ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εγκλήματα στο Διαδίκτυο: Εναλλακτικοί τρόποι εκδήλωσης, τρόποι αντιμετώπισης και διερεύνησή των

Συντάκτης: Μιχαήλ Στεφανουδάκης **ΑΜ: 08066**

Επιβλέπων: Κωνσταντίνος Λαμπρινουδάκης **Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς**

-Πειραιάς, Ιούνιος 2011-

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της διπλωματικής μου, κύριο Κωνσταντίνο Λαμπρινουδάκη, για τη βοήθεια και τον πολύτιμο συμβουλευτικό του ρόλο. Επίσης θα ήθελα να ευχαριστήσω θερμά την οικογένειά μου που με στηρίζει σε κάθε μου βήμα. Για όλα αυτά που μου προσφέρουν στη ζωή μου, τους αγαπώ και τους ευχαριστώ.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1 ΕΓΚΛΗΜΑΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1.1 ΟΡΙΣΜΟΣ ΕΓΚΛΗΜΑΤΟΣ

Ως έγκλημα μπορεί να νοηθεί κάθε ενέργεια που παρεκκλίνει από αποδεκτούς κοινωνικούς κανόνες. Σύμφωνα με τον Γάλλο κοινωνιολόγο Durkheim «Το έγκλημα υπάρχει σε όλες τις κοινωνίες. Δεν υπάρχει κοινωνία η οποία δεν αντιμετωπίζει το πρόβλημα της εγκληματικότητας. Εκείνο που αλλάζει είναι η μορφή του. Έτσι οι πράξεις που παίρνουν τον χαρακτηρισμό αυτό δεν είναι παντού οι ίδιες, θα υπάρχουν όμως παντού και πάντοτε άνθρωποι των οποίων η συμπεριφορά θα επισύρει ποινικές κυρώσεις σε βάρος τους. Απλά λοιπόν εκείνο το οποίο θα πρέπει να θεωρηθεί σαν κάτι το φυσιολογικό είναι η ύπαρξη της εγκληματικότητας»[1].

Η επισκόπηση της σχετικής βιβλιογραφίας φανερώνει την μη ύπαρξη ενός κοινού ορισμού, γύρω από το έγκλημα, προκειμένου να προσδιοριστεί με σαφήνεια η έννοια αυτή. Βασιζόμενοι σε κλάδους που ασχολούνται με το έγκλημα - τέτοιοι κλάδοι θεωρούνται κατά κύριο λόγο η νομική επιστήμη και η επιστήμη της Εγκληματολογίας- το έγκλημα έχει έννοια νομική και εγκληματολογική. Η πρώτη άποψη, η νομική, στηρίζεται στον σχετικό προσδιορισμό που κάνει σε αυτό ο εκάστοτε ισχύον Ποινικός Νόμος μιας χώρας ενώ η δεύτερη άποψη, η εγκληματολογική, έχει βάση της τις απόψεις της Εγκληματολογίας, η οποία εξετάζει το έγκλημα σαν κοινωνικό φαινόμενο, προσπαθεί να το ερμηνεύσει σαν τέτοιο και για το λόγο αυτό το ονομάζει «πραγματικό».

Έτσι η νομική έννοια του εγκλήματος όπως αυτή προσδιορίζεται στο άρθρο 14 & 1 του Ποινικού μας Κώδικα είναι πως, «έγκλημα είναι πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο».

Από τους διάφορους εγκληματολογικούς ορισμούς του εγκλήματος, οι οποίοι στηρίζονται σε διαφορετικά κάθε φορά κριτήρια, αναφέρουμε ως περισσότερο περιεκτικό εκείνον που δίνει ο Καθηγητής της Νομικής Σχολής του Α.Π.Θ., Στέργιος Αλεξιάδης (1996:50) και σύμφωνα με τον οποίο:

[1] Τσουραμάνης Χ. (2003). Σύγχρονα Κοινωνικά προβλήματα. Η ελληνική πραγματικότητα. Αθήνα : Παπαζήσης, σελ 110

«πραγματικό έγκλημα είναι κάθε εκδήλωση ανθρώπινης δράσης η οποία είναι επικίνδυνα αντικοινωνική». Ο συνολικός αριθμός των εγκλημάτων που διαπράττονται σε ορισμένη τοπικά και χρονικά κοινωνική ομάδα συνιστά την εγκληματικότητα (Αλεξιάδης, 1996: 99) που καταγράφεται σ' αυτή[2].

Έχοντας προσδιορίζει κάπως, την έννοια του εγκλήματος, μπορούμε να ισχυριστούμε ότι ηλεκτρονικό έγκλημα, είναι κάθε άδικη πράξη και καταλογιστή, επικίνδυνα αντικοινωνική, που τελείται μέσω ηλεκτρονικού υπολογιστή.

Σύμφωνα με τον Τσουραμάνη (2005) «ψηφιακό έγκλημα είναι κάθε παράνομη πράξη για τη διάπραξη αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής τεχνολογίας»[3].

1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΕΓΚΛΗΜΑΤΟΣ

Η βιομηχανική επανάσταση του 18ου αιώνα, έφτασε στο αποκορύφωμά της στις δύο πρώτες δεκαετίες του 19ου αιώνα και έθεσε τις βάσεις για την πρώτη διεθνή κοινωνία, και το μετασχηματισμό της ανθρωπότητας σε κοινωνικούς σχηματισμούς με εθνικά κράτη που ανταλλάσσουν μεταξύ τους μαζικής παραγωγής τυποποιημένα εμπορεύματα. Μετά το δεύτερο παγκόσμιο πόλεμο και σε ουσιαστικά πολύ σύντομο χρονικό διάστημα - μέσα σε δύο γενιές - άρχισε να αναπτύσσεται η πληροφορική επανάσταση. Η ταχύτατη ανάπτυξη και διάδοση και εφαρμογή των εφαρμογών της πληροφορικής προσφέρει σημαντικά πλεονεκτήματα σε πολλούς τομείς της κοινωνικής ζωής

[2] Αλεξιάδης Σ. (1996). Εγχειρίδιο εγκληματολογίας. Θεσσαλονίκη: Εκδόσεις Σάκκουλα, σελ 50

[3] Τσουραμάνης Χ. (2005). Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου. Αθήνα: Εκδόσεις Κατσαρού Β. Ν., σελ. 15

ώστε σήμερα γίνεται λόγος για μια αυξανόμενη εξάρτηση του κράτους, της οικονομίας αλλά και της παιδείας και του πολιτισμού από την πληροφορική. Σύμφωνα με τον Edwards[4], η σύγχρονη κοινωνία τείνει να φθάσει στο σημείο όπου τα πάντα θα εξαρτώνται από το λογισμικό. Ο κύριος όγκος των πληροφοριών κάθε είδους που διακινούνται καθημερινά στον πλανήτη, μεταβιβάζεται μέσω συστημάτων πληροφορικής. Αλλά και αντίστροφα, κάθε πληροφορία, άξια λόγου, τείνει να θεωρείται η πληροφορία που μπορεί να μεταβιβασθεί μέσω των συστημάτων αυτών. Η έρευνα στην υγεία και τη γενετική αλλά και η εφαρμογή τους, ο έλεγχος των συγκοινωνιών σε εθνική και διεθνή κλίμακα, η λειτουργία του κρατικού μηχανισμού και η εθνική άμυνα εξαρτώνται από τις εφαρμογές της τεχνολογίας της πληροφορικής. Το ίδιο ισχύει και για τον κύριο όγκο των χρηματικών συναλλαγών μεταξύ των επιχειρήσεων και τη διαχείριση των οικονομικών τους μεγεθών. Ολοένα και συχνότερα, ο έλεγχος και η ρύθμιση της παραγωγικής διαδικασίας μιας επιχείρησης εξαρτάται απόλυτα από τη λειτουργική ικανότητα του συστήματος επεξεργασίας δεδομένων (data-processing system) που διαθέτει[5].

Η πληροφορική επανάσταση με όλα της τα υλικά (hardware) και άυλα (software) συστατικά, αποτελεί μια κοινωνική σχέση και ένα εργαλείο που έχουν στόχο να παραμείνουν στην κοινωνία.

Το ζήτημα συνεπώς είναι ο έλεγχός της ώστε να τεθεί στην υπηρεσία όλων των ανθρώπων. Μία από αυτές τις προσπάθειες ελέγχου της πληροφορικής επανάστασης είναι και η προσπάθεια ελέγχου της χρήσης της ως μέσου και ως πεδίου τέλεσης εγκλημάτων. Οι κίνδυνοι από την ανάπτυξη της πληροφορικής τεχνολογίας δεν είναι δυνατό να αντιμετωπιστούν μόνο μέσω της αντιμετώπισης του εγκληματικού της στοιχείου. Η προσπάθεια αυτή όμως, είναι αναγκαία.

Η πληροφορική επανάσταση δεν περιορίζεται σε τεχνολογικά ζητήματα και αποφάσεις, όπως αυτά κατανοούνται και ορίζονται είτε από τους ειδικούς, είτε από τα κράτη, είτε από τις ιδιωτικές επιχειρήσεις. Ο Hughes[6] διατυπώνει

[4] Edwards O. (1995). Hackers from hell. *Forbes* 9, σελ. 182

[5] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 15-16

[6] Thomas P. Hughes, Networks οι Power: Electrification in Western Society, 1880-1930, Baltimore: John Hopkins University Press, 1983.

τη θέση ότι η τεχνολογία προωθείται σε ένα ευρύ κοινωνικό μέτωπο. Η εφεύρεση μιας καινοτομίας δεν συμπίπτει αναγκαστικά με την πρακτική αποδοχή της. Η εφεύρεση ενός νέου τρόπου οργάνωσης ή διαχείρισης ανθρώπων, πραγμάτων και συμβόλων δεν συνιστά κάτι παραπάνω από μία πρόταση που απευθύνεται στην κοινωνία. Η αφομοίωση και πρακτική εφαρμογή της καινοτομίας αυτής αποτελεί προϊόν πολύπλοκων, πολυέξοδων και χρονοβόρων διευθετήσεων. Οι διευθετήσεις αυτές δεν λαβαίνουν χώρα μόνο στο τεχνολογικό επίπεδο, αλλά και στο οικονομικό, κοινωνικό, πολιτικό, πολιτιστικό, ακόμα και στο ηθικό αξιακό επίπεδο.

Σύμφωνα με τον Bigelow, «κάθε νέα τεχνολογική εξέλιξη δημιουργεί νέα νομικά προβλήματα και απαιτεί επανεκτίμηση των παλαιών εννοιών»[7]. Κατά την εκτίμηση των Michalowski και Pfhul, «κάθε νέα τεχνολογία δημιουργεί αμφιβολίες σε ό,τι αφορά στα δικαιώματα και τις υποχρεώσεις τόσο αυτών που αξιώνουν τον ορισμό της ως ιδιοκτησίας τους όσο και αυτών που επηρεάζονται από την κοινωνική προώθηση και εφαρμογή της.

Οι τεχνολογικές εξελίξεις και καινοτομίες δημιουργούν προβλήματα μέχρι να ενσωματωθούν στα επικρατούντα πρότυπα των κοινωνικών σχέσεων και της κοινωνικής εξουσίας και μέχρι να μορφοποιηθούν με τρόπους που θα ελαχιστοποιηθούν ή θα αμβλύνουν τις προοπτικές διάσπασης αυτών των προτύπων.

Με τη θέση αυτή συντάσσεται η πλειονότητα των επιστημόνων που ασχολούνται με το πληροφοριακό έγκλημα. Εγκληματολόγοι, νομικοί και κοινωνιολόγοι όπως η Nelson, ο Hollinger, ο Meier και Thomas συνιστούν την προσοχή σε μια πολύ σημαντική εκκρεμότητα: η κοινωνία δεν έχει ακόμα αποφασίσει ως προς τις ηθικές και πολιτιστικές συντεταγμένες των σχέσεων που δημιουργήθηκαν με την ταχύτατη ανάπτυξη των νέων τεχνολογιών, δεν έχει αποφασίσει ως προς το τι είναι πληροφορική κακοχρησία και πληροφορικό έγκλημα. Ο νόμος δεν έρχεται τόσο να επικυρώσει κάποια κοινά συμφωνημένα ηθικά και πολιτιστικά πρότυπα για τις σχέσεις και τη χρήση της

[7] Bigelow R. (1985). The challenges of computer law. Western New England Law Review 7(3), sel 397

πληροφορικής, αλλά μάλλον να επιβάλλει τα όρια στα οποία τα πρότυπα αυτά θα πρέπει να αναπτυχθούν[8].

1.3 ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ

Το διαδικτυακό έγκλημα ήδη από τα μέσα της δεκαετία του 1980, εξασφάλισε από κάθε άποψη την αυτόνομη ύπαρξή του. Συντίθεται από «δικούς» του δράστες και δράσεις, πλαισιώνεται από ένα ιδιαίτερο δίκαιο και προσεγγίζεται από προσαρμοσμένες στις ιδιαιτερότητές του, κοινωνικές επιστήμες όπως είναι η πληροφορική εγκληματολογία. Σύμφωνα με τον Volgyes το διαδικτυακό έγκλημα έχει μια «απρόσωπη καθαρότητα». Είναι ένα έγκλημα που στρέφεται απόμακρα, διακριτικά και χωρίς βία ενάντια σε «αντιπαθητικές» κυβερνήσεις και επιχειρήσεις[9].

Στο διαδικτυακό έγκλημα ο υπολογιστής μπορεί να έχει διάφορους ρόλους. Μπορεί να αποτελέσει το υλικό σώμα, hardware το αντικείμενο δηλαδή της επίθεσης, να καεί, να πυροβοληθεί, να κλαπεί, είτε ο ίδιος είτε οι περιφερειακές του συσκευές. Κατ' αυτό τον τρόπο, είναι δυνατό να καταστραφούν τα πολύτιμα προγράμματα και δεδομένα που έχει. Μπορεί επίσης να χρησιμοποιηθεί ως εργαλείο, για τη διάπραξη αδικημάτων. Μία συσκευή ηλεκτρονικής επεξεργασίας δεδομένων μπορεί να χρησιμοποιηθεί για τη διάπραξη κλοπής, καταπάτησης ή παραβίασης δικαιωμάτων. Για παράδειγμα, ο πληροφορικός εγκληματίας, αντί να χρησιμοποιήσει όπλο για να διαπράξει μια ληστεία, έχει τη δυνατότητα να μεταφέρει χρήμα από το λογαριασμό κάποιου στο δικό του λογαριασμό, με τη χρήση ενός τερματικού. Ο ηλεκτρονικός υπολογιστής μπορεί να συμβάλλει επίσης αποφασιστικά στον πειθαναγκασμό, την παραπλάνηση ή την εξαπάτηση. Μία μεγάλη μερίδα ανθρώπων τείνει να θεωρεί ως δεδομένο το προϊόν του ηλεκτρονικού υπολογιστή. Πάνω σ' αυτή τη βάση, έχουν σχεδιασθεί και εκτελεσθεί διάφορες πρωτότυπες απάτες ψευδούς χρέωσης. Απλά και μόνον επειδή αποτελεί προϊόν υπολογιστή, ένας λογαριασμός που πρέπει να πληρωθεί θεωρείται ακριβής και έγκυρος. Ακόμα και στις περιπτώσεις που κάποιος εκφράζει τις

[8] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 17-18

[9] Volgyes M. (1980). The investigation, prosecution and prevention of computer crime: A state-of-the-art review. *Computer and Law journal,* 2, σελ. 385

αμφιβολίες του ως προς το να καταβάλλει το αντίτιμο για υπηρεσίες που δεν του έχουν προσφερθεί (ή να επανακαταβάλλει ή να καταβάλλει πρόσθετο αντίτιμο), συνήθως πείθεται ότι πρόκειται περί άδολου λάθους εάν λάβει ως απάντηση μία τυποποιημένη έκφραση συγνώμης συνοδευόμενη από τη διευκρίνιση ότι «ο υπολογιστής έκανε λάθος»[10].

Οι παραπάνω τρεις ρόλοι του ηλεκτρονικού υπολογιστή, δεν καθιστούν δυνατές νέες, ποιοτικά διαφορετικές μορφές εγκληματικής δράσης, αλλά τείνουν να συντίθενται με τις ήδη γνωστές, με τη διαφορά ότι οι μορφές αυτές έχουν αναδιοργανωθεί με τρόπον ώστε να βελτιώσουν τη λειτουργικότητά τους ή να την προσαρμόσουν στα νέα πληροφορικά περιβάλλοντα που έχουν αναπτυχθεί.

Τέλος υπάρχει και ένας τέταρτος ρόλος του υπολογιστή, που σχετίζεται ειδικά με την πληροφορική τεχνολογία. Ο ρόλος αυτός αφορά ακριβώς στις πληροφορικές ιδιότητες των δεδομένων και των προγραμμάτων, που φιλοξενούνται στο σώμα του υπολογιστή. Η ειδοποιός διαφορά μεταξύ των πληροφοριών σε μη-ηλεκτρονική («παραδοσιακή») μορφή και των πληροφοριών σε ηλεκτρονική μορφή (αποθηκευμένων σε ηλεκτρονικά μέσα), είναι ότι οι πληροφορίες σε ηλεκτρονική μορφή μπορούν να αντιγραφούν, τροποποιηθούν, υπονομευθούν ή διαγραφούν χωρίς οι αναγκαίες ενέργειες να αφήνουν πίσω τους κάποιο φυσικό ίχνος. Για παράδειγμα, το ηλεκτρονικό αντίγραφο (replica) είναι πανομοιότυπο και απολύτως ομόλογο του πρωτότυπου. Ουσιαστικά, η διάκριση μεταξύ πρωτοτύπου και αντιγράφου τείνει να περιορίζεται σε ζητήματα χρονικής διαδοχής και μόνον. Σ' αυτό το πλαίσιο, οι υπολογιστές παίζουν έναν διπλό ρόλο στην πληροφορική προσβολή. Από τη μία πλευρά, «δημιουργούν ένα μοναδικό (unique) περιβάλλον στο οποίο μπορούν να λάβουν χώρα μη-εξουσιοδοτημένες δραστηριότητες», ενώ, συγχρόνως, «ο

[10] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 39

υπολογιστής δημιουργεί μοναδικές μορφές περιουσιακών στοιχείων (assets) που μπορούν να υποστούν προσβολές». «Ο υπολογιστής μπορεί να μην έχει άμεση συμμετοχή σε ανάλογα συμβάντα. Τα ηλεκτρονικά αποθηκευμένα δεδομένα αποτελούν μία εντελώς νέα μορφή - υποκείμενη σε νέες μορφές προσβολής, αλλά η χρήση των υπολογιστών δεν έχει οδηγήσει σε νέα είδη προσβλητικών δραστηριοτήτων, τουλάχιστον ως προς το όνομα. Τα ονόματα των δραστηριοτήτων είναι τα ίδια: απάτη, κλοπή, κατάχρηση, βανδαλισμός, δόλια βλάβη, εκβιασμός, σαμποτάζ. και κατασκοπεία. Όμως, πέρα από την ονομασία της δραστηριότητας με τη χρήση ενός από αυτούς τους παραδοσιακούς όρους, οτιδήποτε άλλο σε σχέση μ' αυτή τη δραστηριότητα, μπορεί να είναι εντελώς μοναδικό: η θέση των δραστών, τα περιβάλλοντα της δραστηριότητας, οι μέθοδοι που χρησιμοποιήθηκαν στην προσβολή, και οι μορφές των περιουσιακών στοιχείων, είναι όλα καινούργια[11].

1.4 ΗΛΕΚΤΡΟΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ ΚΑΙ ΕΓΚΛΗΜΑ

Η αυξανόμενη χρήση των υπολογιστών δεν διαμόρφωσε απλώς νέες συνθήκες στην καθημερινή μας ζωή, την εργασία, την διασκέδαση, την επικοινωνία, αλλά ταυτόχρονα δημιουργώντας ένα πεδίο δράσης διαπλάθει καθημερινά νέες μορφές κοινωνικής συμπεριφοράς. Η εκτεταμένη χρήση των ηλεκτρονικών υπολογιστών στη μηχανοργάνωση εταιρειών, κρατικών οργανισμών και υπηρεσιών, η χρήση τους για την εκτέλεση επαγγελματικών δραστηριοτήτων μετέβαλαν τα δεδομένα των συναλλαγών. Ο υπολογιστής αποτέλεσε έτσι ένα νέο μέσο τέλεσης εγκλημάτων, όπου η χρήση του τεχνικού μέσου επέβαλε απλώς τη συμπλήρωση ή την τροποποίηση των αντίστοιχων διατάξεων, έτσι ώστε να καλύπτει την καινούργια μεθοδολογία τέλεσης: Σε ένα ανταλλακτήριο συναλλάγματος που λειτουργούσε με τον παραδοσιακό τρόπο οι δυνατότητες παράνομης δραστηριότητας του υπαλλήλου συνίστατο στο να ξεγελάσει τον πελάτη σχετικά με το ποσό που αντιστοιχεί, να του δώσει άχρηστα νομίσματα, να τον «κλέψει» στα ρέστα κλπ. Απαιτούσε δηλαδή μία

[11] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ. 40

άμεση προσωπική επαφή δράστη και θύματος και μία κατά τον ένα ή άλλο τρόπο προσβολή του δεύτερου.

Στο αυτόματο ανταλλακτήριο που λειτουργεί με προγραμματισμό από ηλεκτρονικό υπολογιστή αυτή η άμεση επαφή λείπει και παρεμβάλλεται το «μηχάνημα». Ο δράστης δεν χρειάζεται να «ασχοληθεί» με το θύμα, απλώς αλλοιώνει το πρόγραμμα λειτουργίας του μηχανήματος. Το προγραμματίζει να δέχεται τα χαρτονομίσματα και να μην επιστρέφει τίποτα, να «βλέπει» τα τροφοδοτούμενα χαρτονομίσματα στο 50 % της αξίας τους ή αν είναι πιο μεθοδικός- να στρογγυλοποιεί κάποια ποσά αποκομίζοντας ο ίδιος τις διαφορές της καθημερινής είσπραξης[12].

Μία τέτοια εγκληματική χρήση του υπολογιστή δε συνιστά ίσως παρά μικρή απόκλιση από την παραδοσιακή μη τεχνολογική εκδοχή της αξιόποινης συμπεριφοράς και απλώς αναγκάζει το νομοθέτη να διαμορφώσει μία νέα αντικειμενική υπόσταση (άρθρο 386 Α΄ Ποινικού Κώδικα) που θα καλύπτει και αυτόν τον τρόπο τέλεσης της αξιόποινης πράξης.

Το τοπίο του ψηφιακού εγκλήματος μετέβαλε ριζικά η εμφάνιση του Διαδικτύου στο οποίο συνδέθηκαν δεκάδες εκατομμύρια άνθρωποι σε όλον τον κόσμο, ανταλλάσσοντας καθημερινά έναν τεράστιο όγκο δεδομένων κειμένου, εικόνας, ήχου, αλλά και προγραμμάτων υπολογιστών χρησιμοποιώντας το ως ένα παγκόσμιο forum ανταλλαγής ιδεών, ειδήσεων, πληροφοριών, ως χώρο διασκέδασης, ως πεδίο εμπορικών και οικονομικών συναλλαγών και αναπόφευκτα, ως χώρο και εγκληματικής δραστηριότητας.

1.5 ΜΟΡΦΕΣ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

1.5.1 ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

Ο κύριος όγκος των πληροφορικών εγκλημάτων εντάσσεται στην υποκατηγορία των πληροφορικών οικονομικών εγκλημάτων. Ακριβέστερα, τα πληροφορικά οικονομικά εγκλήματα απαρτίζουν, τον κύριο όγκο των διαπιστωμένων πληροφορικών εγκλημάτων και τα εγκλήματα που τραβούν

[12] Κιούπης Δ. (1999) Ποινικό δίκαιο και ίντερνετ. Αθήνα: Σάκουλας , σελ. 17-18

την προσοχή της πλειονότητας των ερευνητών του πληροφορικού εγκλήματος. Στη διεθνή βιβλιογραφία, η αναλογία μεταξύ των διάφορων υποκατηγοριών πληροφορικού εγκλήματος που απασχολούν τους ειδικούς είναι χαρακτηριστική: σε κάθε δώδεκα περιπτώσεις πληροφορικού οικονομικού εγκλήματος αναλογεί μόλις μία περίπτωση των άλλων κατηγοριών.

Ένας παράγοντας που συμβάλλει σ' αυτή τη δυσαναλογία ως προς ενδιαφέρον αποτελεί το ευκολότερα διαπιστώσιμο, το «χειροπιαστό», του πληροφορικού οικονομικού εγκλήματος: Κατά κανόνα, γίνεται αντιληπτό από τους ενδιαφερόμενους σε σχετικά μικρό χρονικό διάστημα μετά την τέλεσή του. Επιπλέον, από τη στιγμή που θα γίνει αντιληπτό, είναι μετρήσιμο με μεγάλη ακρίβεια - τουλάχιστον όσον αφορά στα άμεσα οικονομικά του μεγέθη[13].

Ένας δεύτερος παράγοντας είναι το γεγονός ότι οι ίδιες οι επιχειρήσεις έχουν δείξει μεγάλο ενδιαφέρον γι' αυτό τον τύπο πληροφορικού εγκλήματος και έχουν διαθέσει πολύ σημαντικούς πόρους για τη διερεύνησή του. Συνεπώς, η ισχύς των επιχειρήσεων συμβάλλει σε σημαντικό βαθμό στην αύξηση της αντιπροσώπευσης του πληροφοριακού οικονομικού εγκλήματος μέσα στο ευρύτερο πληροφορικό έγκλημα.

Ένας τρίτος παράγοντας είναι ότι συχνά το πληροφορικό οικονομικό έγκλημα είναι ευκολότερα ανακοινώσιμο, τόσο σε σύγκριση με μία σημαντική μερίδα υπερατομικών πληροφορικών εγκλημάτων όπως είναι οι περιπτώσεις κατασκοπείας, όσο και σε σύγκριση με μερίδα των πληροφορικών εγκλημάτων κατά των προσωπικών δικαιωμάτων όπου, συχνά, το ίδιο το θύμα δεν επιθυμεί την αποκάλυψη.

Στο πλαίσιο των πληροφορικών οικονομικών εγκλημάτων, η απάτη μέσω υπολογιστή περιλαμβάνει την παραποίηση κάποιων δεδομένων ή πληροφοριών που φιλοξενούνται στις βάσεις δεδομένων ή σε προγράμματα με σκοπό το οικονομικό κέρδος. Λεπτομερέστερα, αφορά κυρίως στην κλοπή, διαγραφή, αλλοίωση ή προσθήκη δεδομένων ή πληροφοριών με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο οικονομικό κέρδος. Κεντρικό αντικείμενο-

[13] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ. 121

στόχος της συγκεκριμένης μορφής απάτης είναι τα δεδομένα που φιλοξενούνται στον υπολογιστή και αφορούν σε οικονομικά μεγέθη. Η συγκεκριμένη απάτη μετεξελίχθηκε στο πέρασμα του χρόνου από ένα ομοιογενές σύνολο αδικημάτων, της εποχής των κεντρικών πληροφορικών συστημάτων, σε μία διαφοροποιημένη ενότητα που περιγράφει ένα μεγάλο φάσμα διαφορετικών υποθέσεων στο πεδίο του οικονομικού εγκλήματος.

Παραποίηση λογιστικών λογαριασμών

Η απάτη σε βάρος μιας επιχείρησης ή ενός ιδιώτη μέσω της εστίασης, και παραποίησης, σε πληροφορίες και δεδομένα, τα οποία τους αφορούν άμεσα και έμμεσα, έχει να κάνει με τους άυλους πόρους, όπως χρηματικές καταθέσεις, οικονομικούς τίτλους, για παράδειγμα, ομόλογα, και λογιστικά μεγέθη, όπως ισολογισμούς. Συχνά, υπάρχουν περιπτώσεις βελτίωσης της πίστης (credit rating) μέσω της παραποίησης των δεδομένων που αναφέρονται σε ένα άτομο ή μία επιχείρηση, ώστε για παράδειγμα, να μπορεί να πάρει δάνειο ή να πάρει δάνειο με καλύτερους όρους, αλλά και χειροτέρευσης της φερεγγυότητας ενός ατόμου ή μιας επιχείρησης, για τους αντίθετους λόγους, που μπορεί να πραγματοποιηθεί από κάποιο άτομο ή επιχείρηση εχθρικά διακείμενων ή αντίθετων συμφερόντων.

Αναφορικά με τους άυλους πόρους, ένα παράδειγμα τυπικής παραποίησης, μέσω εισαγωγής δεδομένων για προσωπικό όφελος, αποτελεί η περίπτωση υπαλλήλου που εργαζόταν ως χειριστής και ελεγκτής δεδομένων στο τμήμα επεξεργασίας δεδομένων τράπεζας στη Ζυρίχη, μιας από τις μεγαλύτερες τράπεζες της Ελβετίας. Ο υπάλληλος πέτυχε να θέσει μερικώς, υπό τον έλεγχό του, το αυτόματο σύστημα μεταβίβασης ξένων πληρωμών. Στη συνέχεια, υπέκλεψε πολλές και διάφορες εντολές μεταβίβασης από τους συνεργάτες του στο τμήμα κωδικοποίησης της τράπεζας. Κατόπιν, αντί να τροφοδοτεί τον υπολογιστή με τα ακριβή ποσά μεταβίβασης, κάθε φορά τροφοδοτούσε τα εν λόγω ποσά με ανακριβή δεδομένα. Έχοντας άφθονο χρόνο στη διάθεσή του, εντόπισε με ακρίβεια και παρέκαμψε τα μέτρα ασφαλείας της τράπεζας που είχαν οργανωθεί με σκοπό την αποτροπή τέτοιων χειρισμών. Έτσι, για παράδειγμα, όταν 98 Γερμανικά

μάρκα καταθέτονταν στην Φρανκφούρτη, οι συνεργοί του - αποσύροντας τα χρήματα στο Λουγκάνο και το Νταβός - δεν παραλάμβαναν 100 αλλά 100.000 Ελβετικά φράγκα. Παρόμοια, για μία κατάθεση 97 δολαρίων στην Νέα Υόρκη, δεν αποκόμιζαν 251 αλλά 251.000 Ελβετικά φράγκα. Κατ' αυτό τον τρόπο, οι δράστες αποκόμισαν συνολικά κέρδη της τάξης των 700.000 Ελβετικών φράγκων[14].

Παραποιημένη εφαρμογή ηλεκτρονικών πληρωμών

Η απάτη μέσω υπολογιστή με την παρέμβαση στο σύστημα επεξεργασίας δεδομένων ενός οργανισμού ή μιας επιχείρησης απαντάται συχνά σε ζητήματα μισθών, συντάξεων αλλά και των τραπεζικών καταθέσεων. Σε ένα «ανοχύρωτο» σύστημα, η δημιουργία ενός τραπεζικού λογαριασμού πολλών μηδενικών είναι ζήτημα λεπτών - και για έναν έμπειρο hacker, είναι ζήτημα δευτερολέπτων. Αν το πληροφορικό σύστημα διαθέτει έναν αμυντικό μηχανισμό προηγούμενης γενιάς και αν ο συγκεκριμένος hacker δε βιάζεται, αλλά αρκείται σε έναν αρχικό λογαριασμό ενός ή δύο μηδενικών, και κατόπιν εισάγει μία ρουτίνα προσθήκης πέντε μηδενικών σε κάποια συχνά μεν, αλλά άτακτα χρονικά διαστήματα, δεν έχει λόγους να φοβάται τις συνέπειες. Πέρα όμως, από τις περιπτώσεις παράνομης κατασκευής δεδομένων, συχνά εμφανίζονται στη διεθνή βιβλιογραφία και ειδησεογραφία, πολλές περιπτώσεις παραβίασης καρτών συναλλαγής (ATM cards) και ανάλογων μέσων πληρωμής. Ακόμη και αν τέτοιου είδους απάτες οδηγούν σε μικρές συνολικά ζημιές, οι στατιστικές δείχνουν πως η κακοχρησία των καρτών αποτελεί μία από τις πιο συχνές υποθέσεις πληροφορικού εγκλήματος.

Μια παραποιημένη πληρωμή διαπράττεται μέσω τράπεζας, που διαθέτει σύστημα αυτόματης ανάληψης ή χορήγησης χρήματος. Με διάφορες μεθόδους, είναι δυνατή η παράνομη ανάληψη χρήματος από τερματικά των συστημάτων επεξεργασίας δεδομένων των τραπεζών[15].

[14] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ. 125-126

[15] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ. 127

1.5.2 ΠΟΡΝΟΓΡΑΦΙΑ

Η διακίνηση πορνογραφικού υλικού, δεν είναι ένα έγκλημα νέο. Η εξάπλωση όμως, του Διαδικτύου, έχει διευκολύνει τη διάπραξή του. Στατιστικές μελέτες έχουν καταδείξει ότι η διακίνηση υλικού πορνογραφίας μέσω Διαδικτύου, αποτελεί μια από τις πιο συχνές μορφές εγκλήματος[16].

Ειδικότερα:

Δικτυακοί τόποι με πορνογραφικό υλικό	4,2 εκατομμύρια (12% του συνόλου)
Σελίδες με πορνογραφικό υλικό	420 εκατομμύρια
Αιτήματα ανά ημέρα για πορνογραφικό υλικό σε μηχανές αναζήτησης	68 εκατομμύρια (25% του συνόλου)
E-mail με πορνογραφικό υλικό / χρήστη	4,5 ανά χρήστη
Δικτυακοί τόποι που προσφέρουν παιδική πορνογραφία	100.000
Μέσος όρος ηλικίας πρώτης επαφής με την πορνογραφία	11 ετών
Μεγαλύτερη κατανάλωση πορνογραφίας	12-17 ετών
Ποσοστό παιδιών ηλικίας 7-17 ετών που δίνουν ελεύθερα τη διεύθυνση κατοικίας τους	29%
Σεξουαλική παρενόχληση νέων σε δωμάτια συζητήσεων	89%

Πηγή: http://www.familysafemedia.com/pornography_statistics.html

Τα αδικήματα που συνδέονται με τη μορφή αυτή του υλικού, σχετίζονται τόσο με τη δημιουργία του υλικού όσο και με τη μη νόμιμη διακίνησή του. Η παράνομη διακίνηση υλικού παιδικής πορνογραφίας έχει λάβει τεράστιες διαστάσεις, προκαλώντας ιδιαίτερη ανησυχία στις διωκτικές

[16] http://www.familysafemedia.com/pornography_statistics.html [Ημερομηνία πρόσβασης 03-06-2011]

αρχές.

Το πορνογραφικό υλικό, που διακινείται μέσω του Διαδικτύου, μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή και οποιοδήποτε άλλης μορφής πολυμέσων. Ο καθένας μπορεί εύκολα να το «κατεβάσει» στον υπολογιστή του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητά του. Τέτοιου είδους υλικό, βρίσκεται σε διάφορους δικτυακούς τόπους. Μάλιστα, σε συγκεκριμένους δικτυακούς τόπους, γίνεται ανταλλαγή υλικού, δηλαδή αντί να πληρώσει κάποιος τίμημα για το υλικό που προμηθεύεται, προσφέρει νέο υλικό, ως αντάλλαγμα.

Η σεξουαλική κακοποίηση ανηλίκων και γυναικών είναι μια από τις αρχαιότερες εγκληματικές συμπεριφορές. Με την εμφάνιση και τη διάδοση της χρήσης του Διαδικτύου, έχουμε απλά μια νέα γέφυρα[17] προς το έγκλημα.

Η παιδική πορνογραφία στο διαδίκτυο εμφανίζεται με τη μορφή εικόνων, φωτογραφιών καθώς και μαγνητοσκοπημένων σκηνών στις οποίες παρουσιάζονται γυμνά κορμιά ανηλίκων, ανήλικοι να αυνανίζονται και ακόμα χειρότερα, ανήλικοι να κακοποιούνται σεξουαλικά από ενηλίκους. Αυξημένη ζήτηση υπάρχει στην κακοποίηση ανηλίκων από υπερήλικες και γενικά σε οτιδήποτε το αηδιαστικό. Η καινούρια τεχνολογία δίνει τη δυνατότητα παρακολούθησης ή και συμμετοχής σε ζωντανό «σόου».

Το πρόβλημα μπορεί να προσεγγισθεί από δύο διαφορετικές πλευρές, όσον αφορά το πώς επηρεάζεται η συμπεριφορά των παιδόφιλων με την είσοδό τους σε πορνογραφικές ιστοσελίδες. Ενδέχεται οι ορέξεις του δράστη να ικανοποιηθούν και να εκτονωθούν με τον τρόπο αυτό και να μην εκδηλωθούν οι διαστροφικές του τάσεις στο υπόλοιπο κοινωνικό περιβάλλον. Είναι όμως πολύ πιθανό τα θεάματα αυτά να του δημιουργήσουν ψύχωση, την οποία θα εκδηλώσει στον κοινωνικό του περίγυρο, κακοποιώντας σεξουαλικά κάποιο ανήλικο άτομο. Επιπλέον οι παιδόφιλοι δημιουργούν τα δικά τους δωμάτια επικοινωνίας (chat rooms) στο Διαδίκτυο, στα οποία είναι μόνο αυτοί ευπρόσδεκτοι, ανταλλάσσοντας ιδέες, εμπειρίες και τακτικές προσέγγισης ανηλίκων.

[17] Δήμου Γ., Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων, Αθήνα, 2002

Η σεξουαλική κακοποίηση των παιδιών για πορνογραφικούς σκοπούς, μπορεί να αποδειχθεί μια πολύ επικερδής επιχείρηση. Έτσι, με τη δουλειά αυτή ασχολούνται άτομα με τεράστια γνώση στο χώρο των υπολογιστών και μακρά πείρα χρήσης του μέσου.

Τα πιο αισχρά και πλέον διαδεδομένα κυκλώματα παιδικής πορνείας κρύβονται στο Διαδίκτυο, πίσω από κρυπτογραφημένες διευθύνσεις και κωδικούς που γνωρίζουν μόνον όσοι πληρώνουν αδρά. Υπάρχουν δυστυχώς πάρα πολλοί δικτυακοί τόποι που έχουν πορνογραφικό περιεχόμενο και λειτουργούν ως "κλαμπ παιδεραστών" και τα οποία πουλούν φωτογραφίες και βιντεοταινίες ανήλικων πρωταγωνιστών. Πολλοί από αυτούς τους δικτυακούς τόπους διοργανώνουν ακόμα και ταξίδια σε χώρες όπως η Ιαπωνία ή η Ταϊλάνδη και υπόσχονται να ικανοποιήσουν ακόμα και τις πιο απαιτητικές διαστροφικές επιθυμίες των πελατών τους.

Οι δικτυακοί τόποι της παιδικής πορνείας δεν βρίσκονται επισήμως καταχωρημένοι στο διαδίκτυο. Ηλεκτρονικές διευθύνσεις με «μαλακό πορνό» οι ενδιαφερόμενοι μπορούν να τις αναζητήσουν μέσω άλλων ηλεκτρονικών διευθύνσεων ερωτικού ή συναφούς περιεχόμενου. Στις διευθύνσεις εκείνες όμως που έχουν πιο "σκληρό πορνό" μέσα στο δίκτυο μπορεί να φτάσει κάποιος μόνο αν ψάξει ενδελεχώς στο διαδίκτυο.

Οι κωδικοποιημένες πορνογραφικές διευθύνσεις ανακοινώνονται ιδιωτικά, μέσω e-mail, ενώ οι παράνομες υπηρεσίες που προσφέρονται, διαφημίζονται μέσα από διάφορες ομάδες συζητήσεων, που καλύπτονται πίσω από παραπλανητικούς τίτλους και ενδιαφέροντα, όπως μουσική, ταξίδια ή αθλητισμός. Οι μηχανές αναζήτησης σπάνια θα καταδείξουν μία ηλεκτρονική διεύθυνση που έχει ως κύριο περιεχόμενο την παιδική πορνογραφία.

Χώρες όπως η Ρωσία, η Ιαπωνία, η Ταϊλάνδη, η Κορέα, οι Φιλιππίνες καθώς επίσης και οι χώρες της πρώην Σοβιετικής Ένωσης φαίνονται να έχουν τον πρωταγωνιστικό ρόλο στο εμπόριο της παιδικής αθωότητας στο Διαδίκτυο. Στις διάφορες φωτογραφίες που χρησιμοποιούνται ως δολώματα για τους επίδοξους παιδεραστές φιγουράρουν οι αθώοι ανήλικοι πρωταγωνιστές και φαίνονται να χαμογελούν.

Δυστυχώς όμως οι φωτογραφίες γυμνών εφήβων, μικρών αγοριών και κοριτσιών, να χαμογελούν και να ποζάρουν δίπλα σε κήπους, πισίνες και λουλούδια που προσφέρονται δωρεάν, είναι μόνο ο κράχτης που δελεάζει τους επίδοξους πελάτες. Στο Διαδίκτυο παρουσιάζονται και διακινούνται χιλιάδες φωτογραφίες βασανιστηρίων χωρίς έλεγχο, οι οποίες χωρίς δυσκολία χαρακτηρίζονται αδικαιολόγητα ως «ερωτικές». Προκειμένου να στοχεύσουν σε κοινό με συγκεκριμένα ενδιαφέροντα οι έμποροι της παιδικής σάρκας διαφημίζουν την καταγωγή και την ηλικία των ανήλικων θυμάτων.

Η εξάπλωση του φαινομένου της πορνογραφίας και πορνείας ανηλίκων στο διαδίκτυο αλλάζει διαρκώς και αυτό οφείλεται στο γεγονός ότι αυτός είναι ο ιδανικός χώρος όπου οποιοσδήποτε μπορεί να περάσει από το πραγματικό στο φανταστικό, από έναν κόσμο με κανόνες ηθικής και νόμους σε έναν άλλον, όπου όλα επιτρέπονται, και δεν υπάρχουν ηθικοί ή άλλοι φραγμοί.

Ο χρήστης του δικτύου που αναζητά πορνογραφικό υλικό, ζει σε έναν κόσμο φανταστικό όπου μπορεί να βγάλει στην επιφάνεια τις ερωτικές και σεξουαλικές του προτιμήσεις ελεύθερα, χωρίς τον κίνδυνο της αποκάλυψης, της κριτικής, του κοινωνικού ελέγχου, ή ακόμα και της ποινικής διώξεώς του.

Πολλοί από αυτούς τους χρήστες της αναζήτησης υλικού παιδικής πορνογραφίας είναι οικογενειάρχες, επαγγελματίες με υψηλό εισόδημα, ίσως και επιφανή μέλη κάποιας κοινωνίας, που δεν είχαν ευκαιρία να εξωτερικεύσουν ασφαλώς αυτή την ερωτική τους διαστροφή. Μέσω όμως του Διαδικτύου δεν ρισκάρουν απολύτως τίποτα και νιώθουν ασφαλείς, φυσιολογικοί και νόμιμοι, αφού καλύπτονται πίσω από την ανωνυμία μιας τυχαίας διεύθυνσης ηλεκτρονικού ταχυδρομείου.

Είναι χαρακτηριστικό πως ο αριθμός των δικτυακών τόπων (websites), που προβάλλουν την παιδική πορνογραφία έχει ξεπεράσει τις 100.000 και αυξάνεται διαρκώς. Όμως και οι επισκέπτες αυτών των sites αυξάνονται με γρήγορους ρυθμούς. Χαρακτηριστικό της δυναμικής αυτού του φαινομένου είναι το γεγονός ότι τον πρώτο μήνα λειτουργίας μίας τέτοιας ιστοσελίδας έγιναν 3.000 επισκέψεις, τον δεύτερο μήνα 90.000 και τον τρίτο μήνα (λίγο πριν κλείσει) ο αριθμός των επισκεπτών είχε φθάσει τα 3,2 εκατομμύρια.

Προσεγγίζοντας την αιτιολογία του φαινομένου καταλήγουμε ότι η φτώχεια είναι ο κύριος καταλύτης, αλλά δεν μπορεί να εξηγήσει επαρκώς την εμπορική σεξουαλική εκμετάλλευση των παιδιών. Κατά συνέπεια θα πρέπει να εστιάσουμε την προσοχή μας στους ακόλουθους παράγοντες που συμβάλλουν ουσιαστικά στη δημιουργία δεξαμενής άντλησης της «πρώτης ύλης» αυτής της εγκληματικής συμπεριφοράς :

- **Η ενδοοικογενειακή κακοποίηση και παραμέληση παιδιών** : Ένα μεγάλο ποσοστό που αγγίζει το 80% των παιδιών που βρίσκονται υπό σεξουαλική εκμετάλλευση έχουν υποστεί κάποιου είδους σωματική ή ψυχολογική κακοποίηση μέσα στις οικογένειες τους. Μερικά παιδιά που παρευρέθηκαν στη Σύνοδο Κορυφής του 1998 για τη σεξουαλικά κακοποιημένη νεολαία, ανέφεραν ότι εισήλθαν στην παιδική πορνεία όταν συνειδητοποίησαν ότι για τους γονείς τους ήταν ανεπιθύμητα λάθη.

- **Ένοπλες συγκρούσεις** : Πολλά παιδιά είναι συχνά χωρισμένα από τους γονείς τους, ενώ άλλα τους χάνουν στο σκληρό περιβάλλον ενόπλων συγκρούσεων και πολεμικών γεγονότων και μένουν ορφανά και απροστάτευτα. Στο πλαίσιο αυτό τα ανήλικα παιδιά καθίστανται ιδιαίτερα τρωτά στους εκμεταλλευτές. Είναι πολλές οι περιπτώσεις όπου έχουν αναφερθεί εξαφανίσεις παιδιών από στρατόπεδα προσφύγων, κατά την πορεία για αναζήτηση καλύτερης τύχης, στους τόπους προορισμού κλπ. Τα παιδιά αυτά αποτέλεσαν αντικείμενο εμπορικών πράξεων και συναλλαγών στους τόπους των συγκρούσεων και μεταφέρθηκαν για να ριχθούν στην πορνεία, σε πιο ασφαλείς, ή δυτικές χώρες.

- **Καταναλωτισμός** : Σε πολλές αναπτυγμένες χώρες κάποια παιδιά ωθούνται στην πορνεία, επιδιώκοντας μεγαλύτερα εισοδήματα με γρήγορους τρόπους. Αυτή η επιθυμία που δημιουργεί ο υπερκαταναλωτισμός, προσελκύει τα ανήλικα παιδιά και τα οδηγεί στο κύκλωμα της παιδικής πορνείας, αφού η επιδίωξη και ο στόχος τους είναι το άμεσο, υψηλό και γρήγορο κέρδος, με το οποίο θα μετέχουν σε απόλαυση αγαθών και υπηρεσιών πολυτελείας.

- **Ανήλικα ορφανά παιδιά λόγω ασθενειών και επιδημιών (AIDS κλπ.)**: Πρόκειται για εκατομμύρια παιδιά της Αφρικής κυρίως, ηλικίας κάτω

των 15 ετών, που έχουν χάσει τον έναν ή και τους δύο γονείς τους από το AIDS ή και άλλες αιτίες. Αναμένεται ότι σε λίγα χρόνια, πολλές οικογένειες στην Αφρική θα αποτελούνται μόνον από τα αδέρφια, αφού οι γονείς θα έχουν αποβιώσει. Ένα μέρος από αυτά τα παιδιά, καθώς και άλλα που θα προέρχονται από τις παραγκουπόλεις της Αργεντινής και άλλων φτωχών χωρών, θα αποτελέσουν «εμπόρευμα» προς εκμετάλλευση στα χέρια των επιτήδειων.

- **Τα παιδιά των φαναριών**: Τα άστεγα παιδιά που περιφέρονται και ζουν στους δρόμους, καταφεύγουν συχνά στην πορνεία προκειμένου να επιζήσουν, αφού τους αποφέρει υψηλότερες αποδοχές από κάθε άλλη «δραστηριότητα».

- **Εθνοτικές, Κοινωνικές διακρίσεις:** Δεξαμενή άντλησης ανήλικων παιδιών για εκμετάλλευση, αποτελούν διάφορες εθνοτικές ομάδες και ιδίως μειοψηφίες οικονομικά ασθενέστερων στρωμάτων, που έχουν χαμηλό μορφωτικό επίπεδο, αμφισβητείται η εθνική τους ταυτότητα και η πορεία ζωής αυτών προδιαγράφεται αρνητική, αφού περιορίζεται η πρόσβασή της στην εκπαίδευση και την εργασία.

1.5.3 ΚΛΟΠΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η κλοπή ταυτότητας (Identity Theft) είναι ένα από τα πλέον σοβαρά εγκλήματα του Διαδικτύου. Στην ψηφιακή εποχή που διανύουμε, τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς (π.χ. εμπορικούς, ιατρικούς, διαφημιστικούς). Είναι εύκολο για τον καθέναν, να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών.

Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δυο στάδια (Newman, 2004)[18]: Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους, συμβατικούς και ψηφιακούς όπως:

[18] Newman, R. (2004). Identity Theft. US Department of Justice. Διαθέσιμο από http://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf [Ημερομηνία πρόσβασης 5-4-2011]

♦ Αφαιρώντας πορτοφόλια από τσάντες, αυτοκίνητα ή ακόμη και από την τσέπη ανυποψίαστων περαστικών.

♦ Υποκλέπτοντας την αλληλογραφία, παραβιάζοντας μη ασφαλή κιβώτια αλληλογραφίας, υποβάλλοντας ψευδή αλλαγή διεύθυνσης κατοικίας στο ταχυδρομικό γραφείο των νόμιμων παραληπτών κ.ά.

♦ Αποσπώντας τα ενημερωτικά σημειώματα των πιστωτικών καρτών, υποδυόμενο τον υπάλληλο ή συγγενικό πρόσωπο του νόμιμου κατόχου.

♦ Εισβάλλοντας στις βάσεις δεδομένων εταιρειών και οργανισμών, όπου φυλάσσονται προσωπικά δεδομένα.

♦ Χρησιμοποιώντας ειδικό λογισμικό, το οποίο, έχει τη δυνατότητα, να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες, παρακολουθώντας την κίνηση των πακέτων στο Διαδίκτυο.

Το επόμενο βήμα είναι η χρησιμοποίηση των κλεμμένων στοιχείων. Αυτή μπορεί να πραγματοποιηθεί:

♦ Ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, τους οποίους και χρησιμοποιεί για την αγορά αγαθών μέσω του Διαδικτύου.

♦ Ανοίγοντας τραπεζικούς λογαριασμούς, τους οποίους, χρεώνει με ακάλυπτες επιταγές.

♦ Δημιουργώντας πλαστές πιστωτικές κάρτες, άδειες οδήγησης, διαβατήρια και ταυτότητες χρησιμοποιώντας τα στοιχεία του θύματος.

♦ Υποβάλλοντας ψευδείς φορολογικές δηλώσεις (και μέσω Διαδικτύου), για να εισπράξει επιστροφή φόρου.

Πειρατεία ονομάτων χώρου

Η πειρατεία ονομάτων χώρου, γνώρισε ιδιαίτερη άνθηση κατά τα πρώτα χρόνια του Διαδικτύου. Διάφοροι επιτήδειοι, εκμεταλλευόμενοι το γεγονός πως μεγάλες εταιρείες δεν είχαν κατοχυρώσει, ακόμη, ονόματα χώρων για τους δικτυακούς τους τόπους, προέβαιναν σε κατοχύρωση ονομάτων διασήμων εταιρειών, με αποτέλεσμα να αποκτούν τα δικαιώματα

της νέας διεύθυνσης. Στη συνέχεια, μπορούσαν να δράσουν με δύο διαφορετικούς τρόπους: Είτε να παραχωρήσουν την διεύθυνση στην εταιρεία που κατέχει το συγκεκριμένο όνομα, έναντι βέβαια σημαντικού χρηματικού ποσού,[19] είτε να προβούν στην ανάρτηση, στη συγκεκριμένη διεύθυνση, περιεχομένου προσβλητικού (π.χ. πορνογραφία), γεγονός που επιφέρει σημαντικές συνέπειες στην εταιρεία.

Πειρατεία Λογισμικού

Η ψηφιακή μορφή των εφαρμογών λογισμικού, καθιστά ιδιαίτερα εύκολη την αναπαραγωγή τους σε πολλαπλά αντίγραφα. Πριν από την έλευση του Διαδικτύου, οι εφαρμογές λογισμικού διακινούνταν με φυσικό τρόπο (π.χ. με δισκέτες ή CD). Η εξάπλωση, όμως, του Διαδικτύου και ιδιαίτερα των ευρυζωνικών συνδέσεων άνοιξε νέους ορίζοντες στην πειρατεία λογισμικού. Πλέον, το λογισμικό μπορεί να διακινηθεί με διάφορες υπηρεσίες που προσφέρει το Διαδίκτυο, όπως ηλεκτρονικό ταχυδρομείο (e-mail), chat, Usenet, ftp και ιδιαίτερα με τις εφαρμογές ανταλλαγής αρχείων (peer to peer, P2P).

Αν και οι εταιρείες παραγωγής λογισμικού εφαρμόζουν στα προϊόντα τους διάφορα τεχνολογικά μέτρα για να αποτρέψουν την αντιγραφή ή χρήση τους από πολλούς υπολογιστές, οι hackers-crackers πάντα βρίσκουν τεχνικές για να παρακάμψουν τα μέτρα αυτά. Χρησιμοποιώντας την τεχνική "cracking"* έχουν τη δυνατότητα να απενεργοποιούν τους κωδικούς, τα

[19] Τη συγκεκριμένη μέθοδο χρησιμοποίησε ο Dennis Toepen, ο οποίος αντιλαμβανόμενος τον σημαντικό ρόλο που θα διαδραμάτιζαν στο ηλεκτρονικό εμπόριο που μόλις αναπτύσσονταν τα ονόματα χώρων, κατοχύρωσε πάνω από 100 διευθύνσεις σημαντικών εταιρειών, όπως Delta Air Lines, Lufthansa, American Standard και άλλες, αξιώνοντας από τις εταιρείες την πληρωμή σημαντικών χρηματικών ποσών, προκειμένου να τους μεταβιβάσει τα δικαιώματα των διευθύνσεων. Βλ. σχετικά). J. Lipton. Beyond Cybersquatting Taking Domain Name Disputes past Trademark Policy, διαθέσιμο από:*forum.icann.org/lists/gtld-council/doc5pI73SNDTn.doc* σελ.5 [Ημερομηνία πρόσβασης 03-06-2011]

* Το cracking, είναι μια διαδικασία που μπορεί να πραγματοποιηθεί σε επίπεδο γλώσσας μηχανής. Οι crackers χρησιμοποιούν λογισμικό debugger ή hexeditors και επεμβαίνουν στα δυαδικά ψηφία της εφαρμογής αποτρέποντας την εκτέλεση ενός συγκεκριμένου κλειδιού κατά την εκκίνηση της εφαρμογής.

κλειδιά και ό,τι άλλο χρησιμοποιείται για την προστασία ενός προγράμματος. Ακόμα και αν δεν έχουν εξειδικευμένες γνώσεις για να σπάσουν ένα πρόγραμμα, μπορούν να χρησιμοποιήσουν έτοιμο λογισμικό «crack», που διατίθεται ελεύθερα στο Διαδίκτυο και έχει τη δυνατότητα να απενεργοποιεί τα μέτρα προστασίας των εταιρειών παραγωγής λογισμικού.

Σύμφωνα με την ετήσια έρευνα Global Piracy Study 2010, της εταιρείας λογισμικού Business Software Alliance που παρουσιάστηκε τον Μάιο του 2011,[20] το ποσοστό πειρατείας λογισμικού παγκοσμίως έφτασε το 42%, μειωμένο ελάχιστα κατά 1% σε σχέση με το αμέσως προηγούμενο έτος. Ωστόσο, το σχετικά χαμηλό παγκόσμιο ποσοστό, δεν ανταποκρίνεται σε απόλυτο βαθμό στην πραγματικότητα, καθότι τα χαμηλά ποσοστά που εμφανίζονται στις Η.Π.Α. και σε πολλές χώρες της Ευρωπαϊκής Ένωσης, επηρεάζουν σημαντικά τον παγκόσμιο μέσο όρο. Παράλληλα, παρατηρείται ότι για κάθε $100 νόμιμου/γνήσιου λογισμικού που πωλήθηκε, ένα πρόσθετο ποσό αξίας $75 λογισμικού χωρίς άδεια, βγήκε στην αγορά.

ΠΕΡΙΟΧΗ	**ΕΤΟΣ**		**Απώλειες από την πειρατεία σε εκατ. Δολάρια**	
	2009	**2010**	**2009**	**2010**
Μέση Ανατολή και Αφρική	59%	58%	2,887	4,078
Βόρεια Αμερική	21%	21%	9,379	10,623
Δυτική Ευρώπη	34%	33%	11,750	12,771
Ασία	59%	60%	16,544	18,746
Κεντρική και Ανατολική Ευρώπη	64%	64%	4,673	5,506
Λατινική Αμερική	63%	64%	6,210	7,030
Ευρωπαϊκή Ένωση	35%	35%	12,469	13,458
Παγκόσμιο ποσοστό	**43%**	**42%**	**63,912**	**72,212**

Στατιστικά στοιχεία για την πειρατεία λογισμικού

Πηγή: http://portal.bsa.org/globalpiracy2010/downloads/study_pdf/2010_BSA_Piracy_Study-Standard.pdf

[20]Βλ. http://portal.bsa.org/globalpiracy2010/ [Ημερομηνία πρόσβασης 27-06-2011]

1.5.4 ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

Με το ξέπλυμα χρήματος (money laundering), επιχειρείται η εξαφάνιση χρήματος που έχει προέλθει από παράνομες δραστηριότητες. Η διαδικασία, που ακολουθείται από τους εγκληματίες για το ξέπλυμα χρήματος, περιλαμβάνει τρία στάδια:

- Στο πρώτο,[21] επιχειρείται η μετατροπή των χρημάτων, που προέρχονται από παράνομες δραστηριότητες, σε μια μορφή λιγότερο ύποπτη για τις διωκτικές αρχές. Το παράνομο χρήμα περιέρχεται σε διάφορα οικονομικά ιδρύματα ή διοχετεύεται στο λιανεμπόριο.
- Στο δεύτερο στάδιο, επιχειρείται ο διαχωρισμός του χρήματος από την παράνομη πηγή του, χρησιμοποιώντας πολλαπλές οικονομικές συναλλαγές για να αποκρύψουν το χρήμα.
- Στο τελευταίο στάδιο, ολοκληρώνεται η μετατροπή του παράνομου χρήματος, ώστε, να έχει τη μορφή εισοδήματος, που προήλθε από νόμιμες επαγγελματικές δραστηριότητες.

Η ανωνυμία του Διαδικτύου, δυσχεραίνει την πιστοποίηση της ταυτότητας των πελατών μιας εταιρείας. Ως αποτέλεσμα, πολλές εταιρείες, χωρίς να το γνωρίζουν, διευκολύνουν το ξέπλυμα χρήματος. Για παράδειγμα, έχει διαπιστωθεί η αγορά, μέσω του Διαδικτύου, ασυνήθιστα μεγάλων ποσοτήτων αγαθών από συγκεκριμένους πελάτες, που θέλουν, μ' αυτό τον τρόπο, να προωθήσουν χρήματα, που έχουν περιέλθει στην κατοχή τους από παράνομες δραστηριότητες. Άλλη μέθοδος ξεπλύματος χρημάτων είναι η κατάθεση μέσω του Διαδικτύου, σχετικά μικρών ποσών σε πολλαπλούς τραπεζικούς λογαριασμούς.

1.5.5 ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

Η ηλεκτρονική τρομοκρατία αφορά σε εκρηκτικά και σαμποτάζ, που αν και το περισσότερο από αυτό το υλικό είναι ήδη διαθέσιμο σε δημόσιες βιβλιοθήκες και βιβλιοπωλεία, η ευκολία με την οποία γίνεται προσβάσιμο

[21] "Stages of the Money Laundering Progress", A report in accordance with § 356 (c) of the USA PATRIOT Act http://www2.econ.uu.nl/users/unger/publications/dancing.pdf [Ημερομηνία πρόσβασης 7-4-2011]

διαμέσου των ηλεκτρονικών μέσων προσδίδει στο φαινόμενο απειλητικές διαστάσεις. Θεωρείται ότι είναι η μέγιστη απειλή στην εμπορική, οικονομική και πολιτική βιωσιμότητα του διαδικτύου. Τόσο στον ηλεκτρονικό τύπο όσο και στον παραδοσιακό, κάνουν την εμφάνισή τους δημοσιεύματα που ασχολούνται με περιστατικά εκρήξεων και επιθέσεων, για τις οποίες οι δράστες απέκτησαν την αναγκαία ενημέρωση μέσω του διαδικτύου. Στον Καναδά και την Αυστραλία, μεταξύ άλλων χωρών, έχει παρατηρηθεί μία αυξητική τάση στην ηλεκτρονική τρομοκρατία, κυρίως δε όσον αφορά στις εκρήξεις.

Σύμφωνα με τους Strassman and Marlow (1996), η τρομοκρατία πληροφοριών μέσω του διαδικτύου, είναι ένα μοναδικό φαινόμενο στην ιστορία του εγκλήματος. Τα εγκλήματα πληροφοριών μπορούν να διαπραχθούν εύκολα χωρίς αποκάλυψη οποιονδήποτε στοιχείων όπως τα δακτυλικά αποτυπώματα, ή οι σφαίρες[22]. Η θέση αυτή εξηγεί και τους λόγους που χρησιμοποιείται το διαδίκτυο από τους τρομοκράτες. Ο Whine (2000) θεωρεί ότι είναι τέσσερις:

α. Το διαδίκτυο παρέχει τη δυνατότητα στην αλληλοσυνδετικότητα (επικοινωνία και δικτύωση). Ένα παράδειγμα είναι η ιστοσελίδα της Hezbollah, η οποία δημοσιεύει ένα καθημερινό ημερολόγιο των τρομοκρατικών επιθέσεων όπου τα μέλη έχουν πραγματοποιήσει στο νότιο Λίβανο. Όπως αναφέρει και ένας εκπρόσωπος της οργάνωσης, «Η υπηρεσία είναι πολύ σημαντική για το ηθικό των μαχητών αντίστασής μας. Είναι πάντα ευτυχείς να ξέρουν ότι οι άνθρωποι σε όλο τον κόσμο τους υποστηρίζουν[23]».
β. Το διαδίκτυο επιτρέπει την συγκεκαλυμμένη επικοινωνία και την ανωνυμία, πρακτικές που απαιτούνται για την επιτυχημένη δράση εξτρεμιστικών οργανώσεων. Ενδιαφέροντα στοιχεία για το θέμα, δίνονται από τον τρόπο οργάνωσης και λειτουργίας της Hamas. Οι ισραηλινές υπηρεσίες ασφάλειας, ήταν ανίκανες να «σπάσουν» τους διαδικτυακούς κώδικες που χρησιμοποιούνταν από την Hamas.

γ. Ένας τρίτος λόγος χρησιμοποίησης του διαδικτύου είναι ότι αποτελεί ένα φτηνό μέσο επικοινωνίας. Η κατοχή ενός υπολογιστή επιτρέπει σε έναν

[22] Αναστασία Ζαννή (2005). Το διαδικτυακό έγκλημα. Εκδόσεις Αντ.Ν.Σάκκουλα, σελ.81-83
[23] Hizbollah on the Internet, The Daily Telegraph, London, 19.02.1997

τρομοκράτη να γίνει φορέας στα εθνικά και παγκόσμια γεγονότα. Δεδομένου ότι οι υπολογιστές γίνονται όλο και περισσότερο ανέξοδοι, η διάπραξη τρομοκρατικών πράξεων μέσω του διαδικτύου, θα γίνεται όλο και πιο εύκολη υπόθεση. Οι φόβοι αυτοί εκφράζονται από το FBI, όπου θεωρεί ότι όσο οι τεχνικές προστασίας θα αυξάνονται, ευθέως ανάλογη θα είναι και η αύξηση των τεχνικών παραβίασής τους.

δ. Το διαδίκτυο λειτουργεί ως πολλαπλασιαστής της δύναμης που διαθέτουν οι εξτρεμιστικές οργανώσεις, και ταυτόχρονα ως πολλαπλασιαστής της αμεσότητας επικοινωνίας. Αντιπροσωπεύοντας το μηδενισμό της απόστασης και των εθνικών συνόρων βοηθά στη γρηγορότερη προσέγγιση των στόχων επίθεσης, αλλά και στην ταχύτατη ανάπτυξη εξτρεμιστικών οργανώσεων, δίνοντάς τους παγκόσμιο χαρακτήρα, καθώς μέσα από τις ιστοσελίδες τους μπορούν να προσεγγίσουν άτομα από όλο τον κόσμο[24]. Το διαδίκτυο θεωρείται ένα διαδεδομένο κέντρο επικοινωνίας τρομοκρατικών ομάδων και μέσο για τη διάπραξη εγκληματικών ενεργειών. Η 11η Σεπτεμβρίου επέδρασε καταλυτικά ώστε να αποκαλυφθούν περισσότεροι μέθοδοι επικοινωνίας[25].

Στην ηλεκτρονική τρομοκρατία εντάσσεται και η προπαγάνδα μίσους (hate propaganda) η οποία αναφέρεται ευθέως στο εξευτελιστικό και υποτιμητικό περιεχόμενο, το οποίο στρέφεται εναντίον συγκεκριμένων τάξεων ή ομάδων ανθρώπων. Ο πιο συνηθισμένος τύπος που παρουσιάζεται στο διαδίκτυο είναι η ρατσιστική προπαγάνδα (κυρίως η νεοναζιστική και αντισημιτική). Εκτός από αυτόν όμως, δεν είναι ασυνήθιστη η εμφάνιση (α) περιεχομένου με φανατικό θρησκευτικό χαρακτήρα, που προσβάλλει πιστούς άλλων θρησκειών, (β) ομοφυλοφοβικού περιεχομένου, το οποίο προσβάλλει ειδικές μειονότητες με βάση τις σεξουαλικές τους προτιμήσεις, και γ) περιεχομένου με ακραίο πολιτικό στίγμα, όπου γίνεται ευθεία πολεμική ενάντια σε πολιτικούς ή κρατικούς σχηματισμούς. Δεν είναι λίγες οι ανησυχίες

[24] Αφγανοί Taliban δημοσιεύουν την ιδεολογία τους σε απευθείας σύνδεση, θεωρώντας ότι τα δυτικά μέσα θα διαστρεβλώσουν ή θα αρνηθούν να δημοσιεύσουν τα μηνύματά τους. http://taliban.com

[25] Μέσω του προγράμματος Carnivore, οι μυστικές υπηρεσίες των ΗΠΑ αποκάλυψαν την επικοινωνία των μελών της Al Kainta καθώς και τις μεθόδους που χρησιμοποίησαν για να φτάσουν στην καταστροφή του World Trade Center.

που εγείρονται από αυτά τα είδη προπαγάνδας, αφού, συχνά, διαπιστώνονται προκλήσεις για γενοκτόνες και αντεκδικητικές δράσεις[26].

Μορφή ηλεκτρονικής τρομοκρατίας αποτελεί και ο πολιτιστικός ιμπερεαλισμός. Καθώς βρίσκεται σε καθεστώς ευρείας διαθεσιμότητας, μπορεί να προκαλεί την προσοχή και να επισκιάζει περιεχόμενα τοπικού χαρακτήρα. Το γεγονός και μόνον ότι ο κυβερνοχώρος είναι αγγλόφωνος προδιαθέτει για μια απώθηση των άλλων γλωσσών στην περιφέρεια της συνείδησης και μια αντικατάσταση τοπικών προϊόντων και θεσμών με προϊόντα και θεσμούς του δυτικού πολιτισμού. Ενδογενείς μορφές έκφρασης, τέχνης και τοπικές αξίες απειλούνται από την-ανισομερή ανάπτυξη και προώθηση περιεχομένου με υπερτοπικό και διεθνικό χαρακτήρα. Πολύ περισσότερο, γίνονται κατανοητές οι ανησυχίες ορισμένων εθνών και κρατών που αντιμετωπίζουν την τηλεπικοινωνιακή επανάσταση ως βασικό μέσο μιας πιο εντατικής και επιθετικής προώθησης του πολιτισμού αναπτυγμένων χωρών στους τοπικούς πολιτισμούς. Τέλος η αποστολή μηνυμάτων με επιθετικό περιεχόμενο δημιουργεί ένα γνήσιο και διαρκές άγχος σε πολλούς αποδέκτες.

[26] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 167

ΚΕΦΑΛΑΙΟ 2 : ΤΡΟΠΟΙ ΕΠΙΘΕΣΗΣ / ΥΛΟΠΟΙΗΣΗ

2.1 ΜΕΘΟΔΟΙ ΑΠΑΤΗΣ ΣΤΑ ATM

Οι μηχανές αυτές ενεργοποιούνται με τη μαγνητική λωρίδα της κάρτας μετρητών (Cashcard) και την πληκτρολόγηση του προσωπικού κωδικού αριθμού του πελάτη. Μέσω των ATMs (Automatic Teller Machines) μπορούν να γίνουν οι παρακάτω συναλλαγές[27]:

- Ανάληψη και κατάθεση μετρητών
- Μεταφορές ποσών από λογαριασμό σε λογαριασμό
- Ενημέρωση για το υπόλοιπο λογαριασμών
- Ανάληψη μετρητών με πιστωτική κάρτα
- Πληρωμή λογαριασμών πιστωτικών καρτών
- Πληρωμή καταναλωτικών δανείων
- Πληρωμή λογαριασμών ΔΕΗ, ΟΤΕ και ύδρευσης.

Η παράνομη ανάληψη χρημάτων από ATM δεν λαμβάνει χώρα σε βάρος της τράπεζας αλλά σε βάρος του λογαριασμού κάποιου τυχαίου καταθέτη. Η εκτεταμένη εφαρμογή των μεθόδων αυτών εμφανίστηκε στην Ευρώπη στα μέσα της δεκαετίας του '80. Ένα διπλό «πρωτοποριακό» παράδειγμα από τον Sieber είναι χαρακτηριστικό: Το Σεπτέμβριο του 1985, δυο δημοσιογράφοι της τηλεόρασης από το Αμβούργο κατάφεραν να χρησιμοποιήσουν τις μαγνητικές τους κάρτες με σκοπό τη δημιουργία υπερβάσεων σε τραπεζικούς λογαριασμούς τρίτων. Η εν λόγω διαδικασία έλαβε χώρα μέσω της χρήσης μιας συσκευής ανάγνωσης και αναγνώρισης μαγνητικών καρτών, ενός προσωπικού υπολογιστή και ενός προγράμματος που είχαν δημιουργήσει οι ίδιοι. Μαγνητοσκόπησαν αυτήν τους την πράξη και

[27] Μανωλαράκης Ε. (2006) Οι τεχνολογίες πληροφορικής στο Ελληνικό τραπεζικό σύστημα"

στις 27 Οκτωβρίου του 1985 πρόβαλαν το φιλμ στην δυτικογερμανική τηλεόραση.

Η παραπάνω υπόθεση ενέπνευσε δυο άνεργα άτομα από την Κολονία να αναπτύξουν την ακόλουθη τεχνική: Εισήγαγαν ένα κενό αντίγραφο μαγνητικής κάρτας μέσα σε ένα μηχάνημα αυτόματης ανάληψης χρημάτων και, κατόπιν, προσάρμοσαν στη συσκευή ανάγνωσης και αναγνώρισης έναν ειδικό βοηθητικό μηχανισμό. Όταν κάποιος πελάτης εισήγαγε την κάρτα του μέσα στον βοηθητικό μηχανισμό, το αρχικό κενό αντίγραφο έμπαινε στη συσκευή ανάγνωσης και αναγνώρισης της τράπεζας. Από τη στιγμή που ο προσωπικός κωδικός αριθμός του πελάτη δεν ταίριαζε με αυτόν της ειδικά προετοιμασμένης κενής κάρτας, το μηχάνημα «παρακρατούσε» την τελευταία και απέρριπτε μόνιμα την κάρτα του πελάτη, ο οποίος έφευγε. Οι δράστες έβγαζαν την κάρτα του πελάτη από τον βοηθητικό μηχανισμό και προσπαθούσαν να εντοπίσουν τον κωδικό της αναλύοντας τα κουμπιά του πληκτρολογίου, τα οποία είχαν προηγουμένως ευαισθητοποιηθεί με μικρές σταγόνες πετρελαίου. Όταν ανακάλυπταν τους τέσσερις κωδικούς αριθμούς, προσπαθούσαν να εξακριβώσουν τη σωστή τους σειρά μέσα από τον έλεγχο 24 συνδυασμών: Η αυτοάμυνα του μηχανήματος - που θα έπρεπε να δεσμεύσει την κάρτα μετά από τρεις λαθεμένες εισαγωγές - παρακαμπτόταν με την αντιγραφή της κάρτας και την αλλαγή του αυτόματου μετά από δυο λαθεμένες εισαγωγές, ή με τον επιδέξιο χειρισμό του μετρητή ασφαλείας της κάρτας, ο οποίος κατέγραφε τον αριθμό λαθεμένων εισαγωγών. Οι δράστες καταχράστηκαν ποσό της τάξης των 80 χιλιάδων γερμανικών μάρκων. Πιάστηκαν στις 16 Ιανουαρίου του 1986, μετά από συστηματική παρακολούθηση και καταγραφή τους με κρυμμένες βιντεοκάμερες.

Στην Αυστραλία, έλαβε χώρα μία αντίστοιχη περίπτωση, η οποία έφτασε στα δικαστήρια. Ο κατηγορούμενος, ενώ είχε κλείσει τον λογαριασμό του σε μία τράπεζα, δεν είχε παραδώσει την ATM κάρτα του. Βρήκε λοιπόν ένα παράρτημα της τράπεζας στην Αδελαΐδα και από εκεί κατάφερνε να αποσύρει μέχρι 200 δολάρια τη φορά. Το μηχάνημα της τράπεζας ήταν εκτός δικτύου τράπεζας και συνεπώς δε «γνώριζε» ότι ο λογαριασμός είχε κλείσει[28].

Στα πλαίσια της παραποίησης δεδομένων, η «τεχνική του σαλαμιού, αποτελεί μία ενδιαφέρουσα παραλλαγή προσθήκης ενός συμπληρωματικού προγράμματος το οποίο διαστρεβλώνει αυτόματα τα νεοεισερχόμενα δεδομένα σε ένα σύστημα επεξεργασίας. Είναι ιδιαίτερα απλή σαν σύλληψη, αν και απαιτεί σχετικά πολύπλοκους χειρισμούς στην εφαρμογή της. Ο δράστης συντάσσει και εντάσσει στο λογισμικό ένα πρόγραμμα το οποίο αφαιρεί από κάθε οικονομική συναλλαγή χρηματικά μεγέθη τόσο μικρά κάθε φορά ώστε να μην γίνονται αντιληπτά από τους αισθητήρες του λογισμικού ή τον ελεγκτή που θα εστιάσει μία-προς-μία στις συναλλαγές αυτές. Για παράδειγμα, φροντίζει ώστε οι στρογγυλοποιήσεις των χρηματικών μεγεθών να είναι ανακριβείς. Συγχρόνως, έχει υπόψη του έναν λογαριασμό στον οποίο κατατίθενται αυτόματα οι διαφορές αυτές. Η τεχνική αυτή δεν στηρίζεται στο μέγεθος του ποσού που θα αφαιρεθεί αλλά στον αριθμό των αφαιρέσεων ποσών που θα πραγματοποιηθούν. Εδράζεται δε στην ιδιότητα της συγκεκριμένης ρουτίνας να επαναλαμβάνεται μόνιμα και αυτόματα για όσο χρονικό διάστημα δεν ανακαλύπτεται - ή δεν ακυρώνεται από το δράστη[29].

2.2 HACKING

Το hacking ως πρακτική και ως έννοια έχει εξελιχθεί σημαντικά κατά τη μεταπολεμική περίοδο. Σήμερα, το νόημά του εκτείνεται σε τέτοιο βαθμό ώστε να περιλαμβάνει ριζικά αντίθετες, αλληλοαναιρούμενες και αλληλοαποκλειόμενες αντιλήψεις οι οποίες αναφέρονται σε ριζικά διαφορετικές πραγματικότητες. Η έννοια του hacking μπορεί να αφορά από τον νόμιμο και έγκριτο δημιουργικό πληροφορικό προγραμματισμό έως μία

[28] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 127-128

[29] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 126-127

σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να ορισθούν ή ορίζονται ως παράνομες-εγκληματικές. Οπωσδήποτε παρατηρείται μία ένταση μεταξύ του κοινωνικού και του νομικού ορισμού της έννοιας του hacking. Όμως ιστορικά και αναλυτικά, ο κοινωνικός ορισμός του hacking ως τρόπου σκέψης και δράσης προηγείται του νομικού του ορισμού ως εγκλήματος. Είναι σαφώς ευρύτερος, χωρίς όμως αυτό να σημαίνει και ότι είναι «λογικότερος». Ο κάθε ορισμός αφορά σε διαφορετικές κοινωνικές ή άλλες ανάγκες.

Το hacking έγινε για πρώτη φορά αντιληπτό και ορίσθηκε ως διακριτή νοοτροπία, η οποία πρέπει να έχει ένα δικό της όνομα στις ολιγάριθμες επιστημονικές κοινότητες των εργαστηρίων ανάπτυξης της πληροφορικής τεχνολογίας κατά τη δεκαετία του 1950. Ως hack-ιστική (καινοτομική) ορίσθηκε μια ιδέα που αναδιατάσσοντας δεδομένα, δυνατότητες και αυτονόητα, κατάφερνε να εκτονώσει θεωρητικά και πρακτικά τη σύγχυση που προκαλούσε η αύξηση της γνώσης με τις καθιερωμένες μεθόδους. Αμέσως το hacking δε συνδέθηκε, με συγκεκριμένες ιδέες, αλλά με συγκεκριμένους ανθρώπους. Η σύνδεση αυτή μάλλον εδράζεται στην πεποίθηση ότι η hack-ιστική (καινοτομική) ιδέα δε μπορεί να αποτελέσει προϊόν μιας τυχερής στιγμής αλλά ότι αντίθετα, αποτελεί προϊόν βαθιάς γνώσης - αν και όχι απαραίτητα παντρεμένης με πολύχρονη εμπειρία. Γι' αυτό το λόγο και οι έννοιες του hacking και του hacker διαθέτουν αυτόνομο νόημα, ενώ η έννοια της hack-ιστικής (καινοτομικής) ιδέας ή ενέργειας είτε στερείται νοήματος είτε γίνεται αντιληπτή μόνον ως εξαρτημένη από τον παραγωγό της. Ο hacker αποτελεί άτομο με κατάρτιση και έντονο ενδιαφέρον για το αντικείμενο που τον προβληματίζει, όποιο και αν είναι το αντικείμενο αυτό. Επίσης, χαρακτηρίζεται από την προδιάθεση να ερευνήσει για λύσεις που μπορεί να μην προβλέπονται από τις επικρατούσες συμβατικές μεθόδους[30].

Η εισβολή σ' ένα δίκτυο υπολογιστών, το λεγόμενο hacking, αποτελεί βασικό στοιχείο πολλών διαδικτυακών εγκλημάτων. Ο hacker, έχει χαρακτηριστεί από πολλούς ως ο εγκληματίας του 21ου αιώνα. Η θεώρηση του hacking ως εγκλήματος, είναι ένα ζήτημα, που έχει νομικώς

[30] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ. 95-96

αντιμετωπιστεί με διαφορετικές προσεγγίσεις. Οι hackers επιδιώκουν να αποκτήσουν πρόσβαση σε ξένο υπολογιστή ή σύστημα υπολογιστών χωρίς, κατ' αρχήν, να έχουν το σκοπό της υποκλοπής ή της οποιασδήποτε άλλης επιβλαβούς ενέργειας. Όμως, η εισβολή στο δίκτυο, έστω και αν δεν είναι κακόβουλη, υποκρύπτει έναν κακόβουλο χαρακτήρα, διότι ο επιτιθέμενος εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλειά του, εντοπίζει τις ευπάθειές του και μπορεί, πλέον, ευκολότερα να διαπράξει μια κακόβουλη επίθεση ή να διαθέσει τις πληροφορίες αυτές σε κάποιον που θέλει να διαπράξει την επίθεση (Τσουραμάνης, 2005).

Η διείσδυση ενός hacker σ' ένα δίκτυο υπολογιστών, αποσκοπεί στην απομακρυσμένη διαχείριση του συστήματος-στόχου. Ανάλογα με τα δικαιώματα, που αποκτά ο επιτιθέμενος στο σύστημα-στόχο, μπορούμε να διακρίνουμε 2 βασικές κατηγορίες:

- Την πλήρη διείσδυση με δικαιώματα διαχειριστή συστήματος, και
- Τη διείσδυση με δικαιώματα απλού χρήστη συστήματος.

Στην πρώτη περίπτωση η επίθεση είναι πιο επικίνδυνη, γιατί ο επιτιθέμενος με δικαιώματα διαχειριστή έχει τη δυνατότητα να επιφέρει σημαντικές αλλαγές στη λειτουργία του συστήματος. Στη δεύτερη περίπτωση ο κίνδυνος είναι μικρότερος αλλά εξίσου σημαντικός.

Οι τεχνικές, που χρησιμοποιούν οι hackers για να διεισδύσουν σ' ένα δίκτυο ηλεκτρονικών υπολογιστών εξελίσσονται ταυτόχρονα με την ανάπτυξη των υπολογιστικών συστημάτων. Οι πιο συχνά χρησιμοποιούμενες είναι οι ακόλουθες:

Η εκμετάλλευση των cookies: : Τα cookies, είναι πολύ μικρά αρχεία κειμένου, τα οποία τοποθετούνται στον Η/Υ από διάφορες τοποθεσίες του Διαδικτύου που επισκέπτεται ένας χρήστης. Τα αρχεία αυτά, περιέχουν διάφορες πληροφορίες, όπως τα στοιχεία του χρήστη, οι δραστηριότητές του, οι συνήθειες του κ.λ.π. Στην περίπτωση, που σ' ένα αρχείο cookie εμπεριέχονται πληροφορίες, όπως το όνομα χρήστη και ο κωδικός πρόσβασης για μια υπηρεσία, ο hacker έχει την δυνατότητα να τις ανακτήσει εκμεταλλευόμενος κάποια γνωστή ευπάθεια του φυλλομετρητή ή του Λειτουργικού Συστήματος.

Ανίχνευση δικτυακών υπηρεσιών συστημάτων (probes, scans): Μια από τις βασικές ενέργειες των hackers είναι ο εντοπισμός πληροφοριών για το σύστημα στο οποίο θέλουν να επιτεθούν. Για να πετύχουν το σκοπό τους χρησιμοποιούν την τεχνική της σάρωσης θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστή, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας. Οι πληροφορίες αυτές είναι πολύ σημαντικές, γιατί δίνουν τη δυνατότητα στον επιτιθέμενο να παραβιάσει την ασφάλεια του συστήματος, εκμεταλλευόμενος γνωστές αδυναμίες π.χ. του λειτουργικού συστήματος ή άλλων υπηρεσιών που προσφέρονται. Η ανίχνευση, επίσης, μπορεί να αποσκοπεί στην εύρεση και αξιοποίηση λογαριασμών χρηστών που δεν προστατεύονται με κωδικό πρόσβασης, για να επιτευχθεί εύκολη πρόσβαση στο σύστημα.

Ανιχνευτές δικτυακών πακέτων (packet sniffers): Η ανίχνευση δικτυακών πακέτων, πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers, που έχουν τη δυνατότητα να εντοπίζουν όλα τα πακέτα, που κυκλοφορούν στο Διαδίκτυο. Εφόσον, τα πακέτα δεν είναι κρυπτογραφημένα, είναι δυνατή, η απόσπαση πληροφοριών, όπως κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών κ.ά. Επιπλέον, λαμβάνονται πληροφορίες που αφορούν την τοπολογία ενός δικτύου, τις υπηρεσίες που προσφέρονται και τον αριθμό των υπολογιστών, που είναι στο δίκτυο. Όλες οι πληροφορίες, είναι δυνατόν να αποσπασθούν από πακέτα που διακινούνται για την επιτέλεση καθημερινών εργασιών, η δε ανίχνευση τέτοιων επιθέσεων είναι εξαιρετικά δύσκολη.

Πλαστές διευθύνσεις IP (IP Spoofing): Στις επιθέσεις IP Spoofing, οι εισβολείς παρεμβαίνουν στις επικεφαλίδες των πακέτων που διακινούνται σε ένα δίκτυο και τις τροποποιούν ώστε το μήνυμα να φαίνεται ότι προήλθε από αξιόπιστη πηγή. Με την μέθοδο αυτή, επιτυγχάνουν να χρησιμοποιήσουν μια IP διεύθυνση μέσα στο εύρος των διευθύνσεων που εμπιστευόμαστε (εσωτερικές του δικτύου ή κάποιες από τις εξωτερικές) και να αποκτήσουν πρόσβαση σε δικτυακές υπηρεσίες, που προορίζονται για έμπιστους χρήστες του δικτύου. Η τεχνική IP Spoofing χρησιμοποιείται συνήθως σε συνδυασμό με άλλες τεχνικές επιθέσεως. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για

να αποκρύψει την πραγματική IP διεύθυνση του επιτιθέμενου σε μια επίθεση Ping of Death (παλιότερα), μια επίθεση Ping Flood, ή μια επίθεση Smurfe/Fraggle attack.

2.3 ΛΟΓΙΣΜΙΚΑ

Ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του Διαδικτύου, είναι η διασπορά κακόβουλου κώδικα (malicious code). Ο κακόβουλος κώδικας είναι κώδικας Η/Υ, που δημιουργείται με σκοπό να προκαλέσει ζημιά σε Η/Υ ή να εισχωρήσει σ' ένα Η/Υ, για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Ο κακόβουλος κώδικας, όταν εισχωρήσει σ' ένα Η/Υ, έχει την δυνατότητα:

- Να διαγράψει δεδομένα ή προγράμματα
- Να αλλοιώσει δεδομένα ή προγράμματα
- Να υποκλέψει δεδομένα και
- Να παρεμποδίσει τη λειτουργία ενός συστήματος (άρνηση εξυπηρέτησης).

Ο Sinrod (2000), διακρίνει τον κακόβουλο κώδικα σε τρεις βασικές κατηγορίες: *Ιούς*, (viruses), *σκουλήκια* (worms) και *δούρειους ίππους* (Trojan Horses).

Ιοί (viruses)

Οι ιοί, είναι το πιο συνηθισμένο είδος κακόβουλου κώδικα. Ένας ιός είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή, μια διαδικασία που είναι γνωστή ως μόλυνση. Μετά την μόλυνση, το αρχείο λειτουργεί κατά διαφορετικό τρόπο. Μπορεί, για παράδειγμα, να εμφανίζει ένα μήνυμα στην οθόνη, να τροποποιεί ή να διαγράφει αρχεία. Τα βασικά χαρακτηριστικά ενός ιού, είναι τα ακόλουθα:

- Αποτελείται από μια σειρά εντολών, που εκτελούν συγκεκριμένες κακόβουλες ενέργειες σε ένα υπολογιστή.

♦ Προσπαθεί να εγκατασταθεί σε κατάλληλη θέση στο σύστημα αρχείων του Η/Υ- θύματος, που θα του εξασφαλίζει, ότι οι οδηγίες του θα εκτελούνται κατά προτεραιότητα (π.χ. στο μητρώο του συστήματος) ώστε ο χρήστης να μην μπορεί να αντιληφθεί την εκτέλεση του. Κατ' αυτόν τον τρόπο ο εντοπισμός του λογισμικού γίνεται δυσχερής.

♦ Η εκτέλεσή του, έχει δυο βασικές λειτουργίες: Την αναπαραγωγή του και την πρόκληση ζημιάς (payload).

♦ Προσπαθεί να μολύνει προγράμματα, τα οποία είναι πιθανό να σταλούν ή να μεταφερθούν σε άλλο υπολογιστικό σύστημα.

Οι κυριότερες μορφές ιών είναι:

File-infectors ή parasitic viruses: Οι ιοί της μορφής αυτής, ενεργούν μολύνοντας ένα εκτελέσιμο πρόγραμμα, στο οποίο προσθέτουν τον κακόβουλο κώδικα. Παράλληλα γίνεται κάποια τροποποίηση του αρχείου-ξενιστή* ώστε να διασφαλιστεί ότι ο κώδικας του ιού θα εκτελεστεί πρώτος. Αυτού του είδους ο ιός, μολύνει αρχεία με επεκτάσεις : .com, .exe, .sys και .olv. Η μετάδοση του ιού γίνεται με οποιοδήποτε φυσικό μέσο αποθήκευσης (δισκέτα, CD-ROM κ.λ.π.) ή μέσω δικτύου.

Του ιούς της κατηγορίας αυτής, μπορούμε, περαιτέρω, να τους διακρίνουμε σε **memory-resident**, οι οποίοι παραμένουν στη μνήμη του υπολογιστή και έχουν τη δυνατότητα να μολύνουν οποιοδήποτε πρόγραμμα εκτελέσει ο χρήστης και σε **non-Resident ή direct-action viruses**, οι οποίοι δεν παραμένουν στη μνήμη του υπολογιστή, αλλά, προσκολλώνται σε ένα υπάρχον πρόγραμμα και μεταδίδονται όταν ο χρηστής εκτελέσει το πρόγραμμα αυτό.

Οι ιοί αυτοί, ήταν πολύ δημοφιλείς την εποχή των λειτουργικών συστημάτων MS-DOS.

Boot Sector Virus: Ο ιός, «μολύνει» εκτελέσιμο κώδικα συστήματος, που εντοπίζει σε συσκευές βοηθητικής μνήμης (π.χ. δίσκος, δισκέτα), στον Τομέα Εκκίνησης (boot sector) ή στο MBR (Master Boot Record) του δίσκου. Ως αποτέλεσμα, ο ιός φορτώνεται στη μνήμη κατά την εκκίνηση (boot) του

* Αρχείο ξενιστής ονομάζεται αυτό που αρχικά φιλοξενεί τον ιό.

συστήματος. Περαιτέρω, ο ιός ενεργεί μολύνοντας κάθε δίσκο ή δισκέτα, που θα χρησιμοποιηθεί τοπικά στον Η/Υ.

Κλασική περίπτωση του ιού αυτού είναι ο Michelangelo (1992) ο οποίος κατάφερε σε πολύ μικρό χρονικό διάστημα να πάρει μορφή επιδημίας. Οι ιοί αυτοί, ήταν ιδιαίτερα δημοφιλείς μέχρι την έλευση των Windows 95[31].

Multi-practice viruses: Ενεργούν συνδυάζοντας επιμέρους χαρακτηριστικά των δυο παραπάνω κατηγοριών. Έχουν τη δυνατότητα να μολύνουν εκτελέσιμα αρχεία καθώς και τομείς εκκίνησης, με αποτέλεσμα ένας Η/Υ να είναι δυνατόν να μολυνθεί είτε όταν εκκινήσει από μολυσμένο δίσκο είτε όταν εκτελεστεί ένα μολυσμένο πρόγραμμα.

Σκουλήκια (Worms)

Τα σκουλήκια είναι παρόμοια με τους ιούς. Ωστόσο, η βασική διαφορά τους είναι ότι τα σκουλήκια πολλαπλασιάζονται χωρίς να απαιτείται κάποια ενέργεια από τον χρήστη. Ένα σκουλήκι μπορεί να διαδοθεί μέσω του Διαδικτύου, χωρίς να χρειαστεί να επισυναφθεί σε κάποιο αρχείο.

Στην αρχική του μορφή, ένα σκουλήκι τροποποιεί ή διαγράφει αρχεία ενός υπολογιστή. Στη συνέχεια, δημιουργεί πολλαπλά αντίγραφα του εαυτού του και τα στέλνει στους Η/Υ των υποψήφιων θυμάτων.

Οι Δούρειοι Ίπποι

Οι Δούρειοι Ίπποι (Trojan Horses) είναι φαινομενικά, «αθώα» προγράμματα, τα οποία, έχουν μια ή περισσότερες κρυμμένες λειτουργίες οι οποίες δεν είναι εύκολο να εντοπιστούν από τους χρήστες. Τα προγράμματα αυτά, φορτώνονται στο σκληρό δίσκο του υπολογιστή και εκτελούνται, κανονικά, μαζί με τα υπόλοιπα προγράμματα. Πολλές φορές, ο κακόβουλος κώδικας των προγραμμάτων αυτών μπορεί να εμπεριέχεται στα λεγόμενα δημοφιλή προγράμματα.

---

[31] http://en.wikipedia.org/wiki/Michelangelo_%28computer_virus%29 [Ημερομηνία πρόσβασης 7-4-2011]

Με την χρήση ενός δούρειου ίππου ο επιτιθέμενος επιτυγχάνει να αποκτήσει έλεγχο του υπολογιστή του θύματος και να συλλέξει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή να εξαπολύσει μια επίθεση άρνησης εξυπηρέτησης.

Χαρακτηριστικό παράδειγμα της κατηγορίας αυτής, είναι το πρόγραμμα Back Orifice,[32] που εμφανίστηκε το 2000. Έφτανε στα υποψήφια θύματα με την μορφή συνημμένου αρχείου σε μήνυμα ηλεκτρονικού ταχυδρομείου, που όταν εκτελούνταν από το θύμα, εγκαθιστούσε στον υπολογιστή του ένα πρόγραμμα διακομιστή (server). Στη συνέχεια, ο επιτιθεμένος, εγκαθιστούσε στον δικό του υπολογιστή ένα πρόγραμμα πελάτη (client) και έδινε εντολές στον server του θύματος. Με τον τρόπο αυτό, εκτός από τον πλήρη έλεγχο του υπολογιστή του θύματος, ήταν ακόμη δυνατό ο επιτιθέμενος να διαπράξει διαδικτυακά εγκλήματα, τα οποία φαίνεται να τελέστηκαν από τον υπολογιστή του θύματός του (Sinrod, 2002).

Λογικές και ωρολογιακές βόμβες

Μια λογική βόμβα (logic-bomb) είναι ένα πρόγραμμα, το οποίο ενεργοποιείται, όταν συμβεί ένα συγκεκριμένο γεγονός. Το ενεργοποιημένο πρόγραμμα μπορεί να σταματήσει τη λειτουργία του υπολογιστή, να απελευθερώσει έναν ιό, να διαγράψει αρχεία ή να προβεί σε άλλες ζημιογόνες ενέργειες. Η ενεργοποίηση του προγράμματος γίνεται κατόπιν συγκεκριμένης ενέργειας από το χρήστη, είτε αυτόματα σε συγκεκριμένο χρόνο ή ημερομηνία, (ωρολογιακή βόμβα-time bomb).

Ανεπιθύμητη Αλληλογραφία (Spamming)

Η ανεπιθύμητη αλληλογραφία ή Spamming, ορίζεται ως η χρήση οποιοδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με

[32] http://www.irchelp.org/irchelp/security/bo.html [Ημερομηνία πρόσβασης 27-06-2011]

διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιουδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό από αυτόν που το λαμβάνει. Ένα μήνυμα spam, αποστέλλεται με e-mail και περιλαμβάνει πληροφορίες για την προώθηση των προϊόντων μιας εταιρείας. Στην πορεία, πολλές άλλες μορφές και μέσα διάδοσης ενοχλητικής ηλεκτρονικής αλληλογραφίας έχουν χρησιμοποιηθεί, όπως instant messaging spam, Usenet newsgroup spam, Web search engines spam, web logs spam, και mobile phone messaging spam.

Επιθέσεις σε δικτυακούς τόπους

Πρόκειται για ένα είδος επίθεσης, το οποίο παρουσίασε ιδιαίτερη αύξηση τα τελευταία χρόνια. Οι επιθέσεις αυτές, πραγματοποιούνται από τους βάνδαλους (vandals). Τα κίνητρα των επιθέσεων ποικίλουν. Κυρίως, στρέφονται εναντίον κυβερνητικών οργανισμών και υπηρεσιών.

Σε μια τυπική επίθεση σ' έναν δικτυακό τόπο, το αποτέλεσμα είναι αναστρέψιμο. Οι βάνδαλοι θα διαγράψουν ορισμένες σελίδες ή γραφικά και θα ανεβάσουν τις δικές τους σελίδες, το περιεχόμενο των οποίων, μπορεί να είναι από χιουμοριστικό έως προπαγανδιστικό. Όταν ο ιδιοκτήτης του δικτυακού τόπου αντιληφθεί ότι έχει υποστεί μια τέτοια επίθεση, θα διορθώσει τις προβληματικές σελίδες από εφεδρικά αρχεία. Το κρίσιμο ζήτημα, σ' αυτή την περίπτωση, είναι ο χρόνος που θα απαιτηθεί για την επιδιόρθωση. Αν οι ζημιές που προκλήθηκαν είναι μεγάλες, ίσως να χρειαστεί ο δικτυακός τόπος να παραμείνει εκτός δικτύου για μεγάλο χρονικό διάστημα.

Το πλήγμα, που θα δεχθεί η εταιρεία, όταν ο δικτυακός της τόπος, που ομολογουμένως αποτελεί την εικόνα της προς εξωτερικούς συνεργάτες και υποψήφιους πελάτες, πέσει θύμα μιας τέτοιας επίθεσης, είναι τεράστιο.

2.4 ΕΠΙΘΕΣΗ ΣΤΑ SOCIAL MEDIA

Η ανάπτυξη των κοινωνικών δικτύων τα τελευταία χρόνια, έχει οδηγήσει στην αύξηση του ηλεκτρονικού εγκλήματος, το οποίο στοχεύει στα κοινωνικά αυτά δίκτυα όπως είναι το facebook, το twitter κ.α. Σύμφωνα με το

Κέντρο Διαδικτυακών Παραπόνων των ΗΠΑ, από το 2006, περίπου 3.200 λογαριασμοί χρηστών έχουν δεχτεί κάποιας μορφής επίθεση. Η εξαπάτηση ξεκινάει με τη λήψη μηνύματος από κάποιο φίλο, ή ένα φαινομενικά αθώο link για βίντεο. Εάν ο χρήστης το ακολουθήσει, τότε οδηγείται σε ψεύτικα websites, στα οποία δίνει προσωπικά στοιχεία και κωδικούς (η διαδικασία αυτή ονομάζεται phishing). Από εκείνη τη στιγμή, οι απατεώνες πραγματοποιούν την ίδια επίθεση προς όλους τους χρήστες που περιλαμβάνονται στις λίστες διευθύνσεων. Σύμφωνα με μελέτη του πανεπιστημίου της Ιντιάνα, οι επιθέσεις phishing στα κοινωνικά δίκτυα έφταναν το 2005 ποσοστά επιτυχίας 70%. Οι λόγοι των επιθέσεων ποικίλλουν. Συχνά οι hackers επιθυμούν να καθοδηγήσουν τους χρήστες σε ιστοσελίδες το κέρδος των οποίων, καθορίζεται από τον αριθμό επισκεπτών. Ταυτόχρονα επιχειρούν να αποσπάσουν προσωπικές πληροφορίες όπως κωδικούς πρόσβασης σε τραπεζικούς λογαριασμούς[33].

Πολλές φορές οι hackers στοχεύουν σε συγκεκριμένα πρόσωπα ή υψηλόβαθμα στελέχη και συλλέγουν πληροφορίες για αυτούς μέσω κοινωνικών δικτύων και δημόσιων ηλεκτρονικών εργαλείων, όπως Google, Facebook, LinkedIn, Twitter κ.ά. Στη συνέχεια αποστέλλουν ένα email το οποίο απευθύνεται στο στόχο και προσβάλουν τον υπολογιστή του, δημιουργώντας μία κρυφή σύνδεση με τους διακομιστές τους. Τέτοιες επιθέσεις σπάνια είναι ανιχνεύσιμες και οι hackers παραμένουν για αρκετό καιρό στο δίκτυο και συλλέγουν πληροφορίες[34].

[33] Εφημερίδα Καθημερινή (2009). Στόχος εξαπάτησης τα social media. Ανακτημένο από: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_21/10/2009_303476

[34] http://www.secnews.gr/archives/11902

ΚΕΦΑΛΑΙΟ 3 : ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

3.1 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τα περισσότερα κράτη της Ευρωπαϊκής Ένωσης διαθέτουν νομοθεσία, η οποία προστατεύει την ιδιωτική σφαίρα από την ηλεκτρονική συλλογή και επεξεργασία προσωπικών δεδομένων. Τόσο η Σύμβαση της 28 Ιανουαρίου 1981 του Συμβουλίου της Ευρώπης «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα», όσο και η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» της 24 Οκτωβρίου 1995 υποχρεώνουν τα κράτη-μέλη να λάβουν τα αναγκαία μέτρα.

Η εφαρμογή της Ευρωπαϊκής Οδηγίας παρέχει προστασία για επεμβάσεις στην ιδιωτική σφαίρα από:

- ✓ την δημιουργία αρχείων με δεδομένα προσωπικού χαρακτήρα, τα οποία θα αποκτώνται με οποιονδήποτε τρόπο μέσω Διαδικτύου,
- ✓ την μεταφορά αρχείων με δεδομένα προσωπικού χαρακτήρα μέσω του Διαδικτύου,
- ✓ την συγκέντρωση και διασύνδεση τέτοιων αρχείων, τα οποία προέρχονται από διαφορετικούς ηλεκτρονικούς υπολογιστές συνδεδεμένους στο Διαδίκτυο

Στο Ελληνικό Σύνταγμα προστέθηκε με την πρόσφατη αναθεώρηση το άρθρο 9Α, σύμφωνα με το οποίο «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως ο νόμος ορίζει. Κατ' επιταγή της Οδηγίας 95/46/ΕΚ και της Σύμβασης της 28 Ιανουαρίου 1981 του Συμβουλίου της Ευρώπης εφαρμόζεται ο νόμος 2472/1997, που έχει ως αντικείμενο τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού

χαρακτήρα. Δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Αν το υποκείμενο των δεδομένων δεν μπορεί να προσδιοριστεί στο Διαδίκτυο, π.χ. μέσω του PET (Privacy enhanced technology), τότε τα δεδομένα αυτά δεν προστατεύονται (άρθρο 2). Επίσης ο νόμος δεν εφαρμόζεται, αν η επεξεργασία των δεδομένων γίνεται από κάποιο χρήστη του Διαδικτύου για την άσκηση δραστηριοτήτων προσωπικών ή οικιακών (άρθρο 3 παρ. 2). Ο νόμος δεν εφαρμόζεται τέλος στην περίπτωση που την επεξεργασία εκτελεί κάποιος χρήστης μη εγκατεστημένος στην Ελλάδα και η επεξεργασία δεν αφορά υποκείμενα εγκατεστημένα στην Ελλάδα, ούτε χρησιμοποιεί μέσα ευρισκόμενα στην Ελλάδα (βλ. άρθρο 3 παρ. 3).

Με βάση το άρθρο 4 τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο από το Διαδίκτυο, όχι μετά από παραβίαση του απορρήτου ή διείσδυση (hacking). Τα δεδομένα πρέπει να είναι ακριβή και να διατηρούνται μέχρις ότου είναι αναγκαίο σύμφωνα με τους όρους του άρθρου 4. Σε κάθε περίπτωση η επεξεργασία επιτρέπεται μόνο όταν το υποκείμενο έχει δώσει τη συγκατάθεσή του (π.χ. δεχθεί να απαντήσει στα «cookies»). Συγκατάθεση απαιτείται και όταν μια εταιρεία με πρόσβαση στο Διαδίκτυο συγκεντρώνει δεδομένα για ένα χρήστη, στον οποίο σκοπεύει να υποβάλει πρόταση κατάρτισης σύμβασης. Με βάση το άρθρο 6 όλοι οι εγκατεστημένοι στην Ελλάδα υπεύθυνοι επεξεργασίας πρέπει να γνωστοποιούν στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας, ακόμα και αν αυτό γίνεται στο Διαδίκτυο. Το άρθρο 7 απαγορεύει τη συλλογή και την επεξεργασία ευαίσθητων δεδομένων. Έτσι για παράδειγμα δεν μπορεί κάποιος να συλλέγει στοιχεία για τις -επισκέψεις- κάποιου χρήστη σε «διευθύνσεις;» με άσεμνο περιεχόμενο ή σε διευθύνσεις πολιτικών κομμάτων ή θρησκευτικών οργανώσεων κ.λπ., (εκτός αν συντρέχουν οι προϋποθέσεις του άρθρου 7 παρ. 2).

Πολύ σημαντική είναι η διάταξη του άρθρου 8 που επιτρέπει τη διασύνδεση αρχείων μόνο υπό ορισμένες προϋποθέσεις. Στο Διαδίκτυο η διασύνδεση αρχείων είναι πολύ εύκολη, δεδομένου ότι ολόκληρα αρχεία μέσω του πρωτοκόλλου μεταφοράς αρχείων, του ηλεκτρονικού ταχυδρομείου, μπορούν να μεταφερθούν και να τύχουν επεξεργασίας. Αν και είναι εξαιρετικά

δύσκολο κάτι τέτοιο, πρέπει να γίνει δεκτό ότι κάθε διασύνδεση αρχείων μέσω του Διαδικτύου πρέπει να γνωστοποιείται στην Αρχή. Σκόπιμο θα ήταν η άδεια της Αρχής να δίνεται μέσω του Διαδικτύου, μέσω του οποίου θα γίνεται και η προηγούμενη ακρόαση των υπευθύνων επεξεργασίας (8 παρ. 4). Τα προαναφερθέντα πρέπει να ισχύσουν και για τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός Ευρωπαϊκής Ένωσης σύμφωνα με τις διατάξεις του άρθρου 9 ν. 2472/1997.

Η επεξεργασία προσωπικών δεδομένων είναι απόρρητη (άρθρο 10). Αυτό σημαίνει ότι ο υπεύθυνος επεξεργαστής πρέπει να λάβει κάθε αναγκαίο μέτρο για τη θωράκισή της από κάθε πιθανή πρόσβαση. Δεν επιτρέπεται να διαδίδει το αποτέλεσμα της επεξεργασίας των προσωπικών δεδομένων μέσω του Διαδικτύου. Ο χρήστης-υποκείμενο των δεδομένων έχει τα δικαιώματα των άρθρων 11- 15, δηλαδή δικαίωμα α) ενημέρωσης, β) πρόσβασης, γ) αντίρρησης και δ) προσωρινής δικαστικής προστασίας. Οι κυρώσεις των άρθρων 21-23 επιβάλλονται και στους χρήστες που παραβιάζουν το νόμο 2472/1997 στο Διαδίκτυο.

Πρέπει πάντως να τονιστεί ότι κανένας νόμος δεν έχει ως στόχο τη νομιμοποίηση της συλλογής προσωπικών δεδομένων. Απλώς ρυθμίζει πότε αυτή επιτρέπεται. Αυτό που έχει ενδιαφέρον είναι οι εκάστοτε ισχύουσες προϋποθέσεις. Ζητούμενο είναι πώς μπορούμε να εξασφαλίσουμε, ανεξαρτήτως τεχνολογικών και λοιπών συνθηκών, το δικαίωμα του πολίτη να γνωρίζει, αν κάποιος συλλέγει προσωπικά του δεδομένα και για ποιον σκοπό, την κατά το δυνατό μεγαλύτερη ανωνυμία του και την κατά το δυνατόν αποφυγή της συλλογής και επεξεργασίας αυτών. Μ' αυτούς τους στόχους το κέντρο βάρους πρέπει να μετατοπιστεί βαθμιαία από την κλασσική νομική αντίδραση, δηλαδή τη λήψη νομοθετικών μέτρων, στην ίδια την τεχνολογία. Στόχος πρέπει να είναι η ανακάλυψη νέας τεχνολογίας, με την οποία θα προστατεύεται ο πολίτης, εφόσον θα μπορεί αυτός να ελέγχει και να καθορίζει τα της συλλογής προσωπικών του δεδομένων, καθορίζοντας για παράδειγμα ποιος μπορεί να έχει πρόσβαση σε αυτά (πχ με εγκατάσταση ειδικών φίλτρων), ελέγχοντας ο ίδιος ποιος, σε ποια περίπτωση και για ποιους λόγους λαμβάνει τα προσωπικά του δεδομένα (π.χ. με χρήση κρυπτογραφίας). Πρέπει να γίνει συνείδηση όμως ότι η εξέλιξη της προστατευτικής τεχνολογίας

έχει νόημα, μόνο αν συνδυαστεί με αναγκαστική ενσωμάτωσή της στα προϊόντα της πληροφορικής, ενώ είναι απαραίτητος ο συνδυασμός της με νομικούς στόχους και ειδικούς κανόνες για διασφάλιση της ανωνυμίας.

Σε μια δημοκρατική κοινωνία η γνώση ως αρχή (και η αναζήτηση της κατά το δυνατόν μεγαλύτερης ενημέρωσης για κάθε θέμα, ακόμα και για αυστηρά προσωπικά ζητήματα) θα πρέπει μάλλον να αντικατασταθεί με την άγνοια και το απαραβίαστο ορισμένων στοιχείων σύμφωνα με τη βούληση του ενδιαφερόμενου, κατοχυρωμένα από το νομοθέτη, προστατευόμενα από τα δικαστήρια και σεβαστά από την εκάστοτε επιτροπή για την προστασία προσωπικών δεδομένων. Επιπλέον, συνειδητά ασαφείς διατάξεις και γενικές ρήτρες στα εξεταζόμενα ζητήματα (όπως για παράδειγμα το επιτρεπτό της πρόσβασης για λόγους δημοσίου συμφέροντος) κρίνονται ως ακατάλληλες να ρυθμίσουν ζητήματα της κοινωνίας της πληροφορίας, αφού ανοίγουν το δρόμο συχνά σε πρόσβαση και σε μια πληθώρα άλλων περιπτώσεων μη επαρκώς καθοριζομένων, ώστε να δημιουργείται αίσθημα ανασφάλειας στον πολίτη. Γενικές διατάξεις θα πρέπει να αντικατασταθούν από άλλες λεπτομερειακές διατάξεις, από τις οποίες θα προκύπτει με σαφήνεια ποιος, πότε ακριβώς, σε ποια δεδομένα και με ποιο σκοπό θα έχει δικαίωμα πρόσβασης.

3.2 ΜΕΤΡΑ ΠΡΟΦΥΛΑΞΗΣ

Η πρόληψη, αποτελεί τη βασική συνιστώσα της ασφάλειας του πληροφοριακού συστήματος. Στοχεύει στην αποτροπή εκδήλωσης μιας επίθεσης, μέσω της αποθάρρυνσης του επιτιθέμενου και της αντίδρασης από το αρχικό στάδιο εκδήλωσης της επίθεσης. Τα μέτρα προφύλαξης παρουσιάζονται παρακάτω.

3.2.1 ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Τα συστήματα, που χρησιμοποιούν κωδικούς, απαιτούν την εισαγωγή από το χρήστη ενός ονόματος χρήστη (user ID) και ενός κωδικού πρόσβασης

(password) για να επιτρέψουν την είσοδο. Μετά την εισαγωγή των στοιχείων, το σύστημα κάνει έλεγχο των κωδικών με τη βάση δεδομένων από κωδικούς, που έχει από πριν αποθηκευτεί, και εφόσον διαπιστωθεί ταύτιση επιτρέπεται η είσοδος του χρήστη.

Η μέθοδος αυτή, είναι από τις πιο παλιές και λόγω της απλότητάς της αλλά και της μεγάλης ασφάλειας που προσφέρει (εφόσον βέβαια τηρούνται οι απαραίτητες προϋποθέσεις), τυγχάνει ευρείας εφαρμογής. Σήμερα, οι κωδικοί πρόσβασης αποτελούν αναπόσπαστο κομμάτι οποιουδήποτε λειτουργικού συστήματος.

Η διατήρηση της αξιοπιστίας ενός συστήματος, που χρησιμοποιεί κωδικούς πρόσβασης, εξαρτάται από ένα βασικό παράγοντα: κατά πόσο οι κωδικοί πρόσβασης μπορούν να παραμείνουν μυστικοί. Υπάρχουν αρκετοί τρόποι με τους οποίους ένας κωδικός πρόσβασης μπορεί να αποκαλυφτεί, όπως για παράδειγμα, με την χρήση απλών εργαλείων λογισμικού.[35] Επιπλέον, ο ίδιος ο χρήστης, με τις πράξεις και παραλείψεις του, μπορεί άθελα του να συμβάλει στην αποκάλυψη των κωδικών του.

Οι βασικότεροι κίνδυνοι εναντίον της ασφάλειας ενός τέτοιου συστήματος, που βασίζεται στην χρήση κωδικών πρόσβασης, είναι:

Η επιλογή των κωδικών πρόσβασης: Η ορθή επιλογή του κωδικού πρόσβασης είναι πολύ σημαντική. Όταν οι χρήστες αφήνονται μόνοι τους να επιλέξουν τους κωδικούς που επιθυμούν, προτιμούν κωδικούς που μπορούν εύκολα να θυμούνται (π.χ. ονόματα, ημερομηνίες γέννησης κ.λ.π.), με αποτέλεσμα κάποιος κακόβουλος να μπορεί να τους μαντέψει. Όταν η επιλογή των κωδικών δεν αφήνεται στους χρήστες, αλλά πραγματοποιείται από τους διαχειριστές ενός συστήματος, τότε επιτυγχάνεται μεγαλύτερη ασφάλεια, ενδέχεται όμως ο χρήστης, εάν ο κωδικός που του χορηγήθηκε είναι δύσκολο να απομνημονευτεί, να τον γράψει σε ένα κομμάτι χαρτί, διευκολύνοντας την διαρροή του εφόσον το χαρτί απολεσθεί ή κλαπεί.

Διαμοιρασμός των κωδικών πρόσβασης: Πολλές φορές, ένας υπάλληλος μπορεί να δώσει τον κωδικό του σε άλλο υπάλληλο, προκειμένου

[35] Π.χ. εργαλεία σπασίματος κωδικών όπως το Ophcrack, βλ. σχετικά http://ophcrack.sourceforge.net/ [Ημερομηνία πρόσβασης 23-6-2011]

αυτός να έχει πρόσβαση στα αρχεία του, στην συνέχεια, να δοθεί για τον ίδιο λόγο σε κάποιο τρίτο κ.ο.κ. Τέτοιου είδους διαμοιρασμός των κωδικών πρόσβασης εγκυμονεί κίνδυνους προερχόμενοι κυρίως, από το social engineering, οπότε κάποιος προσποιούμενος ότι είναι υπάλληλος μίας π.χ. θυγατρικής εταιρείας, επιτυγχάνει την απόκτηση των κωδικών.

Παρακολούθηση πακέτων: Η παρακολούθηση των πακέτων που διακινούνται στο δίκτυο, μπορεί να έχει ως αποτέλεσμα την ανάκτηση κωδικών πρόσβασης. Για παράδειγμα, η σύνδεση ενός απομακρυσμένου υπολογιστή με ένα κεντρικό υπολογιστή ενός προστατευμένου δικτύου, απαιτεί την εισαγωγή από το χρήστη κωδικών πρόσβασης, οι οποίοι, θα διακινηθούν μέσω του δικτύου.

Πρόσβαση στο αρχείο αποθήκευσης των κωδικών: Οι κωδικοί πρόσβασης αποθηκεύονται σε ένα αρχείο του διακομιστή, προκειμένου, να είναι δυνατή η διαδικασία ταυτοποίησης. Εφόσον το αρχείο αυτό δεν φυλάσσεται καλά ή δεν είναι κρυπτογραφημένο με μία hash function, ο επιτιθέμενος μπορεί να το ανακτήσει και να έχει, πλέον, στην κατοχή του όλους τους κωδικούς ενός οργανισμού.

3.2.2. ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

Η χρήση πακέτων λογισμικού κατά τον σχεδιασμό της ασφάλειας ενός συστήματος, αποτελεί πρωταρχική μέριμνα των διαχειριστών των συστημάτων. Οι πιο διαδεδομένες εφαρμογές είναι τα antivirus και firewalls.

- ✓ **Λογισμικό Antivirus**

Όπως έχει αποδειχθεί από πολλές έρευνες, η διασπορά ιών είναι η πιο διαδεδομένη μορφή επιθέσεων στο Διαδίκτυο. Καθημερινά, δημιουργούνται χιλιάδες νέοι ιοί, που απειλούν, ποικιλοτρόπως, τα υπολογιστικά συστήματα. Η πιο σημαντική μέθοδος αντιμετώπισης των ιών είναι η χρήση αντιβιοτικών προγραμμάτων (antivirus software).

Το λογισμικό αντιμετώπισης ιών, είναι ένα από τα πιο πολύπλοκα εργαλεία λογισμικού. Ένα τέτοιο λογισμικό, επιτελεί τρεις βασικές λειτουργίες:

Ανίχνευση των ιών: για να εξακριβωθεί, εάν έχει μολυνθεί από ιούς. Η διαδικασία αυτή, μπορεί να γίνει είτε κατόπιν ενέργειας του χρήστη, που επιλέγει μέσω του λογισμικού τον έλεγχο του σκληρού του δίσκου για ιούς, είτε, όπως συμβαίνει με τα σύγχρονα λογισμικά, πραγματοποιείται αυτόματα, καθώς, το λογισμικό φορτώνεται στην μνήμη RAM του συστήματος και ελέγχει όλες τις εφαρμογές που εκτελούνται.

Προσδιορισμός της ταυτότητας των ιών: Εάν το σύστημα έχει προσβληθεί από κάποιο ιό, το λογισμικό θα ενημερώσει το χρήστη για την ταυτότητά του. Η δυνατότητα αυτή είναι πολύ σημαντική, γιατί επιτρέπει να εκτιμηθεί το μέγεθος της ζημιάς που έχει προκληθεί, όσο και να εκτελεσθούν οι απαραίτητες ενέργειες, για την αποκατάσταση της ομαλής λειτουργίας του συστήματος.

Καθαρισμός των ιών: Στο τρίτο και τελευταίο στάδιο, αφού έχουν εντοπιστεί οι ιοί που μόλυναν το σύστημα, θα πρέπει να αφαιρεθούν. Τα περισσότερα λογισμικά, όταν έχουν εντοπίσει έναν ιό, προτείνουν στον χρήστη τι ακριβώς να κάνει. Οι πιο συνηθισμένες επιλογές είναι τρεις:

- να επιδιορθώσει το αρχείο που έχει μολυνθεί με τον ιό,
- να θέσει το αρχείο σε καραντίνα, ώστε να μην μπορεί να χρησιμοποιηθεί και
- να διαγράψει το αρχείο.

✓ **Firewalls**

Στην επιστήμη των υπολογιστών, ο όρος Firewall προσδιορίζει μια συσκευή ή εργαλείο λογισμικού (ή και συνδυασμό των ανωτέρω), που παρακολουθεί και φιλτράρει τα πακέτα που επιχειρούν είτε να εισέλθουν, είτε να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Είναι εργαλεία που ξεχωρίζουν ένα «ασφαλές» δίκτυο (π.χ. το Intranet μιας επιχείρησης), από ένα εξωτερικό μη ασφαλές δίκτυο, όπως είναι το Internet.

Τα περισσότερα Firewalls επιτελούν δυο βασικές λειτουργίες ασφαλείας:

Α) Φιλτράρισμα πακέτων (packet filtering) το οποίο βασίζεται στο να επιτρέπει ή να απαγορεύει (permit or deny) την κίνηση των πακέτων που διακινούνται στο δίκτυο, με βάση την υιοθετημένη πολιτική ασφαλείας και

Β) Πύλες εφαρμογών (Application proxy gateways), που προσφέρουν υπηρεσίες στους εσωτερικούς χρήστες και ταυτόχρονα προστατεύουν τους hosts από εξωτερικές απειλές.

3.2.3 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ

Η κρυπτογραφία (cryptography) αποτελεί μέρος της κρυπτολογίας (cryptology), της επιστήμης που ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο έτερος κλάδος της κρυπτολογίας, είναι η κρυπτανάλυση, που ασχολείται με την ανάλυση και το σπάσιμο των αλγορίθμων κρυπτογράφησης. Η κρυπτογραφία, σύμφωνα με τον ορισμό που δίνεται στη βικιπαίδεια,[36] είναι η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας.

Οι βασικότεροι στόχοι της κρυπτογραφίας στην γενικότερη ασφάλεια ενός συστήματος είναι η *εμπιστευτικότητα*[*] (confidentiality) η *αυθεντικοποίηση*[*] (authentication), η *ακεραιότητα*[*] (integrity)και *η μη αποποίηση παραλαβή – αποστολής*[*] (non redudiation).

Με την κρυπτογράφηση επιχειρείται η μετατροπή της πληροφορίας, από μια κατανοητή μορφή σε ένα γρίφο, ο οποίος παραμένει ακατανόητος. Με την αντίθετη διαδικασία, δηλαδή την αποκρυπτογράφηση, ο γρίφος αυτός επανέρχεται στην αρχική του μορφή και η πληροφορία μπορεί να αναγνωστεί.

Τα βασικά στοιχεία, που αποτελούν ένα σύγχρονο σύστημα κρυπτογράφησης είναι τέσσερα:

---

[36] www.wikipedia.gr

[*] Δηλαδή ότι το μήνυμα δεν θα διαρρεύσει σε άτομο ή άτομα που δεν έχουν δικαίωμα να το προσπελάσουν.

[*] Δηλαδή η επιβεβαίωση ότι το μήνυμα εστάλη από το άτομο που πραγματικά το έστειλε.

[*] Δηλαδή το μήνυμα θα φτάσει στον αποδέκτη του χωρίς να έχει αλλοιωθεί ή μετατραπεί.

[*] Δηλαδή ότι ο αποστολέας ή ο παραλήπτης του μηνύματος, δε θα αρνηθούν ότι έστειλαν ή ότι παρέλαβαν το μήνυμα.

α) Το αρχικό μήνυμα (plaintext)

β) Το κρυπτογραφικό σύστημα (cryptosystem) το οποίο αποτελείται από έναν αλγόριθμο κρυπτογράφησης και ένα αλγόριθμο αποκρυπτογράφησης.

γ) Το κρυπτογραφημένο κείμενο (ciphertext) το οποίο είναι το αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη.

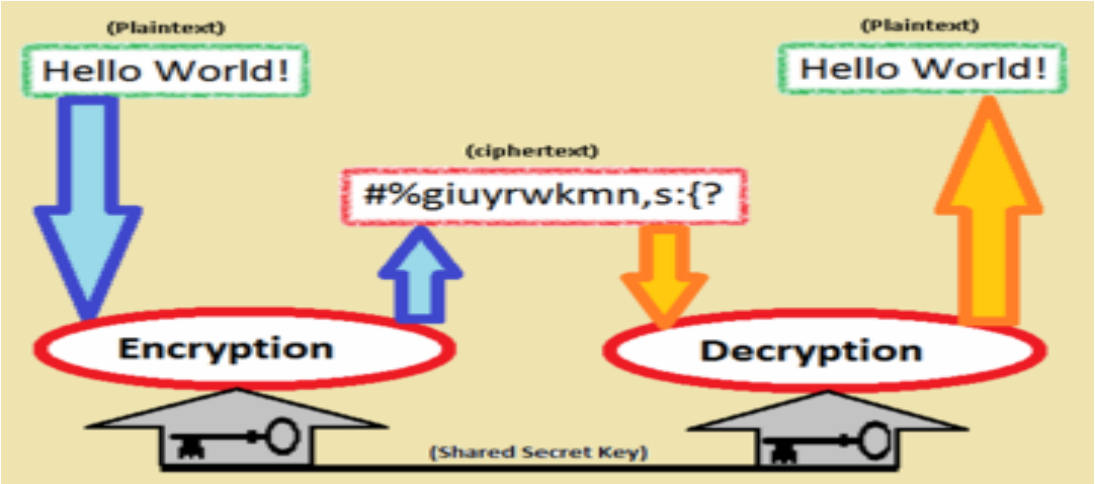
δ)Ένα κλειδί (key), το οποίο είναι μια συμβολοσειρά, η οποία χρησιμοποιείται από τους αλγόριθμοι στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.

Από τεχνικής απόψεως, η κρυπτογραφία διακρίνεται σε δύο βασικές κατηγορίες:

- Την συμμετρική κρυπτογραφία (symmetric cryptography) στην οποία χρησιμοποιείται ένα ιδιωτικό κλειδί και
- Την ασύμμετρη κρυπτογραφία (asymmetric cryptography) στην οποία χρησιμοποιούνται δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό.

✓ **Συμμετρική κρυπτογραφία**

Στη συμμετρική κρυπτογράφηση, το κύριο χαρακτηριστικό είναι ότι χρησιμοποιείται το ίδιο κλειδί, τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση των δεδομένων. Βασική προϋπόθεση αποτελεί, το κλειδί να έχει δοθεί στους χρήστες, που επιθυμούν να επικοινωνήσουν, μέσω ενός ασφαλούς καναλιού επικοινωνίας. Η διαδικασία επικοινωνίας έχει ως εξής: Το αρχικό μήνυμα κρυπτογραφείται με το μυστικό κλειδί του αποστολέα και αποστέλλεται στον παραλήπτη μέσω του καναλιού επικοινωνίας. Ο παραλήπτης παραλαμβάνει το κρυπτογραφημένο μήνυμα και το αποκρυπτογραφεί με το ίδιο μυστικό κλειδί.



Συμμετρική Κρυπτογραφία, όπου το ίδιο κλειδί χρησιμοποιείται και για την κρυπτογράφηση και την αποκρυπτογράφηση

- ✓ **Ασύμμετρη κρυπτογραφία**

Στην ασύμμετρη κρυπτογράφηση των δεδομένων, χρησιμοποιείται ένα κλειδί για την κρυπτογράφηση των δεδομένων και ένα διαφορετικό κλειδί για την αποκρυπτογράφηση. Κύριο χαρακτηριστικό των κλειδιών αυτών είναι, ότι αν και συσχετίζονται μεταξύ τους, η γνώση του ενός δεν μπορεί να οδηγήσει στην αποκάλυψη του άλλου. Το κλειδί, που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, ονομάζεται δημόσιο (public key) και είναι γνωστό σε όλους, ενώ το κλειδί με το οποίο γίνεται η αποκρυπτογράφηση, ονομάζεται ιδιωτικό (private key) και το κατέχει μόνον αυτός που θα κάνει την αποκρυπτογράφηση.

Η προστασία, που προσφέρεται με την ασύμμετρη κρυπτογράφηση, είναι πολύ πιο ισχυρή από την συμμετρική και, επιπλέον, δεν απαιτείται ασφαλής δίαυλος επικοινωνίας για την ανταλλαγή των κλειδιών. Όταν ένας χρήστης θέλει να λάβει ένα κρυπτογραφημένο μήνυμα, δίνει στον αποστολέα το δημόσιο κλειδί του, με το οποίο γίνεται η κρυπτογράφηση του μηνύματος, η δε αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί που μόνο αυτός κατέχει. Το πρόβλημα της μεθόδου αυτής είναι, ότι απαιτούνται πολύ μεγαλύτερα κλειδιά απ' ότι στην συμμετρική κρυπτογράφηση για τον ίδιο βαθμό ασφαλείας.

Χρησιμοποιώντας την ασύμμετρη κρυπτογραφία λίγο διαφορετικά, μπορεί να επιτευχθεί η ταυτοποίηση του αποστολέα ενός μηνύματος. Στην

περίπτωση αυτή, ο αποστολέας κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο με το δημόσιο κλειδί, που μπορεί να το έχει οποιοσδήποτε, αλλά η αρχική κρυπτογράφηση με το ιδιωτικό κλειδί, που συνηθίζει να λέγεται ψηφιακή υπογραφή, προσδιορίζει και μοναδικά τον αποστολέα αυτού.

Διαχείριση δημοσίων κλειδιών-πιστοποιητικά

Το πρόβλημα, που προκύπτει από τη χρήση δημοσίων κλειδιών κατά τη διαδικασία της κρυπτογράφησης, είναι το πώς θα εξακριβωθεί ότι το δημόσιο κλειδί, που λαμβάνει ένας χρήστης, είναι πράγματι αυθεντικό. Η εξακρίβωση αυτή, είναι πολύ σημαντική, διότι κατά την επαλήθευση μιας ψηφιακής υπογραφής, ο χρήστης πρέπει να είναι βέβαιος, ότι το δημόσιο κλειδί που χρησιμοποιεί για την επαλήθευση της υπογραφής, είναι πραγματικά το δημόσιο κλειδί του υποτιθέμενου υπογράφοντος. Χωρίς πρόσθετα μέτρα, θα πρέπει κάθε χρήστης να εξακριβώνει εξωσυστημικά την αυθεντικότητα κάθε δημόσιου κλειδιού, πριν επιλέξει να το εμπιστευθεί. Η πολυπλοκότητα του ζητήματος μπορεί να μειωθεί, εισάγοντας τη δυνατότητα εξακρίβωσης για τα δημόσια κλειδιά μέσω μιας τρίτης οντότητας, την οποία εμπιστεύονται και τα δύο μέρη. Η τρίτη οντότητα, που καλείται επίσης αρχή πιστοποίησης, υπογράφει με το δικό της ιδιωτικό κλειδί τα δημόσια κλειδιά και τα αντίστοιχα ονόματα, προσθέτοντας κάποια επιπλέον στοιχεία, π.χ. περίοδο εγκυρότητας. Το κομμάτι αυτό των δεδομένων, που έχει υπογραφεί από την αρχή πιστοποίησης, ονομάζεται πιστοποιητικό. Το πιστοποιητικό μπορεί να επαληθευτεί, χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης.

3.3 ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ

3.3.1 ΝΟΜΟΘΕΤΙΚΟΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ

- ✓ **Νομική προσέγγιση του Διαδικτύου**

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου, ενός «χώρου» τεράστιου και

αχανούς, με δυσδιάκριτα όρια και απεριόριστες δυνατότητες ανταλλαγής πληροφοριών. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω του Διαδικτύου, υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δυο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιαδήποτε προσπάθειας ρύθμισης του Διαδικτύου (Ζάννη, 2005)[37].

Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:

- Το Διαδίκτυο είναι ανοιχτό σε όλους και απαιτείται η ρύθμιση του για τον έλεγχο του παράνομου περιεχομένου του.
- Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.
- Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπιση της.
- Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.

Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα:

Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις.

Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.[38]

---

[37] Ζάννη Αν. (2005). Το διαδικτυακό έγκλημα. Αθήνα-Κομοτηνή: Εκδόσεις Αντ. Σάκκουλα

[38] Οι έννοιες αυτές αναφέρονται στο «Declaration of the Independence of Cyberspace» του John Perry Barlow. Διαθέσιμο από *w2.eff.org/~**barlow/Declaration**-Final.html* [Ημερομηνία πρόσβασης 03-06-2011]

Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντα αντιμέτωπη με το ζήτημα της λογοκρισίας.

Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις.

Το Διαδίκτυο, με άξονα τη βασική του χρήση ως μέσο επικοινωνίας, απασχόλησε τον νομοθέτη, ιδιαίτερα από το χρονικό σημείο που άρχισε να αναπτύσσεται και να επεκτείνεται. Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον Ο.Τ.Ε. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες (Καρακώστας, 2003)[39]. Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία με δυο Οδηγίες την 90/387[40] και την 90/388,[41] κατήργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιοδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες.

Η προσαρμογή της ελληνικής νομοθεσίας προς τις παραπάνω οδηγίες της Ευρωπαϊκής Κοινότητας, προήλθε, κατ' αρχήν, με τον Ν. 2075/92. Ο νόμος αυτός, πολύ σύντομα καταργήθηκε με τον νέο Ν. 2246/94 και στη συνεχεία με το Ν. 2867/2000, που ως σήμερα είναι σε ισχύ. Με το νόμο αυτό, ιδρύθηκε ρυθμιστική αρχή, η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με αποστολή τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η Αρχή αυτή έχει τη δυνατότητα να ελέγχει τους παρόχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους.

---

[39] Καρακώστας Ι. (2003). Δίκαιο & Internet. Νομικά ζητήματα στο Διαδίκτυο. Αθήνα : Σάκκουλα, σελ 55-58

[40] Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision-ONP).

[41] Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

- ✓ **Το ζήτημα της δικαιοδοσίας στο Διαδίκτυο**

Στο χώρο του Διαδικτύου, το ζήτημα περιπλέκεται. Με τη χρήση ενός Η/Υ, ένα άτομο που βρίσκεται σε οποιοδήποτε σημείο του κόσμου, μπορεί να διαπράξει έγκλημα στην Αμερική. Επομένως, στον κυβερνοχώρο η έννοια της γεωγραφικής κυριαρχίας δεν μπορεί να τύχει εφαρμογής. Οι διακινούμενες πληροφορίες, μέσω του Παγκόσμιου Ιστού και άλλων υπηρεσιών του Διαδικτύου δε στοχεύουν σε ένα συγκεκριμένο αποδέκτη, αλλά διανέμονται ταυτόχρονα σε ένα παγκόσμιο κοινό, επηρεάζοντας μεμονωμένα άτομα και οργανισμούς, που ανήκουν σε διαφορετικές δικαιοδοσίες και υπάγονται σε τελείως διαφορετικό νομικό πλαίσιο (Lakshminarayan, 2001).[42]

Μπορούμε να θεωρήσουμε ότι το ζήτημα της δικαιοδοσίας στο Διαδίκτυο, καθορίζεται από τρεις διαφορετικές νομικές πηγές: Καταρχήν, ισχύουν βέβαια οι εθνικές νομοθεσίες, οι οποίες και καθορίζουν κάποιους βασικούς κανόνες. Επίσης, υπάρχουν διεθνείς συμφωνίες οι οποίες προσπαθούν να ρυθμίσουν το θέμα της δικαιοδοσίας σε πολυεθνικό επίπεδο. Τέλος, υπάρχουν οι αποφάσεις των δικαστηρίων. Η νομολογία αυτή έχει ιδιαίτερη βαρύτητα, διότι σε αυτή εφαρμόζεται η ισχύουσα νομοθεσία ενώ μέσα από τις δικαστικές αποφάσεις, εντοπίζονται προβλήματα, αλλά και παρουσιάζονται ερμηνείες του υφιστάμενου νομοθετικού πλαισίου, που ο νομοθέτης δεν είχε βέβαια υπ' όψιν του.

3.3.2 Η ΔΙΚΑΙΟΔΟΣΙΑ ΣΤΗΝ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

Στην Ευρωπαϊκή Ένωση, η δικαιοδοσία δεν αφήνεται στη κρίση των δικαστηρίων, αλλά βασίζεται σε συγκεκριμένη νομοθεσία. Το βασικό νομοθετικό κείμενο για τον προσδιορισμό της δικαιοδοσίας είναι η Συνθήκη

[42] Lakshminarayan, S. (2001). Jurisdiction and the Internet. Ministry of Information Technology, Government of India. Διαθέσιμο στο http://www.cis-india.org/advocacy/igov/blog/what-are-the-legal-provisions-for-blocking-websites-in-india [Ημερομηνία πρόσβασης 10-5-2011]

των Βρυξελλών[43] (1968), η οποία θέτει τους ακόλουθους βασικούς κανόνες (Glandstone, 2003)[44]:

Ένα άτομο που ζει μόνιμα σε κάποιο κράτος-μέλος της Ευρωπαϊκής Ένωσης, μπορεί να ενταχθεί σε αυτό.

Σε υπόθεση παραβίασης συμβατικής υποχρέωσης, ένα άτομο μπορεί να ενταχθεί στον τόπο, όπου έλαβε χώρα η υποχρέωση, που τίθεται υπό αμφισβήτηση.

Σε αστικά ζητήματα, ένα άτομο μπορεί να ενταχθεί στον τόπο, όπου έλαβε χώρα το ζημιογόνο αποτέλεσμα

Ένας καταναλωτής, μπορεί να ενταχθεί μόνο στον τόπο που ζει μόνιμα, μπορεί όμως να επιλέξει την μεταφορά της υπόθεσης στον τόπο μόνιμης κατοικίας του αντιδίκου, εφόσον σε αυτόν υπέστη μεγαλύτερη ζημία.

Σε συμβάσεις, που δεν εμπλέκεται μόνο ένας καταναλωτής, οι αντίδικοι μπορούν να συμφωνήσουν για τον τόπο εκδίκασης της υπόθεσης.

3.3.3 Η ΕΥΡΩΠΗ ΑΠΕΝΑΝΤΙ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος στον Ευρωπαϊκό χώρο, πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης, το 1976 στο Στρασβούργο, στις εργασίες του Συνεδρίου για τις Εγκληματικολογικές Πλευρές του Οικονομικού Εγκλήματος. Ήταν η πρώτη φορά που παρουσιάστηκαν οι μορφές του ηλεκτρονικού εγκλήματος, συμπεριλαμβανόμενης και της απάτης.

Το 1986, συστήθηκε μια επιτροπή από το Ευρωπαϊκό Συμβούλιο, η οποία εξέτασε την ισχύουσα νομοθεσία στα κράτη-μέλη, τα δε συμπεράσματά της συμπεριλήφθησαν στη Σύσταση του 1989, η οποία όριζε εγκληματικές

[43] Βλ. το πλήρες κείμενό της στο http://curia.europa.eu/common/recdoc/convention/en/c-textes/brux-idx.htm [Ημερομηνία πρόσβασης 10-5-2011]

[44] Glandstone, J. (2003). Determining jurisdiction in Cyberspace: The “Zippo” Test of the “Effects” Test? Informing Science Institute. Διαθέσιμο στο *http://www.informingscience.org/proceedings/IS2003Proceedings/docs/029Glads.pdf* [Ημερομηνία πρόσβασης 10-5-2011].

πράξεις, όπως απάτη και πλαστογραφία με ηλεκτρονικούς υπολογιστές, καταστροφή δεδομένων και λογισμικού, μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη αναπαραγωγή λογισμικού κ.ά. Επίσης, η Σύσταση αυτή περιελάμβανε και μια σειρά από Οδηγίες (μη υποχρεωτικές) προς τα κράτη-μέλη, σχετικά με τη μεθοδολογία θέσπισης νομοθετικών κειμένων για το ηλεκτρονικό έγκλημα.

Το Συμβούλιο της Ευρώπης αντιμετώπισε αποφασιστικότερα το ζήτημα της νομοθεσία για το ηλεκτρονικό έγκλημα το 1996, εκδίδοντας δύο Συστάσεις: (α) τη Σύσταση No K(89)9 σχετικά με το έγκλημα που διαπράττεται με τη χρήση ηλεκτρονικού υπολογιστή και την (β) τη Σύσταση No K(95)13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των ηλεκτρονικών υπολογιστών. Οι συστάσεις αυτές αποτέλεσαν την βάση για την Σύμβαση για τον Κυβερνοχώρο του 2001 (Akdeniz, 2001)[45].

Στην Ευρωπαϊκή Ένωση σήμερα ισχύουν[46]:

Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.

Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.

Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.

---

[45] Akdeniz, Y. (2004). Advocacy Handbook for the Non Governmental Organizations. The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems. Διαθέσιμο στο http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf [Ημερομηνία πρόσβασης 10-5-2011].

[46] Δίκτυα Υπολογιστών και Νομικό Πλαίσιο (2011). Διαθέσιμο στο *utopia.duth.gr/~kdrakato/thesis/chapter5.doc* [Ημερομηνία πρόσβασης 12-5-2011].

Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.

Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.

Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

3.4 «ΠΕΡΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ο νόμος 3431/2006 «Περί Ηλεκτρονικών Επικοινωνιών», ενσωματώνει στο εθνικό δίκαιο μια σειρά από οδηγίες της Ευρωπαϊκής Ένωσης, σχετικές με τον έλεγχο των ηλεκτρονικών επικοινωνιών οποιασδήποτε μορφής. Βασικές επιδιώξεις του νόμου, είναι η απελευθέρωση της αγοράς των τηλεπικοινωνιών και η υιοθέτηση κανόνων για τον έλεγχο των επιχειρήσεων-οργανισμών, που προσφέρουν τηλεπικοινωνιακές υπηρεσίες. Επίσης, δίνεται ιδιαίτερη βαρύτητα, στην προστασία του χρήστη έναντι κάθε παράνομης δραστηριότητας, καθώς υποχρεώνει του πάροχους να λάβουν κάθε απαραίτητο μέτρο, ώστε να εξασφαλιστεί υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.

Με το νόμο αυτό ενδυναμώνεται η *Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων* (Ε.Ε.Τ.Τ.) η οποία πλέον, αποτελεί ανεξάρτητη αρχή και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας. Οι αρμοδιότητες της εκτείνονται σε όλο το φάσμα των ηλεκτρονικών επικοινωνιών. Όσον αφορά τον κυβερνοχώρο, η Ε.Ε.Τ.Τ. είναι αρμόδια για την καταχώρηση ονομάτων χώρου με καταλήξεις .gr και .eu, καθώς και για τη ρύθμιση όλων των θεμάτων που σχετίζονται με τις ηλεκτρονικές υπογραφές.

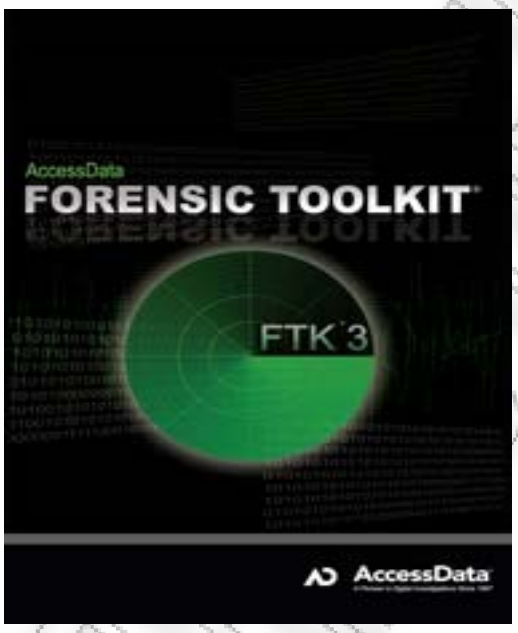
3.5 ΕΡΓΑΛΕΙΑ ΓΙΑ ΕΞΙΧΝΙΑΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Σήμερα θεωρείται δύσκολη η προληπτική αποτροπή του μεγαλύτερου αριθμού των ψηφιακών εγκλημάτων. Η αποτελεσματική εξιχνίαση των ψηφιακών εγκλημάτων και η σωστή απόδοση δικαιοσύνης, είναι η καταλληλότερη προσέγγιση και για την αποτροπή τους. Η διερεύνηση των ψηφιακών εγκλημάτων (digital forensics) αποσκοπεί στην εξασφάλιση και αξιοποίηση ψηφιακών-ηλεκτρονικών αποδεικτικών στοιχείων, με σκοπό να γίνει η μεταγενέστερη επίκλησή τους στην ποινική δικαιοσύνη. Προς την κατεύθυνση αυτή, απαιτείται η αναγνώριση των ψηφιακών πειστηρίων, η συλλογή, η ενδελεχής παρατήρηση και η ασφαλής διατήρησή τους και η ανάλυση και προσεκτική επαλήθευσή τους.

Για να ξεκινήσει η διερεύνηση των ψηφιακών εγκλημάτων, απαιτείται να προηγηθεί καταγγελία για την τέλεσή τους και να εκδοθεί ένταλμα εισαγγελικής έρευνας. Ο ειδικός που συνοδεύει τον εισαγγελέα και τους αστυνομικούς, θα πρέπει να αναγνωρίσει τα ψηφιακά αποδεικτικά στοιχεία που βρίσκονται στον υπό έρευνα χώρο, να τα καταγράψει λεπτομερώς επιτόπου, να τα αφαιρέσει από εκεί που βρίσκονταν, προσέχοντας παράλληλα να μην τα αχρηστεύσει ή τα παραποιήσει κάνοντας κάποιο λάθος χειρισμού και να τα συνοδέψει στον τομέα εξέτασης ψηφιακών πειστηρίων για ανάγνωση, εξέταση, αρχειοθέτηση και αξιολόγηση.

Τα ψηφιακά αποδεικτικά στοιχεία βρίσκονται σε αποθηκευτικά μέσα, όπως οι σκληροί δίσκοι, οι δισκέτες, τα CD-ROM και τα DVD, αλλά μπορεί να βρίσκονται και σε λιγότερο προφανή μέσα, όπως compact flash cards, PCMCIA κάρτες, USB memory sticks κ.ά. Τα δεδομένα των σκληρών δίσκων, ευρισκόμενα σε επανεγγράψιμα μέσα, πρέπει να αντιγραφούν σε άλλους δίσκους και σε καμία περίπτωση δεν πρέπει να γίνει επανεκκίνηση του υπολογιστή που κατασχέθηκε. Κατά την εκκίνηση, ένας υπολογιστής ενημερώνει διάφορα στοιχεία στα αρχεία του συστήματος και σβήνει διάφορα προσωρινά αρχεία γεγονός που μπορεί να οδηγήσει στην καταστροφή αποδεικτικών στοιχείων ή σε ισχυρισμούς, κατά την εκδίκαση της υπόθεσης στο δικαστήριο, περί μεταβολής του περιεχομένου τους.

Προκειμένου να αναγνωριστούν τα δεδομένα από το αντίγραφο του δίσκου, μπορούν να χρησιμοποιηθούν προγράμματα όπως το Forensic Toolkit, το Cyber Security Technologies P2P Marshal Field Edition και το Technology Pathways ProDiscover Incident Response τα οποία παρέχουν τη δυνατότητα να διαβαστεί το αντίγραφο ενός δίσκου και να βρεθούν συγκεκριμένα αρχεία, αλλά και να επαναφερθούν σβησμένα αρχεία.



FTK: Μία εξαιρετική και πολύ ακριβή εφαρμογή (από τις πληρέστερες της αγοράς), εργαλείο για την εξιχνίαση ηλεκτρονικών εγκλημάτων

Για την αποφυγή γραψίματος σε δίσκους υπό εξέταση, υπάρχουν συσκευές που εξουδετερώνουν κάθε προσπάθεια του συστήματος να γράψει στη συσκευή. Πέραν των λύσεων hardware όμως, υπάρχει η δυνατότητα χρήσης λογισμικού, για το κλείδωμα των εγγραφών στους δίσκους. Το ψάξιμο για στοιχεία στο δίσκο με τη χρήση Linux, χρησιμοποιεί πολλές εντολές και μικρά προγράμματα ή scripts, που δέχονται regular expressions, προσφέροντας εξαιρετικές δυνατότητες εντοπισμού στοιχείων, αρχειοθέτησης των ευρημάτων και καταγραφής όλων των βημάτων της έρευνας[47].

[47] Τσουραμάνης Χ. (2005). Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου. Αθήνα: Κατσαρού σελ 143-145

3.6 Η ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ

Η ηλεκτρονική τεχνολογία εκτός από τη μετάδοση της ανθρώπινης σκέψης επεξεργάζεται και μεθόδους, οι οποίες θα μπορέσουν να εγγυηθούν την ασφαλή διαπίστωση του προσώπου που φέρεται ότι έχει υπογράψει το κείμενο. Έτσι ορίζεται η ηλεκτρονική υπογραφή ως το σύνολο των συμβόλων με τα απαραίτητα χαρακτηριστικά για τον προσδιορισμό του προσώπου που έχει υπογράψει με τη μέθοδο αυτή το ηλεκτρονικό μήνυμα. Ο πρότυπος νόμος της UNCITRAL για τις συμβάσεις EDI αναγνωρίζει στο άρθρο 7 την ηλεκτρονική υπογραφή ως μέσο για την εξακρίβωση του εκδότη και επιβεβαιώσεως του γεγονότος ότι αυτός αναγνωρίζει το περιεχόμενο του εγγράφου. Η ηλεκτρονική υπογραφή λειτουργεί στο Διαδίκτυο ως εξής: η εικόνα της υπογραφής, δηλαδή τα γράμματα, τα σύμβολα ή οι χαρακτήρες, τα οποία δημιουργούνται ή υιοθετούνται από ένα μέρος, με σκοπό να καταστήσουν γνήσιο ένα έγγραφο, για να χαρακτηρισθούν ως ηλεκτρονική υπογραφή, πρέπει απλώς να έγιναν φανερά σε τρίτους μέσω του Διαδικτύου.

Για την εξασφάλιση της γνησιότητας της ηλεκτρονικής υπογραφής τα μέρη δημιουργούν το ηλεκτρονικό μέσο αναγνωρίσεως της ταυτότητάς τους με τη βοήθεια κρυπτογραφικών κωδίκων. Μια μέθοδος κρυπτογραφήσεως ηλεκτρονικών δεδομένων για την παραγωγή ηλεκτρονικής υπογραφής στηρίζεται στη χρήση ασύμμετρου κρυπτογραφικού συστήματος. Η ιδιαίτερη αυτή μέθοδος αναγνωρίσεως του εκδότη εγγράφου, που παράγεται μέσω ηλεκτρονικών υπογραφών, ονομάζεται ψηφιακή υπογραφή. Την ορολογία αυτή χρησιμοποιούν ο νόμος περί ψηφιακής υπογραφής του 1995 της πολιτείας Γιούτα, ο νόμος περί ηλεκτρονικής υπογραφής της Φλόριντα (Florida Electronic Signature Act του 1996) καθώς και ο γερμανικός νόμος του 1997, ο οποίος ορίζει ρητά ότι ψηφιακή υπογραφή είναι η μέθοδος αναγνώρισης του εκδότη ηλεκτρονικού εγγράφου, όταν προς το σκοπό αυτό χρησιμοποιείται η ασύμμετρη κρυπτογράφηση. Ο όρος λοιπόν «ψηφιακή υπογραφή» είναι έννοια είδους σε σχέση με τον όρο «ηλεκτρονική υπογραφή», για την οποία χρησιμοποιούνται και συμμετρικά κρυπτογραφικά συστήματα. Τα συμμετρικά κρυπτογραφικά συστήματα χρησιμοποιούν συμμετρικούς αλγόριθμους δηλαδή αλγόριθμους με αποκλειστικά ιδιωτικό κλειδί (μέθοδος DES, Data Encryption Standard). Αντίθετα οι ασύμμετροι

αλγόριθμοι έχουν και δημόσιο και ιδιωτικό κλειδί (μέθοδος RSA). Το δημόσιο κλειδί είναι γνωστό σε όλους τους συναλλασσόμενους ενώ το ιδιωτικό κλειδί το γνωρίζει αποκλειστικά ο υπογράφων.

Το πρώτο νομοθετικό κείμενο που ρύθμισε την ψηφιακή υπογραφή βασισμένη στη μέθοδο των ασύμμετρων αλγορίθμων είναι ο νόμος περί ψηφιακής υπογραφής της πολιτείας Γιούτα των ΗΠΑ ο οποίος ισχύει από τις 9 Μαρτίου 1995. Ο νόμος αυτός επιτρέπει τη συγκρότηση οργανισμών, δημοσίου ή ιδιωτικού δικαίου, οι οποίοι κατόπιν αδείας του Υπουργείου Εμπορίου, μπορούν να εκδίδουν πιστοποιητικά σχετικά με την ταυτότητα συγκεκριμένου συνδρομητή τους. Τα πιστοποιητικά βεβαιώνουν ότι συγκεκριμένο δημόσιο κλειδί ανήκει σε ορισμένο πρόσωπο και παρέχει όλα τα αναγκαία στοιχεία για τη χρησιμοποίησή του στην αποκρυπτογράφηση της ψηφιακής υπογραφής του αποστολέα εγγράφου. Οι οργανισμοί αυτοί υποχρεούνται να τηρούν αρχεία τουλάχιστον για 40 χρόνια. Το ιδιωτικό κλειδί ανήκει στην ιδιοκτησία του συνδρομητή, ο οποίος είναι υπεύθυνος για την ασφαλή τήρησή του. Ο νόμος καθιερώνει επίσης νόμιμο τεκμήριο, σύμφωνα με το οποίο η αποκρυπτογράφηση ενός μηνύματος με τη χρησιμοποίηση του δημόσιου κλειδιού, όπως είναι αυτό καταχωρημένο στο πιστοποιητικό που βεβαιώνει την αντιστοιχία του συγκεκριμένου δημόσιου κλειδιού και του συνδρομητή και συγχρόνως αποστολέα του μηνύματος, θεωρείται ως αναγνώριση της γνησιότητας της υπογραφής. Το τεκμήριο ανατρέπεται, αν αποδειχθεί ότι η ψηφιακή υπογραφή δεν μπορεί να αποκρυπτογραφηθεί με το δημόσιο κλειδί ή αν ο δικαιούχος ιδιωτικού κλειδιού έχει απολέσει τον αποκλειστικό έλεγχό του κατά το χρόνο θέσεως της υπογραφής. Αν δεν ανατραπεί το τεκμήριο, τότε το ηλεκτρονικό έγγραφο ισχύει όπως το χάρτινο.

3.6.1 Η ΕΥΡΩΠΑΙΚΗ ΕΜΠΕΙΡΙΑ

Σε Ευρωπαϊκό επίπεδο έχουν ήδη ληφθεί νομοθετικές πρωτοβουλίες σχετικά με την καθιέρωση της ηλεκτρονικής υπογραφής. Ο πρώτος νόμος για την ψηφιακή υπογραφή σε επίπεδο κράτους ψηφίστηκε από το ιταλικό κοινοβούλιο στις 15 Μαρτίου 1997. Το άρθρο 15 του νόμου αυτού παρέχει πλήρη αναγνώριση των πράξεων, δεδομένων, εγγράφων (ιδιωτικών και

δημόσιων) και συμβάσεων καθώς και της αρχειοθέτησης, διαβίβασης και αναπαραγωγής τους με ηλεκτρονικά μέσα και μάλιστα όχι μόνο στις σχέσεις μεταξύ ιδιωτών αλλά και όσον αφορά τη δημόσια διοίκηση. Ο νόμος προβλέπει την έκδοση πιστοποιητικών σχετικά με την ταυτότητα των ηλεκτρονικά συμβαλλομένων με τη βοήθεια συμβολαιογράφων και μιας ανεξάρτητης διοικητικής αρχής, της Αρχής για την πληροφορική της δημόσιας διοίκησης. Προβλέπεται επίσης η τήρηση αρχείων από τις διοικητικές αρχές για τις δημόσιες κλείδες.

Ο γερμανικός νόμος της 22ας Ιουλίου 1997 σχετικά με τη ρύθμιση των όρων για τις πληροφοριακές και επικοινωνιακές υπηρεσίες προβλέπει ένα ιδιαιτέρως αναλυτικό πλαίσιο για την ψηφιακή υπογραφή. Οι 16 παράγραφοι του άρθρου 3 έχουν ως σκοπό τη διασφάλιση της γνησιότητας των ψηφιακών υπογραφών και τον αποκλεισμό αλλοίωσης των υπογεγραμμένων μηνυμάτων. Ειδικότερα προβλέπεται η χορήγηση από δημόσια αρχή εξατομικευμένης μυστικής κλείδας σε φυσικά πρόσωπα, η οποία κρυπτογραφεί το μήνυμα σε αλγοριθμικό σύστημα.

Ο παραλήπτης από την άλλη μεριά αποκρυπτογραφεί με άλλο κλειδί το μήνυμα, χωρίς να είναι σε θέση να το αλλοιώσει. Σύμφωνα με την παράγραφο 1 σκοπός του νόμου είναι να θέσει τις γενικές αρχές που εξασφαλίζουν τη γνησιότητα των ψηφιακών υπογραφών. Με βάση το άρθρο 3 παρ. 2 υιοθετείται το ασύμμετρο αλγοριθμικό σύστημα με τη χρήση δημόσιας και μυστικής κλείδας. Μια ανεξάρτητη διοικητική αρχή για τις τηλεπικοινωνίες χορηγεί άδεια σε φυσικά ή νομικά πρόσωπα, τα οποία θα μπορούν με τη σειρά τους να πιστοποιούν τη χορήγηση της δημόσιας κλείδας σε κάποιο χρήστη του Διαδικτύου. Με την παράγραφο 4 προβλέπονται αυστηρές προϋποθέσεις για τη χορήγηση αδειών, ενώ με την παράγραφο 5 ορίζονται οι προϋποθέσεις για τη χορήγηση των πιστοποιητικών. Τα πιστοποιητικά πρέπει να περιέχουν το όνομα του δικαιούχου, τη δημόσια κλείδα, τους αλγόριθμους χρήσης της κλείδας, τον αριθμό του πιστοποιητικού, την ημερομηνία έναρξης και λήξης των πιστοποιητικών, το όνομα του παρόχου υπηρεσιών πιστοποίησης καθώς και τυχόν περιορισμούς της χρήσης του πιστοποιητικού (αρ. 3 παρ. 7). Το άρθρο 3 παρ. 8 προβλέπει την έκτακτη διακοπή της ισχύος των πιστοποιητικών κατόπιν αιτήσεως του δικαιούχου ή της Αρχής των

τηλεπικοινωνιών, καθώς και στην περίπτωση που το πιστοποιητικό βασίζεται σε λάθος πληροφορίες ή το φυσικό ή νομικό πρόσωπο διέκοψε τις δραστηριότητές του. Ο νόμος προβλέπει επίσης τη δυνατότητα να τίθεται σε κάθε ηλεκτρονικό έγγραφο η ημερομηνία του με ψηφιακό τρόπο, ενώ υπαγορεύει και την υποχρέωση προστασίας προσωπικών δεδομένων. Στην παράγραφο 14 προβλέπεται η αναγνώριση των πιστοποιητικών από άλλες χώρες της Ε.Ε., εφόσον πληρούν τις προϋποθέσεις ασφάλειας και γνησιότητας. Το ίδιο ισχύει και για τις τρίτες χώρες. Ο γερμανικός νόμος δεν δεσμεύει το δικαστή ως προς τη διαδικασία, με την οποία θα αποκτήσει γνώση του αντικειμένου της αποδείξεως ad hoc, ούτε ως προς τη θεώρηση της συνδρομής ορισμένων γεγονότων, όπως της επιτυχούς λειτουργίας της δημόσιας κλείδας στη συγκεκριμένη περίπτωση, ως ασφαλών ενδείξεων της γνησιότητας της ψηφιακής υπογραφής. Ο γερμανικός νόμος ρυθμίζει απλώς τα ζητήματα υποδομής για τη δημιουργία των κρυπτογραφικών κλειδιών.

Αναφορικά με το ζήτημα της ψηφιακής υπογραφής έχει ασχοληθεί και ο γάλλος νομοθέτης με το ν. 96-659 της 26ης Ιουλίου 1996 για τις τηλεπικοινωνίες. Στις 8 Μαΐου 1998 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσαν μία πρόταση Οδηγίας για το κοινό πλαίσιο των ηλεκτρονικών υπογραφών. Η πρόταση έγινε δεκτή ένα χρόνο μετά.

Η Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» εκδόθηκε στις 13 Δεκεμβρίου 1999. Στόχος της Οδηγίας ήταν να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς. Δεν καλύπτει όμως πτυχές που αφορούν τη σύναψη και την ισχύ συμβάσεων ή άλλων υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου και δεν θίγει κανόνες και περιορισμούς σχετικά με τη χρήση εγγράφων, οι οποίοι περιέχονται στο εθνικό ή κοινοτικό δίκαιο (άρθρο 1). Κατά την Οδηγία ηλεκτρονική υπογραφή είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. Σύμφωνα με το

άρθρο 5 τα κράτη-μέλη οφείλουν να εξισώσουν την ηλεκτρονική υπογραφή με την ιδιόχειρη και να την κάνουν δεκτή ως αποδεικτικό στοιχείο σε νομικές διαδικασίες. Αυτό ισχύει μόνο για τις προηγμένες ηλεκτρονικές υπογραφές, που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής. Προηγμένη είναι η ηλεκτρονική υπογραφή που συνδέεται μονοσήμαντα με τον υπογράφοντα, είναι ικανή να τον «ταυτοποιήσει», δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και συνδέεται με τα δεδομένα, στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων (άρθρο 2 αρ. 2). Τα κράτη-μέλη δεν πρέπει να απορρίπτουν τη νομική ισχύ και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι υπό μορφή ηλεκτρονικών δεδομένων ή ότι δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό ή δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο παροχέα υπηρεσιών πιστοποίησης ή δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Η Οδηγία περιέχει σημαντικές διατάξεις για τους παροχείς υπηρεσιών πιστοποίησης των ηλεκτρονικών υπογραφών. Καμία έγκριση δεν χρειάζεται για την παροχή υπηρεσιών πιστοποίησης. Κάθε κράτος-μέλος όμως οφείλει να εξασφαλίζει την καθιέρωση κατάλληλου συστήματος που καθιστά δυνατή την επιτήρηση των εγκατεστημένων στο έδαφός τους παροχέων υπηρεσιών πιστοποίησης, οι οποίοι εκδίδουν για το κοινό αναγνωρισμένα πιστοποιητικά (άρθρα 3 και 4).

Το άρθρο 6 αναφέρεται στην ευθύνη των φορέων πιστοποίησης. Ο παροχέας τέτοιων υπηρεσιών υπέχει ευθύνη για την προκληθείσα ζημία έναντι οποιουδήποτε τρίτου που ευλόγως βασίζεται στο πιστοποιητικό: α) όσον αφορά την ακρίβεια, κατά τη στιγμή έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη στο πιστοποιητικό όλων των στοιχείων, τα οποία απαιτούνται για ένα αναγνωρισμένο πιστοποιητικό, β) για τη διαβεβαίωση, ότι κατά το χρόνο έκδοσης του πιστοποιητικού, ο υπογράφων, που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό, ήταν κάτοχος των δεδομένων δημιουργίας

υπογραφής που αντιστοιχούν στα δεδομένα επαλήθευσης υπογραφής που αναφέρονται ή ταυτοποιούνται στο πιστοποιητικό, γ) για τη διαβεβαίωση ότι τα δεδομένα δημιουργίας υπογραφής και τα δεδομένα επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, στις περιπτώσεις που αμφότερα προέρχονται από τον παροχέα υπηρεσιών πιστοποίησης. Ο παροχέας υπηρεσιών πιστοποίησης ευθύνεται ακόμα και για ελαφρά αμέλεια. Το ίδιο ισχύει και αν ο παροχέας παρέλειψε να καταγράψει την ανάκληση του πιστοποιητικού.

Το αναγνωρισμένο πιστοποιητικό μπορεί να έχει περιορισμένη χρήση και να μπορεί να χρησιμοποιείται για ορισμένο ύψος συναλλαγών. Ο παροχέας υπηρεσιών πιστοποίησης δεν ευθύνεται για ζημίες που απορρέουν από την υπέρβαση αυτών των ορίων (άρθρο 6). Το άρθρο 7 της Οδηγίας αναγνωρίζει υπό προϋποθέσεις τα πιστοποιητικά που εκδίδονται από φορείς πιστοποίησης τρίτων χωρών ενώ το άρθρο 8 εγγυάται την προστασία των προσωπικών δεδομένων των χρηστών. Με τα άρθρα 9 και 10 συνιστάται «Επιτροπή ηλεκτρονικής υπογραφής» και καθορίζονται τα καθήκοντά της.

3.7 ΖΗΤΗΜΑΤΑ ΕΚΠΑΙΔΕΥΣΗΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η εκπαίδευση του προσωπικού ενός οργανισμού ή μιας επιχείρησης σε ζητήματα πληροφορικής ασφάλειας αποτελεί – σε συνδυασμό με την ανάπτυξη μιας ηθικής της χρήσης της πληροφορικής τεχνολογίας – ένα από τα σημαντικότερα μέτρα αντιμετώπισης του πληροφοριακού εγκλήματος σε όλες του τις μορφές εμφάνισης.

Εκτός από τη γενική ενημέρωση σε ζητήματα πληροφορικής ασφάλειας έχουν ήδη σχεδιασθεί και προωθηθεί στην αγορά εξειδικευμένα προγράμματα εκπαίδευσης τα οποία αποτελούν ένα δείκτη των κατευθύνσεων αλλά και της τρέχουσας ιεράρχησης των κινδύνων από πληροφορικές προσβολές.

Το 1999, η SAIC, εταιρεία που εξειδικεύεται στην προσφορά στρατιωτικών και κατασκοπευτικών υπηρεσιών, ανακοίνωσε ένα πτυχιακό πρόγραμμα, το οποίο απευθυνόταν στο προσωπικό ασφάλειας πληροφοριών. Ταυτόχρονα, η εταιρεία εγκαινίασε και ένα Κέντρο Εκπαίδευσης για την Ασφάλεια Πληροφοριών. Το πρόγραμμα προσφέρεται σε συνεργασία με το πανεπιστήμιο George Washington, ενώ οι ενδιαφερόμενοι έχουν τη δυνατότητα συμμετοχής σε μεταπτυχιακά προγράμματα. Οι δυο οργανισμοί - η εταιρεία και το πανεπιστήμιο - προσδοκούσαν σπουδαστές (προπτυχιακούς και μεταπτυχιακούς) που εργάζονται σε πραγματικές συνθήκες ασφάλειας πληροφοριών, υποβοηθούμενοι από προγράμματα της CIA, NSA και του Υπουργείου Άμυνας των ΗΠΑ[48].

Μερικοί ειδικοί στο χώρο της ασφάλειας πληροφοριών αντιμετώπισαν τη συγκεκριμένη ανακοίνωση ως την απαρχή υλοποίησης των σχεδίων της επιστημονικής επιτροπής του Υπουργείου Άμυνας, σχεδίων τα οποία περιλαμβάνουν τη συγκρότηση μιας κλειστής κοινότητας επιστημόνων ειδικών σε θέματα «πολέμου πληροφοριών» (information warfare). Η εκπαίδευση ενός σκληρού πυρήνα προσωπικού ήταν η κεντρική πρόταση της προεδρικής Επιτροπής Κριτικής Προστασίας Υποδομής. Σε αναφορά που δημοσιεύθηκε τον Οκτώβριο του 1998 και είχε τίτλο «Η κριτική προστασία υποδομής και ο κίνδυνος για τις αστικές ελευθερίες», το Κέντρο Ηλεκτρονικής Προστασίας της Ιδιωτικότητας προειδοποίησε ότι οι προτάσεις της κυβέρνησης θα μπορούσαν να οδηγήσουν στη δημιουργία μιας «εικονικής κυβερνοστάζι» (a virtual cyber_Stasi).

Η εταιρεία Internet Security systems (ISS) έχει προγραμματίσει και αναγγείλει την έναρξη σειράς δωρεάν online σεμιναρίων - γνωστών ως «Webinars», με σκοπό την άνοδο του εκπαιδευτικού επιπέδου των τελικών

[48] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 229-230

χρηστών σε ζητήματα ασφάλειας συστημάτων. Στα συγκεκριμένα σεμινάρια παρέχεται στους χρήστες πρόσβαση στο προσωπικό ασφαλείας της εταιρείας, στα τελευταία ερευνητικά σχέδια, και σε προγράμματα εκμάθησης πρακτικών για την αποφυγή επιθέσεων από hackers. Μερικά από τα θέματα των σεμιναρίων περιλαμβάνουν: α) την ακριβή και λεπτομερή καταγραφή των απειλών και της τρωτότητας ενός πληροφορικού συστήματος, β) την προσφορά συμβουλών από ειδικούς για τις επιπτώσεις των απειλών σε δημόσια και ιδιωτικά συστήματα πληροφοριών, γ) την ανατομία διάφορων τύπων επίθεσης, περιλαμβανομένων των εργαλείων και των τεχνικών που χρησιμοποιούν οι hackers, και δ) την προσφορά συμβουλών και τεχνικών για τη μεγιστοποίηση της ασφάλειας των βάσεων δεδομένων.

Η εταιρεία Sophos ανακοίνωσε τη δημιουργία ενός Σχολείου Κυβερνοασφάλειας (Cyber Security School) με την έναρξη μιας νέας σειράς μαθημάτων, τα οποία απευθύνονται σε όσους θέλουν να αμυνθούν εναντίον των απειλών στο διαδίκτυο και, γενικότερα, το πληροφορικό έγκλημα. Επειδή ο αριθμός των ιών αυξάνεται με ρυθμούς της τάξης των 300 με 800 κάθε μήνα, τα μαθήματα έχουν σχεδιαστεί κατά τέτοιον τρόπο ώστε να εξασφαλίζεται ότι τα άτομα που υπερασπίζονται πληροφορικά συστήματα έχουν τη δυνατότητα χειρισμού και αντιμετώπισης οποιασδήποτε απειλής. Τα μαθήματα περιλαμβάνουν θέματα όπως η αντιμετώπιση του προβλήματος των hackers μέσα από διαδικασίες ενδοεπιχειρησιακών ελέγχων, η απάτη με τη χρήση υπολογιστή, και το οργανωμένο πληροφορικό έγκλημα.

Την ίδια χρονιά (1999), ο στρατός των ΗΠΑ σχεδίασε την έναρξη online μαθημάτων με αντικείμενο την «επιβιωσιμότητα» πληροφορικών συστημάτων. Παρακολουθώντας αυτά τα μαθήματα, οι ενδιαφερόμενοι ήταν σε θέση να αναπτύξουν συστήματα ικανά να «επιβιώνουν» από κάθε τεχνική δυσλειτουργία και δικτυακή επίθεση. Το πρόγραμμα, διάρκειας 14 εβδομάδων, προσφερόταν μέσω του πανεπιστημίου του Maryland ως μια online εξ΄αποστάσεως διδασκαλία, βασικός χορηγός της οποίας ήταν το Στρατιωτικό Εργαστήριο Ερευνών των ΗΠΑ. Κατά τη διάρκεια των μαθημάτων, οι σπουδαστές με ένα ελάχιστο γνώσεων μηχανικής (engineering) εμπλούτιζαν την εκπαίδευσή τους με οδηγίες πάνω σε κινδύνους αξιοπιστίας, ασφάλειας και εκτέλεσης, στοιχεία που πρέπει να

υπάρχουν στις πρώτες φάσεις ζωής ενός πληροφορικού συστήματος. Συμμετοχή στο πρόγραμμα επεδίωξαν και άλλα πανεπιστήμια όπως αυτό του Tennessee, της Pennsylvania και το Harvard[49].

3.8 ΗΘΙΚΗ, ΔΙΑΠΑΙΔΑΓΩΓΗΣΗ ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ

Η μεγάλη πλειονότητα των εγκληματολόγων που ασχολούνται με το πληροφορικό έγκλημα συμφωνούν ότι ο νόμος έχει τον πρωτεύοντα ρόλο στην αντιμετώπιση του πληροφορικού εγκλήματος. Αρχικά, διότι ορίζει τη σχετιζόμενη με τους υπολογιστές και ευρύτερα την πληροφορική τεχνολογία εγκληματική συμπεριφορά. Στη συνέχεια, διότι θέτει τους όρους και διατάσσει την ενεργοποίηση των διωκτικών μηχανισμών για τη δίωξη του πληροφορικού εγκλήματος. Τα φυσικά και ψηφιακά μέσα προστασίας από τις ποικίλες πληροφορικές προσβολές έχουν επίσης μεγάλη σημασία χάρη στην ικανότητά τους να αναχαιτίζουν μία πληροφορική προσβολή. Επιπλέον, ο νόμος και, σε μικρότερο βαθμό, οι μέθοδοι ασφάλειας των πληροφορικών συστημάτων, διαθέτουν και μια έμμεση κοινωνικοποιητική επίδραση, κατά κανόνα - αλλά όχι χωρίς σημαντικές εξαιρέσεις - αποτρεπτικού χαρακτήρα. Όμως, τα δύο αυτά όργανα στεγανοποίησης της κοινωνίας από το πληροφορικό έγκλημα δεν είναι δυνατό, να ασκήσουν τον ισχυρό αποτρεπτικό ρόλο της ανάπτυξης μιας ηθικής συνείδησης σε σχέση με τη χρήση της πληροφορικής τεχνολογίας, μιας ηθικής η οποία αποτρέπει την ανάπτυξη αντικοινωνικών συμπεριφορών που θα ήταν δυνατό να μετεξελιχθούν ή παγιωθούν σε παραβατικές μορφές.

Εγκληματολόγοι και κοινωνιολόγοι, αποδίδουν πρωτεύοντα ρόλο στην ηθική διαπαιδαγώγηση σε ό,τι αφορά τη χρήση των ηλεκτρονικών υπολογιστών και προτείνουν μικτές δικαιικές και μη δικαιικές αντιμετωπίσεις του ειδικού εγκλήματος. Ορισμένοι υποστηρίζουν ότι η ηθική διαπαιδαγώγηση αποτελεί τη μοναδική απάντηση στο πληροφορικό έγκλημα. Κλίνουν προς την άποψη ότι η συντεταγμένη κοινωνία δεν θα πρέπει να περιμένει, τη σταδιακή ανάπτυξη μιας ηθικής μέσω της καθημερινής πράξης και επαφής με την πληροφορική τεχνολογία. Αντίθετα, οφείλει να χαράξει μία πολιτική

[49] Λάζος Γ. (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη, σελ 231

ενεργητικής μετάδοσης των βασικών ηθικών συντεταγμένων, δηλαδή να προχωρήσει στην ηθική διαπαιδαγώγηση και εκπαίδευση του πληθυσμού.

Οι υποστηρικτές της ηθικής διαπαιδαγώγησης στη χρήση της πληροφορικής τεχνολογίας διακρίνουν μεταξύ τεσσάρων κοινωνικών κατηγοριών, η κάθε μία από τις οποίες απαιτεί διαφορετική προσέγγιση με τη χρήση διαφορετικών επικοινωνιακών μέσων.

Η πρώτη και ευρύτατη είναι ο συνολικός πληθυσμός της κοινωνίας. Ο Hollinger και η Lanza-Kaduce διαπιστώνουν ότι, κατά την διάρκεια της δεκαετίας του 1980, υπήρχε ελάχιστο ενδιαφέρον και ανησυχία από το κοινό, σχετικά με τους κινδύνους που ανακύπτουν από το πληροφορικό έγκλημα και σχεδόν καμία απαίτηση για θέσπιση νομοθεσίας, παρόλο που ήταν η περίοδος της μεγάλης νομοθετικής μεταρρύθμισης, σχετικά με το νέο είδος εγκλήματος. Σε αντίθεση με παραδοσιακά εγκλήματα όπως ο φόνος και η ληστεία, στην περίπτωση του πληροφορικού εγκλήματος η πλειονότητα των ανθρώπων βλέπει ένα έγκλημα χωρίς θύμα ή που τα θύματά του είναι απρόσωπες γραφειοκρατίες και πανίσχυρες επιχειρήσεις. Το πληροφορικό έγκλημα γίνεται αντιληπτό ως ένα έγκλημα χωρίς θύματα ή έστω ένα έγκλημα που δεν αφορά στους ίδιους, καθώς δεν θα υπάρξουν ποτέ θύματά του.

Σύμφωνα με τους δύο εγκληματολόγους, τα ΜΜΕ αποτελούν το βασικότερο μέσο για την αποτελεσματικότερη μετάδοση μιας ανάλογης ελάχιστης ηθικής διαπαιδαγώγησης. Σημείο αφετηρίας των ΜΜΕ στην προσπάθεια αυτή θα πρέπει να είναι μια αλλαγή στην αντιμετώπιση του πληροφορικού εγκληματία. Η καλλιέργεια της εικόνας του παραδοσιακού ήρωα πρέπει να αντικατασταθεί από την εικόνα του συνηθισμένου παραβάτη του νόμου. Επίσης, τα ΜΜΕ είναι αναγκαίο να καλλιεργήσουν μία εικόνα για το πληροφορικό έγκλημα ως απειλής για την κοινωνία.

Ο BloomBecker πιστεύει ότι τα ΜΜΕ έχουν τον πρώτο ρόλο στη μετάδοση βασικών ηθικών σε σχέση με την πληροφορική. Ο ρόλος του γραπτού και ηλεκτρονικού τύπου είναι καθοριστικός προς την κατεύθυνση μιας ενημέρωσης και εκπαίδευσης του κοινού. Επιπρόσθετα, θα πρέπει να εντυπώσουν στη συνείδηση του κοινού μία αίσθηση για τη συχνότητα και το πραγματικό μέγεθος του πληροφορικού εγκλήματος. Ο Chen είναι βέβαιος ότι,

ακολουθώντας αυτή την πολιτική κάλυψης, το κοινό θα ευαισθητοποιηθεί ακόμα περισσότερο απέναντι στα περιστατικά πληροφορικού εγκλήματος. Επίσης, ο Chen και πολλοί άλλοι ειδικοί στο πληροφορικό έγκλημα θεωρούν ότι η εκπαίδευση πρέπει να λάβει χώρα τόσο στις μικρές ηλικίες όσο και σε μεγαλύτερες. Προτεραιότητα πρέπει να δοθεί στην ενημέρωση σχολείων και πανεπιστημίων σχετικά με το πληροφορικό έγκλημα. Τα παιδιά που θα μάθουν από νωρίς τι δεν επιτρέπεται θα μεταφέρουν αυτή την γνώση τόσο στο πανεπιστήμιο όσο και στον μελλοντικό τους εργασιακό χώρο.

Η δεύτερη κοινωνική κατηγορία που πρέπει να τύχει μιας ενημέρωσης σε σχέση με τις ηθικές συντεταγμένες της χρήσης της πληροφορικής τεχνολογίας είναι οι χρήστες της, οι «καθημερινοί χρήστες» των υπολογιστών. Το Computer Ethics Institute στις ΗΠΑ σχεδίασε μία σειρά από απλές εντολές προς το χρήστη, οι οποίες είναι:

- ✓ Δεν πρέπει να χρησιμοποιεί κάποιος τον υπολογιστή για να κάνει κακό σε άλλους ανθρώπους.
- ✓ Δεν πρέπει να παρεμβαίνει κάποιος στην με υπολογιστή εργασία των άλλων.
- ✓ Δεν πρέπει κάποιος να «κάνει βόλτες» στα αρχεία των άλλων.
- ✓ Δεν πρέπει κάποιος να χρησιμοποιεί τον υπολογιστή για να κλέβει.
- ✓ Δεν πρέπει κάποιος να χρησιμοποιεί τον υπολογιστή για να γίνει ψευδομάρτυρας (αλλοίωση στοιχείων)
- ✓ Δεν πρέπει κάποιος να αντιγράφει ή να χρησιμοποιεί λογισμικό για το οποίο δεν έχει πληρώσει.
- ✓ Δεν πρέπει κάποιος να χρησιμοποιεί χωρίς εξουσιοδότηση ή αποζημίωση τους πόρους των άλλων.
- ✓ Δεν πρέπει κάποιος να ιδιοποιείται παράνομα το πνευματικό έργο των άλλων.

- ✓ Πρέπει οι χρήστες να σκέφτονται τις κοινωνικές συνέπειες των προγραμμάτων που δημιουργούν ή του συστήματος που σχεδιάζουν.
- ✓ Θα πρέπει όλοι να χρησιμοποιούν το υπολογιστή με τρόπο που να διασφαλίζεται το ενδιαφέρον και ο σεβασμός για τους συνανθρώπους τους.

Μια αξιοσημείωτη αλλαγή έλαβε χώρα στο επίπεδο έναρξης ορισμένων προγραμμάτων ηθικής και ενημέρωσης, τα οποία χρηματοδοτήθηκαν από την αμερικανική Υπηρεσία Εθνικής Ασφαλείας (NSA) και το Εθνικό Ινστιτούτο για την Επιστήμη και την Τεχνολογία (NIST). Για τον Bloombecker το αυξανόμενο ενδιαφέρον θα πρέπει να κατευθύνει το περιεχόμενο αυτών των προγραμμάτων στην εκπαίδευση των γονέων, των μαθητών και των υπαλλήλων. Επιπρόσθετα, οι κάθε είδους ελεγκτές είναι αναγκαίο να αντιμετωπίσουν ως πρόκληση τη συμμετοχή τους σε προγράμματα ηθικής ασφάλειας υπολογιστών.

Κατά την τελευταία κυρίως δεκαετία έχουν διατυπωθεί προβληματισμοί στην κατεύθυνση της ανάπτυξης ορισμένων πρακτικών ηθικών συντεταγμένων και, στη χρήση ή επικοινωνία μέσω του διαδίκτυου. Η Johnson προτείνει την ανάπτυξη ενός, μοντέλου «καλής γειτονίας» που θα μετατρέψει το διαδίκτυο σε ένα ασφαλές και επωφελές πεδίο δραστηριοτήτων. Η Johnson παρομοιάζει τη σχέση μεταξύ των χρηστών στο διαδίκτυο με αυτή των κατοίκων μιας γειτονιάς. Το ενοποιητικό στοιχείο, ο παράγοντας συνοχής μιας γειτονιάς, είναι η εμπιστοσύνη. Υπάρχει εμπιστοσύνη μεταξύ των μελών ότι θα ακολουθήσουν κάποιους κανόνες και θα ζήσουν με βάση τις κοινές τους υποχρεώσεις. Αναλαμβάνουν την ευθύνη από κοινού και είναι πρόθυμα να βοηθήσουν το ένα το άλλο. Αυτή η ειδυλλιακή κατάσταση θα μπορούσε να ισχύει και στις κοινότητες του διαδικτύου. Οι χρήστες θα μπορούσαν να προσέχουν οποιαδήποτε ύποπτη συμπεριφορά και να την αναφέρουν είτε στα κατάλληλα άτομα είτε στους παροχείς πρόσβασης στο διαδίκτυο. Ακόμα, θα μπορούσαν να οργανώσουν ομάδες εποπτείας για αυτά που συμβαίνουν στο διαδίκτυο, με μακροπρόθεσμο στόχο την βελτίωση της λειτουργίας του. Το ζήτημα δεν είναι η επιβολή νέων κανόνων από τις αρχές αλλά η δημιουργία άτυπων συμφωνιών και, πολύ περισσότερο, υπεύθυνων

χρηστών. Κατά την Johnson, οι χρήστες απαιτείται να κατανοήσουν τη σχέση ανάμεσα στη συμπεριφορά που έχουν και τις πιθανές επιπτώσεις της σε άλλους χρήστες. Ενέργειες όπως η μη εξουσιοδοτημένη πρόσβαση, η δημιουργία και διάδοση ιών και η κατασκευή παράνομων αντιγράφων από προγράμματα ή αρχεία θα πρέπει να βιωθούν, σχεδόν αυτόματα και αυτονόητα, ως μη αποδεκτές.

Ο Kehoe έχει επίσης προτείνει την καθιέρωση ορισμένων γενικών άτυπων συμβάσεων επικοινωνίας μεταξύ των χρηστών. Τους άτυπους αυτούς οδηγούς της συμπεριφοράς τους έχει ονομάσει «netiquette». Σημαντικές προσπάθειες καταβάλλονται και στη μετάδοση ορισμένων κωδίκων ηθικής σε όσους έχουν επαγγελματική σχέση με την πληροφορική τεχνολογία. Στις ΗΠΑ οι δυο κυριότερες επαγγελματικές ενώσεις που δραστηριοποιούνται στο πεδίο της πληροφορικής τεχνολογίας είναι η Assosiation of Computing Machinery (ACM) και η Data Processing Management Association (DPMA). Σκοπός τους είναι η συμπλήρωση των προσωπικών κωδίκων ηθικής με κώδικες συμπεριφοράς, στους οποίους περιγράφονται οι υποχρεώσεις και τα δικαιώματα των μελών προς τους υπαλλήλους τους, το κοινό και την κοινωνία ως όλο. Βέβαια, οι επαγγελματικές κώδικες ηθικής συμπεριφοράς ενώσεων όπως η ACM και η DPMA έχουν να αντιμετωπίσουν συχνά αξεπέραστες δυσκολίες στην πρακτικής τους εφαρμογή.

Πολλές επιχειρήσεις δρουν ανεξάρτητα από αυτές τις δυο ενώσεις και υιοθετούν τους δικούς τους κώδικες συμπεριφοράς, ελπίζοντας ότι θα βοηθήσουν το προσωπικό στην κατανόηση αυτού που αναμένεται ως καλή συμπεριφορά. Όπως αναφέρουν και οι Laudon, Traver και Laudon, «στο χώρο εργασίας, μερικές φορές τα άτομα κρεμάνε τα «καπέλα της ηθικής» στην πόρτα και πειθαρχούν σ' αυτό που αντιλαμβάνονται ως επιθυμία της διοίκησης, είτε είναι ηθικό είτε είναι ανήθικο».

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα εργασία μελέτησε τα εγκλήματα που διενεργούνται μέσω του διαδικτύου, πρόβαλε τους εναλλακτικούς τρόπους εκδήλωσής τους και διερεύνησε τους τρόπους αντιμετώπισής τους. Αποτελεί γεγονός ότι η νέα κοινωνική πραγματικότητα που έχει δημιουργήσει η εξάπλωση του διαδικτύου δεν είναι δυνατόν να μείνει αρρύθμιστη. Το Διαδίκτυο δεν είναι «η τελευταία δημοκρατία στον κόσμο», όπως το χαρακτηρίζουν πολλοί λόγω της φαινομενικής ελλείψεως κάθε είδους κανονιστικού πλαισίου ή έστω κάποιας ελεγκτικής αρχής. Δεν είναι ένας εξωδικαιικός χώρος.

Νόμος για το Διαδίκτυο δεν υπάρχει, όπως δεν υπάρχει νόμος για το χαρτί, τη μηχανή του fax, τη συσκευή της τηλεόρασης και του ραδιοφώνου. Εφαρμόζεται όμως όλο το γνωστό νομικό πλαίσιο που ισχύει για τα υπόλοιπα μέσα επικοινωνίας. Αυτό ωστόσο που πρέπει να κάνουν όλα τα κράτη, οι πολίτες των οποίων είναι χρήστες του Διαδικτύου, είναι να βελτιώσουν και να εφαρμόσουν τη νομοθεσία τους, εξασφαλίζοντας την κοινωνική συνοχή και προστατεύοντας τους πολίτες τους από κάθε είδους επέμβαση στα δικαιώματά τους, από οπουδήποτε και αν αυτή προέρχεται.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΞΕΝΟΓΛΩΣΣΗ

1. Bigelow R. (1985). The challenges of computer law. Western New England Law Review 7(3), pg. 397
2. Edwards O. (1995). Hackers from hell. *Forbes* 9, pg. 182
3. Glick L, (1995). Criminology. Boston: Allyn and Bakon, pg. 12
4. Thomas P. Hughes, Networks οι Power: Electrification in Western Society, 1880-1930, Baltimore: John Hopkins University Press, 1983.
5. Volgyes M. (1980). The investigation, prosecution and prevention of computer crime: A state-of-the-art review. *Computer and Law journal,* 2, pg. 385

ΕΛΛΗΝΟΓΛΩΣΣΗ

6. Αλεξιάδης Στέργιος (1996). Εγχειρίδιο εγκληματολογίας Θεσσαλονίκη: Εκδόσεις Σάκκουλα
7. Δήμου Γ., (2002). Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων, Αθήνα
8. Ζάννη Αναστασία (2005). Το διαδικτυακό έγκλημα. Αθήνα-Κομοτηνή: Εκδόσεις Αντ. Ν. Σάκκουλα
9. Καρακώστας Ι. (2003). Δίκαιο & Internet. Νομικά ζητήματα στο Διαδίκτυο. Αθήνα : Σάκκουλα
10. Κιούπης Δ. (1999) Ποινικό δίκαιο και ίντερνετ. Αθήνα: Σάκουλας , σελ. 17-18
11. Λάζος Γρηγόρης (2001). Πληροφορική και έγκλημα. Νομική βιβλιοθήκη
12. Μανωλαράκης Ε. (2006) Οι τεχνολογίες πληροφορικής στο Ελληνικό τραπεζικό σύστημα"
13. Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών

υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision-ONP).

14. Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.
15. Τσουραμάνης Χ. (2003). Σύγχρονα Κοινωνικά προβλήματα. Η ελληνική πραγματικότητα. Αθήνα : Παπαζήσης
16. Τσουραμάνης Χ. (2005). Ψηφιακή Εγκληματικότητα. Η (αν)ασφαλής όψη του Διαδικτύου. Αθήνα: Κατσαρού

ΠΗΓΕΣ ΔΙΑΔΙΚΤΥΟΥ

17. Akdeniz, Y. (2004). Advocacy Handbook for the Non Governmental Organizations. The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems. Διαθέσιμο στο http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf [Ημερομηνία πρόσβασης 10-5-2011].
18. Glandstone, J. (2003). Determining jurisdiction in Cyberspace: The "Zippo" Test of the "Effects" Test? Informing Science Institute. Διαθέσιμο στο *http://www.informingscience.org/proceedings/IS2003Proceedings/docs/029Glads.pdf* [Ημερομηνία πρόσβασης 10-5-2011].
19. http://curia.europa.eu/common/recdoc/convention/en/c-textes/brux-idx.htm [Ημερομηνία πρόσβασης 10-5-2011]
20. http://en.wikipedia.org/wiki/Michelangelo_%28computer_virus%29 [Ημερομηνία πρόσβασης 7-4-2011]
21. http://ophcrack.sourceforge.net/ [Ημερομηνία πρόσβασης 10-5-2011]
22. http://portal.bsa.org/globalpiracy2009/index.html [Ημερομηνία πρόσβασης 7-4-2011]
23. http://www.familysafemedia.com/pornography_statistics.html [Ημερομηνία πρόσβασης 5-4-2011]

24. http://www.irchelp.org/irchelp/security/bo.html [Ημερομηνία πρόσβασης 7-4-2011]

25. http://www.secnews.gr/archives/11902

26. http:/familyinternet.about.com/library/weekly/aa031903a.htm [Ημερομηνία πρόσβασης 5-4-2011].

27. J. Lipton. Beyond Cybersquatting Taking Domain Name Disputes past Trademark Policy, διαθέσιμο από : *forum.icann.org/lists/gtld-council/doc5pI73SNDTn.doc* [Ημερομηνία πρόσβασης 5-4-2011]

28. Lakshminarayan, S. (2001). Jurisdiction and the Internet. Ministry of Information Technology, Government of India. Διαθέσιμο στο http://www.cis-india.org/advocacy/igov/blog/what-are-the-legal-provisions-for-blocking-websites-in-india [Ημερομηνία πρόσβασης 10-5-2011]

29. Newman, R. (2004). Identity Theft. US Department of Justice. Διαθέσιμο από http://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf [Ημερομηνία πρόσβασης 5-4-2011]

30. Stages of the Money Laundering Progress", A report in accordance with § 356 (c) of the USA PATRIOT Act http://www2.econ.uu.nl/users/unger/publications/dancing.pdf [Ημερομηνία πρόσβασης 7-4-2011]

31. www.wikipedia.gr

32. *w2.eff.org/~**barlow**/**Declaration**-Final.html* [Ημερομηνία πρόσβασης 10-5-2011]

33. Δίκτυα Υπολογιστών και Νομικό Πλαίσιο (2011). Διαθέσιμο στο *utopia.duth.gr/~kdrakato/thesis/chapter5.doc* [Ημερομηνία πρόσβασης 12-5-2011].

34. Εφημερίδα Καθημερινή (2009). Στόχος εξαπάτησης τα social media. http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_21/10/2009_303476