαγγέλματα που ασκούν δημόσια εξουσία. Η ηλεκτρονική παραγγελία θεωρείται έγκυρη όταν ο παροχέας ενημερώσει τον πελάτη για τις λεπτομέρειες της σύμβασης και μετά την παραγγελία, αποστείλει και ηλεκτρονικό μήνυμα επιβεβαίωσης.
- **άρθρο 20**, το όποιο εξαιρεί την εφαρμογή του Διατάγματος από ορισμένες δραστηριότητες όπως π.χ. το φορολογικό τομέα και θέματα που ήδη ρυθμίζονται με το νόμο περί προστασίας των προσωπικών δεδομένων.

Γενικά οι απάτες με υπολογιστή ελέγχονται βάση του Άρθρου. 386 Α και ορίζει ότι όποιος λαμβάνει για τον εαυτό του κάποιο παράνομο περιουσιακό όφελος ή βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Μπορεί όμως να επιβάλλονται και ποινές φυλάκισης τουλάχιστον δύο ετών εάν η ζημία είναι ιδιαίτερα υψηλή (>15.000 ευρώ).

5.2.3 Ποινική κύρωση της παραβίασης πνευματικής ιδιοκτησίας

Στις μέρες μας το πρόβλημα της παράβασης των πνευματικών δικαιωμάτων είναι μείζων ζήτημα .Η μετατροπή της πληροφορίας σε ψηφιακή μορφή δίνει τη δυνατότητα εύκολης και γρήγορης αναπαραγωγής της. Μερικά παραδείγματα είναι τα ψηφιακά λεξικά και εγκυκλοπαίδειες. Εκτός από τη βάση δεδομένων, χρήζουν προστασίας και τα προγράμματα των Η/Υ. Στην ελληνική νομοθεσία έχει ποινικοποιηθεί η αντιγραφή προγραμμάτων και η παραβίαση πνευματικής ιδιοκτησίας (370 Γ παραγρ. 1). Η διάταξη προβλέπει ότι όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή 290 € έως 5.900 €.

5.2.4 Παράνομη «παρέμβαση» στο σύστημα και στα δεδομένα

Τα προσωπικά δεδομένα και η προστασία του απορρήτου είναι ένα θέμα αμφισβητούμενο στο χώρο του διαδικτύου. Καθημερινά ζητούνται τα προσωπικά δεδομένα από οργανισμούς κι επιχειρήσεις για εμπορικούς και διαφημιστικούς λόγους. Ο χρήστης του διαδικτύου δίνει πληροφορίες για τα προσωπικά δεδομένα του με μια σχετική ευκολία χωρίς να το αντιλαμβάνεται πολλές φορές. Δίνει πληροφορίες σχετικά με την προσωπικότητά του, τις προτιμήσεις του μέχρι και πληροφορίες ταυτότητας και αριθμούς πιστωτικών καρτών.

Με το άρθρο 370Β ελέγχεται η απόκτηση απορρήτων και με το άρθρο 370Γ η χωρίς άδεια διείσδυσης σε πρόγραμμα υπολογιστή (Hacking). Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή χωρίς άδεια τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον 29 ευρώ. Σε περίπτωση βέβαια που παραβιάζονται οι διεθνείς σχέσεις τιμωρείται με ποινή της κατασκοπείας

5.2.5 Παράνομη πρόσβαση σε απόρρητα

Όποιος παράνομα αντιγράφει, αποκαλύπτει σε τρίτον ή παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία αποτελούν κρατικά, ή επαγγελματικά απόρρητα τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών βάση του άρθρου 370Β και 370Γ. Ο νόμος προβλέπει αυστηρότερη ποινή για όποιον πραγματοποιεί την παράβαση αυτή και είχε σχέσεις εμπιστοσύνης με τον κάτοχο των στοιχείων αυτών ή αν πρόκειται για στρατιωτικό απόρρητο που αφορά την ασφάλεια του κράτους.

Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Αυτά είναι:

- Η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων.
- Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.
- Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173 - CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεση μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών.

5.2.6 Κατοχή και διακίνηση παιδικής πορνογραφίας

Σύμφωνα με το άρθρο 348 Α ΠΚ, όπως αυτό αντικαταστάθηκε από το άρθρο 10 του Ν. 3625/2007 και τροποποιήθηκε με την παρ. 12 του άρθρου 3 του Ν. 3727/2008.

- Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτή, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.
- Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.
- Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ:

α. αν τελέσθηκαν κατ' επάγγελμα ή κατά συνήθεια»

β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή σωματικής δυσλειτουργίας λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος».

Αν η πράξη της περίπτωσης β' είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθούντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.

Ένα από τα σημαντικότερα βήματα για την καταπολέμηση της παιδικής πορνογραφίας στην Ελλάδα ήταν το ότι με το Ν. 3666/2008 προστέθηκε το έγκλημα

της διακίνησης παιδικής πορνογραφίας στις περιπτώσεις άρσης του απορρήτου των επικοινωνιών (άρθρο 4 παρ. 1 εδ. α' του Ν. 2225/1994). Με βάση αυτή τη ρύθμιση πλέον η Δίωξη Ηλεκτρονικού Εγκλήματος έχει τη δυνατότητα να παρέμβει, να βρει στοιχεία και εν τέλει να συλλάβει τους διαπράττοντες τα εγκλήματα. Σε αυτήν ακριβώς τη νέα διάταξη οφείλεται και η πληθώρα των υποθέσεων διακίνησης παιδικής πορνογραφίας που έχουν παραπεμφθεί στη δικαιοσύνη.

5.2.7 Ιοί- Προστασία των δεδομένων από ιούς

Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ.

Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

5.2.8 Εγκλήματα κατά της ηθικής και της αξιοπρέπειας-Προστασία ανηλίκων-Προστασία από παράνομο και βλαβερό περιεχόμενο

Ο προσβληθείς στην προσωπικότητα του από κάποιο μήνυμα που διακινείται στο Διαδίκτυο προστατεύεται από τις διατάξεις 361, 362, 366 και 367 του Π.Κ. Δυσχερέστερο είναι το ζήτημα της διάδοσης πορνογραφικού υλικού στο Διαδίκτυο ιδιαίτερα σε σχέση με τους ανηλίκους και την προστασία τους από την έκθεση σε αυτό. Στην Ευρωπαϊκή Ένωση έχουν ληφθεί και ισχύουν αρκετά μέτρα για την αντιμετώπισης αυτού του είδους εγκληματικότητας τα οποία είναι :

- Η Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06 που περιέχει προτροπές του Συμβουλίου προς τα κράτη μέλη και την Επιτροπή ώστε να ληφθούν

μέτρα για την προστασία των ανηλίκων στα οπτικοακουστικά μέσα και στο Ίντερνετ

- Η Σύσταση με αριθμό 98/560/ΕΚ όπου αναφέρονται οι συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης,
- Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ όπου γίνεται λόγος για τα μέτρα που λαμβάνουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης ώστε οι χρήστες του Διαδικτύου να βοηθήσουν στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα παιδιά,
- Η Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301 όπου υπάρχουν οι προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων σε όλα τα οπτικοακουστικά μέσα και για την προστασία των ανηλίκων στο ψηφιακό περιβάλλον και με την συμμετοχή των γονέων,
- Η Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06 όπου αναφέρεται ότι τα κράτη μεταξύ τους πρέπει να συνεργάζονται ώστε να διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη ποινικών αδικημάτων που αφορούν την παιδική πορνογραφία στο Ίντερνετ,
- Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών
- Η Απόφαση 276/1999/ΕΚ για την έγκριση, την διάρκεια, τη χρηματοδότηση και τους στόχους προγράμματος για την προώθηση της ασφαλέστερης χρήσης του Ίντερνετ,
- Η Απόφαση 1151/2003/ΕΚ που τροποποιεί την απόφαση αριθ. 276/1999/ΕΚ και
- Η Ανακοίνωση της Επιτροπής COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου (internet) μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα.

5.2.9 Spamming

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming. Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι *«η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους»* καθώς και από άλλα νομοθετήματα.

Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο.

Συνοπτικά οι νόμοι κατά του Ηλεκτρονικού Εγκλήματος

Ν. 2472/1997 –«Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ενσωματωμένες τροποποιήσεις).

Ν. 2867/2000 - «Οργάνωση και Λειτουργία των Τηλεπικοινωνιών και άλλες διατάξεις».

Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»

Ν. 3115/2003 – «Αρχή Διασφάλισης του απορρήτου των επικοινωνιών»

Ν. 3431/2006 – «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις».

Ν. 3471/2006 - «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997».

Ν. 3917/2011 - «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»

5.3 Άρθρα Ποινικού Κώδικα σχετικά με το Ηλεκτρονικό Έγκλημα

Άρθρο 337. Προσβολή της γενετήσιας αξιοπρέπειας

1. Όποιος με ασελγείς χειρονομίες ή προτάσεις που αφορούν ασελγείς πράξεις, προσβάλλει βάναυσα την αξιοπρέπεια άλλου στο πεδίο της γενετήσιας ζωής του τιμωρείται με Φυλάκιση μέχρι ενός έτους ή χρηματική ποινή.
2. Με Φυλάκιση τριών μηνών μέχρι δύο ετών τιμωρείται η πράξη της προηγούμενης παραγράφου, αν ο παθών είναι νεότερος από 12 ετών.
3. Ενήλικος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα δεκαπέντε έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με Φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.
4. Ενήλικος, ο οποίος μέσω **διαδικτύου** ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που εμφανίζεται ως ανήλικο κάτω των δεκαπέντε ετών και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του στο πεδίο της γενετήσιας ζωής του, τιμωρείται με Φυλάκιση τουλάχιστον ενός έτους. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση με το εμφανιζόμενο ως ανήλικο πρόσωπο, τιμωρείται με Φυλάκιση τουλάχιστον τριών ετών.
5. Όποιος τελεί την πράξη της παραγράφου 1 του άρθρου αυτού, εκμεταλλευόμενος την εργασιακή θέση του παθούντος ή τη θέση προσώπου

που έχει ενταχθεί σε διαδικασία αναζήτησης θέσης εργασίας διώκεται κατ` έγκληση και τιμωρείται με Φυλάκιση από έξι (6) μήνες μέχρι τρία (3) έτη και με χρηματική ποινή τουλάχιστον χιλίων (1.000) ευρώ.

Άρθρο 348 - Διευκόλυνση ακολασίας άλλων

1. Όποιος κατ` επάγγελμα διευκολύνει με οποιοδήποτε τρόπο την ασέλγεια μεταξύ άλλων τιμωρείται με Φυλάκιση μέχρι ενός έτους.
2. Με φυλάκιση μέχρι τριών ετών και με χρηματική ποινή τιμωρείται όποιος διευκολύνει την ασέλγεια μεταξύ άλλων χρησιμοποιώντας απατηλά μέσα και αν ακόμη δεν ενεργεί κατ` επάγγελμα.
3. Όποιος κατ` επάγγελμα ή από κερδοσκοπία επιχειρεί να διευκολύνει, έστω και συγκαλυμμένα, με τη δημοσίευση αγγελίας, εικόνας, αριθμού τηλεφωνικής σύνδεσης ή με τη **μετάδοση ηλεκτρονικών μηνυμάτων** ή με οποιονδήποτε άλλο τρόπο την ασέλγεια με ανήλικο τιμωρείται με Φυλάκιση και με χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

Άρθρο 348 Α - Πορνογραφία ανηλίκων

1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην επικράτεια ή εξάγει από αυτή, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.
2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

4. Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ: «α. αν τελέσθηκαν κατ' επάγγελμα ή κατά συνήθεια» «β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή σωματικής δυσλειτουργίας λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος». Αν η πράξη της περίπτωσης β' είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθούντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.

Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους

Όποιος με πρόθεση, μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας, προτείνει σε ενήλικο να συναντήσει ανήλικο, που δεν συμπλήρωσε τα δεκαπέντε έτη, με σκοπό τη διάπραξη σε βάρος του των αδικημάτων των παραγράφων 1 και 2 του άρθρου 339 και 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν στη διάπραξη των αδικημάτων αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ.

Άρθρο 370 Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να

μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση**.**

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή μαγνητοφωνεί προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Με την ίδια ποινή τιμωρείται και όποιος μαγνητοφωνεί ιδιωτική συνομιλία μεταξύ αυτού και τρίτου χωρίς τη συναίνεση του τελευταίου. Το δεύτερο εδάφιο της παραγράφου 1 αυτού του άρθρου εφαρμόζεται και σε αυτή την περίπτωση.

3. Με φυλάκιση τουλάχιστον ενός έτους τιμωρείται όποιος κάνει χρήση των πληροφοριών ή των μαγνητοταινιών ή των μαγνητοσκοπήσεων που αποκτήθηκαν με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

4. Η πράξη της παραγράφου 3 δεν είναι άδικη, αν η χρήση έγινε ενώπιον οποιασδήποτε δικαστικής ή άλλης ανακριτικής αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος, που δεν μπορούσε να διαφυλαχθεί διαφορετικά**.**

5. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.

6. Όποιος διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει για εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων των παραγράφων 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και με χρηματική ποινή.

Άρθρο 370 Β Παράνομη αντιγραφή απορρήτων δεδομένων

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του

δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση

Άρθρο 370 Γ – Παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή "διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ".

2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον "είκοσι εννέα (29) ευρώ". Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386 Α - Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα.

Στους πίνακες που ακολουθούν αναφέρονται συνοπτικά τα Προεδρικά διατάγματα, οι Οδηγίες της Ευρωπαϊκής Ένωσης ,οι Διεθνείς Συμβάσεις και οι Αποφάσεις.

Πίνακας 2

ΠΡΟΕΔΡΙΚΑ ΔΙΑΤΑΓΜΑΤΑ
Π.Δ. 131/2003 – «Ηλεκτρονικό εμπόριο κ.λπ. Υπηρεσίες της Κοινωνίας της Πληροφορίας»
Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές»
Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του»

Πίνακας 3

ΟΔΗΓΙΕΣ ΕΥΡΩΠΑΙΚΗΣ ΕΝΩΣΗΣ
Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών
Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου του 1996,αναφορικά με τη νομική προστασία των βάσεων δεδομένων
Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»)
Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση)
Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002 για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών
Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών

Πίνακας 4

ΔΙΕΘΝΕΙΣ ΣΥΜΒΑΣΕΙΣ
Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας.
Σύμβαση για τον Κυβερνοχώρο-Βουδαπέστη 23-11-2011
Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948: Στις 10 Δεκεμβρίου 1948, η Γενική Συνέλευση του Ο.Η.Ε. υιοθέτησε την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου. Στην συνέλευση αυτή αναφέρεται στο « κοινό ιδανικό στο οποίο πρέπει να κατατείνουν όλοι οι λαοί και όλα τα έθνη, έτσι ώστε κάθε άτομο και κάθε όργανο της κοινωνίας, με τη διακήρυξη αυτή διαρκώς στη σκέψη, να καταβάλλει, με τη διδασκαλία και την παιδεία, κάθε προσπάθεια για να αναπτυχθεί ο σεβασμός των ανθρωπίνων δικαιωμάτων και των ελευθεριών αυτών, και να εξασφαλιστεί προοδευτικά, με εσωτερικά και διεθνή μέσα, η παγκόσμια και αποτελεσματική εφαρμογή τους, τόσο ανάμεσα στους λαούς των ιδίων των κρατών μελών όσο και ανάμεσα στους πληθυσμούς χωρών που βρίσκονται στη δικαιοδοσία τους»
Σύμβαση της Ρώμης «Για την προάσπιση δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ). Στις 4 Νοεμβρίου 1950 στην Ρώμη υπογράφει η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου το οποίο ήταν ένα πρωτότυπο σύστημα διεθνούς προστασίας των ανθρωπίνων δικαιωμάτων με δικαίωμα δικαστικής παρεμβολής και επικυρώθηκε στο Στρασβούργο από όλα κράτη μέλη της Ένωσης.

Πίνακας 5

ΑΠΟΦΑΣΕΙΣ
Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».
Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»
Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής»

5.4 Γενικές Αρχές

5.4.1 Αρχή Προστασίας Προσωπικών Δεδομένων (Α.Π.Π.Δ)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Π.Δ) λειτουργεί από το 1977 βάση των διατάξεων του ν.2472/1997 και έχει ως σκοπό την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδικτύου. Σύμφωνα με το νόμο για την «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα», ν.2774/1999, οι ιστοσελίδες που συγκεντρώνουν προσωπικά στοιχεία των επισκεπτών τους, όπως για παράδειγμα ονόματα, τηλέφωνα, διευθύνσεις e-mail, έχουν νομική υποχρέωση να τους ενημερώνουν για το σκοπό που συλλέγονται αυτά τα στοιχεία καθώς και για το αν αυτά τα στοιχεία διατίθενται σε τρίτους.

5.4.2 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε) λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του ν.3115/2003. Σκοπός της Α.Δ.Α.Ε. είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο.

Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. Στις αρμοδιότητες της Α.Δ.Α.Ε περιλαμβάνεται το δικαίωμα διενέργειας ελέγχων, αποδοχής και εξέτασης καταγγελιών αλλά και έκδοσης κανονιστικών κειμένων.

ΚΕΦΑΛΑΙΟ 6°

Διαχείριση Παραβατικότητας μέσω Τεχνικών Ασφαλείας

Έχοντας αναφέρει σε προηγούμενο κεφάλαιο (κεφάλαιο 3) όλες τις κατηγορίες ηλεκτρονικών εγκλημάτων (παραβατικότητα), σε αυτό το κεφάλαιο καλούμαστε να παρουσιάσουμε τις τεχνικές αντιμετώπισης-προστασίας των εγκλημάτων αυτών.

6.1 Προστασία από Γνήσια ηλεκτρονικά εγκλήματα

6.1.1 Προστασία από Εισβολή Κακόβουλου Λογισμικού

Το οπλοστάσιο για την προστασία έναντι κακόβουλου λογισμικού περιλαμβάνει εκτός των άλλων τα προγράμματα Antivirus. Η αντιμετώπιση των ιών έχει δύο σκέλη: τον *εντοπισμό* του ιού και την *απάλειψη* του. Τα προγράμματα antivirus πραγματοποιούν έλεγχο των αρχείων ενός Η/Υ για τον εντοπισμό μολυσματικού λογισμικού. Τα αρχεία αυτά μπορεί να είναι αρχεία δεδομένων, αρχεία συστήματος, αρχεία εφαρμογών. Επίσης, μπορεί να είναι αποθηκευμένα σε κάποια μονάδα βοηθητικής μνήμης ή να εισέρχονται στο σύστημα μέσω δικτύου (LAN, Internet).

Ανίχνευση κώδικα ιού. Ο κώδικας κάθε ιού έχει ορισμένα χαρακτηριστικά που τον διαφοροποιούν από τους υπόλοιπους ιούς. Το τμήμα εκείνο του κώδικα ενός ιού που χαρακτηρίζει μοναδικά τον ιό ονομάζεται υπογραφή ή αποτύπωμα του ιού. Ένα πρόγραμμα antivirus τηρεί μια *Βάση Δεδομένων* με τις υπογραφές όλων των γνωστών ιών, και ελέγχει όλα τα εκτελέσιμα αρχεία ενός Η/Υ (κατά την αποθήκευση ή εκτέλεση τους) για τον εντοπισμό μιας υπογραφής που έχει ήδη αποθηκευτεί στη Β.Δ. Εφόσον βρει κάποιο «ταίριασμα» (matching), το πρόγραμμα antivirus μπλοκάρει την εκτέλεση του κακόβουλου προγράμματος και ενημερώνει το χρήστη.

Συνήθως προτρέπει το χρήστη να αποφασίσει αν επιθυμεί α) διαγραφή (delete), β)απομόνωση (isolation, quarantine) ή επιδιόρθωση (repair, clean) του μολυσμένου αρχείου.

Πίνακας 6

Βασικές δυνατότητες που περιέχει μία εφαρμογή Antivirus	
Εύχρηστο Interface & χαμηλή κατανάλωση πόρων	Απλό και φιλικό περιβάλλον για το χρήστη-μικρό ποσοστό δέσμευσης των πόρων του Η/Υ.
Προστασία σε πραγματικό χρόνο	Διάγνωση και προστασία σε real time-Το antivirus λειτουργεί στο παρασκήνιο από τη στιγμή που φορτώνεται στον υπολογιστή.
Αυτόματη ενημέρωση	Αυτόματη ενημέρωση των βάσεων δεδομένων με υπογραφές ιών (σε συχνή βάση).
Προστασία Ηλεκτρονικής Αλληλογραφίας	Έλεγχος ηλεκτρονικής αλληλογραφίας για την ύπαρξη Ιών στα συνημμένα αρχεία.
Προγραμματισμένος Έλεγχος	Καθορισμός προγραμματισμένων ελέγχων στους δίσκους του συστήματος(ανά τακτά χρονικά διαστήματα ή συγκεκριμένες ημερομηνίες).
Δισκέτα Εκκίνησης	Δισκέτα με εφαρμογές διάγνωσης και καθαρισμού του boot sector,σε περίπτωση επικάλυψης από κακόβουλο λογισμικό.
Καταγραφή Συμβάντων	Καταγραφή όλων των συμβάντων(event logging).

Το πρόγραμμα antivirus μπορεί να εντοπίσει και να απομακρύνει ιούς που είναι ήδη γνωστοί. Αυτό σημαίνει πως δεν προσφέρει προστασία έναντι ιών που δεν έχουν ανιχνευθεί ακόμα(τουλάχιστον, μέχρι να γίνει η ενημέρωση-λήψη της υπογραφής τους από τον διακομιστή Web). Επιπλέον, τα προγράμματα antivirus

παραδοσιακά δυσκολεύονται στην καταπολέμηση πολυμορφικών ιών καθώς και ιών τύπου stealth/rootkits.

Για το λόγο αυτό τα προγράμματα antivirus συχνά επιστρατεύουν προηγμένες τεχνικές όπως *heuristic scanning*, *behavior blocking* και *integrity checking* που θα εξετάσουμε στη συνέχεια. Οι μέθοδοι αυτές εντοπίζουν κώδικα που μπορεί να μη βρίσκεται στη ΒΔ αλλά συγκεντρώνει αρκετές πιθανότητες να είναι κακόβουλος. Αυτό έχει ως αποτέλεσμα η διάγνωση να μην είναι πάντα επιτυχημένη (π.χ. *λάθος συναγερμός*-false alarm).

6.1.1.1 Προγράμματα Antivirus. Προηγμένες δυνατότητες

- **Ευρετικές (heuristic) μέθοδοι.** Έλεγχος κώδικα για εύρεση πιθανού (άγνωστου) ιού. Σε αντίθεση με τους αλγόριθμους ελέγχου της υπογραφής ενός ιού, η ευρετική μέθοδος εξετάζει τον εκτελέσιμο κώδικα ενός αρχείου με σκοπό την εύρεση εντολών (ή συνόλου από εντολές) που θα μπορούσαν να αποτελούν τμήμα κακόβουλου κώδικα, με μεγάλη πιθανότητα. Παραδείγματα αποτελούν η ύπαρξη μακροεντολών σε ένα έγγραφο Office, εντολές κλήσης-τροποποίησης άλλων προγραμμάτων, ρουτίνες αποκρυπτογράφησης, εντολές διαγραφής αρχείων ή τροποποίησης του μητρώου του συστήματος, κ.λ.π. Η τεχνική αυτή είναι προενεργή (proactive), δηλαδή προσπαθεί να εντοπίσει «ύποπτο» τμήμα κώδικα πριν αυτός εκτελεστεί.
- **Έλεγχος Ακεραιότητας (integrity checks).** Κατά την αποθήκευση ενός αρχείου, υπολογίζονται και αποθηκεύονται το μέγεθος του αρχείου, καθώς και ένα άθροισμα ελέγχου (checksum). Το άθροισμα ελέγχου είναι ένας αριθμός μοναδικός για το αρχείο αυτό: Η αλλαγή έστω και ενός bit στο αρχείο θα έχει ως αποτέλεσμα την αλλαγή του αθροίσματος ελέγχου με μεγάλη πιθανότητα. Για μεγαλύτερη ασφάλεια, μπορεί να χρησιμοποιηθεί η *κρυπτογραφική τιμή hash* του κώδικα του προγράμματος. Κάθε φορά που εκτελείται ένα αρχείο, το antivirus υπολογίζει το άθροισμα ελέγχου και το συγκρίνει την αποθηκευμένη τιμή. Αν οι δύο αριθμοί δεν είναι ίδιοι, αυτό σημαίνει πως α) ο χρήστης έχει προβεί σε μια καθ' όλα νόμιμη ενέργεια (π.χ. ενημέρωση-επιδιόρθωση του προγράμματος), ή β) ένας ιός άλλαξε τον κώδικα του αρχείου.

- **Έλεγχος Συμπεριφοράς (behaviour blocking).** Η τεχνική αυτή μοιάζει με την τεχνική εκτέλεσης σε «προστατευμένο περιβάλλον» (sandbox) που χρησιμοποιείται κατά την εκτέλεση των προγραμμάτων Java. Δεν ελέγχεται ο κώδικας του εκτελέσιμου αρχείου καθ' αυτός, ωστόσο ελέγχεται η συμπεριφορά του προγράμματος καθώς εκτελείται. Έχοντας δηλαδή υπ' όψιν ένα σύνολο από συμπεριφορές που θεωρούνται «ύποπτες-επικίνδυνες» (π.χ. κλήση του Μητρώου του συστήματος, προσπάθεια διαγραφής ή μετονομασίας αρχείων, κ.λπ.) το πρόγραμμα antivirus προσπαθεί να ανιχνεύσει και να αποτρέψει σε πραγματικό χρόνο τις παρενέργειες ενός (άγνωστου) ιού. Αν ανιχνευτεί «ύποπτη» συμπεριφορά, το πρόγραμμα εφαρμόζει την πολιτική ασφαλείας (την οποία διαμορφώνει ο χρήστης μέσα από τις επιλογές-ρυθμίσεις του προγράμματος). Για παράδειγμα, α) Το «ύποπτο» πρόγραμμα συνεχίζει την εκτέλεση του και ενημερώνεται το αρχείο συμβάντων, β) Αναστέλλεται η λειτουργία του «υπόπτου» προγράμματος, γ) Ερωτάται ο χρήστης. Η τεχνική αυτή είναι «*αντιδραστική*» (reactive) δηλαδή το πρόγραμμα antivirus προσπαθεί να εντοπίσει «ύποπτο» κώδικα αφού αυτός εκτελεστεί.
- **Επιπλέον προστασία.** Τα σύγχρονα προγράμματα antivirus ενσωματώνουν ορισμένες επιπλέον λειτουργίες προστασίας. Μεταξύ άλλων, προσφέρουν τη δυνατότητα ελέγχου αλληλογραφίας (εισερχόμενης/εξερχόμενης) για κακόβουλο λογισμικό, έλεγχο και παρεμπόδιση «υπόπτων» αρχείων που ανταλλάσσονται μέσω προγραμμάτων ανταλλαγής αρχείων P2P, φιλτράρισμα αρχείων που ανταλλάσσονται μέσω προγραμμάτων συνομιλίας (chat, ανταλλαγή μηνυμάτων instant messaging), προστασία από κινητό κώδικα στο Web, κ.λ.π. Επιπλέον, αρκετά προγράμματα antivirus συχνά αποτελούν ολοκληρωμένα πακέτα εφαρμογών και ενσωματώνουν λειτουργίες firewall, ανίχνευσης εισβολών (IDS), καθώς και προστασίας από (μη μολυσματικό) λογισμικό τύπου spyware-adware.

Πίνακας 7

Λογισμικό Antivirus(Συνοπτικά)	
Τι μπορεί να κάνει	**Τι δεν μπορεί**
Ανίχνευση Ιών πριν τη μόλυνση	*Ανάκτηση αρχείων που* *Έχουν διαγραφεί από Ιό*
Επιδιόρθωση αρχείων δεδομένων που έχουν ήδη μολυνθεί από τον ιό	*Αποκατάσταση αρχείων συστήματος που έχουν αλλοιωθεί ή καταστραφεί από Ιό*
Ανίχνευση λογικών βομβών	*Αποτροπή επιθέσεων*
	Ανίχνευση λογισμικού τύπου spyware-adware

6.1.1.2 Προσωπικά Συστήματα Firewall

Πριν 250 χρόνια, ο Sun Tzu, στρατηγός στην Κινέζικη Βασιλεία των Wu, έγραψε ένα βιβλίο με τίτλο «Η Τέχνη του Πολέμου». Στην εισαγωγή του βιβλίου έγραφε:

«Η μόνη ασφαλής άμυνα είναι όταν κρατάς θέσεις που δε γίνεται να υποστούν επίθεση»

Κάποτε, οι άνθρωποι χτίζανε τοίχους από τούβλα και τους τοποθετούσαν ανάμεσα από κτίρια και ξύλινα σπίτια, έτσι ώστε σε περίπτωση που ξεσπούσε μια πυρκαγιά, να μην εξαπλωνόταν σε διπλανά σπίτια (firewalls). Μια παρόμοια προσέγγιση χρησιμοποιείται στην Ασφάλεια Η/Υ. Τα συστήματα firewall προστατεύουν τους πληροφοριακούς πόρους ενός Η/Υ ή ενός δικτύου Η/Υ από επιθέσεις μη εξουσιοδοτημένης πρόσβασης. Αποτελούν έναν μηχανισμό *ελέγχου πρόσβασης*, βάσει μιας πολιτικής ασφάλειας που δίνει κυρίως έμφαση στην προστασία του εσωτερικού περιβάλλοντος από επιθέσεις που προέρχονται από το

εξωτερικό περιβάλλον. Λέγοντας εξωτερικό περιβάλλον εννοούμε άλλους Η/Υ ή/και άλλα δίκτυα. Στην Ενότητα αυτή δίνουμε έμφαση στα προσωπικά firewall, δηλαδή σε εφαρμογές λογισμικού για την προστασία του Η/Υ από μη ανεπιθύμητες εισβολές. Τα προσωπικά firewalls λειτουργούν σε όλα τα επίπεδα του μοντέλου TCP/IP, λειτουργούν δηλαδή ως *packet filters* (φιλτράρισμα πακέτων) και ως *application gateways* (πύλες επιπέδου εφαρμογής).

Σημείωση: Εναλλακτικά, το firewall ρωτάει το χρήστη για την ενέργεια στην οποία θα προβεί. Πρόκειται για μια διαδεδομένη τακτική στα προσωπικά firewalls, κάτι που σημαίνει πως, τουλάχιστον στην αρχή, ο χρήστης θα πρέπει να «εκπαιδεύσει» το firewall. Το firewall στη συνέχεια μπορεί να «απομνημονεύει» τις επιλογές του χρήστη και να εφαρμόζει την εκάστοτε πολιτική πρόσβασης.

Επιπλέον, τα προσωπικά firewalls μπορούν να λάβουν αποφάσεις ανάλογα με το εάν τα δεδομένα που εισέρχονται (εξέρχονται), προέρχονται (προορίζονται) από (για) έναν Η/Υ του τοπικού δικτύου ή του εξωτερικού δικτύου (Internet).

Σε επίπεδο χρήστη, πολλά από τα προσωπικά firewall προσφέρουν δυνατότητες όπως:

- Φιλτράρισμα με βάση την ταυτότητα της εφαρμογής (ή του service) που λαμβάνει ή δέχεται δεδομένα
- Φιλτράρισμα με βάση το αν η εφαρμογή που επιχειρεί πρόσβαση έχει κληθεί από μια άλλη εφαρμογή (μια συνήθης πρακτική είναι ένα κακόβουλο λογισμικό να προσπαθεί να μεταμφιεστεί ως μια άλλη «νόμιμη» εφαρμογή προκειμένου να αποκτήσει πρόσβαση από και προς το σύστημα).
- Φιλτράρισμα με βάση το αν η εφαρμογή που ζητεί πρόσβαση έχει τροποποιηθεί από την τελευταία φορά που είχε πρόσβαση (μια λειτουργία παρόμοια με τον έλεγχο ακεραιότητας που εφαρμόζουν πολλά προγράμματα (antivirus).

6.1.1.3 Ανιχνευτές Ευπαθειών (Vulnerability Scanners)

Ένα εργαλείο που μπορεί να χρησιμοποιηθεί από διαχειριστές Η/Υ, διαχειριστές δικτύων, καθώς και εισβολείς (στη συγκεκριμένη περίπτωση hackers) για την ανίχνευση των ευπαθειών ενός αντικειμένου. Το αντικείμενο μπορεί να είναι ένα πρόγραμμα, ένας Η/Υ, ή ένα δίκτυο Η/Υ.

Ο scanner ελέγχει διεξοδικά το «αντικείμενο» προκειμένου να διαπιστώσει εάν το αντικείμενο είναι ευπαθές σε ένα εύρος (γνωστών) επιθέσεων (exploits).

Ο έλεγχος αυτός μπορεί να γίνει εφάπαξ, να είναι συνεχής (π.χ. προειδοποιήσεις ασφάλειας των Windows XP Professional SP2) ή περιοδικός (ανά τακτά χρονικά διαστήματα).

Η ανίχνευση ευπαθειών μπορεί επίσης να γίνει απομακρυσμένα (remotely): αρκετοί δικτυακοί τόποι (sites), που επικεντρώνονται στον τομέα της ασφάλειας (π.χ. symantec.com), προσφέρουν απομακρυσμένες υπηρεσίες ανίχνευσης ευπαθειών, για χρήστες προσωπικών Η/Υ.

Σημείωση: Πέρα από την «προληπτική» (preventive) του διάσταση, είναι αυτονόητο ότι ένας scanner μπορεί να χρησιμοποιηθεί και αφού πραγματοποιηθεί μια επίθεση, προκειμένου να εντοπιστεί η ευπάθεια που έκανε την επίθεση εφικτή.

6.1.1.4 Λήψη Αντιγράφων Ασφάλειας (Backup)

Μελετάται η διαδικασία της δημιουργίας και της ασφαλούς αποθήκευσης αντιγράφων ενός ή περισσότερων πληροφοριακών πόρων του συστήματος (π.χ. δεδομένα, προγράμματα, βάσεις δεδομένων), καθώς και της ασφαλούς επαναφοράς τους σε περίπτωση επίθεσης ή λάθους. Το αποθηκευμένο αντίγραφο ονομάζεται *αντίγραφο ασφάλειας* ή εφεδρείας (backup data). Εάν οι αρχικοί (original) πόροι χαθούν ή καταστραφούν ή αλλοιωθούν, τότε επαναφέρονται τα αντίγραφα που έχουν ληφθεί.

Σε επίπεδο Η/Υ, η ανάγκη για τη λήψη αντιγράφων ασφάλειας σχετίζεται με:

- Την επαναφορά ενός αντιγράφου ολόκληρου του συστήματος (Λ.Σ., δεδομένα και προγράμματα) εφόσον το σύστημα δυσλειτουργεί ή καταστραφεί, π.χ. απώλεια ή κλοπή σκληρού δίσκου, αλλοίωση αρχείων συστήματος, κακόβουλο λογισμικό με καταστρεπτικές παρενέργειες, εισβολή (hacking) και καταστροφή αρχείων, δεδομένων, ή εφαρμογών (cracking).
- Την επαναφορά συγκεκριμένων αρχείων και δεδομένων, εφόσον αυτά καταστράφηκαν, αλλοιώθηκαν, εκλάπησαν, ή δεν είναι διαθέσιμα για οποιοδήποτε άλλο λόγο (π.χ. διαγραφή δεδομένων από λάθος του χρήστη).

Σημείωση: Ένα αντίγραφο ασφάλειας συνήθως αποθηκεύεται σε μαγνητικά μέσα (π.χ. σκληροί δίσκοι, μαγνητικές ταινίες) ή οπτικά μέσα (π.χ. CD-R, DVD-R, κ.λπ.). Η αύξηση των ρυθμών διαμεταγωγής δεδομένων στα τοπικά δίκτυα και στις ευρυζωνικές συνδέσεις έχει επίσης καταστήσει δυνατή την *απομακρυσμένη λήψη* αντιγράφων ασφάλειας (remote backup).

6.1.1.5 Κρυπτογραφικά συστήματα που χρησιμοποιούνται σήμερα

Τα τελευταία χρόνια έχουν αναπτυχθεί και χρησιμοποιηθεί αρκετά κρυπτογραφικά συστήματα για το Internet. Μπορούμε να τα χωρίσουμε σε δύο κατηγορίες. Η πρώτη είναι προγράμματα και πρωτόκολλα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mail). Τα πιο δημοφιλή είναι τα παρακάτω:

- PGP
- S/MIME

Η δεύτερη κατηγορία είναι πρωτόκολλα δικτύου που χρησιμοποιούνται για να παρέχουν εμπιστευτικότητα, ακεραιότητα, αναγνώριση ταυτότητας σε περιβάλλον δικτύου. Τέτοια συστήματα χρειάζονται αλληλεπίδραση πραγματικού χρόνου

ανάμεσα στο client και ενός server για να δουλέψουν σωστά. Τα πιο δημοφιλή είναι τα παρακάτω:

- SSL
- PCT
- S-HTTP
- SET & CyberCash
- DNSSEC
- IPsec & IPv6
- Kerberos
- SSH

6.1.1.6 PGP (Pretty Good Privacy)

Το PGP είναι το πρώτο πρόγραμμα κρυπτογράφησης δημόσιου κλειδιού, γραμμένο από τον Phil Zimmerman που κυκλοφόρησε στο Internet τον Ιούνιο του 1991. Το PGP είναι ένα ολοκληρωμένο σύστημα που προσφέρει κρυπτογραφική προστασία των e-mails και των αρχείων γενικότερα. Το PGP επίσης είναι ένα σύνολο από standards που περιγράφουν τα formats των κρυπτογραφημένων μηνυμάτων, των κλειδιών και των ψηφιακών υπογραφών. Το PGP είναι ένα κρυπτογραφικό σύστημα διασταύρωσης που χρησιμοποιεί τον RSA αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού για την διαχείριση των κλειδιών και τον IDEA συμμετρικό αλγόριθμο για την κύρια κρυπτογράφηση των δεδομένων.

Το PGP προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος που χρησιμοποιεί είναι ο IDEA. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης που χρησιμοποιεί είναι η MD5. Προσφέρει αναγνώριση γνησιότητας με την χρήση των δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

Το PGP είναι διαθέσιμο με δυο τρόπους, σαν μια μεμονωμένη εφαρμογή και σαν ένα ολοκληρωμένο πρόγραμμα ηλεκτρονικού ταχυδρομείου διαθέσιμο από την

PGP Inc. Το μεμονωμένο πρόγραμμα τρέχει. σε πολύ περισσότερα συστήματα από ότι το ολοκληρωμένο πρόγραμμα, αλλά είναι περισσότερο δύσχρηστο. Ένα τέτοιο παράδειγμα που ήταν πολύ διαδεδομένο είναι οι εκδόσεις του PGP για περιβάλλον DOS. Επίσης η PGP Inc. αναπτύσσει διάφορα plug-ins για δημοφιλή προγράμματα ηλεκτρονικού ταχυδρομείου για να επιτρέψει σε αυτά να στέλνουν και να λαμβάνουν κρυπτογραφημένα μηνύματα με το PGP. Ένα πρόβλημα με το PGP είναι η διαχείριση και πιστοποίηση των δημόσιων κλειδιών. Τα δημόσια κλειδιά δεν έχουν ημερομηνία λήξης, αντί αυτού, όταν τα κλειδιά εκτεθούν, εξαρτάται από τον ιδιοκτήτη εάν αυτός θέλει να διανέμει σε όλους αυτούς με τους οποίους είχε επικοινωνία μια ειδική PGP πιστοποίηση απόσυρσης (ακύρωσης). Οι ανταποκριτές που δεν μαθαίνουν το γεγονός αυτό και χρησιμοποιούν το εκτιθέμενο κλειδί για εβδομάδες, μήνες και χρόνια αργότερα για να στείλουν κρυπτογραφημένα μηνύματα ρισκάρουν την ασφάλεια των μηνυμάτων. Αυτό έχει σαν αποτέλεσμα, εάν δημιουργήσουμε και διανέμουμε ένα δημόσιο κλειδί, πρέπει να κρατήσουμε το μυστικό κλειδί για πάντα επειδή το κλειδί αυτό δεν λήγουν (expire) ποτέ. Η πρόσφατη έκδοση του PGP5 χρησιμοποιεί ένα νέο τύπο κλειδιών με κρυπτογραφικούς αλγόριθμους τον DSS και τον Diffie-Helman.

6.1.1.7 Κρυπτογράφηση SSL (Secure Socket Layer)

Αυτού του είδους η κρυπτογράφηση αποτελεί πια το στάνταρ για τις εμπορικές συναλλαγές μεταξύ ιδιωτών και εταιρειών μέσω του Παγκόσμιου Ιστού. Δεν αποτελεί κάποια συγκεκριμένη μέθοδο αλλά είναι ένα πρωτόκολλο που χρησιμοποιείται επιπρόσθετα με τα βασικά πρωτόκολλα του Διαδικτύου και έτσι μπορεί να παρέχει ασφάλεια σε διάφορες διαδικτυακές υπηρεσίες και όχι μόνο στον Παγκόσμιο Ιστό. Δημιουργήθηκε αρχικά από την εταιρεία Netscape Communications με σκοπό να εξομοιώνει σε επίπεδο λογισμικού, την κρυπτογράφηση σε επίπεδο σύνδεσης (Link Encryption) που παρέχεται από εξειδικευμένο δικτυακό εξοπλισμό. Έτσι χάρη στο SSL, άπειροι χρήστες μπορούν να εφαρμόσουν κρυπτογραφική ασφάλεια παρόμοια με αυτήν που πριν μερικά χρόνια ήταν δεσμευμένη για χρήση από τράπεζες και κυβερνήσεις. Η προσφερόμενη από το SSL κρυπτογράφηση έδωσε την δυνατότητα στο αγοραστικό κοινό να μεταδίδει αριθμούς πιστωτικών καρτών με ασφάλεια μέσα από τις ανασφαλείς γραμμές του Διαδικτύου. Όταν

πρωτοεμφανίστηκε το SSL στην αγορά, πολλοί ήταν αυτοί που είπαν ότι η δημιουργία του ήταν αναγκαία για την έκρηξη του ηλεκτρονικού εμπορίου. Γι' αυτόν τον λόγο η εταιρεία Netscape θεωρείται γενικά ότι ήταν αυτή που έκανε δυνατή την εμπορευματοποίηση του Διαδικτύου και του Παγκόσμιου Ιστού.

Η βασική του λειτουργία είναι να δημιουργεί ένα κρυπτογραφημένο δίαυλο επικοινωνίας διπλής κατεύθυνσης ανάμεσα σε δύο υπολογιστές (ή ανάμεσα σε δύο διαδικασίες που εκτελούνται στον ίδιο υπολογιστή) στο Διαδίκτυο. Οτιδήποτε μεταφέρεται ανάμεσα στο χρήστη και τον Web server, όπως η ηλεκτρονική διεύθυνση του κειμένου, τα περιεχόμενα του, τα περιεχόμενα φορμών (άρα και τα στοιχεία του χρήστη-πελάτη καθώς και ο αριθμός της πιστωτικής του κάρτας) πρώτα κρυπτογραφείται και έπειτα μεταδίδεται (ταυτόχρονα συμπιέζεται) για να αποκρυπτογραφηθεί από τον υπολογιστή που πρόκειται να τα λάβει. Αυτό αποτελεί μια αδιαφανή διαδικασία για τον χρήστη, ο οποίος δεν αντιλαμβάνεται τίποτα από όλα αυτά. Επίσης το SSL κάνει πιστοποίηση του web server με τον οποίο επικοινωνεί, δηλαδή ο υπολογιστής του χρήστη επιβεβαιώνει ότι ο server είναι πράγματι αυτός που δηλώνει ότι είναι. Συνοπτικά το SSL προσθέτει τις ακόλουθες λειτουργίες στο δίαυλο επικοινωνίας: Πιστοποίηση (authentication) και απαγόρευση απάρνησης (non repudiation) στον εξυπηρετητή, χρησιμοποιώντας ψηφιακές υπογραφές.

- **Πιστοποίηση** (authentication) και απαγόρευση απάρνησης (nonrepudiation) στον πελάτη, χρησιμοποιώντας ψηφιακές υπογραφές.
- **Εμπιστευτικότητα δεδομένων** (data confidentiality) μέσω κρυπτογράφησης.
- **Ακεραιότητα δεδομένων** (data integrity) μέσω της χρήσης κωδικών πιστοποίησης μηνύματος (message authentication codes).

Το SSL χρησιμοποιεί υβριδική τεχνική κρυπτογράφησης, υλοποιούμενη όμως με διάφορους αλγόριθμους οι οποίοι μπορούν να επεκταθούν. Σήμερα το SSL είναι ενσωματωμένο σε όλα τους εμπορικά προγράμματα περιήγησης στον Παγκόσμιο Ιστό (web browsers - φυλλομετρητές) καθώς και σχεδόν σε όλους τους εμπορικούς εξυπηρετητές, έτσι ώστε η υποστήριξη του να μην αποτελεί πια ανταγωνιστικό πλεονέκτημα αλλά μια αναγκαιότητα. Τυπικά, ο χρήστης μπορεί να αναγνωρίσει την ενεργοποίηση αυτού του πρωτοκόλλου αναζητώντας τα αρχικά "https://" (αντί των

συνηθισμένων “http://”) στην αναγραφή της τοποθεσίας της ηλεκτρονικής σελίδας με την οποία έχει συνδεθεί. Άλλα ανταγωνιστικά πρωτόκολλα του χώρου περιλαμβάνουν τα PCT της Microsoft, Cybercash και S-HTTP.

6.2 Προστασία και Κοινωνική Δικτύωση

6.2.1 Τρόποι προστασίας της Ιδιωτικότητας-Facebook

Το Facebook όπως και τα περισσότερα μέσα κοινωνικής δικτύωσης δίνουν τη δυνατότητα στο χρήστη να διαχειρίζεται το ποιοι έχουν πρόσβαση στα δεδομένα του. Δεν θα πρέπει να προκαλεί εντύπωση ότι σύμφωνα με έρευνες τουλάχιστον 13 εκατ. χρήστες δηλώνουν πως δεν έχουν ποτέ χρησιμοποιήσει τα privacy settings ενώ κάποιοι από αυτούς δεν γνώριζαν καν την ύπαρξη τους. Επίσης το 30% των ερωτηθέντων χρηστών δήλωσαν ότι χρησιμοποιούσαν το Facebook εν γνώση τους με public επιλογή δεδομένων. Παρακάτω παρατίθενται προτάσεις για σωστή χρήση των μέσων κοινωνικής δικτύωσης και κυρίως του Facebook και αξιοποίηση των privacy settings:

- **Γινόμαστε φίλοι μόνο με άτομα που γνωρίζουμε -** Τα πάντα στο Facebook ξεκινούν από τις επαφές με τις οποίες συναναστρεφόμαστε και μοιραζόμαστε τα δεδομένα μας αφού οι συνδέσεις πρέπει να είναι αμφίδρομες.
- **Συμμετέχουμε και μοιραζόμαστε πληροφορίες αλλά όχι σε υπερβολικό βαθμό -** Δεν είναι όλες οι πληροφορίες προς κοινοποίηση. Αναρωτιόμαστε αν αυτό που θέλουμε να δημοσιοποιήσουμε θα θέλαμε να το μάθουν οι γονείς μας, ο εργοδότης μας.
- **Ξέρουμε τι πληροφορίες μοιραζόμαστε και με ποιόν -** Ορίζουμε ποιοι από τις επαφές μας θα έχουν πρόσβαση στις φωτογραφίες σου, status updates.
- **Περιορίζουμε την δυνατότητα να μας ψάξει** και να μας στέλνει μηνύματα ο οποιοσδήποτε.

- **Χρησιμοποιούμε όλα τα privacy settings** και θυμόμαστε ότι πρέπει να τα ελέγχουμε ανά τακτά χρονικά διαστήματα γιατί αλλάζουν και δεν ειδοποιούμαστε.
- **Να χρησιμοποιείται HTTPS** για ασφαλή περιήγηση και μεταφορά των δεδομένων το οποίο είναι απενεργοποιημένο by default.
- **Προσέχουμε σε ποια applications δίνουμε πρόσβαση στα δεδομένα μας -** προτού τους δώσουμε πρόσβαση ενημερωνόμαστε για τον δημιουργό και για τυχόν παράπονα άλλων χρηστών καθώς πολλές από τις προσφερόμενες εφαρμογές τις φτιάχνουν χρήστες.
- **Ό,τι αναρτάται όσο απόρρητο και αν είναι,** αποθηκεύεται σε κάποια βάση δεδομένων.

6.2.2 Τρόποι προστασίας της Ιδιωτικότητας-Twitter

Παρακάτω παρατίθενται ορισμένες προτάσεις με τις οποίες η δικτύωση στο Twitter ενός χρήστη γίνεται ασφαλέστερη.

- **Ενεργοποιούμε το tweet privacy -** με αυτό τον τρόπο όσα δημοσιεύουμε θα μπορούν να το δουν μόνο όσοι επιλέγουμε.
- **Απενεργοποιούμε το tweet location –** για να αποφύγουμε περιπτώσεις ληστειών, stalking.
- **Σκέψου πριν «τιτιβίσεις».**
- **Προσοχή στα phishing/hoax emails –** χρησιμοποιούμε τις τελευταίες ενημερώσεις στον email client και δεν ανοίγουμε συνημμένα από αγνώστους.
- **Χρησιμοποιούμε Add-ons** για να προστατευτούμε από επιθέσεις XSS, Click-jacking.

6.2.3 Εξειδικευμένα μέτρα προστασίας-Κοινωνική Δικτύωση

Σε αυτό το σημείο θα αναφέρουμε ορισμένα εξειδικευμένα μέτρα προστασίας τα οποία θα πρέπει να λαμβάνει ένας ερευνητής Ασφάλειας και Ιδιωτικότητας στις Τεχνολογίες Πληροφορίας και Επικοινωνίας, ο οποίος κάνει τακτική χρήση των κοινωνικών δικτύων. Πριν αναφερθούμε στα μέτρα αυτά, παρουσιάζονται κυριότερες απειλές οι οποίες συναντώνται κατά τη χρήση των κοινωνικών δικτύων και είναι συνοπτικά οι εξής:

α. Διαδικτυακή Παρενόχληση (Cyber bullying), Παρακολούθηση (stalking).

β. Ευπάθειες στις εφαρμογές.

γ. Phishing και Spam.

δ. Συλλογή και επεξεργασία προσωπικών δεδομένων.

ε. Κλοπή ταυτότητας (Identity Theft).

Οι παραπάνω απειλές μπορεί να έχουν επιπτώσεις στον επαγγελματικό τομέα, στις διαπροσωπικές σχέσεις με τρίτους, ακόμα και στην φυσική ασφάλεια ενός ατόμου.

Τα μέτρα προστασίας που θα πρέπει να λάβει ο ερευνητής διαχωρίζονται σε δύο κατηγορίες, οι οποίες είναι, η προστασία του συστήματος το οποίο χρησιμοποιεί για να αποκτήσει πρόσβαση στα κοινωνικά δίκτυα (υπολογιστής, κινητό τηλέφωνο, laptop, tablet,κτλ), και η διασφάλιση της προστασίας του κατά τη χρήση των κοινωνικών δικτύων.

Πιο συγκεκριμένα για την πρώτη κατηγορία ο ερευνητής θα πρέπει:

- Για την πρόσβαση στο σύστημα που χρησιμοποιεί να έχει ορίσει κάποιο κωδικό πρόσβασης και ειδικά αν το σύστημα είναι φορητό (κινητό τηλέφωνο, tablet, laptop).
- Θα πρέπει να προστατεύει το σύστημά του με τα κατάλληλα μέτρα ασφαλείας, όπως antivirus, firewall, antispyware τα οποία θα πρέπει να

είναι και σωστά ρυθμισμένα, αλλά και να λαμβάνουν τις απαραίτητες ενημερώσεις (updates).

- Επίσης με τις φορητές συσκευές, θα πρέπει να είναι ιδιαίτερα προσεκτικός, καθώς αυτές μπορεί να καταλήξουν στα χέρια κάποιου κακόβουλου, είτε ηθελημένα είτε από αμέλεια.
- Επιπλέον όσο αυτό είναι εφικτό να μην κάνει χρήση δημόσιων ασύρματων δικτύων για την πρόσβαση στα κοινωνικά δίκτυα αλλά να προτιμάει δίκτυα στα οποία μόνο αυτός έχει πρόσβαση. Στην περίπτωση όμως που γίνεται χρήση δημόσιων ασύρματων δικτύων θα πρέπει να προτιμάται η χρήση είτε Virtual Private Networks (VPN) είτε η χρήση proxy server (Tor Browser).
- Χρήση ενός ξεχωριστού mail account για τη σύνδεση στα κοινωνικά δίκτυα. Καθώς σχεδόν όλα τα κοινωνικά δίκτυα απαιτούν για τη σύνδεση σε αυτά την παροχή ενός email account, ο ερευνητής θα πρέπει να δημιουργήσει ένα ξεχωριστό λογαριασμό, τον οποίο θα χρησιμοποιεί μόνο για αυτό το σκοπό.

Στην δεύτερη κατηγορία που αφορά τη χρήση των κοινωνικών δικτύων αυτή καθεαυτή, το μεγαλύτερο πρόβλημα όσον αφορά τη διασφάλιση της ιδιωτικότητας του ερευνητή, είναι η παροχή των προσωπικών δεδομένων του προς τα κοινωνικά δίκτυα (όνομα, ημερομηνία γέννησης, σχολείο κτλ) αλλά και η παροχή πληροφοριών που αυτός μοιράζεται με τις επαφές του. Για τους λόγους αυτούς ο ερευνητής θα πρέπει να ακολουθεί τα εξής:

- Σε αρκετές περιπτώσεις δεν αρκεί μόνο η παροχή ενός ξεχωριστού email account, καθώς ορισμένα κοινωνικά δίκτυα όπως το Facebook για την παροχή ορισμένων υπηρεσιών απαιτούν την παροχή ενός αριθμού κινητού τηλεφώνου. Σε αυτή την περίπτωση, αν είναι εφικτό ο ερευνητής θα πρέπει να δίνει έναν εφεδρικό αριθμό κινητού τηλεφώνου το οποίο θα χρησιμοποιεί μόνο για συγκεκριμένες περιστάσεις και δεν θα είναι το προσωπικό του νούμερο.

- Πριν από την εγγραφή του σε ένα κοινωνικό δίκτυο ο ερευνητής θα πρέπει να ελέγξει προσεκτικά τόσο την πολιτική ιδιωτικότητας (privacy policy), όσο και τις ρυθμίσεις ιδιωτικότητας (privacy settings).Σε περίπτωση που κάποιο κοινωνικό δίκτυο είτε διαμοιράζει υποχρεωτικά τα δεδομένα (email, όνομα, κατοικία, προτιμήσεις) σε τρίτους, είτε δεν υπάρχει επαρκής παραμετροποίηση των ρυθμίσεων ιδιωτικότητας, ο ερευνητής δεν θα πρέπει να εγγραφεί σε αυτό.
- Κατά την εγγραφή του, το όνομα χρήστη που θα επιλέξει θα πρέπει να αποκαλύπτει όσον το δυνατόν λιγότερες πληροφορίες για το πραγματικό του όνομα. Για παράδειγμα αν ο ερευνητής ονομάζεται Γιάννης Παπαδόπουλος, τα ονόματα χρήστη John_Papadopoulos, και J_P@P αποτελούν τη λάθος και σωστή εκδοχή αντίστοιχα για το όνομα χρήστη.
- Στην περίπτωση που ο ερευνητής είναι εγγεγραμμένος σε περισσότερα από ένα κοινωνικά δίκτυα, οι κωδικοί χρήστη για καθένα από αυτά θα πρέπει να είναι επιλεγμένοι σωστά (τουλάχιστον 8 ψηφίων, με αλφαριθμητικά), και διαφορετικοί μεταξύ τους. Επίσης θα πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα. Οι ίδιες αρχές ισχύουν κα για τους κωδικούς πρόσβασης για το σύστημα που χρησιμοποιείται.
- Το προφίλ του ερευνητή θα πρέπει να είναι ρυθμισμένο να είναι ιδιωτικό και όχι δημόσιο, και οι πληροφορίες που θα περιέχονται σε αυτό να είναι οι λιγότερες δυνατές. Επίσης θα πρέπει να αποφεύγεται η χρήση φωτογραφίας 9 προσώπου του χρήστη καθώς αυτή μπορεί εύκολα να οδηγήσει στην ταυτοποίησή του.
- Ο ερευνητής θα πρέπει να ενεργεί σύμφωνα με τη σκέψη ότι όλα όσα αναρτά (σχόλια, φωτογραφίες, σύνδεσμοι) είναι δημόσια, και η ενέργεια αυτή δεν είναι αναστρέψιμη. Οπότε θα πρέπει να υπάρχει περιορισμός στις πληροφορίες που αναρτά ο ερευνητής και θα μπορούσαν να αποτελέσουν απειλή για την ιδιωτικότητά του όπως το πρόγραμμα που ακολουθεί κάθε μέρα, ή που βρίσκεται ή βρέθηκε τη συγκεκριμένη χρονική στιγμή.
- Οι επαφές του επίσης θα πρέπει να περιορίζονται σε άτομα τα οποία εμπιστεύεται (οικογένεια, φίλοι, συνεργάτες) και να μην αποδέχεται εύκολα και άκριτα αιτήματα φιλίας από άτομα τα οποία δεν γνωρίζει ή έχει μικρή

επαφή και γνώση για αυτά. Με τον τρόπο αυτό περιορίζει τον κίνδυνο οι πληροφορίες που μοιράζεται, να χρησιμοποιηθούν με κακόβουλο τρόπο από τις επαφές του.

- Ο ερευνητής θα πρέπει να είναι προσεκτικός στα δεδομένα που του αποστέλλονται από τις επαφές του, έστω και αν αυτός τις θεωρεί έμπιστες, καθώς υπάρχει η πιθανότητα, κάποιος κακόβουλος να έχει αποκτήσει πρόσβαση στο λογαριασμό τους. Για το λόγο αυτό πρέπει να δίνεται ιδιαίτερη μέριμνα σε e-mail με ασυνήθιστο τίτλο, και σε συνδέσμους (links) οι οποίοι δεν φανερώνουν την πραγματική τοποθεσία του ιστότοπου.
- Οι εφαρμογές που εγκαθιστά ο ερευνητής θα πρέπει να προέρχονται από έμπιστους ιστότοπους, και πριν την εγκατάσταση θα πρέπει να ελεγχθούν από το antivirus καθώς μπορεί να περιέχουν κακόβουλο λογισμικό.
- Επίσης για τη σύνδεση με τα κοινωνικά δίκτυα, θα πρέπει να επιλέγεται η κρυπτογραφημένη σύνδεση (https),να διαγράφονται τα cookies ανά τακτά χρονικά διαστήματα, και η ιδιωτική περιήγηση (private browsing) όπου αυτό είναι εφικτό, καθώς σε αυτή την περίπτωση δεν καταγράφονται από τον περιηγητή (browser) οι κωδικοί, το ιστορικό και τα cookies.

ΚΕΦΑΛΑΙΟ 7^{Ο}

Συμβουλές Προστασίας-Συμπεράσματα

7.1 Συμβουλές Προστασίας-Διαχείριση παραβατικότητας (Συνοπτικά)

1. Προστασία κατά την περιήγηση στο διαδικτύου
2. Συμβουλές για ασφαλείς οικονομικές συναλλαγές
3. Συμβουλές για τους χρήστες Αυτομάτων Τραπεζικών Μηχανών (Α.Τ.Μ)
4. Προστασία από τα spam
5. Προστασία από κακόβουλο λογισμικό
6. Προστασία από παρενοχλήσεις

7.1.1 Προστασία κατά την περιήγηση στο διαδίκτυο

Α) Για τους Γονείς

- Προτιμήστε να τοποθετήσετε τον Η/Υ σας σε χώρους όπως είναι το σαλόνι και όχι σε υπνοδωμάτια. Έτσι θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.
- Κάντε την πλοήγηση στο Διαδίκτυο μία οικογενειακή δραστηριότητα. Χρησιμοποιείστε τον Η/Υ μαζί με τα παιδιά σας.
- Ενημερώστε τα παιδιά σας για τους κινδύνους που υπάρχουν όταν συνομιλούν με αγνώστους μέσω chat rooms.
- Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο.
- Διδάξτε τους να μην δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου,

οικογενειακό εισόδημα, ακόμα και ωράρια σχολείου ονόματα φίλων κ.λπ.) και να μην χρησιμοποιούν την κάρτα σας.

- Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου.
- Νουθετήστε τα επίσης, να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν, μπορεί να είναι επικίνδυνοι.
- Χρησιμοποιείστε τα λεγόμενα «φίλτρα» που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητές σελίδες (βία, πορνογραφία).
- Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.α., που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους.
- Ενημερωθείτε σχετικά με τις αρμόδιες αρχές, που θα πρέπει να επικοινωνήσετε σε περίπτωση που συναντήσετε βλαβερό ή παράνομο περιεχόμενο στο Internet.

Β) Για τους Νέους

- Επιλέγετε να μη δίνετε σε κανέναν τον κωδικό πρόσβασης.
- Μην απαντάται σε ηλεκτρονικά μηνύματα που σας κάνουν να αισθάνεστε «άβολα».
- Αποφεύγετε να στέλνετε προσωπικά σας στοιχεία ή φωτογραφίες σας σε αγνώστους στο διαδίκτυο.
- Ελέγξτε τα στοιχεία του ατόμου που γνωρίσατε μέσω διαδικτύου ώστε να βεβαιωθείτε ότι είναι αυτό που υποστηρίζει και σκεφτείτε το καλά πριν συναντηθείτε μαζί του.
- Σε περίπτωση που αποφασίσετε να συναντηθείτε με το «διαδικτυακό σας φίλο», ενημερώστε τους γονείς σας ή κάποιο στενό φίλο και φροντίστε η συνάντηση να γίνει σε δημόσιο χώρο.

- Καλό είναι να αναπτύξετε κριτική διάθεση και να «φιλτράρετε» αυτά που βλέπετε στο διαδίκτυο.

7.1.2 Συμβουλές για ασφαλείς οικονομικές συναλλαγές

- Αποφεύγετε να πραγματοποιείτε συναλλαγές μέσω διαδικτύου σε Internet Cafe, βιβλιοθήκες και άλλους χώρους όπου υπάρχουν πολλοί χρήστες με πρόσβαση στους ίδιους υπολογιστές.
- Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείτε για διαδικτυακές συναλλαγές:
    - Αλλάξτε τους κωδικούς αν έχει πέσει στην αντίληψή σας ότι έχουν εκτεθεί.
    - Αποφεύγετε να χρησιμοποιείτε ως κωδικό πρόσβασης ημερομηνία γέννησης και άλλα προσωπικά σας στοιχεία.
    - Αποφεύγετε να έχετε τους κωδικούς σας σε πορτοφόλια, τσάντες ή ατζέντες, διότι σε περίπτωση κλοπής θα διευκολύνετε ιδιαίτερα τους δράστες.
    - Μη δίνετε τον κωδικό πρόσβασης σε οποιονδήποτε και κάτω από οποιεσδήποτε περιπτώσεις
- Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία Internet banking.
- Απενεργοποιήστε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.
- Κάνετε αγορές μόνο από γνωστές εταιρείες που σας παρέχουν εγγυήσεις ασφάλειας. Αν κάνετε συχνά αγορές από το Διαδίκτυο, χρησιμοποιείτε μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.

- Φροντίστε να διατηρείτε σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας.
    - Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιήστε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρείες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείτε και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοση του.
    - Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές «εισβολές» που θα δεχτείτε κατά τις περιηγήσεις σας στο διαδίκτυο.
    - Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.
- Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου (e-mails):
    - Μην ανοίγετε τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό σας.
    - Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μην στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μίας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail). Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.
- Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζετε για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων.

- Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και ειδοποιήστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά.
- Φροντίστε να καταστρέφετε όσα έγγραφα δεν σας χρειάζονται πλέον, όπως οι πιστωτικές και τραπεζικές κάρτες που ακυρώνετε, τα αντίγραφα των λογαριασμών σας ακόμα και τις αποδείξεις που λαμβάνετε από τα Α.Τ.Μ.

7.1.3 Συμβουλές για τους χρήστες Α.Τ.Μ

- Αποφεύγετε να χρησιμοποιείτε ως κωδικό (PIN) την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να γίνουν εύκολα αντιληπτά από επιτήδειους.
- Αποφεύγετε να γράφετε το PIN οπουδήποτε.
- Αποφεύγετε να χρησιμοποιείτε το ίδιο PIN σε περισσότερες από μια κάρτες σας.
- Επιλέξτε και απομνημονεύστε τον κωδικό PIN που μόνο εσείς θα γνωρίζετε και που δεν θα μπορεί να προσδιορισθεί από προσωπικά σας αντικείμενα που υπάρχουν στο πορτοφόλι ή στη τσάντα σας.
- Μην δίνετε τον κωδικό σας PIN σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεσθεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό του PIN για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.
- Μην αφήνετε ποτέ την απόδειξη συναλλαγής που έχει εκδώσει το Α.Τ.Μ.
- Συγκρίνετε τις αποδείξεις ανάληψης χρημάτων του Α.Τ.Μ. με το μηνιαίο ενημερωτικό δελτίο κίνησης του λογαριασμού σας. Εάν παρατηρήσετε οποιαδήποτε συναλλαγή που δεν έχετε πραγματοποιήσει ενημερώστε αμέσως την Τράπεζα.

- Να υπογράφετε την κάρτα σας. Αυτό εμποδίζει τον οποιοδήποτε να παραποιήσει το όνομά σας πάνω σε αυτήν.
- Μη δίνετε και μη δανείζετε ποτέ και σε κανέναν την κάρτα σας.
- Όταν κυκλοφορείτε έχετε μαζί σας μόνο τις κάρτες που προτίθεστε να χρησιμοποιήσετε.
- Αναφέρατε αμέσως την κλοπή ή την απώλεια κάρτας στην Τράπεζα και στην Αστυνομία.

7.1.4 Προστασία από τα Spam

- Να μην απαντάτε ποτέ σ' ένα spam e-mail και να μην κάνετε πουθενά κλικ, γιατί απλούστατα η απάντησή σας ή και η άρνησή σας θα επιβεβαιώσει την εγκυρότητα του δικού σας e-mail και έτσι το e-mail σας θα γίνει μια πολύτιμη πληροφορία για πολλούς spammers.
- Να έχετε μια πρόχειρη και μη συχνά χρησιμοποιούμενη ηλεκτρονική διεύθυνση, εκτός φυσικά από την κανονική, και να την δίνετε σε πρώτη ζήτηση έτσι ώστε να πηγαίνουν εκεί όλα τα ανεπιθύμητα e-mails.
- Αναζητήστε και εγκαταστήστε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails. Να ελέγχετε πάντα αν αυτά τα προγράμματα-φίλτρα κάνουν σωστά το μπλοκάρισμα των spam e-mails.

7.1.5 Προστασία από κακόβουλο λογισμικό

- Επιλογή ενός καλού antivirus προγράμματος
- Συνεχής ανανέωση (update) του antivirus και τακτική ανίχνευση όλου του δίσκου.
- Έλεγχος κάθε δισκέτας/cd με το antivirus πριν την ανοίξετε.
- Τήρηση αντιγράφων ασφαλείας όλων των αρχείων σας σε cd ή δισκέτα.
- Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού σας.

- Αν χρησιμοποιείτε IRC chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.
- Επιλέξτε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσετε το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.
- Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.
- Διατήρηση της ανωνυμίας σας με την ενημέρωση του φυλλομετρητή που χρησιμοποιείτε. Προτιμήστε πάντα την πιο πρόσφατη έκδοση και φυσικά φροντίστε να την ενημερώνετε τακτικά. Στον Internet Explorer, για να απενεργοποιήσετε τα «third party cookies» (τα cookies που «φυτεύονται» στο σύστημα όχι από τα sites που επισκέπτεστε αλλά από τριτογενείς φορείς).
- Σωστή ρύθμιση των δικτυακών εφαρμογών. Οι περισσότεροι φυλλομετρητές διαθέτουν ρυθμίσεις ασφαλείας που καθορίζουν ποια πρόσθετα μπορούν να «εκτελεστούν», ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies.
- Αν χρησιμοποιείτε instant messengers, να αποφεύγετε να συνομιλείτε με αγνώστους.

7.1.6 Προστασία από παρενοχλήσεις

- Επιλέξτε ένα ουδέτερο όνομα χρήστη, e-mail κλπ. Αποφύγετε οτιδήποτε χαριτωμένο, σεξουαλικό, ή γυναικείο.
- Διατηρείστε τη βασική σας διεύθυνση ηλεκτρονικού ταχυδρομείου μυστική. Να την χρησιμοποιείται μόνο με ανθρώπους που γνωρίζετε και εμπιστεύεστε.
- Δημιουργείστε ένα ελεύθερο λογαριασμό ηλεκτρονικής αλληλογραφίας τον οποίο να χρησιμοποιείται στις on-line δραστηριότητές σας.
- Μην δίνετε προσωπικές σας πληροφορίες απλά επειδή τις ζητάνε. Πολλοί δικτυακοί τόποι ζητάνε να δώσετε το πλήρες όνομά σας, ημερομηνία γέννησης, διεύθυνση, αριθμό τηλεφώνου,e-mail, κ.α. Δώστε όσο το δυνατόν λιγότερες πληροφορίες.

- Όταν συνομιλείτε σε ένα chat room, να αποκλείεται χρήστες που σας ενοχλούν ρυθμίζοντας τους παραμέτρους του προγράμματος συνομιλίας που χρησιμοποιείται.
- Μην επιτρέπεται στους άλλους να δημιουργούν συγκρούσεις μαζί σας. Είναι προτιμότερο να μην ανοίγετε διάλογο με κάποιον που σας επιτίθεται και να τον αγνοείται. Όταν αντιληφθεί ότι δεν αντιδράτε θα αναζητήσει άλλο στόχο.
- Εάν χρειαστεί να αλλάξετε το όνομα χρήστη για να αποφύγετε κάποιον που σας παρενοχλεί, να φροντίσετε ώστε το νέο όνομα που θα διαλέξετε να μην έχει καμιά σχέση με αυτό που χρησιμοποιούσατε.
- Ποτέ μην χρησιμοποιείτε τα στοιχεία της εταιρείας που εργάζεστε (διεύθυνση, τηλέφωνο κλπ.) σε μια δημόσια συζήτηση στο διαδίκτυο.
- Ποτέ μην δίνετε το κωδικό πρόσβασης σε κανέναν.

7.2 Συμπεράσματα

Τόσο η ταχεία υιοθέτηση της χρήσης του διαδικτύου όσο και η συνεχής ανάπτυξή του την τελευταία δεκαετία έχει αποτελέσει κοινό τόπο συνάντησης, συνύπαρξης και συνεργασίας για άτομα, επιχειρήσεις και οργανώσεις προσδίδοντας τους ένα παγκόσμιο ψηφιακό χαρακτήρα αλλά και δημιουργώντας ταυτόχρονα μια φυσική παγκόσμια παρουσία που είναι άρρηκτα συνδεδεμένη με την ψηφιακή τους παρουσία. Η συνεχής πρόοδος της τεχνολογίας προσφέρει πολύ περισσότερα από απλή πληροφόρηση. Το διαδίκτυο προσφέρει σε πραγματικό χρόνο τη δυνατότητα δυναμικής αλληλεπίδρασης σε πολλούς τομείς, όπως γρήγορη επικοινωνία, κοινωνικοποίηση, ενημέρωση, ανταλλαγή δεδομένων, τραπεζικές συναλλαγές, πώληση και αγορά αγαθών και γενικά σε ένα ευρύ φάσμα των δραστηριοτήτων και υπηρεσιών πληροφόρησης.

Είναι σύνηθες λοιπόν καθώς αναπτύσσεται η τεχνολογία και οι ευκαιρίες στο διαδίκτυο πληθαίνουν, να εμφανίζονται επίσης και νέες ευκαιρίες για να γεννηθούν εγκληματικές συμπεριφορές. Η ευκολία πρόσβασης σε έναν μεγάλης κλίμακας κυβερνοχώρο βρίθει ευκαιριών εκμετάλλευσης από επιτήδειους. Έτσι ο όρος

ηλεκτρονικό έγκλημα χρησιμοποιείται για να περιγράψει παράνομες δραστηριότητες που αφορούν τη χρήση του διαδικτύου. Ο Grabosky et al. (2001) υποστηρίζει ότι η θεμελιώδης αρχή της εγκληματολογίας είναι ότι το έγκλημα ακολουθεί πάντα μία ευκαιρία. Δεδομένου ότι το διαδίκτυο και η υποκείμενη τεχνολογία δικτύου αναπτύσσεται και προοδεύει θα αυξάνεται αναπόφευκτα και η εγκληματικότητα-παραβατικότητα.

Για την αντιμετώπιση λοιπόν της παραβατικότητας απαιτούνται εξειδικευμένες γνώσεις τόσο σε νομικό όσο και σε τεχνολογικό επίπεδο. Στις μέρες μας οι ανεπτυγμένες κυρίως χώρες έχουν καταρτίσει σχετική νομοθεσία για ηλεκτρονικά εγκλήματα όπως εξετάσαμε στο κεφάλαιο 5. Το ίδιο ισχύει και σε τεχνικό επίπεδο, όπως αναφέραμε στο κεφάλαιο 6. Δεν πρέπει όμως να εφησυχαζόμαστε διότι σε κάθε στάδιο εξέλιξης της τεχνολογίας της πληροφορικής και των ψηφιακών συστημάτων ελλοχεύουν κίνδυνοι. Κάθε φορά που εμφανίζονται νέες ευκαιρίες θα εμφανίζονται και νέες απειλές. Είναι σημαντικό λοιπόν να ενημερωνόμαστε για κάθε νέο μέτρο προστασίας των πληροφοριακών συστημάτων και να φιλτράρουμε κάθε είδους πληροφορία πριν την οποιαδήποτε δραστηριότητα μας στο διαδίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξενόγλωσση

Antoci, A., Sabatini, F., Sodini, M., 2012. *"See you on Facebook! A framework for analyzing the role of computer-mediated interaction in the evolution of social capital"*, Journal of Socio-Economics.

Antoci, A., Sabatini, F., Sodini, M., 2012. *"The Solaria syndrome: Social capital in a growing hyper-technological economy"*, Journal of Economic Behavior & Organization, 81(3), 802-814.

Barrett, N., 1997. *Digital crime: Policing the cybernation*. Kogan Page.

Chuhay, R., 2010. *"Marketing via friends: strategic diffusion of information in social networks with homophily"*.

Ellison, N.B., Steinfield, C., Lampe, C., 2011. *"Connection strategies: Social capital implications of Facebook-enabled communication practices"*, New Media & Society, 13(6), 873-892.

Gentile, C., 2010. *"Florida student suspended for Facebook page can sue"*, New York Times.

Goldbaum, D., 2008. *Follow the Leader: Simulations on a Dynamic Social Network*, School of Finance and Economics, University of Technology, Sydney.

Grabosky, P., Smith, R., Dempsey, G., 2001. *"Electronic Theft: Unlawful Acquisition in Cyberspace"*, Cambridge University Press.

Hamill, L., Gilbert, N., 2009. *"Social circles: A simple structure for agent-based social network models"*, Journal of Artificial Societies and Social Simulation, 12(2), 3.

Hunton, P., 2009. *"The growing phenomenon of crime and the internet: A cybercrime execution and analysis model"*, Computer Law & Security Review, 25(6), 528-535.

Kyas, O., 1997. "*Internet Security: Risk Analysis, Strategies, and Firewalls"*. Network Security, (7), 15-15.

Lampe, C., Ellison, N.B., Steinfield, C., 2008. *"Changes in use and perception of Facebook"*, In Proceedings of the 2008 ACM conference on Computer supported cooperative work, pp. 721-730.

Mali, P., 2008. *A textbook of cybercrimes and penalties*.

Monkovic, T., 2009. *"Eagles Employee Fired for Facebook Post"*.

Murphy, S., 2012. "*Facebook's Facial-Recognition Acquisition Raises Privacy Concerns"*.

Steinfield, C., Ellison, N.B., Lampe, C., 2008. *"Social capital, self-esteem, and use of online social network sites: A longitudinal analysis"*, Journal of Applied Developmental Psychology, 29(6), 434-445.

Tzu, S., 1963. *The Art of War*, Translated by Samuel B. Griffith. New York: Oxford University, 65.

Ελληνική

Αναστασόπουλος, Β., Σκόρδας, Α., 2001. *Εισαγωγή στην Πληροφορική*, Β' Έκδοση, Εκδόσεις Ελληνικά Γράμματα.

Βλαχόπουλος, Κ., 2007. *Ηλεκτρονικό Έγκλημα*, Νομική Βιβλιοθήκη.

Γιαννακουδάκης, Ε.Ι, 1998. *Αντικειμενοστραφείς Βάσεις Δεδομένων*, Εκδόσεις Οικονομικού Πανεπιστημίου Αθηνών.

Ζάννη, Αν., 2005. *Διαδικτυκό Έγκλημα,* Εκδόσεις Σάκκουλα.

Κάβουρας, Ι.Κ., 1990. *Δομημένος Προγραμματισμός με Pascal*, Εκδόσεις Κλειδάριθμος.

Λάζος, Γρ., 2001. *Πληροφορική και Έγκλημα*, Νομική Βιβλιοθήκη.

Μαγκάκης, Α., 1984. *Ποινικό Δίκαιο*, έκδοση γ΄ βελτιωμένη, Εκδόσεις Παπαζήση.

Συμεωνίδου-Καστανίδου, Ε., 2006. *Εγκλήματα κατά προσωπικών αγαθών*, Νομική Βιβλιοθήκη.

Σφακιανάκης, Μ., 2003 & 2006. *Εισαγωγή στην πληροφορική σκέψη*, Εκδόσεις Κλειδάριθμος.

Τσουραμάνης, Χρ., 2005. *Ψηφιακή Εγκληματικότητα*, Εκδόσεις Β.Ν.Κατσαρού.

Χλούπη, Γ., *«Νομιμοποίηση εσόδων από παράνομες δραστηριότητες: περιγραφή του φαινομένου και τρόποι αντιμετώπισης»*, Ποιν.Δικ. 2000/369 επ.

Furnell, S., 2006. *Κυβερνοέγκλημα, καταστρέφοντας την κοινωνία της πληροφορίας*, μετάφραση Φωτεινή Μηλιώνη, Εκδόσεις Παπαζήση.

Διαδίκτυο

http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/www.it.security.gr

www.sch.gr/ sch_portlets/static/manualabout spam/index.php?listavoid

http://www.namuseum.gr/

http://www.astynomia.gr/

www.microsoft.com

www.guardian.co.uk

www.computer.howstuffworks.com/ phishing.html

www.pharming-fishing.gr

www.netsecurity.about.com

www.threatpost.com.enus/slideshow/sevenstepsto recovering from Scareware.htm

www.e-crime.gr

www.fbi.gov

www.pgp.com και http://www.ifi.uio.no/pgp.

www.economist.com

Dikeos, T., 23/7/2009. *"Teen's death highlights cyber bullying trend"*, ABC news (http://www.abc.net.au/news/2009-07-23/teens-death-highlights-cyber-bullying-trend/1363362)

Dinerman, B., *"Social networking and security risks"*, (http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf)

Golijan, R., *"Facebook privacy problems are on the rise, NBC News Consumer Reports"*, (http://www.nbcnews.com/technology/consumer-reports-facebook-privacy-problems-are-rise-749990)

Gunatilaka, D., "*Survey of Privacy and Security Issues in Social Networks"*, (http://www.cse.wustl.edu/~jain/cse571-11/ftp/social.pdf)

Mills, E., *"Using Facebook and Twitter safely"*, (http://news.cnet.com/8301-27080_3-10420861-245.html)

Popkin, H., *"Twitter gets you fired in 140 characters or less"*, (http://www.nbcnews.com/id/29796962/ns/technology_and_science-tech_and_gadgets/t/twitter-gets-you-fired-characters-or-less/)