ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ
ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ
ΤΜΗΜΑ: ΤΕΧΝΟΛΟΓΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΕΣ ΑΠΟΚΑΛΥΨΗΣ ΚΑΙ ΤΕΚΜΗΡΙΩΣΗΣ

Συγγραφή Εργασίας: Μιχαήλ Θεανώ, Μπυράκης Νίκος
Εισηγητής: Μηλιώνης Ματθαίος

Σπάρτη 2009

ΠΡΟΛΟΓΟΣ

Η πτυχιακή αυτή εργασία εκπονήθηκε για το Τεχνολογικό Εκπαιδευτικό Ίδρυμα Καλαμάτας, στο Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Παράρτημα Σπάρτης με θέμα «Ηλεκτρονικό Έγκλημα και μεθοδολογίες αποκάλυψης και τεκμηρίωσης ».

Θα θέλαμε να ευχαριστήσουμε τον καθηγητή μας κρ. Μηλιώνη Ματθαίο, για την βοήθεια, την στήριξη και την καθοδήγηση που μας έδωσε για την εκπόνηση της εργασίας. Χωρίς την βοήθεια του και τις κατευθυντήριες γραμμές που μας έδωσε θα ήταν σχεδόν αδύνατο να συλλέξουμε τις πληροφορίες που χρειαζόμασταν καθώς και να συγγράψουμε την πτυχιακή εργασία. Επίσης θα θέλαμε να ευχαριστήσουμε τον κρ. Κάρκα Γεώργιο, Αν. Λοχ 1623 του γραφείου καταπολέμησης ηλεκτρονικού εγκλήματος Κύπρου, για την μεγάλη βοήθεια του, στη συλλογή των διάφορων πληροφοριών που χρειαστήκαμε για την εργασία. Ακόμη θα θέλαμε να ευχαριστήσουμε τον κρ. Garry Davis, διευθυντής της εταιρείας "Why Communicate" όπου εξειδικεύεται στο SEO (Search Engine Optimization), για την βοήθεια του στην εύρεση πληροφοριών μέσω διαδικτύου. Τέλος ευχαριστούμε τον κρ. Μιχελιουδάκη Νεκτάριο, διαχειριστής δικτύων και ασφάλειας της εταιρείας "ANEK LINES", για το ενδιαφέρον που έδειξε και την βοήθεια του στα θέματα ασφάλειας των υπολογιστών.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Είναι κοινή πλέον η διαπίστωση για την ραγδαία εξέλιξη της τεχνολογίας, την ανάπτυξη της πληροφορικής και την ευρύτατη χρήση του Διαδικτύου ότι έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών ανθρώπινων δραστηριοτήτων, στην παραγωγική διαδικασία, στην εκπαίδευση, στις συναλλαγές, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα συμβάλλουν στην βελτίωση της ποιότητας της ζωής μας, υπάρχουν και οι παράμετροι που ευνοούν την δημιουργία, ανάπτυξη και διάδοση νέων μορφών εγκλημάτων. Οι νέες αυτές μορφές εγκλημάτων έχουν θεσμοθετηθεί με τον όρο «Ηλεκτρονικό Έγκλημα».

Το ηλεκτρονικό έγκλημα, είναι έγκλημα χωρίς πατρίδα, που αποτελεί ένα φαινόμενο, που συνεχώς αναπτύσσεται και εξελίσσεται , ακολουθώντας τους ταχύτερους ρυθμούς ανάπτυξης της τεχνολογίας σε όλο τον κόσμο. Το δίκτυο των παρανόμων, χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές και συσκευές ηλεκτρονικής επεξεργασίας δεδομένων, για να αποκτήσουν πρόσβαση σε δεδομένα και πληροφορίες, με σκοπό οικονομικό, προσωπικό ή οποιοδήποτε άλλο όφελος. Οι διωκτικές αρχές και η αστυνομία καλούνται να ακολουθήσουν τις νέες τεχνολογικές εξελίξεις και να προσαρμόσουν τις παραδοσιακές τεχνικές έρευνες στα νέα δεδομένα, προκειμένου να εντοπίσουν τα ηλεκτρονικά ίχνη των δραστών.

Η παρούσα μελέτη, αποτελεί μια συνολική περιγραφή των παραμέτρων που επηρεάζουν και επηρεάζονται από το ηλεκτρονικό έγκλημα. Βασικός σκοπός της μελέτης είναι να εισάγει τον αναγνώστη σε όλες τις πτυχές που αφορούν το ηλεκτρονικό έγκλημα, να τον ενημερώσει για την ψηφιακή επανάσταση που συντελείται στην εποχή μας, να λάβει τα κατάλληλα αντίμετρα για την προστασία και ασφάλεια του, να τον ευαισθητοποιήσει για τους κινδύνους που απορρέουν από την κακή χρήση του Διαδικτύου και να τον καθοδηγήσει σε περαιτέρω αναζήτηση .

Η μελέτη περιλαμβάνει επτά κεφάλαια:

Στο Κεφάλαιο 1 «Ηλεκτρονικό Έγκλημα» προσεγγίζεται το φαινόμενο του εγκλήματος και αναζητούνται οι ρίζες του. Ορίζεται το ηλεκτρονικό έγκλημα, περιγράφονται τα χαρακτηριστικά του, οι κατηγορίες του και παρουσιάζονται οι ριζοσπαστικές και φιλελεύθερες απόψεις για το φαινόμενο.

Στο Κεφάλαιο 2 «Απειλές Ηλεκτρονικού Εγκλήματος», εξετάζονται οι βασικότερες απειλές έναντι της ασφάλειας ενός συστήματος, οι οποίες διακρίνονται σε εξωτερικές και εσωτερικές. Σε κάθε περίπτωση, εξετάζεται η προσωπικότητα του επιτιθέμενου, η σοβαρότητα της επίθεσης και οι ειδικότερες τεχνικές που χρησιμοποιούνται. Παρατίθενται επίσης, συνοπτικές πληροφορίες για τα βασικά εργαλεία λογισμικού που χρησιμοποιεί ο επιτιθέμενος.

Στο Κεφάλαιο 3 «Μορφές Ηλεκτρονικού Εγκλήματος», επιχειρείται η εξέταση των διαφόρων μορφών εγκλήματος , τα οποία και διακρίνονται σε γνήσια ηλεκτρονικά εγκλήματα, που τελούνται μόνο στον κυβερνοχώρο και σε εγκλήματα που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών, στα οποία ο Η/Υ διαδραματίζει βοηθητικό ρόλο.

Στο Κεφάλαιο 4 «Έρευνες Ηλεκτρονικής Εγκληματικότητας», παρουσιάζονται έρευνες σχετικά με την έκταση του φαινομένου, διάφορα στατιστικά στοιχεία από Η.Π.Α., Ελλάδα και Κύπρο.

Στο Κεφάλαιο 5 «Ασφάλεια και μέτρα πρόληψης», καταδεικνύονται τα προβλήματα ασφάλειας, που προκύπτουν από την εμφάνιση και εξάπλωση του ηλεκτρονικού εγκλήματος. Η ασφάλεια προσδιορίζεται με τις έννοιες πρόληψη, ανίχνευση και αντιμετώπιση. Αναλύονται τα βασικά εργαλεία υλικού και λογισμικού, που απαιτούνται για την ασφάλεια ενός οργανισμού και προσεγγίζεται το ζήτημα των πολιτικών ασφαλείας. Τέλος προέρχονται ειδικότερες πληροφορίες για σημαντικά ζητήματα, όπως η ασφάλεια των βάσεων δεδομένων, του ηλεκτρονικού ταχυδρομείου και των ηλεκτρονικών συναλλαγών.

Στο Κεφάλαιο 6 «Νομοθεσία και Ηλεκτρονικό Έγκλημα», προσεγγίζονται τα νομικά ζητήματα, που προκύπτουν από την εφαρμογή του ισχύοντος δικαίου τόσο σε ποινικό όσο και σε δικονομικό επίπεδο. Επισημάνεται ότι τα μεγαλύτερα προβλήματα στον τομέα αυτό, οφείλονται στον παγκόσμιο χαρακτήρα της νέας αυτής εγκληματικής συμπεριφοράς και στις ειδικότερες τεχνικές γνώσεις που απαιτούνται για την αντιμετώπιση της. Αναφέρεται μια αναδρομή στην ισχύουσα διεθνή νομοθεσία, αξιολογούνται σημαντικές διεθνείς συμβάσεις και παρατίθεται η ισχύουσα στην Ελλάδα νομοθεσία για το ηλεκτρονικό έγκλημα.

Στο Κεφάλαιο 7 «Διερεύνηση του Ηλεκτρονικού Εγκλήματος. Εργαλεία και Μεθοδολογίες», καταδεικνύεται ο ρόλος των διωκτικών αρχών και κυρίως της Αστυνομίας, στην δίωξη του ηλεκτρονικού εγκλήματος. Εξετάζεται ο τρόπος διερεύνησης της σκηνής του εγκλήματος, οι μέθοδοι εξέτασης ψηφιακών τεκμηρίων και οι δυνατότητες αναζήτησης του εγκληματία στο Διαδίκτυο. Συγκρίνονται τα βασικότερα μοντέλα έρευνας του ηλεκτρονικού εγκλήματος (Digital Forensic Models), προσεγγίζονται νομικά ζητήματα και παρουσιάζεται η Ελληνική Αστυνομική Πραγματικότητα. Τέλος, εξετάζονται ορισμένα από τα εργαλεία λογισμικού που χρησιμοποιούν οι διωκτικές αρχές για την έρευνα του ηλεκτρονικού εγκλήματος.

1. ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

1.1. Ρίζες του ηλεκτρονικού εγκλήματος

Το έγκλημα, ένα αναπόσπαστο κομμάτι κάθε κοινωνίας , σαν ένας ζωντανός οργανισμός. Συνεχώς μεταβάλλονται οι μορφές του, τα μέσα διάπραξης του και η νομοθεσία που το διέπει.

Στις αρχές του 20ου αιώνα, καινούριοι τρόποι –τεχνικές για την διάπραξη εγκλημάτων έκαναν την εμφάνιση τους. Το τηλέφωνο άρχισε να χρησιμοποιείτε για απάτες και άλλα εγκλήματα, μεταφορικά μέσα διευκόλυναν τη διάπραξη κλοπών και ληστειών, ενώ διάφορα άλλα τεχνολογικά επιτεύγματα με τη χρήση και λειτουργία τους επέφεραν μια αρχική διαφοροποίηση στον τρόπο διάπραξης του εγκλήματος[1].

Τότε κανείς δεν μπορούσε να υποψιαστεί τι θα επακολουθούσε. Με την εμφάνιση και ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών, συντελούνται αλλαγές στο εγκληματικό φαινόμενο, που ποτέ πριν δεν είχε γνωρίσει η ανθρωπότητα. Οι εγκληματικές απειλές στηρίζονται πλέον σε πιο περίπλοκη τεχνολογία, καταργώντας τα φυσικά όρια. Οι νέες μορφές εγκλήματος , με χαρακτηριστικότερη αυτή του ηλεκτρονικού εγκλήματος , του εγκλήματος δηλαδή που ένας ηλεκτρονικός υπολογιστής ή παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων , διαδραματίζουν κυρίαρχο ρόλο.

Αναζητώντας τις ρίζες του ηλεκτρονικού εγκλήματος ,διαπιστώνουμε ότι ταυτόχρονα με την εμφάνιση των υπολογιστών, έγιναν οι πρώτες προσπάθειες από τους επίδοξους ηλεκτρονικούς εγκληματίες να βρουν τρόπους να εκμεταλλευτούν τις νέες αυτές τεχνολογίες για να προσπορίσουν όφελος για τους εαυτούς τους ή για τρίτους. Η νέα τεχνολογία , που αναπτύσσονταν με γρήγορους ρυθμούς ,έδινε νέες ευκαιρίες για εύκολη διάπραξη πλήθους εγκλημάτων.

Ακόμη όμως και τα πρώτα χρόνια έπειτα από την εμφάνιση των υπολογιστών , το ηλεκτρονικό έγκλημα ήταν σπάνιο, διότι ο αριθμός τους ήταν περιορισμένος. Επιπλέον ,οι υπάρχοντες υπολογιστές χρησιμοποιούσαν γλώσσα μηχανής, καθιστώντας αδύνατο για τους επίδοξους εγκληματίες να κατέχουν την απαραίτητη γνώση ή τον εξοπλισμό. Ο ηλεκτρονικός υπολογιστής αποτελούσε είδος πολυτελείας και κατ' αυτή την έννοια το ηλεκτρονικό έγκλημα ήταν έγκλημα για λίγους.

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

[1] Goodman and Brenner 2002 (Ημερομηνία πρόσβασης 10-07-09)

Χρονικά, η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείτε στην τελευταία δεκαετία του περασμένου αιώνα, σε μια εποχή που χαρακτηρίστηκε από την αλματώδη εξέλιξη των υπολογιστικών συστημάτων. Σήμερα , το μεγαλύτερο ποσοστό του πληθυσμού στις αναπτυγμένες χώρες, έχει πρόσβαση σε ένα Η/Υ, η δε χρήση του έχει απλοποιηθεί τόσο που ακόμη και ένα παιδί μπορεί να χειρίζεται ένα ηλεκτρονικό υπολογιστή με ιδιαίτερη δεξιότητα.

Η μεγάλη επανάσταση στον τομέα του ηλεκτρονικού εγκλήματος, επήλθε μετά την εμφάνιση των δικτύων. Τα δίκτυα, δημιούργησαν νέες διόδους πρόσβασης προς την πληροφορία, καθιστώντας μη αναγκαία την παρουσία του επιτιθέμενου στο χώρο όπου αυτή φυλάσσεται. Η τεράστια πληροφοριακή δεξαμενή που δημιουργήθηκε και συνεχίζει να επεκτείνεται , αποτέλεσμα της διασύνδεσης εκατομμυρίων υπολογιστών ανά τον κόσμο, μετέβαλε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου. Σήμερα, οι υπολογιστές χρησιμοποιούνται σε όλες τις εκφάνσεις της καθημερινής μας δραστηριότητας και στους σκληρούς τους δίσκους αποθηκεύονται πληροφορίες για τα προσωπικά μας στοιχεία , τους τραπεζικούς μας λογαριασμούς , τις συνήθειες μας, τις προτιμήσεις μας κ.α.

Το νέο περιβάλλον, χαρακτηρίζεται από την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου, την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου ,την άμεση επικοινωνία σε όλα τα επίπεδα με νέες διόδους (e-mail, chat, newsgroups κ.λπ.) αλλά και την εξ αποστάσεως εκπαίδευση, την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες, την τηλεδιάσκεψη κ.ά.

Οι ευκαιρίες για εγκληματική δραστηριότητα είναι περισσότερες από ποτέ. Το ηλεκτρονικό έγκλημα είναι ευκολότερο, οι δε δυνατότητες δίωξης του από τις αρμόδιες αρχές είναι περιορισμένες λόγο έλλειψης εμπειρίας στο σχετικό τομέα, ελλιπούς εκπαίδευσης αλλά και ασαφούς νομοθετικού πλαισίου, γεγονός που ενθαρρύνει τους επίδοξους εγκληματίες.

1.2. Ορισμός Ηλεκτρονικού εγκλήματος

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester and Morrison (1994)[2] προσδιόρισε το ηλεκτρονικό έγκλημα ως «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσης της». Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Υιοθετώντας μια τριπλή προσέγγιση το ηλεκτρονικό έγκλημα ως:

- Μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
- Μια νέα παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- Μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει κάθ' οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν : e-crime, cybercrime, computer-crime, internet related crime και hitech-crime είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων

---

[2] Giannis Stamatellos 2007 (Ημερομηνία πρόσβασης 20-07-09)

είναι ελάχιστες. Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξης μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής κινητό τηλέφωνο, notebook κ.λπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί[3]:

- Να αποτελεί τον στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το θύμα της επίθεσης.
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

Παράλληλα ο ορισμός του ηλεκτρονικού εγκλήματος εξαρτάται σε μεγάλο βαθμό από την οπτική γωνία που το εξετάζουμε. Αν αυτός άπτεται τις νομικής επιστήμης, απαιτείται πιο αυστηρός προσδιορισμός των όρων, για να είναι δυνατή η στοιχειοθέτηση των εγκλημάτων. Η πολυπλοκότητα της μορφής αυτής της εγκληματικότητας, δυσχεραίνει ακόμη και το νομοθέτη, ο οποίος αποφεύγει να ορίσει και είτε αφήνει την αρμοδιότητα αυτή στα δικαστήρια και την παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

Κρίνεται επίσης σκόπιμο να επισημανθεί, ότι η εμπλοκή ενός ηλεκτρονικού υπολογιστή ή δικτύου δεν σημαίνει αναγκαστικά ότι έχουμε να κάνουμε με ηλεκτρονικό έγκλημα. Για παράδειγμα, αποτελεί ηλεκτρονικό έγκλημα ο βιασμός μιας γυναίκας από έναν άνδρα, τον οποίο γνώρισε μέσω ενός chat room στο Διαδίκτυο και ο χρόνος και τόπος συνάντησης, που διαπράχθηκε το έγκλημα, καθορίστηκε μέσω e-mail; Σαφώς, η απάντηση στο παραπάνω ερώτημα είναι αρνητική. Πρόκειται για ένα συμβατικό έγκλημα, που διαπράχθηκε με την βοήθεια των δυνατοτήτων επικοινωνίας που προσφέρει το Διαδίκτυο.

Βασικές μορφές Ηλεκτρονικού εγκλήματος

Συνοψίζοντας, διακρίνουμε τρεις βασικές κατηγορίες όσον αφορά στις μορφές του ηλεκτρονικού εγκλήματος[4]:

- Σε εγκλήματα που διαπράττονται τόσο σε κοινό περιβάλλον, όσο και στο Διαδίκτυο. Στην κατηγορία αυτή εντάσσουμε πολλές κατηγορίες εγκλημάτων. Για παράδειγμα, η συκοφαντική δυσφήμηση μπορεί να διαπραχθεί με τη δημοσίευση στο Διαδίκτυο μιας σελίδας με προσβλητικό περιεχόμενο για ένα πρόσωπο. Ουσιαστικά στην περίπτωση αυτή το Διαδίκτυο αποτελεί ένα ακόμη μέσο για την τέλεση ενός εγκλήματος.
- Σε εγκλήματα που διαπράττονται με τη χρήση υπολογιστών χωρίς την ύπαρξη δικτύωσης. Χαρακτηριστικό έγκλημα της κατηγορίας αυτής, είναι η παράνομη αντιγραφή λογισμικού. Για παράδειγμα τέτοιο έγκλημα είναι η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM σε ηλεκτρονικό υπολογιστή.

---

[3] Shinder, D. and Tittel, E. 2002 page:5
[4] Ανδρέας Δ. Αργυρόπουλος 2001 σελ.19-23

- Σε εγκλήματα που έχουν να κάνουν αποκλειστικά με τη χρήση του Διαδικτύου. Η συνηθέστερη εγκληματική συμπεριφορά της κατηγορίας αυτής, είναι η διασπορά κακόβουλου λογισμικού (ιών).

Οι δύο τελευταίες περιπτώσεις, συνιστούν μια εντελώς νέα μορφή εγκλήματος, η οποία δεν υπήρχε πριν την εμφάνιση των ηλεκτρονικών υπολογιστών. Από τα παραπάνω διαφαίνεται ότι το ηλεκτρονικό έγκλημα συμμετέχει ποικιλοτρόπως στο εγκληματικό φαινόμενο, τα δε επιμέρους συστατικά του είναι δύσκολο να καθοριστούν με σαφήνεια.

1.3. Χαρακτηριστικά γνωρίσματα του εγκλήματος στον κυβερνοχώρο

Ο όρος ηλεκτρονικό έγκλημα, χρησιμοποιείται όλο και πιο συχνά, καθώς η νέα αυτή μορφή εγκλήματος φέρει ορισμένα ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το κοινό έγκλημα[5].

1. Είναι γεγονός ότι το ηλεκτρονικό έγκλημα διαπράττεται άμεσα, σε ελάχιστα δευτερόλεπτα και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα. Ο επιτιθέμενος με την χρήση ενός Η/Υ συνδεδεμένου στο Διαδίκτυο, μπορεί να εισβάλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του κόσμου. Δεν απαιτείται η φυσική μετακίνηση του, καθώς οι ενέργειες του μπορούν να ολοκληρωθούν από την οικία του ή άλλο χώρο, με τη χρήση ενός δικτυωμένου προσωπικού υπολογιστή
2. Είναι εύκολο στην διάπραξη του. Φαινομενικά, η εισβολή σε κάποιο υπολογιστικό σύστημα φαντάζει δύσκολο. Όμως, η άποψη ότι απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση τέτοιου είδους επίθεσης, αποτελεί μύθο. Στο Διαδίκτυο διατίθενται ελεύθερα εφαρμογές λογισμικού, που επιτρέπουν στους επίδοξους hackers την εισβολή σε δίκτυα και υπολογιστικά συστήματα, τη διασπορά ιών και την πραγματοποίηση πλήθους άλλων ηλεκτρονικών επιθέσεων, καθιστώντας περισσότερο εύκολη την διάπραξη του ηλεκτρονικού εγκλήματος σε σχέση με το κοινό-συμβατικό
3. Μπορεί να διαπραχθεί χωρίς τη φυσική μετακίνηση του δράστη. Το Διαδίκτυο προσφέρει μια σειρά από νέες δυνατότητες επικοινωνίας. Το ηλεκτρονικό ταχυδρομείο (e-mail), τα δωμάτια συζητήσεων (chat rooms) και οι ομάδες ειδήσεων (newsgroups), επιτρέπουν σε πολλά άτομα ταυτόχρονα να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα. Η επανάσταση αυτή στις επικοινωνίες συνέβαλε στη διάδοση εγκλημάτων, όπως η παιδοφιλία, η παιδική πορνογραφία και η ανεπιθύμητη αλληλογραφία (spamming). Στις περιπτώσεις αυτές, τα υποψήφια θύματα αναζητούνται μέσω των νέων καναλιών επικοινωνίας , που προσφέρει το Διαδίκτυο.
4. Είναι έγκλημα «χωρίς πατρίδα». Πολλές φορές καθίσταται αδύνατο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος, διότι κάθε εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου, αρκεί να έχει στην διάθεση του έναν ηλεκτρονικό υπολογιστή.
5. Επίσης είναι δύσκολο να προσδιοριστεί και ο ακριβής χρόνος τέλεσης τους, καθώς τα θύματα συχνά αντιλαμβάνονται μια ηλεκτρονική επίθεση πολύ αργότερα από τον χρόνο κατά τον οποίο αυτό συνέβη. Επίσης, συχνά είναι δυνατή

[5] Αναστασία Ζάννη 2005 σελ.63-64

η διαγραφή από τον εισβολέα των «ιχνών» του ηλεκτρονικού εγκλήματος κάτι που δυσχεραίνει ή εμποδίζει την ανίχνευση του.

6. Σε μια διαδικτυακή έρευνα, συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (δηλαδή του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία) .τα δε αρμόδια όργανα των διωκτικών αρχών πρέπει να κατέχουν εξειδικευμένες γνώσεις και να εκπαιδεύονται συνεχώς στις νέες τεχνολογικές εξελίξεις. Σε ορισμένες περιπτώσεις, τέτοιου είδους γνώσεις απαιτείται να κατέχουν και όσοι άλλοι ασχολούνται με τη δίωξη του ηλεκτρονικού εγκλήματος όπως δικαστές, εισαγγελείς και δικηγόροι.
7. Δυστυχώς δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον Ελληνικό αλλά και στον διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται, και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων, οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια, οι διαστάσεις της εγκληματικότητας στο χώρο του διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον «κοινό» εγκληματικό χώρο (θεωρεία του παγόβουνου).

1.4. Ριζοσπαστικές και φιλελεύθερες απόψεις και για το ηλεκτρονικό έγκλημα[6]

DOROTHY E. DENNING: Στο νέο πλαίσιο που δημιουργήθηκε από την πληροφορική τεχνολογία εμφανίστηκε μια νέα μορφή απειλής για την κοινωνία – ο πληροφορικός εγκληματίας. Ο νέος αυτός τύπος εγκληματία έχει τη δυνατότητα καταστροφής της ηλεκτρονικής υποδομής, παραβίασης της ιδιωτικότητας, και άσκησης βιομηχανικής κατασκοπίας. Από οικονομικής πλευράς, το οικονομικό κόστος που προκαλείται από ενέργειες των hackers είναι περιορισμένο σε σύγκριση με το ανάλογο κόστος του πληροφορικού εγκλήματος από μέρους των «insiders»-υπαλλήλων και πρώην υπαλλήλων μιας επιχείρησης. Συγχρόνως, το πληροφορικό έγκλημα αποτελεί ένα δυναμικό και αναπτυσσόμενο φαινόμενο. Με αυτή τη γενική αφετηρία και στηριγμένη σε πραγματικά περιστατικά, η Denning διατυπώνει μια σειρά επιφυλάξεων και φόβων για τον τρόπο δράσης των μυστικών υπηρεσιών, της ομοσπονδιακής αστυνομίας, αλλά και των εισαγγελικών αρχών στην κατεύθυνση της επίθεσης κατά των hackers [κατάσχεση ηλεκτρονικών συστημάτων από επιχειρήσεις, κατάσχεση bulletin boards (που αποτελούν ηλεκτρονικούς χώρους συγκέντρωσης πολιτών και γενικότερα ατόμων με κοινά ενδιαφέροντα), υπερβολική άσκηση βίας, προσαγωγή σε δίκη με ανεπαρκή στοιχεία ως μέσο τιμωρίας και παραδειγματισμού κ.ά.]. Η Denning προχώρησε στην εκτίμηση ότι οι hackers δεν είναι εύλογο να αντιμετωπίζονται αποκλειστικά με ποινικά-κατασταλτικά μέσα, συστήνει δε μια πιο ήπια ποινική αντιμετώπιση. Ειδικά σε ό,τι αφορά τις χωρίς εξουσιοδότηση προσβάσεις σε Η/Υ, εκτιμά ότι πρέπει να αντιμετωπίζονται κυρίως στο επίπεδο του πταίσματος. Η αυστηρότερη αντιμετώπιση που χαρακτηρίζει τις περισσότερες σύγχρονες νομοθεσίες εγκυμονεί τον κίνδυνο μετατροπής σε πληροφορικούς εγκληματίες νεαρών ατόμων που «έπαιξαν» ή «πειραματίστηκαν» για ένα διάστημα με παράνομες ενέργειες, και τις οποίες σύντομα θα ξεπερνούσαν ανώδυνα όταν θα συνειδητοποιούσαν τις ευρύτερες συνέπειες των ενεργειών τους. Κατά τη γνώμη της, η κουλτούρα των hackers πρέπει να προσεγγιστεί και να κατανοηθεί, όπως πρέπει να κατανοηθεί και η ποικιλία των κινήτρων που συμβάλλουν στην ανάπτυξη του hacking.

---

[6] http://archive.enet.gr/online/online_print?id=81420156 (Ημερομηνία πρόσβασης 31/08/09)

JOHN P. BARLOW: Το «Crime and Puzzlement» του Barlow απευθύνεται σε δύο διαφορετικά κοινά. Σε πρώτο πρόσωπο και τόνους οικειότητας, απευθύνεται σε όσους δραστηριοποιούνται στον κυβερνοχώρο ως πλαίσιο κοινωνικής δράσης και προβληματισμού, στους «ιθαγενείς» του κυβερνοχώρου. Μια μεγάλη υποκατηγορία τους –ίσως η μεγαλύτερη- δεν έχει διαπράξει κάποια παράβαση. Όχι τόσο γιατί αποτελείται από άτομα ενήμερα των νομοθετικών εξελίξεων και νομοταγή, όσο γιατί ο ειδικός τύπος δράσης τους δεν έχει ακόμα απασχολήσει το νόμο. Μία άλλη υποκατηγορία τους περιλαμβάνουν στο συνολικό τρόπο δράσης τους ενέργειες ή σκοπούς που με την εμφάνιση των πρώτων νόμων άρχισαν να αντιμετωπίζονται ποινικά ή να αποτελούν αντικείμενο συζητήσεων για το αν θα πρέπει να ποινικοποιηθούν. Τέλος, υπάρχει και μια Τρίτη υποκατηγορία, μια ισχυρή μειονότητα, οι cyberpunks ή techno-hippies. Μέρος των δραστηριοτήτων τους είναι hack-ιστικές (καινοτομικές), ένα μικρότερο μέρος είναι επιθετικές hack-ιστικές (cracking), και, τέλος, ένα ελάχιστο μέρος τους είναι κοινωνικά επιβλαβείς. Όλοι αυτοί, των οποίων η δράση στον κυβερνοχώρο αποτελεί συστατικό στοιχείο του τρόπου ζωής και του ορισμού τους ως προσωπικοτήτων, ονομάζονται συλλήβδην hackers, εξισώνονται με τους επιθετικούς hackers και η συμπεριφορά τους ορίζεται διά νόμου ως εγκληματική. Η μεγάλη πλειονότητα των hackers με την ευρεία έννοια αρνείται να συμμορφωθεί στους όρους και τύπους δράσης που ορίζονται ως νόμιμοι. Οι άλλες δύο υποκατηγορίες προβληματίζονται για τις πιθανές μελλοντικές εξελίξεις. Συνολικά, στη μεγάλη τους πλειονότητα, οι «ιθαγενείς του κυβερνοχώρου» βλέπουν την εμφάνιση των πρώτων νόμων –των συγκεκριμένων πρώτων νόμων- σαν γνήσια αυθαιρεσία και επιβολή. Έχουν την αντίληψη ότι σε ολοένα και αυξανόμενους ρυθμούς οι μεγάλες επιχειρήσεις της πληροφορικής δηλώνουν αυθαίρετα σαν ιδιοκτησία τους ένα τμήμα του κυβερνοχώρου. Απαγορεύουν τη χρήση ή τη διέλευση ή απαιτούν από τους πολίτες να καταβάλουν τίμημα για κάτι που λίγο πριν ήταν ελεύθερο και αβίαστα κοινωνικό. Με την άρνηση των πολιτών, που ενδημούν και στον κυβερνοχώρο, να συμμορφωθούν, ύστερα από μια ηθικοϊδεολογική επεξεργασία της κοινής γνώμης μέσω των ΜΜΕ, ο νομοθετικός και ο διωκτικός μηχανισμός του κράτους έρχονται να ορίσουν και να επιβάλουν τα συμφέροντα των επιχειρήσεων και της εξουσίας σαν συμφέροντα της κοινωνίας.

Οι προτάσεις του Barlow προς όσους η αξιοποίηση του κυβερνοχώρου αποτελεί συστατικό της καθημερινότητάς τους είναι δύο. Η πρώτη περιλαμβάνει την προτροπή για σεβασμό και τήρηση των άτυπων συμβάσεων επικοινωνίας και κοινωνικότητας που έχουν αναπτυχθεί σταδιακά, καθώς και την προτροπή για αποφυγή των άμετρων αντιδράσεων. Η δεύτερη πρόταση του Barlow έχει ως πρόλογό της μία δήλωση και μία προειδοποίηση. Αφού δηλώνει την κοινότητα των συμφερόντων του με τους αδελφούς του στον κυβερνοχώρο («my silicon brothers»), προειδοποιεί ότι «αν έρθουμε σαν μάγισσες, θα μας κάψουν». Και αντιπροτείνει: «Αν εθελοντικά τους οδηγήσουμε με ηπιότητα σ' αυτούς τους νέους τόπους, ο Εικονικός Κόσμος θα μπορούσε να γίνει ένας πιο φιλικός χώρος για όλους μας από αυτόν που ήταν κάποτε».

R. J. MICHALOWSKI ΚΑΙ E. H. PFUHL: Οι Michalowski και Pfuhl εκτιμούν ότι, μέχρι την εμφάνιση των πρώτων νόμων για το πληροφορικό έγκλημα, η απουσία σαφών νομικών ελέγχων πάνω στην ηλεκτρονική πληροφορία είχε αρχίσει να προκαλεί μιαν αποσταθεροποίηση των σχέσεων εξουσίας.

Στον καπιταλισμό, το ποιος παράγει ή δημιουργεί ένα νέο αγαθό ή μία νέα αξία έχει δευτερεύουσα σημασία. Πρωτεύουσα σημασία έχει το ποιος είναι ο ιδιοκτήτης τους, ποιος έχει το αγαθό αυτό ή την αξία κάτω από τον έλεγχό του, και είναι σε θέση να

καθορίσει τους όρους –κυρίως το αν, το πότε και το αντίτιμο- της παροχής του στους άλλους. Η αμφισβήτηση ή η απώλεια του ελέγχου πάνω στην ηλεκτρονική πληροφορία αποτελεί πρόκληση στην κατεστημένη σύνθεση γνώσης και δύναμης.

Είναι για αυτούς τους λόγους που, αν και ο κύριος όγκος των πληροφορικών εγκλημάτων δεν είχε κάποια σχέση με τους hackers και το hacking, είναι ακριβώς το hacking που αναβαθμίστηκε σε έμβλημα του πληροφορικού εγκλήματος. Οι νομοθεσίες που αναπτύχθηκαν δεν απαντούσαν στο πληροφορικό έγκλημα με βάση τα πραγματικά δεδομένα που οι σχεδιαστές τους διέθεταν, αλλά με βάση τους κινδύνους που αντιπροσώπευε για τις σχέσεις ιδιοκτησίας και εξουσίας. Το να κλέψει κάποιος τον εργοδότη του με τη χρήση της πληροφορικής τεχνολογίας λίγο-πολύ μπορεί να αντιμετωπιστεί με την ήδη υπάρχουσα νομοθεσία. Το να έχει κάποιος τη δυνατότητα πρόσβασης στα αρχεία μιας επιχείρησης ή του κράτους δημιουργεί όμως νέες δυναμικές και κινδύνους που βρίσκονται πολύ κοντά στον πυρήνα του καπιταλισμού και της ιεραρχίας. Το ουσιαστικό πρόβλημα δεν είναι η έναρξη του τρίτου παγκόσμιου πολέμου από κάποιον ανώριμο hacker ή η καταστροφή κάποιου αρχείου από κάποιο βάνδαλο hacker. Εάν δεν ρυθμιστούν με επάρκεια και σαφήνεια οι κανόνες της ιδιοκτησίας και της ιεραρχημένης εξουσίας, το ουσιαστικό πρόβλημα είναι ότι οι πολίτες θα έχουν τη δυνατότητα να δουν την εξουσία γυμνή όταν σχεδιάζει προγράμματα στρατιωτικών εξοπλισμών ή εκπαιδευτικά προγράμματα, ή ότι οι εργαζόμενοι θα είναι σε θέση να απομυθοποιήσουν το management των επιχειρήσεων και να γνωρίσουν τους τρόπους λήψης αποφάσεων. Ίσως τότε οι πολίτες-εργαζόμενοι συνειδητοποιήσουν ότι οι πολιτικές και οικονομικές εξουσίες στις οποίες υπακούουν δεν έχουν κάποιον ουσιαστικό λόγο ύπαρξης ή, έστω, ότι δεν προσφέρουν στην κοινωνία τα ανάλογα των προνομίων και των ηδονών που απολαμβάνουν. Η παρέμβαση του νομοθέτη ώστε να ποινικοποιηθεί η ελεύθερη πρόσβαση (στην πληροφορία και τη γνώση) και να μετατραπεί σε με/χωρίς εξουσιοδότηση πρόσβαση είναι αναγκαία για τη διατήρηση της ιδιοκτησίας και της ιεραρχίας.

2. ΑΠΕΙΛΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.1. Βασικές μορφές απειλών

Προσπαθώντας να οριοθετήσουμε το μοντέλο των απειλών έναντι της ασφάλειας ενός συστήματος, μπορούμε να διακρίνουμε 2 βασικές κατηγορίες: τις εξωτερικές και τις εσωτερικές.

Οι εξωτερικές απειλές είναι ίσως η πιο συνηθισμένη μορφή επιθέσεων. Οι επιθέσεις του τύπου αυτού, προέρχονται από τους hackers και τους crackers, που ανήκουν στο εξωτερικό περιβάλλον ενός συστήματος. Οι πιο συχνές μορφές που συναντάμε είναι η μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο, οι επιθέσεις άρνησης εξυπηρέτησης και η διασπορά κακόβουλου λογισμικού.

Οι εσωτερικές απειλές, προέρχονται από το εσωτερικό ενός οργανισμού και συνήθως από το ίδιο το εργαζόμενο σε αυτόν προσωπικό. Οι επιθέσεις της μορφής αυτής, πραγματοποιούνται από πρώην υπαλλήλους που γνωρίζουν πολύ καλά τις πολιτικές ασφάλειας του οργανισμού, ιδιαιτέρως αν είχαν εργαστεί σε σημαντικές θέσεις. Εκτός όμως των επιθέσεων από άτομα, στις εσωτερικές απειλές εντάσσουμε και προβλήματα που οφείλονται στο σχεδιασμό των συστημάτων, στις ευπάθειες λογισμικού και εξοπλισμού, στις πολιτικές ασφάλειας ακόμη και στους ίδιους τους χρήστες, που ενδεχομένως, να υποπέσουν σε λάθη, ικανά να θέσουν σε κίνδυνο την ασφάλεια του συστήματος.

2.2. Εξωτερικές απειλές

2.2.1. Hackers

Στην σύγχρονη τεχνολογία των ηλεκτρονικών υπολογιστών, ο όρος hacker έχει για τα καλά συμβάλει στη ζωή μας. Αντίστοιχο συνώνυμο δεν υπάρχει στην Ελληνική Γλώσσα . Και στην Αγγλική όμως γλώσσα, η προέλευση του όρου δεν είναι απόλυτα καθορισμένη. Μάλιστα υπάρχει διχογνωμία για το τι σημαίνει hacker.

Ένα από τα εγκυρότερα λεξικά όρων στο χώρο των υπολογιστών και ιδιαίτερα στο χώρο της κοινότητας των hackers, αποτελεί το Jargon File. Σύμφωνα με ότι αναγράφεται στο αντίστοιχο λεξικό, hacker είναι:

1. Αυτός που απολαμβάνει να εξερευνά τις λεπτομέρειες των προγραμματιστικών συστημάτων και να οδηγεί τις δυνατότητες τους στα όρια, σ αντιδιαστολή με τους κοινούς χρήστες, οι οποίοι προτιμούν να μάθουν μόνο τα ελάχιστα απαραίτητα.
2. Αυτός που ευχαριστιέται όταν κατανοεί πλήρως την εσωτερική λειτουργία των συστημάτων, των υπολογιστών και των δικτύων υπολογιστών.
3. Αυτός που ασχολείται με ενθουσιασμό (ακόμη και με εμμονή) με τον προγραμματισμό και το προτιμά παρά να θεωρητικολογεί γι᾽ αυτό.
4. Αυτός που σέβεται τις αξίες των hackers.
5. Αυτός που είναι ικανός να προγραμματίζει γρήγορα.
6. Αυτός που είναι ειδικός σε ένα συγκεκριμένο πρόγραμμα ή που συχνά δουλεύει με αυτό ή πάνω σε αυτό.

7. Αυτός που είναι ειδικός σε κάτι ή ενθουσιάζεται με κάτι, το οποίο μπορεί να είναι οτιδήποτε ανεξάρτητα από υπολογιστές.
8. Αυτός που απολαμβάνει τη διανοητική πρόκληση να δημιουργήσει κάτι ξεχωριστό ή να παρακάμψει τους υπάρχοντες περιορισμούς.
9. Αυτός που κάνει ένα σύστημα να λειτουργήσει με τρόπο που δεν ήταν προορισμένο από τον κατασκευαστή του.
10. Ένας κακόβουλος παρείσακτος που προσπαθεί να επισημάνει ευαίσθητες πληροφορίες με τις έρευνες του. Συναντώνται όροι όπως password hacker, network hacker. Ο σωστός όρος γι' αυτή την κατηγορία είναι cracker.

Αρχικά, χρησιμοποιήθηκε από το Ίδρυμα Τεχνολογίας MIT (Massachusetts Institute of Technology) για να δηλώσει γενικώς την ενδελεχή ασχολία με τον υπολογιστή. Ετυμολογικά, προέρχεται από τον όρο «hack writer» που σε ελεύθερη μετάφραση υποδηλώνει αυτόν που ελέγχει πάρα πολύ καλά το κείμενο του πριν το ολοκληρώσει[7].

Στην δεκαετία του '60 και '70, ο όρος χρησιμοποιούταν για τους τελειομανείς των υπολογιστών αλλά και για τον καθένα που επιτελούσε οποιαδήποτε δραστηριότητα που σχετίζονταν με πολύπλοκα συστήματα.

Οι hackers προέρχονται από τους phreakers, που αποτελούν τους πρώτους ηλεκτρονικούς εγκληματίες. Εμφανίστηκαν πολύ πριν την εφεύρεση των ηλεκτρονικών υπολογιστών και κατάφεραν να εκμεταλλευτούν τα τηλεφωνικά δίκτυα, που μόλις τότε άρχισαν να αναπτύσσονται, για να πραγματοποιούν τηλεφωνικές κλήσεις χωρίς χρέωση.

Οι hackers, αποτελούν άτομα με εξαιρετική γνώση της τεχνολογίας των ηλεκτρονικών υπολογιστών, που καταφέρνουν να διεισδύσουν σε υπολογιστικά συστήματα αποκτώντας πρόσβαση σε γνώση και πληροφορίες. Σκοπός τους, σύμφωνα με τις ιδεολογικές αρχές που τους διέπουν, δεν είναι ούτε η πρόκληση ζημιάς ούτε η αποκόμιση οικονομικού οφέλους. Παρόλα αυτά, οι περισσότεροι αντιμετωπίζουν τον όρο hacker με αρνητική διάθεση, θεωρώντας ότι αποτελεί συνώνυμο του εγκληματία του Διαδικτύου.

2.2.2. Οι σημαντικές κατηγορίες

Όταν σε οποιαδήποτε ενέργεια, που σχετίζεται με τους ηλεκτρονικούς υπολογιστές και τα δίκτυα, υπεισέρχεται το στοιχείο της εγκληματικής πρόθεσης ο επιτιθέμενος χαρακτηρίζεται ως cracker. Οι crackers είναι hackers που χρησιμοποιούν την γνώση τους για τους ηλεκτρονικούς υπολογιστές για να αποκομίσουν όφελος για τους ίδιους ή και για τρίτους.

Εκτός από τους όρους hacker και cracker, έχουν κατά καιρούς χρησιμοποιηθεί και άλλοι όροι για να περιγράψουν τους εγκληματίες του Διαδικτύου όπως, hacktivist, vandals cyberterroists. Σε όλες αυτές τις περιπτώσεις, αναφερόμαστε στους hackers, που λόγω του συγκεκριμένου τρόπου υλοποίησης των εγκληματικών τους προθέσεων έχουν λάβει και τα ανάλογα προσωνύμια.

Ο όρος hacktivist, αποτελεί το συνδυασμό των λέξεων hacker και activist(ακτιβιστής). Ο γενικότερος όρος hactkivism, αναφέρεται σε μια "ηλεκτρονική απείθεια κατά των αρχών" που πραγματώνεται στον κυβερνοχώρο. Οι hacktivist χρησιμοποιούν παρόμοιες με τους hackers μεθόδους, όπως π.χ. επιθέσεις άρνησης εξυπηρέτησης μέσω της μαζικής επίσκεψης σε ένα δικτυακό τόπο σε συγκεκριμένη χρονική στιγμή ή μαζικής αποστολής

[7] Barlow, J.P. 1990 (Ημερομηνία πρόσβασης 15/07/2009)

μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail bombs), παράνομη εισβολή σε κυβερνητικά site, διασπορά κακόβουλου λογισμικού κ.ά.[8]

Με τον όρο vandals, αναφέρονται οι hackers που εισβάλουν σε δικτυακούς τόπους με μοναδικό σκοπό την τροποποίηση τους κατά τρόπο προπαγανδιστικό, προσβλητικό ή ακόμα και χιουμοριστικό, ανάλογα με το σκοπό που θέλουν να επιτύχουν. Οι επιθέσεις αυτές δεν προκαλούν ανεπανόρθωτες ζημιές στους δικτυακούς τόπους, καθώς μπορεί να γίνει εύκολα αποκατάσταση από εφεδρικά αρχεία. Ωστόσο πλήττεται το κύρος και η αξιοπιστία του οργανισμού εναντίον του οποίου στρέφεται η επίθεση.

Ο όρος cyberterrorist, αναφέρεται σ' αυτούς που χρησιμοποιούν το Διαδίκτυο για την εκπλήρωση τρομοκρατικών επιθέσεων. Ειδικότερα, μετά το χτύπημα της 11ης Σεπτεμβρίου 2001 στους δίδυμους πύργους, ο φόβος για τρομοκρατικές επιθέσεις είναι ακόμα μεγαλύτερος. Οι έρευνες για την επίθεση αυτή αφήνουν ερωτηματικά σχετικά με το εάν τα μέλη της τρομοκρατικής οργάνωσης Al-Kaida, που σχεδίασαν την επίθεση, χρησιμοποίησαν το διαδίκτυο τόσο για την μεταξύ τους επικοινωνία, όσο και για την εύρεση σημαντικών πληροφοριών. Εκτιμάται, ότι στο μέλλον θα γίνουμε μάρτυρες τρομοκρατικών επιθέσεων, με μοναδικό όπλο έναν ή περισσότερους ηλεκτρονικούς υπολογιστές συνδεδεμένους στο Διαδίκτυο (cyber terrorism).

Η παραπάνω κατηγοριοποίηση των επιτιθέμενων είναι ενδεικτική, καθώς τα μεταξύ τους όρια δεν είναι δυνατόν να καθοριστούν με σαφήνεια. Αυτό που χαρακτηρίζει τον επιτιθέμενο δεν είναι η χρησιμοποιούμενη μέθοδος, αλλά ο σκοπός που θέλει να επιτύχει.[9]Για παράδειγμα, η διασπορά ιών μπορεί να αποτελεί επίθεση ενός μεμονωμένου hacker, μπορεί όμως να αποτελεί και έργο ενός cyber terrorist, εφόσον, στρέφεται εναντίον των υπολογιστικών συστημάτων ενός αεροδρομίου με σκοπό την κατάρριψη ενός αεροσκάφους.

2.2.3. Το προφίλ του ηλεκτρονικού εγκληματία

Όπως αναφέρθηκε και παραπάνω, υπάρχουν διάφοροι τύποι εγκληματιών του Διαδικτύου. Ο βασικότερος όλων είναι ο hacker. Οι hackers έχουν αναπτύξει μια δική τους κουλτούρα και διέπονται από ηθικές αρχές και κανόνες συμπεριφοράς, τους οποίου και τηρούν με απόλυτο σεβασμό.

Τα κίνητρα των επιθέσεων διαφέρουν ανάλογα με την περίπτωση και την προσωπικότητα του επιτιθέμενου. Σε γενικές γραμμές, μπορούμε να διακρίνουμε τις ακόλουθες κατηγορίες[10]:

- **Ερασιτέχνες (amateurs):** Πρόκειται για ανθρώπους χωρίς ιδιαίτερες δεξιότητες στους υπολογιστές, που προσπαθούν να εντοπίσουν μια ευπάθεια σε ένα υπολογιστικό σύστημα και στη συνέχεια να την εκμεταλλευτούν. Τα κίνητρα τους είναι η περιέργεια και να αποκτήσουν γνώσης, χωρίς όμως να αποκλείεται το γεγονός να αποσκοπούν σε οποιοδήποτε είδους όφελος(υλικό και μη). Χρησιμοποιούν σχεδόν πάντα έτοιμα εργαλεία, καθότι στη συντριπτική πλειοψηφία των περιπτώσεων δεν κατέχουν τις απαραίτητες γνώσεις για να τα κατασκευάσουν. Είναι συνήθως εσωτερικοί εχθροί και ευθύνονται για το μεγαλύτερο ποσοστό των επιθέσεων.

---

[8] Denning, D. 2001 (Ημερομηνία πρόσβασης 15/07/09)
[9] Denning, D. 2001 (Ημερομηνία πρόσβασης 14/07/09)
[10] Anderson, R. 2001 (Ημερομηνία πρόσβασης 15/07/09)

- **Hackers:** Οι hackers είναι άριστοι γνώστες προγραμματισμού, δικτύων Η/Υ και Internet. Τα εργαλεία που χρησιμοποιούν τα αναπτύσσουν οι ίδιοι. Σκοπός των επιθέσεων τους είναι η ικανοποίηση της περιέργειας τους και η επιβεβαίωση της ικανότητας τους για εισβολή σε ένα σύστημα.
- **Crackers:** Οι crackers προέρχονται από τους hackers. Έχουν ως σκοπό την πρόκληση ζημιάς ή την αποκόμιση οφέλους από τα συστήματα στα οποία επιτίθενται. Οι δημιουργοί ιών και γενικότερα κακόβουλου λογισμικού μπορούν να θεωρηθούν ως crackers.

- **Επαγγελματίες εισβολείς (career criminals):** Οι εγκληματίες της κατηγορίας αυτής, έχουν το επίπεδο γνώσεων των hackers. Οι επιθέσεις τους σχετίζονται με τα σοβαρότερα εγκλήματα του κυβερνοχώρου, όπως η βιομηχανική κατασκοπία. Κερδίζουν μέρος ή το σύνολο του εισοδήματος τους από επιθέσεις.

2.2.4. Η ηθική των hackers

Το hacking, για τους εμπνευστές και συνεχιστές του αποτελεί τρόπο ζωής. Μέσα από τη συνεχή ενασχόληση με τους υπολογιστές, οι hackers δημιούργησαν ένα σύνολο κανόνων, το οποίο χαρακτηρίζει την κουλτούρα τους και έχει επικρατήσει διεθνώς ως η «ηθική των hackers» (hacker ethics). Οι κανόνες ηθικής, επιδιώκουν να αντικρούσουν τη λανθασμένη, κατά την άποψη τους, γνώμη ότι οι hackers είναι εγκληματίες, αυτοί που κατεξοχήν τελούν ηλεκτρονικά εγκλήματα.

Βασικοί κανόνες ηθικής

Η διεθνής βιβλιογραφία, που σχετίζεται με την ηθική των hackers, είναι ανεξάντλητη. Ο Steven Levy (2001), κατέγραψε τους βασικότερους κανόνες που διέπουν την ηθική των hackers:

- Η πρόσβαση στους υπολογιστές, καθώς και σ' οποιοδήποτε μέσο, ενδεχομένως, θα μπορούσε να σε διδάξει και να σε πληροφορήσει για τον τρόπο που λειτουργεί το καθετί στον κόσμο – θα πρέπει να είναι ολοκληρωτική και χωρίς κανένα περιορισμό. Πάντα να υπακούς στην προσταγή: «Πάρ' τον έλεγχο στα χέρια σου!».
- Κάθε είδους πληροφορία θα πρέπει να είναι ελεύθερη.
- Μην εμπιστεύεσαι εξουσία και αυθεντία. Να υποστηρίζεις τον αντισυγκεντροτισμό.
- Οι hackers θα πρέπει να κρίνονται από την ίδια την δράση τους, όχι από λανθασμένα κριτήρια, όπως πτυχία, ηλικία, φυλή ή κοινωνική θέση.
- Μπορείς να δημιουργήσεις τέχνη και ομορφιά σε έναν υπολογιστή.
- Οι υπολογιστές μπορούν να αλλάξουν τη ζωή σου προς το καλύτερο.

Ο Levy, παρουσιάζει τους hackers ως μοντέρνους «Ρομπέν των Δασών», ανθρώπους με αγνές προθέσεις που θέλουν να επεκτείνουν τη γνώση τους για τους ηλεκτρονικούς υπολογιστές και να την κάνουν ευρέως γνωστή. Όμως το έγκλημα, ως αναπόσπαστο κομμάτι κάθε οργανωμένης κοινωνίας, αποτελεί αναμενόμενη συμπεριφορά και η παραβίαση πάσης φύσεως κανόνων(κοινωνικών, ηθικών, ποινικών κ.λπ.) φυσικό επακόλουθο της καθημερινής επαφής των ανθρώπων. Στο πλαίσιο αυτό, όταν κάποιος γνωρίζει ότι μπορεί πολύ εύκολα και χωρίς να εντοπιστεί να υποκλέψει μεγάλα χρηματικά ποσά, είναι αρκετά πιθανό να διαπράξει εγκλήματα, παρά να ακολουθήσει τους κανόνες ηθικής.

Οι hackers θεωρούν του εαυτούς τους το υγιές κομμάτι του Διαδικτύου και κατηγορούν τους crackers για την διάπραξη των εγκλημάτων. Ποιους όμως να χαρακτηρίσουμε hackers και ποιους crackers; Αναλογιζόμενοι ότι οι hackers είναι αυτοί που εφευρίσκουν τις τεχνικές διείσδυσης σε υπολογιστικά συστήματα, που δημιουργούν κακόβουλο λογισμικό, που εντοπίζουν τις ευπάθειες των συστημάτων και τις κάνουν ευρέως γνωστές φρονώ ότι θα έπρεπε να τους θεωρούμε εξίσου κακόβουλους με τους crackers καθότι δημιουργούν τις προϋποθέσεις, τις τεχνικές και τα μέσα τέλεσης του ηλεκτρονικού εγκλήματος.

Η κουλτούρα των hackers

Για την επιβίωση οποιασδήποτε ομάδας που θεωρεί τον εαυτό της οργανωμένη, απαιτείται η ύπαρξη μιας συγκεκριμένης κουλτούρας. Οι hackers έχουν δική τους κουλτούρα, η οποία υπεισέρχεται σε όλες τις εκφάνσεις της καθημερινής τους ζωής. Ας δούμε, ορισμένα στοιχεία τις κουλτούρας των hackers.

Οι hackers έχουν το δικό τους έμβλημα[11] .Το ντύσιμο τους, είναι casual και συνηθίζουν να αφήνουν μακριά μαλλιά και γένια. Διαβάζουν πολλά βιβλία, κυρίως επιστημονικής φαντασίας. Παίζουν παιχνίδια που έχουν να κάνουν με την ευφυΐα όπως σκάκι, τάβλι κ.λπ. και απεχθάνονται τον αθλητισμό, με εξαίρεση ορισμένα ατομικά αθλήματα και το βόλεϊ. Όσο αφορά τις γαστρονομικές τους συνήθειες, προτιμούν τις εθνικές κουζίνες και ιδιαίτερα τις ασιατικές. Οι περισσότεροι hackers είναι άνδρες, ενώ αποτελεί μύθο ότι πίνουν και καπνίζουν πολύ.

Εικόνα 2.1: Έμβλημα που πρότεινε ο Raymond και συμβολίζει την κουλτούρα των hackers

Σε όλες τις δραστηριότητες τους με τους υπολογιστές χρησιμοποιούν, αποκλειστικά, την Αγγλική γλώσσα. Ενδιαφέρονται για την τέχνη, την οποία όμως, προσπαθούν να προσαρμόσουν στο δικό τους ψηφιακό κόσμο. Η σχέση τους με τη θρησκεία είναι ουδέτερη, καθώς δεν ταυτίζονται με συγκεκριμένες θρησκευτικές πεποιθήσεις, ενώ, όσον αφορά τις πολιτικές τους πεποιθήσεις, δεν μετουσιώνονται σε κάποιο πολιτικό ή έστω κοινωνικό κίνημα ή ομάδα.

Αξίζει όμως να σημειωθεί, ότι η κουλτούρα δεν ακολουθείται από όλους. Είναι περισσότερο ενδεικτική του χαρακτήρα των hackers και αποτελεί την κουλτούρα του χακερικού στερεότυπου με όλη την αφαίρεση που μπορεί να έχει ένα στερεότυπο σε σχέση με την πραγματική ζωή και με όλη τη στασιμότητα ενός στερεότυπου, παρά την εξέλιξη που υφίστανται τα στοιχεία που το απαρτίζουν.

[11] Raymond, Eric S. 2004 (Ημερομηνία πρόσβασης 15/07/09)

2.2.5. Οι γενιές των hackers[12]

Η πρώτη γενιά των hackers περιλαμβάνει τους επιστήμονες που είχαν συμμετοχή στην ανάπτυξη των πρώτων μεθόδων προγραμματισμού (ηλεκτρικών στην αρχή και ηλεκτρονικών στη συνέχεια) υπολογιστών. Οι πρώτοι hackers χαρακτηρίζονταν από μιαν απόλυτη προσήλωση στο έργο τους. Ζούσαν για να προγραμματίζουν. Κλεισμένοι στα εργαστήρια, κυρίως του MIT, κατά τις δεκαετίες του 1950 και του 1960, δεν είχαν κάποια συστηματική και μόνιμη επαφή με την ευρύτερη κοινωνική πραγματικότητα και τις εξελίξεις της. Ο Ψυχρός Πόλεμος τούς ήταν κάτι το μακρινό, και το γεγονός ότι εργάζονταν για λογαριασμό στρατιωτικό βιομηχανικών κύκλων και μυστικών υπηρεσιών δεν τους απασχολούσε ιδιαίτερα. Πάντως, οι ηθικές αρχές του hacking είχαν νόημα για τη μικρή ομάδα των πρώτων hackers - και μάλλον δεν προβλημάτιζαν τους εργοδότες τους. Στο πλαίσιο μιας πληροφορικής επανάστασης, περιορισμένης σε εργαστήρια υψίστης ασφαλείας, οι αρχές αυτές δεν αποτελούσαν ιδιαίτερο κίνδυνο.

Η δεύτερη γενιά περιλαμβάνει τους επιστήμονες και επιχειρηματικά προσανατολισμένους επιστήμονες που έθεσαν ως σκοπό τους τη μετάδοση της χρήσης της πληροφορικής τεχνολογίας στον ευρύτερο πληθυσμό. Πρόκειται για τους επιστήμονες που ανέπτυξαν τους πρώτους προσωπικούς υπολογιστές, συστήματα υπολογιστών που περιλάμβαναν όλες τις ουσιαστικές ιδιότητες της πληροφορικής τεχνολογίας, έστω και αν δεν διέθεταν παρά περιορισμένες δυνατότητες. Επιπλέον, η δεύτερη γενιά ασχολήθηκε συστηματικά «με τη μελέτη και τον πειραματισμό πάνω στους τρόπους βελτίωσης της επικοινωνίας μεταξύ ανθρώπων και υπολογιστών».

Η τρίτη γενιά αναφέρεται στους προγραμματιστές που σχεδίασαν τις πρώτες αρχιτεκτονικές, πάνω στις οποίες θα αναπτύσσονταν στο κοντινό μέλλον τα ηλεκτρονικά παιχνίδια. Είναι φανερό ότι η τρίτη αυτή γενιά είναι πλέον σαφώς προσανατολισμένη σε μια ήδη δημιουργημένη αγορά πληροφορικής τεχνολογίας γύρω από τον προσωπικό υπολογιστή και προσπαθεί να ανταποκριθεί στη ζήτηση ή να δημιουργήσει μια ζήτηση με βάση πιθανές δυναμικές ανάγκες.

Οι τρεις πρώτες γενιές των hackers δεν έχουν ιδιαίτερη σχέση με το πληροφορικό έγκλημα, αν και έχουν κάποια ασταθή σχέση καταγωγής και έναν -αμφισβητούμενο ως προς το αν είναι ευρύς ή στενός- κοινό τόπο με την έννοια του hacker, όπως επικράτησε και καθιερώθηκε στις αρχές της δεκαετίας του 1980. Είναι η τέταρτη γενιά των hackers - γνωστών και ως crackers, cyberpunks κ.ο.κ.- που προσεγγίζει τους διάφορους νομικούς ορισμούς του hacking ως εγκληματικής συμπεριφοράς.

Η τέταρτη γενιά αποδέχεται τις ηθικές αρχές των προηγούμενων γενεών - όπως τουλάχιστον τις συνέθεσε ο Levy. Συγχρόνως όμως, είναι σαφώς πολυπληθέστερη, έχει γεννηθεί και κοινωνικοποιηθεί σε ένα ήδη υπάρχον πληροφορικό περιβάλλον, και αποτελείται από άτομα που ζουν σε διαφορετικές συνθήκες και έχουν διαφορετικούς στόχους και σκοπούς από τις προηγούμενες. Μεγάλο μέρος των δραστηριοτήτων, που στο πλαίσιο του εργαστηρίου πληροφορικής ή του Διαδικτύου μεταξύ ερευνητικών κέντρων και επιστημόνων θεωρούνταν ως αυτονόητες, αναπτύσσουν έναν ουσιαστικά διαφορετικό χαρακτήρα όταν μεταφέρονται στην ευρύτερη κοινωνία ή, ακριβέστερα, στον ευρύτερο κυβερνοχώρο. Στο νέο αυτό, ποιοτικά διαφορετικό, πλαίσιο, η πρόσβαση σε έναν υπολογιστή δεν θεωρείται πλέον αμέσως ελεύθερη. Απαιτεί ορισμένες ρυθμίσεις

---

[12] http://archive.enet.gr/online/online_print?id=81420156 Ελευθεροτυπία (Ημερομηνία πρόσβασης 28/06/09)

κοινωνικότητας, η κυριότερη από τις οποίες είναι η εξουσιοδότηση. Ευνόητο είναι ότι η χωρίς εξουσιοδότηση πρόσβαση σε έναν υπολογιστή αρχίζει να γίνεται αντιληπτή ως παραβίαση, μια παραβίαση που μπορεί να αξιολογείται ως ανήθικη ή ως ανήθικη και εγκληματική.

2.3. Εσωτερικές απειλές

2.3.1. Υπάλληλοι

Οι εσωτερικές απειλές, συχνά είναι ο μεγαλύτερος κίνδυνος που καλείται να αντιμετωπίσει ένας οργανισμός. Διάφορες έρευνες εγκληματικότητας στο Διαδίκτυο έχουν καταδείξει, ότι το 75% των επιθέσεων πραγματοποιείται από υπαλλήλους εταιρειών και μάλιστα αυτών που κατέχουν διευθυντικές θέσεις. Τα κίνητρα των επιθέσεων ποικίλουν. Μπορεί ο υπάλληλος να διαγράψει ένα έγκλημα για να προσπορίσει οικονομικό ή άλλο όφελος, για να βλάψει κάποιο συνεργάτη του, ή ακόμη για να εκδικηθεί κάποιο πρόσωπο ή την εταιρεία. Η γνώση των πολιτικών ασφάλειας της εταιρείας, των κωδικών πρόσβασης στα συστήματα καθώς και άλλων λεπτομερειών για την ασφάλεια των συστημάτων καθιστούν μια εσωτερική επίθεση ιδιαιτέρως εύκολη, και τον εντοπισμό της εξαιρετικά δυσχερή.

2.3.2.Λάθη στο σχεδιασμό των συστημάτων-Ευπάθειες

Οι εξωτερικές απειλές, που αναλύθηκαν παραπάνω, αποτελούν ουσιαστικά την άμεση απειλή. Οι hackers ή crackers, εκμεταλλεύονται μια αδυναμία του στόχου, ένα σημείο που μπορεί να τους δώσει πρόσβαση σ' ένα σύστημα. Επομένως, απειλή δεν είναι μόνο ο επιτιθέμενος αλλά και η ελλιπής ασφάλεια του συστήματος που χρησιμοποιούμε.

Ένα σύστημα, όσο καλά και αν έχει δοκιμαστεί, πάντα θα έχει κάποια αδύνατα σημεία: τις ευπάθειες (vulnerabilities). Οι ευπάθειες των συστημάτων μπορούν να οριστούν ως «Αδυναμία ή ελάττωμα στο υλικό, στο λογισμικό ή στην αρχιτεκτονική ενός συστήματος, καθώς και στις διαδικασίες ασφάλειας που ακολουθούνται, που μπορεί κάποιος να εκμεταλλευτεί προκειμένου να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα του εν λόγω συστήματος». Τις πιο σημαντικές ευπάθειες τις συναντάμε στο λογισμικό, τόσο διότι ο σχεδιασμός ασφαλούς λογισμικού είναι ομολογουμένως μια διαδικασία δύσκολη, σε σχέση με τη δημιουργία ασφαλούς υλικού.

Σ' ένα σύστημα υπολογιστών, το λειτουργικό σύστημα είναι το σημαντικότερο κομμάτι λογισμικού. Η ασφάλεια του λειτουργικού συστήματος αποτελεί κεφαλαιώδες ζήτημα για κάθε χρήστη που θέλει να προστατέψει τα δεδομένα του, καθότι, οι ευπάθειες του λειτουργικού συστήματος μπορούν να επηρεάσουν τις πληροφορίες, τα δεδομένα καθώς και άλλες εφαρμογές λογισμικού που είναι εγκατεστημένες σε ένα υπολογιστή. Η US-CERT στην ετήσια έκθεση της[13] σχετικά με τις ευπάθειες των λειτουργικών συστημάτων αναφέρει ότι για το 2005 εντοπίστηκαν συνολικά 5198 ευπάθειες από τις οποίες οι 812 αναφέρονται στα λειτουργικά συστήματα Windows, οι 2328 σε Linux-Unix και οι 2058 σε διάφορα λειτουργικά συστήματα.

Οι αδυναμίες στο λογισμικό εφαρμογών, προέρχονται τόσο από το λανθασμένο αρχικό σχεδιασμό τους όσο και από την ελλιπή συντήρηση και διαχείριση, για την οποία ευθύνεται ο διαχειριστής του συστήματος. Όπως προαναφέρθηκε, οι ευπάθειες ενός συστήματος δεν μπορούν να εντοπιστούν εξ' αρχής. Κατά κύριο λόγο, μια ευπάθεια

[13] http://www.us-cert.gov/cas/bulletins/SB2005.html#Multiple (Ημερομηνία πρόσβασης 21/07/09)

γίνεται γνωστή και λαμβάνονται τα κατάλληλα μέτρα, αφού κάποιος επιτιθέμενος έχει επιτύχει να την εκμεταλλευτεί, ή κατόπιν ενδελεχούς μελέτης της ασφάλειας των συστημάτων Η/Υ και δικτύων του οργανισμού, σύμφωνα με την πολιτική ασφάλειας που υλοποιείται.

Ένας ορθολογικός σχεδιασμός ασφάλειας ενός συστήματος, περιλαμβάνει κατ' ελάχιστον την δυνατότητα κρυπτογράφησης των δεδομένων, καθώς και ασφαλείς τεχνικές ελέγχου πρόσβασης και αυθεντικοποίησης (π.χ. επιλογή σωστών συνθηματικών, χρήση εναλλακτικών μεθόδων ταυτοποίησης)

Όσο αφορά τα δίκτυα και τα υπολογιστικά συστήματα, λάθη σχεδιασμού μπορούν να εντοπιστούν στην λειτουργία των firewalls[14] (υλικό και λογισμικό), στα συστήματα ελέγχου και καταγραφής συμβάντων καθώς και στο λογισμικό προστασίας από ιούς.

2.4. Μέσα τέλεσης του ηλεκτρονικού εγκλήματος

Για να αποκτήσουν πρόσβαση σε ένα δίκτυο ή υπολογιστικό σύστημα, οι hackers χρησιμοποιούν εργαλεία που εκμεταλλεύονται τις αδυναμίες των συστημάτων. Τα εργαλεία αυτά, έχουν δημιουργηθεί, για να χρησιμοποιούνται από τους διαχειριστές δικτύων, προκειμένου να ελέγχουν την ευπάθεια των συστημάτων. Οι hackers, όμως, τα χρησιμοποιούν για το αντίθετο ακριβώς σκοπό, δηλαδή για να εκμεταλλευτούν τις αδυναμίες συστημάτων.

Πολλά από τα εργαλεία, διανέμονται ελεύθερα στο Διαδίκτυο με αποτέλεσμα ακόμη και αρχάριοι χρήστες να μπορούν να το εντοπίσουν και να το χρησιμοποιήσουν εναντίον κάποιου συστήματος.

Port Scanners
Έχουν την δυνατότητα να ελέγχουν πολλές IP διευθύνσεις και να δίνουν στο χρήστη πληροφορίες για τις διαθέσιμες θύρες, τα υπάρχοντα λειτουργικά συστήματα, εφαρμογές που εκτελούνται και άλλες σημαντικές πληροφορίες για το σύστημα[15]

Vulnerability Scanners

Τα εργαλεία αυτά, ελέγχουν το λογισμικό εφαρμογών ενός Η/Υ, προσπαθώντας να εντοπίσουν κάποια ευπάθεια. Συνήθως, χρησιμοποιούνται από τους διαχειριστές για να εντοπίσουν και επιδιορθώσουν τις ευπάθειες των συστημάτων. Οι επιτιθέμενοι τα χρησιμοποιούν για το αντίθετο, ακριβώς, σκοπό.[16]

Rootkits

Ο όρος[17], χρησιμοποιείται για να περιγράψει ένα σύνολο από σενάρια (scripts) και εκτελέσιμα πακέτα, τα οποία επιτρέπουν στους εισβολείς, να κρύψουν οποιαδήποτε πληροφορία προδίδει ότι απέκτησαν πρόσβαση σε ένα σύστημα ή δίκτυο. Τα εργαλεία αυτά, επιτελούν μια σειρά από διαδικασίες στο σύστημα στο οποίο επιτέθηκαν, όπως:

- Τροποποίηση των αρχείων καταγραφής (log files).

---

[14] http://cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf (Ημερομηνία πρόσβασης 21/07/09)
[15] http://netsecurity.about.com/cs/hackertools/a/aa121303.html (Ημερομηνία πρόσβασης 21/07/09)
[16] http://netsecurity.about.com/cs/hackertools/a/aa030404.html (Ημερομηνία πρόσβασης 21/07/09)
[17] www.rootkit.com (Ημερομηνία πρόσβασης 21/07/09)

- Τροποποίηση των εργαλείων του συστήματος.
- Δημιουργία κρυφών σημείων πρόσβασης στο σύστημα (backdoors).
- Χρησιμοποίηση του συστήματος ως αρχικό σημείο εξαπόλυσης επιθέσεως σε άλλα συστήματα.

Sniffers

Τα προγράμματα αυτά, χρησιμοποιούνται για να αναγνώσουν τις πληροφορίες, που αφορούν την κίνηση σ' ένα τοπικό δίκτυο υπολογιστών. Πραγματοποιώντας το κατάλληλο φιλτράρισμα στα δεδομένα που συλλέγουν, έχουν τη δυνατότητα να ανακτούν ευαίσθητες πληροφορίες όπως ονόματα χρηστών, κωδικούς πρόσβασης και δεδομένα συναλλαγών, που διακινούνται σε ένα δίκτυο μέσω των πρωτοκόλλων επικοινωνίας TCP/IP. Οι επιθέσεις τύπου sniffing είναι ιδιαιτέρως αποτελεσματικές όταν δεν γίνεται κρυπτογράφηση των δεδομένων που διακινούνται σε ένα δίκτυο.

Anonymous re-mailers

Ένας ανώνυμος re-mailer[18] είναι ένα πρόγραμμα, το οποίο εκτελείται σε κάποιον υπολογιστή στο Διαδίκτυο και επιτρέπει στον οποιοδήποτε, να στείλει μηνύματα σε ομάδες συζητήσεων ή σε μεμονωμένα άτομα, χωρίς να γίνει γνωστή η ταυτότητα του.

Όταν ένα μήνυμα στέλνεται σε μια τέτοια διεύθυνση, το πρόγραμμα αφαιρεί το όνομα και την διεύθυνση του αποστολέα και το προωθεί στον προορισμό του. Μάλιστα, πολλές φορές, τα μηνύματα αυτά διέρχονται από διαδοχικούς re-mailers, με αποτέλεσμα να καθίσταται δύσκολη η παρακολούθηση ή ο εντοπισμός τους.

Password Crackers

Οι Password Crackers είναι εργαλεία λογισμικού, τα οποία χρησιμοποιούνται για να ανακτήσουν τους κωδικούς πρόσβασης ενός συστήματος. Για τον σκοπό αυτό οι Password Crackers κάνουν χρήση ενός αρχείου με πιθανούς κωδικούς (δηλαδή ένα σύνολο από λέξεις που έχουν επιλεγεί από κάποιους χρήστες με μεγάλη πιθανότητα), που συχνά αναφέρεται και ως «λεξικό», ενώ η σχετική επίθεση ως «επίθεση λεξικού». Οι επιθέσεις αυτές εκμεταλλεύονται τρεις βασικές ευπάθειες των συστημάτων ελέγχου πρόσβασης με κωδικούς. Πρώτον, το μήκος των κωδικών είναι μικρό με αποτέλεσμα ένα πρόγραμμα να είναι εύκολο να δοκιμάσει όλους τους κωδικούς μήκους 8 χαρακτήρων που επιλέγονται από τους 96 διαθέσιμους χαρακτήρες του πληκτρολογίου. Δεύτερον, οι χρήστες συχνά επιλέγουν εύκολους κωδικούς, όπως ημερομηνίες γέννησης, ονόματα, ταυτότητες κ.λπ. κάτι που καθιστά το έργο των crackers ακόμη πιο εύκολο. Και τρίτον, τα αρχεία με τους κωδικούς των χρηστών δεν προστατεύονται σωστά, με αποτέλεσμα, να είναι συχνά εύκολη η υποκλοπή τους από τον διακομιστή όπου έχουν αποθηκευτεί.[19]

Spoofers

Πρόκειται για προγράμματα που αλλάζουν τη διεύθυνση IP του Η/Υ του επιτιθέμενου ώστε να μην ανιχνεύονται οι επιθέσεις του, ή με σκοπό την ενοχοποίηση κάποιου άλλου

---

[18] http://www.strassmann.com/pubs/anon-remail.html (Ημερομηνία πρόσβασης 09/08/09)

[19] Στο διαδίκτυο υπάρχουν εκατοντάδες εργαλεία σπασίματος κωδικών http://www.passwordportal.net/ (Ημερομηνία πρόσβασης 28/07/09)

χρήστη. Συχνά, ανυποψίαστοι χρήστες του Διαδικτύου κατηγορούνται για ηλεκτρονικά εγκλήματα επειδή κάποιος κακόβουλος χρησιμοποίησε την IP διεύθυνση τους.[20]

[20]http://iss.net/security_center/advice/Underground/Hacking Methods Technical Spoofing default.htm (Ημερομηνία πρόσβασης 21/07/09)

3. ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1.Εισαγωγή

Το ηλεκτρονικό έγκλημα, σήμερα, έχει εισχωρήσει στην δομή και οργάνωση των ανεπτυγμένων κοινωνιών. Νέες μορφές εμφανίζονται και οι υπάρχουσες αναπτύσσονται και εξελίσσονται με γοργούς ρυθμούς. Το ηλεκτρονικό έγκλημα περιλαμβάνει εγκλήματα, που τελούνται με οποιαδήποτε συσκευή ηλεκτρονικής επεξεργασίας δεδομένων. Πολλά από τα εγκλήματα του κοινού Ποινικού Δικαίου, υπήρχαν πολύ πριν την εμφάνιση των συσκευών αυτών, ωστόσο, οι νέες τεχνολογίες και κυρίως οι ηλεκτρονικοί υπολογιστές και τα δίκτυα, διεύρυναν σε μεγάλο βαθμό τα μέσα διάπραξης τους. Παράλληλα δημιουργήθηκαν νέες εγκληματικές απειλές,

Για την καταγραφή και ανάλυση των βασικότερων μορφών ηλεκτρονικού εγκλήματος, διακρίνουμε 2 βασικές κατηγορίες:

α) Τα εγκλήματα, που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και των δικτύων. Τα εγκλήματα αυτά τα χαρακτηρίζουμε ως «γνήσια».

β) Τα εγκλήματα, που υπήρξαν και πριν την εμφάνιση των ηλεκτρονικών υπολογιστών, τελούνται, όμως, με τη χρήση ή βοήθεια των ηλεκτρονικών υπολογιστών ή και δικτύων.

3.2. Γνήσια ηλεκτρονικά εγκλήματα

3.2.1. Κακόβουλες εισβολές σε δίκτυα

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 $21^{ου}$ αιώνα. Η θεώρηση του hacking ως εγκλήματος, είναι ένα ζήτημα, που έχει νομικώς αντιμετωπιστεί με διαφορετικές προσεγγίσεις. Όπως επισημάνθηκε και στο Κεφάλαιο 2 οι hackers, επιδιώκουν να αποκτήσουν πρόσβαση σε ξένο υπολογιστή ή σύστημα υπολογιστών χωρίς, κατ' αρχήν, να έχουν το σκοπό της υποκλοπής ή της οποιαδήποτε άλλης επιβλαβούς ενέργειας. Όμως, η εισβολή στο δίκτυο, έστω και αν δεν είναι κακόβουλη, υποκρύπτει ένα κακόβουλο χαρακτήρα, διότι ο επιτιθέμενος εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του, εντοπίζει τις ευπάθειες του και μπορεί, πλέον, ευκολότερα να διαπράξει μια κακόβουλη επίθεση ή να διαθέσει τις πληροφορίες αυτές σε κάποιον που θέλει να διαπράξει την επίθεση

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.

3.2.1.1. Βασικές τεχνικές των hackers[21]

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 δραστηριότητες του, οι συνήθειές του κ.λπ. 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, scan): 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 διακομιστές, 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 την 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 των αριθμών 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 αυτές, οι εισβολείς παρεμβάλουν 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 επιθέσεων. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για να αποκρύψει την πραγματική IP διεύθυνση του επιτιθέμενου σε μία επίθεση Ping of Death.

Επιθέσεις σε επίπεδο εφαρμογής: Στις επιθέσεις αυτές, γίνεται εκμετάλλευση γνωστών αδυναμιών των δικτυακών εφαρμογών. Για παράδειγμα, οι φυλλομετρητές, όπως ο Internet Explorer, συχνά παρουσιάζουν σημαντικά προβλήματα ασφαλείας. Επιπλέον, οι

---

[21] Κωνσταντίνος Βλαζόπουλος 2007σελ 40

σύγχρονες γλώσσες προγραμματισμού (π.χ. java, php κ.λπ.), που χρησιμοποιούνται για τη δημιουργία δικτυακών τόπων με δυναμικό περιεχόμενο, εμφανίζουν σημαντικές αδυναμίες ασφάλειας.

3.2.2. Επιθέσεις άρνησης εξυπηρέτησης

Οι επιθέσεις Άρνησης εξυπηρέτησης (Denial of Service Attacks) αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή, ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό συχνά ισοδυναμεί με τη διακοπή λειτουργίας μιας κρίσιμης υπηρεσίας ή συνόλου υπηρεσιών που προσφέρονται από έναν ή περισσότερους διακομιστές, με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό. Οι επιθέσεις αυτές στοχεύουν:

- Στην παρεμπόδιση της μετάδοσης των δεδομένων στο δίκτυο.
- Στην παρεμπόδιση σύνδεσης μεταξύ δύο σημείων, κάτι που ενδεχομένως σημαίνει αδυναμία πρόσβασης σε συγκεκριμένες υπηρεσίες
- Στην αλλοίωση της ποιότητας μιας υπηρεσίας, που προσφέρεται σ' έναν χρήστη.

Οι επιθέσεις άρνησης εξυπηρέτησης, δεν απαιτούν τη χρήση σύγχρονου υλικού και λογισμικού και ευρυζωνικών. Ακόμη και ένας παλιός υπολογιστής με μια απλή dial-up σύνδεση, μπορεί να χρησιμοποιηθεί εναντίον μεγάλων συστημάτων υπολογιστών και δικτύων προκαλώντας την πλήρη κατάρρευση τους. Αυτός ο τύπος επίθεσης, χαρακτηρίζεται ως ασύμμετρη επίθεση.

Τεχνικές επιθέσεων DOS

Ποικίλες τεχνικές χρησιμοποιούνται για επιθέσεις άρνησης εξυπηρέτησης, όπως SYN Flood Attacks, UDP Flood Attacks, ICMP Flood Attacks, Teardrop Attacks, ping of death, port flooding, OOP Attacks, Fragmentation, Smurf Attacks, Fraggle Attacks και Papasmurf Attacks[22]. Ας δούμε συνοπτικά τις σημαντικότερες από αυτές:

SYN Flood Attacks: Στις επιθέσεις, αυτές ο επιτιθέμενος εκμεταλλεύεται τα πακέτα SYN και ACK. Όταν ένας Η/Υ (έστω Α) θέλει να συνδεθεί μ' έναν άλλο (έστω Β) του αποστέλλει ένα πακέτο SYN, στο οποίο ο Α απαντάει με ένα πακέτο SYN/ACK (acknowledge). Όταν ο Α λάβει το SYN/ACK, θεωρεί ότι, η σύνδεση έχει ολοκληρωθεί και στέλνει για επιβεβαίωση ένα ακόμη πακέτο ACK[23]. Για να πραγματοποιηθεί η επίθεση, ο επιτιθέμενος στέλνει συνεχώς στον Β πακέτα SYN, αλλά όχι ACK. Ο Β απαντάει στα SYN και περιμένει τα ACK για επιβεβαίωση, τα οποία, όμως, ουδέποτε στέλνονται από το Β. Αποτέλεσμα είναι, η δέσμευση των πόρων του Α, που οδηγεί στην κατάρρευσή του.

Ping of Death: το Ping είναι μια δικτυακή εφαρμογή, με την οποία διαπιστώνεται εάν μια δεδομένη διεύθυνση IP είναι προσβάσιμη. Ο επιτιθέμενος, στέλνει έναν αριθμό πακέτων σε μια διεύθυνση Η/Υ, ο οποίος, απαντάει στέλνοντας παρόμοια μηνύματα (ping). Για να ολοκληρωθεί η επίθεση αρκεί η αποστολή πάρα πολλών μηνυμάτων ping στα οποία ο server είναι αναγκασμένος να απαντήσει δαπανώντας υπολογιστή ισχύ και bandwidth, με

---

[22] Για μια πλήρη περιγραφή των επιθέσεων άρνησης εξυπηρέτησης βλέπε Sinrod, E. And Reilly, W. Page:14

[23] Η διαδικασία αυτή, αποτελεί βασικό χαρακτηριστικό του πρωτοκόλλου TCP/IP και ονομάζεται χειραψία τριών βημάτων (three-way handshake).

αποτέλεσμα οι πόροι του να εξαντλούνται και να μην μπορεί να προσφέρει άλλες υπηρεσίες (π.χ. αποστολή web σελίδων)

Fragmentation: Όταν δύο Η/Υ επικοινωνούν με το πρωτόκολλο TCP/IP, τα πακέτα δεδομένων που αποστέλλονται, περιέχουν μια σειρά από στοιχεία ελέγχου, μέσω των οποίων, ο παραλήπτης ελέγχει, αν έφτασαν σε καλή κατάσταση. Σε αρνητική περίπτωση, ο παραλήπτης επικοινωνεί με τον αποστολέα και του ζητάει να ξαναστείλει τα πακέτα που αλλοιώθηκαν, κατά τη μεταφορά. Εκμεταλλευόμενος αυτό το χαρακτηριστικό, ο επιτιθέμενος στέλνει, συνεχώς, πακέτα με λανθασμένα στοιχεία ελέγχου. Έτσι, υποχρεώνει τον παραλήπτη, να σπαταλά υπολογιστική ισχύ και εύρος ζώνης (bandwidth), ζητώντας την επανάληψη της αποστολής τους. Αν η επίθεση συνεχιστεί για μεγάλο χρονικό διάστημα ή αν γίνεται από μια γρήγορη γραμμή, το θύμα θα υποχρεωθεί να αποσυνδεθεί από το δίκτυο.

Κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης

Οι «κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης» (Distributed Denial of Service Attacks), χρησιμοποιούν ένα συνδυασμό των παραπάνω τεχνικών και ολοκληρώνονται σε τέσσερα βήματα:

1. Αρχικά, ο επιτιθέμενος εγκαθιστά προγράμματα απομακρυσμένης διαχείρισης σε συνήθως μεγάλο αριθμό Η/Υ, που διαθέτουν ευρυζωνικές συνδέσεις στο Διαδίκτυο. Το πρόγραμμα απομακρυσμένου ελέγχου, κατόπιν εντολής του επιτιθέμενου (trigger), πραγματοποιεί απόπειρες σύνδεσης προς το θύμα (π.χ. πακέτα ping ή σύνδεση σε δικτυακό τόπο)

2. Όταν ο επιτιθέμενος είναι έτοιμος να αρχίσει την επίθεση του, δίνει εντολή στο πρόγραμμα, να ξεκινήσει να στέλνει «ping» σε μια συγκεκριμένη διεύθυνση. Ο υπολογιστής που περιέχει το απομακρυσμένο πρόγραμμα διαχείρισης, λειτουργεί ως «zombie»[24].

3. Ο υπολογιστής του θύματος (έστω Α) απαντάει σε κάθε ping, αλλά, επειδή, ο υπολογιστής zombie (έστω Β) έχει δώσει λάθος διεύθυνση για τα pings (π.χ. επίθεση IP spoofing), ο Α δεν μπορεί να επιτύχει σύνδεση με το Β. Ωστόσο, ο Α περιμένει απάντηση στα ping που έχει στείλει, ενώ ο Β και όσοι άλλοι υπολογιστές λειτουργούν ως zombie, συνεχίζουν να στέλνουν νέα ping , με αποτέλεσμα, οι πόροι του Α να εξαντλούνται από την πληθώρα των αιτημάτων και να μην μπορούν να προσφέρουν άλλες υπηρεσίες.

4. Συνήθως, μετά από κάποιο χρονικό διάστημα, ο επιτιθέμενος δίνει εντολή στα προγράμματα απομακρυσμένου ελέγχου, να σταματήσουν να στέλνουν ping, προκειμένου, να μην είναι δυνατό να εντοπιστεί από που προέρχεται η επίθεση.

[24] Με τον όρο zombie αναφέρεται ένα σύστημα, το οποίο μέσω της χρήσης κατάλληλων εργαλείων λογισμικού, επιτρέπει στον επιτιθέμενο να το διαχειρίζεται από απόσταση

Υπόθεση Mafiaboy

Κατά το έτος 2000, έλαβαν χώρα μια σειρά από επιθέσεις άρνησης εξυπηρέτησης σε δικτυακούς τόπους σημαντικών εταιριών, που δραστηριοποιούνται στο χώρο του Διαδικτύου. Ανάμεσα στα θύματα ήταν: Yahoo, Amazon.com, buy.com, cnn.com, ebay.com κ.α. Για τις επιθέσεις αυτές, χρησιμοποιήθηκαν οι υπολογιστές των Πανεπιστημίων του Stanford στην Καλιφόρνια, οι οποίοι έστελναν, συνεχώς, «ping». Κατά τη διερεύνηση της υπόθεσης, αποκαλύφθηκε ότι ο δράστης της επίθεσης, ήταν ένας 15χρονος μαθητής από το Montreal του Καναδά, ο οποίος εμφανιζόταν στο Διαδίκτυο με το ψευδώνυμο MafiaBoy.

Ο MafiaBoy απασχόλησε τις διωκτικές αρχές έως τα τέλη του 2001. Εντυπωσιακές είναι οι ποινές που του επιβλήθηκαν, καθότι ως ανήλικος αντιμετωπίζονταν επιεικώς από το ισχύον νομικό πλαίσιο. Για παράδειγμα, μετά την αποκάλυψη της δράσης του, η αστυνομία του Καναδά, τον άφησε ελεύθερο με τους ακόλουθους περιοριστικούς όρους:

- Μπορούσε να χρησιμοποιήσει τον Η/Υ μόνο υπό την επίβλεψη του καθηγητή του.
- Του απαγορεύτηκε να συνδέεται στο Διαδίκτυο.
- Του απαγορεύτηκε να εισέρχεται σε εταιρίες και καταστήματα που δραστηριοποιούνταν στο χώρο της πληροφορικής.
- Του απαγορεύτηκε η επικοινωνία με τρεις από τους στενούς φίλους του.

Πηγή: http://www.rbs2.com/ccrime.htm#anchor111666

3.2.3. Κακόβουλο λογισμικό

Ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του Διαδικτύου, είναι η διασπορά κακόβουλου κώδικα. Ο κακόβουλος κώδικας είναι κώδικας Η/Υ, που δημιουργείται με σκοπό να προκαλέσει ζημιά σε 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

Ο κακόβουλος κώδικα σε τρεις βασικές κατηγορίες : Ιούς, σκουλήκια και δούρειους ίππους.

3.2.3.1. Ιοί

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,
  1. Που θα του εξασφαλίζει, ότι οι οδηγίες του θα εκτελούνται κατά προτεραιότητα
  2. Ώστε ο χρήστης να μην μπορεί να αντιληφθεί την εκτέλεση του. Κατ'αυτόν τον τρόπο ο εντοπισμός του λογισμικού γίνεται δυσχερής
- Η εκτέλεση του, έχει δύο βασικές λειτουργίες: Την αναπαραγωγή του και την πρόκληση ζημίας.
- Προσπαθεί να μολύνει προγράμματα, τα οποία είναι πιθανό να σταλούν ή να μεταφερθούν σε άλλο υπολογιστικό σύστημα.

Κυριότερες μορφές ιών[25]:

- File inflectors or Parasitic viruses
- Boot Sector Virus
- Multi-partite Viruses
- Companion Viruses
- Link and Flash Bios
- Macro viruses

Αναζητώντας την απαρχή των ιών θα πρέπει να ανατρέξουμε στο 1949[26], τότε που ο μαθηματικός John Von Neumann περιέγραψε για πρώτη φορά τα προγράμματα που έχουν δυνατότητα να αυτό-αναπαράγονται τα οποία θα μπορούσε πει κανείς ότι μοιάζουν με τους ιούς όπως τους ξέρουμε σήμερα. Ωστόσο, ο πραγματικός πρόγονος των σύγχρονών ιών δεν εμφανίστηκε παρά μόνο την δεκαετία του 60. Σ' εκείνη την δεκαετία, μια ομάδα προγραμματιστών ανέπτυξαν ένα παιχνίδι με όνομα «Core Wars», το οποίο μπορούσε να αναπαράγει τον εαυτό του κάθε φορά που εκτελούνταν, καταφέρνοντας ακόμη και να προκαλεί τον κορεσμό της μνήμης των υπολογιστών των υπόλοιπων παικτών. Οι δημιουργοί αυτού του μάλλον παράξενου παιχνιδιού δημιούργησαν επίσης, το πρώτο antivirus: μια εφαρμογή ονόματι «Reeper», η οποία μπορούσε να «καταστρέφει» τα αντίγραφα που δημιουργούσε το «Core Wars».

Η πρώτη επιστημονική μελέτη του φαινομένου των ιών έγινε το 1983 από τον Cohen[27]. Εκείνη την εποχή, το νεαρότατο σε ηλικία MS-DOS μόλις άρχιζε την εκπληκτική πορεία του σαν το πλέον επικρατέστερο λειτουργικό σύστημα με πολλές αρετές, αλλά και πολλές αδυναμίες, οι οποίες οφείλονταν, κυρίως, στο γεγονός ότι η ανάπτυξη τόσο του λογισμικού, όσο και του υλικού ήταν ακόμη σε πολύ πρώιμο στάδιο. Παρόλα αυτά, όμως,

---

[25] Κωνσταντίνος Βλαχόπουλος 2007 σελ 48
[26] Αναστασία Ζάννη 2005 σελ 91-93
[27] http://all.net. (Ημερομηνία πρόσβασης 15/07/09)

το νέο λειτουργικό σύστημα αποτέλεσε στόχο ενός ιού το 1966: συγκεκριμένα του «Brain», μιας μορφής εχθρικού κώδικα, δημιουργημένης στο Πακιστάν , η οποία μόλυνε τον τομέα εκκίνησης των δίσκων, καθιστώντας απροσπέλαστο το περιεχόμενο τους. Εκείνη την χρονιά γεννήθηκε, επίσης, ο πρώτος Δούρειος Ίππος: μια εφαρμογή με όνομα PC- Write. Πολύ γρήγορα, οι δημιουργοί ιών αντελήφθησαν ότι η μόλυνση των αρχείων θα μπορούσε να είναι ακόμα πιο καταστροφική για τα συστήματα υπολογιστών. Το 1987 εμφανίστηκε ένας ιός με όνομα Suriv-02, ο οποίος μόλυνε αρχεία με επέκταση COM και, ουσιαστικά, «άνοιγε την πόρτα» για δύο άλλους ιούς που έμειναν στην ιστορία : τον Jerusalem και τον Viernes 13.

Ωστόσο τα χειρότερα έπονταν: το 1988 ήταν η χρονιά που εμφανίστηκε το worm «Morris», μολύνοντας 6,00 υπολογιστές. Από εκείνη την χρονιά μέχρι το 1995, άρχισαν να αναπτύσσονται οι διάφορες μορφές εχθρικού κώδικα που γνωρίζουμε σήμερα: εμφανίστηκαν οι πρώτοι ιοί μακροεντολών, οι πολυμορφικοί ιοί, κ.α. Ορισμένοι εξ αυτών κατάφεραν να προκαλέσουν φαινόμενα επιδημίας, όπως ο MichaelAngelo. Ωστόσο υπήρξε ένα επόμενο συμβάν, το οποίο άλλαξε ένα επόμενο συμβάν, το οποίο άλλαξε άρδην τα πάντα για τον κόσμο των ιών: η μαζική χρήση του Internet και του ηλεκτρονικού ταχυδρομείου. Σιγά σιγά οι ιοί άρχισαν να προσαρμόζονται στη νέα κατάσταση των πραγμάτων, μέχρι το 1999, όταν εμφανίστηκε ο ιός Melissa -η πρώτη μορφή εχθρικού κώδικα που προκάλεσε πραγματικά παγκόσμια επιδημία- σηματοδοτώντας την αρχή μιας νέας εποχής για τους ιούς υπολογιστών. Σήμερα υπάρχουν 18,000 διαφορετικοί ιοί, που χωρίζονται σε δύο μεγάλες κατηγορίες. Η πρώτη περιλαμβάνει τους ιούς που προβάλλουν εκτελέσιμα προγράμματα και η δεύτερη τους μακροιούς που βασίζονται στα χαρακτηριστικά της visual basic και μολύνουν αρχεία δεδομένων.

Melissa Marco Virus

Ο Melissa Marco Virus, αποτελεί την κλασικότερη μορφή μακρο-ιού. Εμφανίστηκε τον Μάρτιο του 1999. Έφτανε στον παραλήπτη μέσω e-mail, σε ένα συνημμένο αρχείο τύπου Word, το οποίο όταν ανοίγονταν περιείχε μια λίστα από κωδικούς για δικτυακούς τόπους, που προσφέρουν πορνογραφικό υλικό. Παράλληλα, όμως, χωρίς να το γνωρίζει ο χρήστης, ενεργοποιούνταν μια μακροεντολή, η οποία διάβαζε τις 50 πρώτες διευθύνσεις του βιβλίου διευθύνσεων του Outlook και έστελνε τον εαυτό της, στις διευθύνσεις αυτές. Ο ιός διαδόθηκε τόσο γρήγορα, που μέσα σε 48 ώρες ανάγκασε την Microsoft και την Intel, να κλείσουν τους διακομιστές τους. Μάλιστα μια εταιρεία 500 υπαλλήλων ανέφερε ότι μέσα σε 45 λεπτά, έλαβε πάνω από 32000 e-mails. Πηγή: Sinrod, E. and Reilly, W. (2000).

Οι ιοί μας ανησυχούν γιατί επιτελούν, πλέον σε μεγάλο ποσοστό καταστροφικό έργο. Τι μπορεί να κάνει ένας ιός; Όπως αναφέραμε και πιο πάνω, στο πιο ευνοϊκό σενάριο είναι μία απλή ενόχληση. Στη χειρότερη περίπτωση μπορεί να οδηγήσει στην πλήρη καταστροφή των δεδομένων του υπολογιστή και να επεκτείνει την δράση του, μέσω δικτύων, δισκετών ή CD-ROM σε συνεργάτες, φίλους και συναδέλφους ακόμα, όμως, και σε άγνωστους παραλήπτες. (Για παράδειγμα ο Sobig[28] ή αλλιώς «ο ιός του email» μπλόκαρε τα συστήματα χιλιάδων υπολογιστών ανά τον κόσμο και διέκοψε τις εργασίες, μέσω Διαδικτύου, διεθνών οργανισμών, κρατικών υπηρεσιών και μεγάλων εταιριών.

[28] Αναστασία Ζάννη 2005 σελ. 93

Υπολογίζεται ότι προσβλήθηκαν 150 χώρες) Στην τελευταία αυτή περίπτωση αν δεν έχουν ληφθεί τα κατάλληλα μέτρα, οι οικονομικές συνέπειες είναι τεράστιες, συνέπειες που μπορούν να οδηγήσουν στην κατάρρευση της παραγωγικότητας της εργασίας ,η οποία θα διαρκέσει μεγάλο χρονικό διάστημα, στην αναστολή των εργασιών και ενδεχομένως, αν πρόκειται περί επιχειρήσεων σε πτώχευση

3.2.3.2. 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.

ILOVEYOU WORM

Το πιο διάσημο σκουλήκι όλων των εποχών, είναι το I LOVE YOU[1]. Το σκουλήκι έφτανε στον Η/Υ του θύματος με e-mail, με θέμα ILOVEYOU και ένα συνημμένο αρχείο LOVE-LETTER-FOR-YOU.VPS. Το e-mail, από μόνο του είναι αθώο, όμως, όταν κάποιος χρήστης άνοιγε το συνημμένο αρχείο, εκτελούνταν ένα πρόγραμμα Visual Basic το οποίο:

1. Διέγραφε αρχεία από τον υπολογιστή.
2. Όριζε, ως αρχική σελίδα το Internet Explorer, μία σελίδα σ' ένα διακομιστή στις Φιλιππίνες και αυτόματα γινόταν λήψη ενός δούρειου ίππου, ο οποίος είχε την δυνατότητα να υποκλέπτει κωδικούς πρόσβασης του χρήστη και να τους αποστέλλει στο e-mail του δημιουργού του ιού.
3. Πολλαπλασιάζονταν, χρησιμοποιώντας της μεθοδολογία του Melissa Virus, με την διαφορά ότι έστελνε τον εαυτό του σ' όλες τις διευθύνσεις, που υπήρχαν στο βιβλίο διευθύνσεων και όχι μόνο στις πρώτες 50

Το σκουλήκι ILOVEYOU, επηρέασε περισσότερους από τους μισούς ηλεκτρονικούς υπολογιστές στην Αμερική και πάνω από 100.00 διακομιστές στην Ευρώπη. Εκτιμάται, ότι προκάλεσε την μεγαλύτερη καταστροφή στην εταιρεία των ηλεκτρονικών υπολογιστών, καθώς οι συνολικές ζημιές ξεπέρασαν τα 9.000.000.000$

Πηγή: http://www.pchell.com/virus/loveletter.shtml

Το 2001 το σκουλήκι Code Red II [19]προκάλεσε μια από τιε μεγαλύτερες καταστροφές στην ιστορία του Διαδικτύου. Σε χρονικό διάστημα 14 ωρών, προσέβαλε 359.00 συστήματα ανά λεπτό. Ο μολυσμένος πληθυσμός διπλασιάζονταν κάθε 37 λεπτά. Η συνολική οικονομική ζημιά, πολύ λίγο χρόνο μετά την εμφάνιση του, ξεπέρασε τα δύο δισεκατομμύρια δολάρια, με ρυθμό διακόσια εκατομμύρια δολάρια την ημέρα. Άλλα

[19] Για τον τρόπο λειτουργίας και εξάπλωσης του σκουληκιού http://www.cert.org/advisories/CA-2001-19.html (Ημερομηνία πρόσβασης 20/07/09)

σύγχρονα σκουλήκια, που προκάλεσαν σημαντικές ζημιές είναι : Slammer, Blaster, So Big, Beagle, My Doom και Netsky[30].

3.2.3.3. Δούρειοι Ίπποι (Trojan Horses)

Οι Δούρειοι Ίπποι 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.(π.χ. acrobat, winzip κ.α.)

Με την χρήση ενός Δούρειου Ίππου ο επιτιθέμενος επιτυγχάνει να αποκτήσει απομακρυσμένο 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 Bark Orifice[31], που εμφανίστηκε το 2000. Έφτανε στα υποψήφια θύματα με την μορφή συννημένου αρχείου σε μήνυμα ηλεκτρονικού ταχυδρομείου, που όταν εκτελούνταν από το θύμα εγκαθιστούσε στον υπολογιστή του ένα πρόγραμμα διακομιστή. Στη συνέχεια, ο επιτιθέμενος, εγκαθιστούσε στο δικό του υπολογιστή ένα πρόγραμμα πελάτη και έδινε εντολές στον server του θύματος. Με τον τρόπο αυτό, εκτός από τον πλήρη έλεγχο του υπολογιστή του θύματος, ήταν ακόμη δυνατόν, ο επιτιθέμενος να διαπράξει διαδικτυακά εγκλήματα, τα οποία να φαίνεται ότι τελέστηκαν από τον υπολογιστή του θύματος του[32]

3.2.3.4. Ad-ware, Spyware και dialers

Το ad-aware και spyware είναι προγράμματα που περιέχουν κακόβουλο κώδικα. Θεωρούνται υποκατηγορία των δούρειων ίππων, ωστόσο τα εξετάζουμε χωριστά λόγω της μεγάλης εξάπλωσης τους. Τα ad-aware χρησιμοποιούνται, για την διαφημιστική προώθηση συγκεκριμένων δικτυακών τόπων και προϊόντων που προσφέρονται μέσω του Διαδικτύου. Ενδέχεται να αποτελούν νόμιμο λογισμικό εφόσον η λειτουργία τους ορίζεται ρητά στους όρους χρήσης που αποδέχεται ο χρήστης κατά την εγκατάσταση τους. Σε αντίθετη περίπτωση θεωρούνται κακόβουλο λογισμικό.

Σε αντίθεση με τα ad-aware τα spyware είναι, κατεξοχήν, κακόβουλο λογισμικό που υποκλέπτει πληροφορίες, που αφορούν το χρήστη. Οι πληροφορίες αυτές αφορούν ευαίσθητα δεδομένα, όπως τα προσωπικά στοιχεία του χρήστη, τους κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, στοιχεία λογαριασμών και συναλλαγών κ.α. Για την υποκλοπή των δεδομένων χρησιμοποιούνται διάφορες τεχνικές όπως για παράδειγμα λογισμικό keylogger[33], το οποίο υποκλέπτει κάθε χαρακτήρα που

---

[30] R. Standler. Examples of malicious computer programs (Part 1 &2). Διαθέσιμα στο: http://www.rbs2.com/cvirus2.pdf (Ημερομηνία πρόσβασης 20/07/09)
[31] http://irchelp.org/irchelp/security/bo.html (Ημερομηνία πρόσβασης 20/07/09)
[32] Sinrod, E. and Reilly, W. 2000. (Ημερομηνία πρόσβασης 25/07/09)
[33] Τρόπος λειτουργίας των keyloggers http://www.securityfocus.com/infocus/1829/ (Ημερομηνία πρόσβασης 21/07/09)

πληκτρολογεί ο χρήστης. Τα δεδομένα που υποκλάπηκαν είναι δυνατό να σταλούν στον επιτιθέμενο ακόμα και με e-mail.

Συνήθως τα spyware συνεργάζονται με τα ad-aware για την δημιουργία προφίλ χρηστών, που αποσκοπούν στην αποστολή στοχευόμενων διαφημίσεων, όμως, μπορούν να προκαλέσουν και μια σειρά από άλλα ανεπιθύμητα αποτελέσματα, όπως καταστροφή αρχείων, αποσταθεροποίηση του συστήματος, επιβράδυνση της περιήγησης στο Διαδίκτυο και της εν γένει λειτουργίας του υπολογιστή. Η απεγκατάσταση τους είναι εξαιρετικά δύσκολη.

Χαρακτηριστική κατηγορία των προγραμμάτων spyware, είναι η dialers. Οι dialers είναι μικρά προγράμματα τα οποία έχουν την δυνατότητα να αποσυνδέουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής και τον τοπικό πάροχο υπηρεσιών internet(ISP) και να καλούν αυτόματα ένα υψηλής χρέωσης αριθμό για πρόσβαση, σε συγκεκριμένες υπηρεσίες χωρίς την συνειδητή συγκατάθεση του χρήστη.

Οι dialers προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες. Αυτές μπορεί να παρέχουν πειρατικό λογισμικό, πορνογραφικό ή άλλο αμφιλεγόμενο περιεχόμενο. Οι ιδιώτες αυτών των ιστοσελίδων έχουν το dialer λογισμικό ενσωματωμένο στον κώδικα του δικτυακού τους τόπου, ώστε να γίνεται αυτόματα λήψη και να εγκαθίσταται στο σύστημα του χρήστη, χωρίς να γίνεται αντιληπτό και χωρίς να ζητείται απαραίτητα η συγκατάθεση του. Ένας άλλος τρόπος μετάδοσης αυτών των προγραμμάτων, είναι με τη μορφή συνημμένο αρχείων σε μηνύματα ηλεκτρονικής αλληλογραφίας. Το συνημμένο αρχείο φέρει ένα συνηθισμένο όνομα το οποίο παραπλανά των χρήστη (π.χ. askisi.doc) όταν όμως εκτελεστεί, εγκαθιστά χωρίς να το γνωρίζει μια εφαρμογή dialer.

Αποτέλεσμα της χρήσης των dialers είναι ο πλουτισμός των κατόχων συγκεκριμένων δικτυακών τόπων, από τις υπέρογκες τηλεφωνικές χρεώσεις.

3.2.3.5. Λογικές και ωρολογιακές βόμβες (logic-bomb)

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

Οι ιοί Jerusalem και Michaelangelo

Ο ιός Jerysalem αποτελεί κλασική περίπτωση λογικής βόμβας. Εμφανίστηκε το 1987 και είχε την δυνατότητα να σβήνει όλα τα προγράμματα που εκτελούσε ο χρήστης εφόσον η ημερομηνία του συστήματος ήταν Παρασκευή και 13.

Ο ιός Michaelangelo ήταν προγραμματισμένος να απενεργοποιήσει τους μολυσμένους Η/Υ στις 6 Μαρτίου 1992

Πηγή:http://www.faqs.org/abstracts/News-opinion-and-commentary/Be-careful-computing-its-almost-virus-season-On-the-road-with-a-little-modem-called-Worldport-9600-i.html

3.2.3.6. Φάρσες (hoax)

Μια φάρσα είναι μια προειδοποίηση για έναν ιό, που δεν υπάρχει. Στη συνήθη μορφή, είναι μηνύματα ηλεκτρονικού ταχυδρομείου που στέλνονται στο χρήστη και τον προειδοποιούν για κάτι άσχημο, που θα συμβεί στον υπολογιστή του, χωρίς όμως αυτό να ανταποκρίνεται στην πραγματικότητα. Μια πρώτη σκέψη είναι, ότι οι φάρσες δεν θα έπρεπε να περιληφθούν στο κακόβουλο λογισμικό. Αναλογιζόμενοι, όμως, ότι κατά καιρούς, έχουν χρησιμοποιηθεί για διάφορα επιβλαβή αποτελέσματα (κατανάλωση bandwidth, επιθέσεις DOS σε mail server) και έχουν προκαλέσει πανικό στους χρήστες, που οδηγήθηκαν ακόμη και στην διαγραφή χρήσιμων αρχείων από τους υπολογιστές τους, μπορούμε να τις θεωρήσουμε ως μια ιδιαίτερη μορφή λογισμικού, με κακόβουλες προεκτάσεις.

Το ακόλουθο μήνυμα-φάρσα προειδοποιεί τον παραλήπτη ότι ο υπολογιστής του θα σταματήσει να λειτουργεί, καθώς έχει μολυνθεί από ένα σκουλήκι που δεν είναι δυνατόν να εντοπισθεί από το λογισμικό antivirus. Εντοπίστηκε στις 11-09-2003

"GOT YOU"

If you were dumb enough to open this email then you will find a WORM has executed itself through your mailbox and by the time you read this into your hard-drive. This is PAYBACK for the Virus you disguised in the email you sent to us recently which destroyed our hard-drive and back-up system. This costs us thousands of dollars and we lost a lot of irreplaceable files on our system.

Now it's your turn to have your computer infected. This WORM it is undetectable by AntiVirus software and it will drive your computer crazy because it's always hiding and causing havoc in your system. Using your computer recovery disks will not remove the problem cause it still stays on your computers Motherboard. This will probably cost you a new computer and I sincerely hope this teaches you a lesson not to send people nasty viruses again.

Evocash Administration Inc.
Phone:+17674499922
Fax: +1 767 4499922
----^+Start^=Auto^Execute+^WORM^---------
----^+Start^=Auto^Execute+^WORM^----------
----^+Start^=Auto^Execute+^WORM^---------
----^+Start^=Auto^Execute+^WORM^---------
----^+Start^=Auto^Execute+^WORM^---------

Πηγή: http://www.lindqvist.com/index.php?ID=1434

3.2.3.7. Τεχνικές απόκρυψης ιών

Οι περισσότεροι ιοί, λίγο χρόνο μετά την δημιουργία τους, εντοπίζονται από εταιρείες αντιβιοτικού λογισμικού (antivirus software) , οι οποίες ενημερώνουν τις βάσεις τους με το κατάλληλο λογισμικό, για την αντιμετώπισή τους. Ωστόσο, οι τεχνικές που χρησιμοποιούν για τη δημιουργία των νέων ιών συνεχώς βελτιώνονται.

Οι αόρατοι ιοί (stelth), έχουν την δυνατότητα, να παραμένουν ενεργοί στη μνήμη, να μολύνουν τα προγράμματα που εκτελούνται, κατόπιν, μιας νόμιμης εντολής του χρήστη και ταυτόχρονα να παρακάμπτουν το πρόγραμμα antivirus, όταν εκτελεί έλεγχο ακεραιότητας.

Οι Πολυμορφικοί ιοί (polymorphic, self-mutating) δημιουργούν αντίγραφα του εαυτού τους, τα οποία διαφέρουν μεταξύ τους, ωστόσο έχουν, τα ίδια καταστροφικά αποτελέσματα. Τα καινούρια αντίγραφα εμπεριέχουν μια μορφή «θορύβου» (π.χ. άσκοπες εντολές ή τροποποίηση της σειράς τους), με αποτέλεσμα, τα προγράμματα antivirus να μην μπορούν να τους εντοπίσουν.

3.2.4. Ανεπιθύμητη Αλληλογραφία (Spamming)

Η ανεπιθύμητη αλληλογραφία, 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 διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιοδήποτε 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.[34]

Η δυνατότητα που προσφέρει το Διαδίκτυο, για φθηνή και άμεση αποστολή εκατομμύριων μηνυμάτων, ωθεί τις ανά τον κόσμο εταιρείες, στην υιοθέτηση τέτοιων μεθόδων για την προώθηση των προϊόντων τους. Η συλλογή των ηλεκτρονικών διευθύνσεων, μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Οι spammers παίρνουν τις διευθύνσεις από τους καταλόγους εταιρειών, που διατηρούν ηλεκτρονικά καταστήματα ή χρησιμοποιούν λογισμικό τύπου harvester[35], το οποίο σαρώνει όλο το internet και συλλέγει χιλιάδες διευθύνσεις από κατάλογους, δωμάτια συζητήσεων newsgroups κ.λπ. Άλλοι, υποκλέπτουν ηλεκτρονικές διευθύνσεις από τους καταλόγους μελών των εταιρειών παροχής internet (ISP). Τέλος, μπορεί να χρησιμοποιηθεί και ειδικό λογισμικό, το οποίο παράγει τεράστιες λίστες τυχαίων διευθύνσεων.[36]

> Σύμφωνα με την αμερικανική εταιρεία Postini, ο αριθμός των ανεπιθύμητων διαφημιστικών e-mail σε όλο τον κόσμο τριπλασιάστηκε από τον Ιούνιο έως το Νοέμβριο καταγράφηκαν 7 δις. μηνύματα spam συγκριτικά με 2,5 δις. τον Ιούνιο. Πλέον το spam αντιστοιχεί σε πάνω από 80% του συνόλου των μηνυμάτων που διακινούνται στο Διαδίκτυο.

Εκτός από διαφημιστικούς σκοπούς, το spamming μπορεί να χρησιμοποιηθεί και ως βασικό εργαλείο για μια σειρά άλλων επιθέσεων, όπως τις επιθέσεις άρνησης

---

[34] http://en.wikipedia.org/wiki/Spam_%28electronic%29#History (Ημερομηνία πρόσβασης 18/08/09)

[35] http://www.programurl.com/software/harvester.htm (Ημερομηνία πρόσβασης 25/08/09)

[36] Για παράδειγμα το εμπορικό λογισμικό EmailGenerator Platinum 9.0, έχει την δυνατότητα όχι μόνο να παράγει τεράστιες λίστες τυχαίων διευθύνσεων αλλά να εξακριβώνει εάν είναι έγκυρες ή όχι. Για περισσότερες πληροφορίες http://www.email-business.com/index_en.htm (Ημερομηνία πρόσβασης 25/08/09)

εξυπηρέτησης. Στις περιπτώσεις αυτές, οι επιτιθέμενοι κατακλύζουν το διακομιστή με πλήθος μηνυμάτων και τον οδηγούν έτσι σε υπερφόρτωση.

3.2.5. Επιθέσεις σε Δικτυακούς τόπους

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

Σε μια τυπική επίθεση σ' ένα δικτυακό τόπο, το αποτέλεσμα είναι αναστρέψιμο. Ο βάνδαλος θα διαγράψει ορισμένες σελίδες ή γραφικά και θα ανεβάσει 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.

Επίθεση hackers σε δικτυακούς τόπους υπουργείων των ΗΠΑ

Τον Απρίλιο του 2001, Κινέζοι hackers παραβίασαν τους δικτυακούς τόπους των Υπουργείων Εργασίας και Υγείας των ΗΠΑ, θέτοντας τους για μικρό χρονικό διάστημα εκτός λειτουργίας. Ο δικτυακός τόπος του Υπουργείου Εργασίας δεν λειτούργησε για λίγες ώρες, καθώς το περιεχόμενο μιας ιστοσελίδας αντικαταστάθηκε από τους hackers με φωτογραφία Κινέζου πιλότου που χάθηκε κατά την εναέρια σύγκρουση του μαχητικού του με αμερικάνικο κατασκοπευτικό αεροσκάφος.

Επίσης, ο δικτυακός τόπος του Υπουργείου Υγείας είχε αλλοιωθεί για κάποια ώρα από την φωτογραφία ενός ένστολου Κινέζου, η οποία συνοδευόταν από ένα ακατάληπτο μήνυμα.

Πηγή: Κωνσταντίνος Βλαχόπουλος 2007 σελ.57

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.

3.2.6. 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, προέβαινα σε κατοχύρωση ονομάτων διάσημων εταιρειών, με αποτέλεσμα να αποκτούν τα δικαιώματα της νέας διεύθυνσης. Στη συνέχεια, μπορούσαν να δράσουν με δύο διαφορετικούς τρόπους: είτε να προχωρήσουν την διεύθυνση στην εταιρεία που κατέχει το συγκεκριμένο όνομα, έναντι, βέβαια σημαντικού χρηματικού ποσού[37], είτε να προβούν

[37] Τη συγκεκριμένη μέθοδο χρησιμοποίησε ο David Topen, ο οποίος αντιλαμβανόμενος τον σημαντικό ρόλο που θα διαδραμάτιζαν στο ηλεκτρονικό εμπόριο που μόλις αναπτύσσονταν τα ονόματα χωρών, κατοχύρωσε πάνω από 100 διευθύνσεις σημαντικών εταιρειών, όπως Delta Air Lines, Lufthansa, American

στην ανάρτηση, στην συγκεκριμένη διεύθυνση, περιεχόμενου προσβλητικού (π.χ. πορνογραφία), γεγονός που επιφέρει σημαντικές συνέπειες στην εταιρεία.

Στην πορεία, βέβαια, χρησιμοποιήθηκαν και άλλοι τρόποι για την πειρατεία ονομάτων χώρου. Χαρακτηριστικό παράδειγμα, αποτελεί η μεταφορά πάνω από πενήντα διευθύνσεων (συμπεριλαμβανόμενης και των εταιρειών Adidas και Manchester United) σε διαφορετική διεύθυνση. Η ενέργεια αυτή[38] πραγματοποιήθηκε από Σέρβους hackers, οι οποίοι απέστειλαν στην εταιρεία κατοχύρωσης ονομάτων χώρου, πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου[39], με τα οποία πέτυχαν την μεταφορά των διευθύνσεων.

3.2.7. Phising και Pharming

Οι επιθέσεις τύπου phising[40], έχουν χρησιμοποιηθεί, ευρέως, από τους hackers τα τελευταία χρόνια. Με την μορφή αυτού του εγκλήματος, επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κ.λπ. προκειμένου να χρησιμοποιηθούν σ' άλλες παράνομες δραστηριότητες. Κύριο χαρακτηριστικό των επιθέσεων αυτών, είναι ότι επιχειρείται η εξαπάτηση του θύματος, η οποία, συνήθως, συντελείται με την αποστολή ενός e-mail με παραπλανητικό περιεχόμενο.

Τρόπο δράσης: Το υποψήφιο θύμα δέχεται ένα e-mail π.χ. από την υπηρεσία Ηλεκτρονικής Τραπεζικής (homebanking) της τράπεζας που χρησιμοποιεί, που τον πληροφορεί ότι είναι σε εξέλιξη κάποιες εργασίες συντήρησης του συστήματος και τον προτρέπει να επισκεφτεί την υπηρεσία Ηλεκτρονικής Τραπεζικής επιλέγοντας τον σύνδεσμο, που έχει επισυναφθεί στο μήνυμα και να επιβεβαιώσει τους κωδικούς πρόσβασης της υπηρεσίας. Το ανυποψίαστο θύμα θα επιλέξει το σύνδεσμο, που θα τον οδηγήσει σε μια τοποθεσία-αντίγραφο της πραγματικής[41]. Όταν πληκτρολογήσει τα προσωπικά του στοιχεία, αυτά θα υποκλαπούν από τον επιτιθέμενο.

Μελέτη περίπτωσης: Επίθεση phising εναντίον των χρηστών της υπηρεσίας Homebanking της Εθνικής Τράπεζας τον Νοέμβριο 2006

Πολλοί χρήστες της υπηρεσίας Internet Banking της Εθνικής Τράπεζας έλαβαν ένα e-mail, που τους προέτρεπε να ακολουθήσουν το σύνδεσμο που υπήρχε σε αυτό, προκειμένου να εισέλθουν στο σύστημα On-line Banking και να επιβεβαιώσουν τους κωδικούς τους, αλλιώς ο λογαριασμός θα απενεργοποιούνταν. Ο σύνδεσμος στο μήνυμα, παρέπεμπε σε μια σελίδα σχεδόν όμοια με την πραγματική σελίδα της Εθνικής Τράπεζάς.

Standard και άλλες, αξιώνοντας από τις εταιρείες την πληρωμή σημαντικών χρηματικών ποσών, προκειμένου να τους μεταβιβάσει τα δικαιώματα των διευθύνσεων.

[38] Τα κίνητρα των hackers ήταν περισσότερο πολιτικά, καθότι στις σελίδες που οδηγούσαν τα sites των εταιρειών, κυριαρχούσαν τα μηνύματα: «Το Κόσσοβο είναι Σερβία» και «Να είστε χαρούμενοι που παραβιάσαμε τον δικτυακό σας τόπο, γιατί παραβιάζουμε μόνο τα καλύτερα site στο Internet». http://news.zdnet.co.uk/security/0,1000000189,2085647,00.htm (Ημερομηνία πρόσβασης 23/07/09)

[39] Η εταιρεία ισχυρίστηκε ότι για την αλλαγή των διευθύνσεων αρκούσε η αποστολή ενός από ένα συγκεκριμένο όνομα χώρου, εφόσον η εμπλεκόμενη εταιρεία είχε επιλέξει το χαμηλότερο επίπεδο ασφαλείας για τον δικτυακό της τόπο.

[40] Μ.Παπαδόπουλος: Phising: Η νέα μέθοδος εξαπάτησης στο διαδίκτυο. Διαθέσιμο από http://www.marinos.com.gr/bbpdf/pdfs/msg50.pdf (Ημερομηνία πρόσβασης 23/07/09)

[41] Για να εξαπατηθεί ο χρήστης, προτιμώνται διευθύνσεις που μοιάζουν πάρα πολύ με τις πραγματικές π.χ. η διεύθυνση homebank.nbg.gr μπορεί να χαρακτηριστεί ώς homebang.nbg.gr

Όποιος χρήστης παρασυρόταν και πληκτρολογούσε τους κωδικούς του, αυτοί αυτόματα υποκλέπτονταν[42].

Το phising μήνυμα

Τίτλος:
NBG Security Measure ID Number: CA9908-8989
Κείμενο:
Αγαπητέ on- line πελάτη της ΕΘΝΙΚΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ
Στα πλαίσια μέτρων ασφαλείας, εξετάζονται κατά τακτά διαστήματα οι δραστηριότητες στο σύστημα της ΕΘΝΙΚΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ. Πρόσφατα παρατηρήσαμε το εξής ζήτημα σχετικά με το λογαριασμό σας. Μετά από πρόσφατο έλεγχο του λογαριασμού σας, θα πρέπει να απαιτήσουμε κάποιες πρόσθετες πληροφορίες από εσάς έτσι ώστε να σας παρέχουμε ασφαλείς υπηρεσίες. Μονοσήμαντος Αριθμός σας: CA9908-8989. Για την ασφάλειά σας, περιορίσαμε την πρόσβαση στο λογαριασμό σας έως ότου ολοκληρωθούν τα πρόσθετα μέτρα ασφαλείας. Σας ζητούμε συγνώμη για οποιαδήποτε πιθανή ενόχληση. Παρακαλείσθε να κάνετε εισαγωγή στο σύστημα της Διαδικτυακής Τραπεζικής της Εθνικής Τράπεζας της Ελλάδος μέσω της περιοχής «TAN» για να ανακτήσετε την πρόσβαση στο λογαριασμό σας το συντομότερο δυνατό. Θα πρέπει να πατήσετε τον παρακάτω σύνδεσμο και μέσω της περιοχής «TAN» να κάνετε εισαγωγή στο σύστημα, στην ιστοσελίδα της Διαδικτυακής Τραπεζικής της Εθνικής Τράπεζας της Ελλάδος για την ολοκλήρωση της διαδικασίας επαλήθευσης.
Σύμφωνα με τη Συμφωνία Χρήστη της ΕΘΝΙΚΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ, η πρόσβαση στο λογαριασμό σας θα παραμείνει περιορισμένη έως ότου λυθεί το ζήτημα. Δυστυχώς, εάν η πρόσβαση στο λογαριασμό σας παραμείνει περιορισμένη για μια εκτεταμένη χρονική περίοδο, είναι πιθανό να υπάρξουν επιπλέον περιορισμοί ή ακόμη και κλείσιμο του λογαριασμού. Σας προτρέπουμε να κάνετε εισαγωγή στο λογαριασμό σας στη Διαδικτυακή Τραπεζική της Εθνικής Τράπεζας της Ελλάδος το συντομότερο δυνατό ώστε να βοηθήσετε στην αποφυγή των παραπάνω. Για να κάνετε έλεγχο στο λογαριασμό σας και σε κάποιες ή όλες τις πληροφορίες τις οποίες χρησιμοποίησε η ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΕΛΛΑΔΟΣ για να περιορίσει την πρόσβαση στο λογαριασμό σας, παρακαλούμε επισκεφτείτε το Κέντρο Επίλυσης Προβλημάτων. Εάν μετά τον έλεγχο των πληροφοριών σχετικά με το λογαριασμό σας, χρειαστείτε επεξηγήσεις σχετικά με την πρόσβαση στο λογαριασμό σας, παρακαλώ επικοινωνήστε με την ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΕΛΛΑΔΟΣ μέσω του Κέντρου Βοήθειας στην ιστοσελίδα **[link removed for security reasons]** και πατώντας «Επικοινωνήστε μαζί μας». Σας ευχαριστούμε για την άμεση προσοχή σας στο θέμα. Παρακαλούμε να λάβετε υπόψη σας ότι αυτό είναι ένα μέτρο το οποίο αποσκοπεί στη δική σας ασφάλεια και την προστασία του λογαριασμού σας.

Ειλικρινά,
Εθνική Τράπεζα της Ελλάδος
Τμήμα Ελέγχου Λογαριασμών
Πηγή: http://www.taxheaven.gr/acforum/index.php?showtopic=21127

[42] Πηγή: www.e-politismos.gr (Ημερομηνία Πρόσβασης: 20/08/09)

Οι επιθέσεις αυτές, έχουν πραγματοποιηθεί με διάφορες παραλλαγές, για να παραπλανήσουν τους χρήστες. Για παράδειγμα, μαζί με το e-mail αποστέλλεται και ένας δούρειος ίππος, ο οποίος εκτελείται στο παρασκήνιο και τη στιγμή που το θύμα θα επισκεφτεί ένα δικτυακό τόπο για να δώσει τα στοιχεία του, καταγράφονται αυτόματα και αποστέλλονται στον επιτιθέμενο. Άλλες φορές ο χρήστης οδηγείται στο πραγματικό δικτυακό τόπο της υπηρεσίας Ηλεκτρονικής Τραπεζικής και εκεί, χωρίς να το αντιληφθεί εμφανίζεται ένα αναδυόμενο (pop-up) παράθυρο, στο οποίο ο χρήστης προτρέπεται να πληκτρολογήσει τα προσωπικά του στοιχεία. Το αναδυόμενο παράθυρο είναι αποτέλεσμα παρέμβασης του επιτιθέμενου, που επιχειρεί με αυτό τον τρόπο να υποκλέψει τα προσωπικά στοιχεία του χρήστη, την στιγμή που πληκτρολογούνται.

Μια παραλλαγή των επιθέσεων phising αποτελούν οι επιθέσεις pharming. Και στην περίπτωση αυτή, ο σκοπός του εγκλήματος είναι ο ίδιος: η απόσπαση ευαίσθητων δεδομένων από το θύμα. Η διαφορά έγκειται στην τεχνική. Ο hacker επεμβαίνει στο Σύστημα Ονομάτων Χώρου (DNS)[43] και όταν ο ανυποψίαστος χρήστης πληκτρολογήσει την διεύθυνση π.χ. της υπηρεσίας Ηλεκτρονικής Τραπεζικής, που χρησιμοποιεί, χωρίς να το γνωρίζει μεταφέρεται σε άλλο δικτυακό τόπο, όπου ο κακόβουλος θα επιχειρήσει να αποσπάσει το όνομα χρήστη και τον κωδικό πρόσβασης του θύματος.

3.3. Εγκλήματα που τελούνται με τη χρήση Η/Υ

Πολλά από τα υπάρχοντα εγκλήματα του κοινού ποινικού δικαίου τελούνται με τη βοήθεια και τη χρήση των ηλεκτρονικών υπολογιστών. Ο υπολογιστής μπορεί να χρησιμοποιηθεί, ποικιλοτρόπως, στην τέλεση των εγκλημάτων αυτών, όπως:

- Για την αποθήκευση δεδομένων, που σχετίζονται με πρόσωπα και αντικείμενα που εμπλέκονται σε μια παράνομη δραστηριότητα π.χ. προσωπικά στοιχεία εμπόρων ναρκωτικών.
- Για την εύρεση πληροφοριών, σχετικών με μια παράνομη δραστηριότητα π.χ. πώς κατασκευάζεται μια βόμβα.
- Για την διάδοση πληροφοριών, π.χ. την αγορά αγαθών με χρήση πιστωτικών καρτών που έχουν κλαπεί με φυσικό τρόπο.
- Για τη διακίνηση παράνομου οπτικοακουστικού υλικού π.χ. παιδική πορνογραφία.

3.3.1 Απάτη στο Διαδίκτυο

Η απάτη στο συμβατικό κόσμο είναι ένα από τα πιο συνηθισμένα εγκλήματα. Η εμφάνιση, όμως, και ανάπτυξη του Διαδικτύου, μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης. Η τάση αυτή, αυξήθηκε ακόμη περισσότερο, με την εξάπλωση του ηλεκτρονικού εμπορίου, που είχε ως επακόλουθο την ανάπτυξη οικονομικών συναλλαγών με τη χρήση του Διαδικτύου.

3.3.1.1. Απάτη με e-mail

Η απάτη, με τη χρήση του ηλεκτρονικού ταχυδρομείου, αποτελεί την συχνότερη μορφή επιθέσεως, έναντι των χρηστών του Διαδικτύου. Δύο μορφές απάτης με e-mail είναι το phising και το pharming. Οι επαγγελματίες του είδους, συνεχώς, βρίσκουν νέους τρόπους για να εξαπατήσουν ανυποψίαστους χρήστες, χρησιμοποιώντας μηνύματα ηλεκτρονικού

[43] Το Domain Name System ή DNS (σύστημα ονομάτων τομέα) είναι ένα σύστημα με το οποίο αντιστοιχίζονται οι διευθύνσεις IP σε ονόματα τομέων.

ταχυδρομείου, που προβάλλουν διάφορες δικαιολογίες με μοναδικό σκοπό, την απόσπαση χρηματικών ποσών ή προσωπικών στοιχείων. Χαρακτηριστικές περιπτώσεις απάτης με e-mail, αποτελούν οι νιγηριανές επιστολές και το ισπανικό λόττο.
Στην πρώτη περίπτωση, το θύμα λαμβάνει ένα e-mail[44] από φερόμενο υπήκοο Αφρικανικής χώρας, ο οποίος, ζητάει την βοήθεια του για την μεταφορά μεγάλου χρηματικού ποσού από την χώρα του στο εξωτερικό. Ο αποστολέας προβάλλει διάφορες δικαιολογίες (πόλεμος, θάνατος γονέων, φυσικές καταστροφές κ.λπ.) και ζητά από το θύμα, το άνοιγμα τραπεζικού λογαριασμού με συνδικαιούχο τον ίδιο, τη γνωστοποίηση των στοιχείων του και την κατάθεση χρηματικού ποσού για έξοδα κίνησης. Σε αντάλλαγμα, προσφέρει μεγάλο μερίδιο του μεταφερόμενου ποσού, όταν ολοκληρωθεί η συναλλαγή. Το θύμα ενδίδει και προχωρά στις ενέργειες που του έχουν υποδειχθεί. Ο δράστης, με διάφορες δικαιολογίες, αποσπά συνεχώς χρηματικά ποσά, μέχρι τη στιγμή που αποφασίζει να κλείσει τον λογαριασμό, αφού προηγουμένως έχει μεταφέρει όλα τα χρήματα, που υπήρχαν μέχρι τότε, σε δικό του λογαριασμό.

From: Abbas Abdulla Esmail
Subject: URGENT RESPONSE NEEDED

From The Desk of Mr. Abbas Abdulla Esmail,
Manager National Bank of Abu Dhabi Dubai
United Arab Emirate (U.A.E.)
Dear,
I am Mr. Abbas Abdulla Esmail , Branch Manager National Bank of Dubai Abu Dhabi branch, I have urgent and very confidential business proposition for you A America consultant and construction company Mr., Thomas Stone made a numbered time (Fixed) Deposit for twelve calendar months, valued at US$25m (Twenty Five Million United States American Dollars). in my branch. Upon maturity,
I sent a routine notification to his forwarding address but got no reply After a month, we sent a reminder and finally we discovered from his contract employers, America consultant construction company that Thomas Stone. Died in a plane crash in Egypt Air Flight 990, 1999 air crash for more information about this crash and person you can contact this website:
h.t.t.p.://w.w.w.cbsnews.com/stories/1999/11/01/iran/main49778.shtml
h.t.t.p.://news.bbc.co.uk/1/hi/world/americas/502503.stm
Since we got this information about his death and on further investigation I found out that he died without making a WILL and all attempts to trace his next of kin was fruitless. I therefore made further investigation and discovered that Mr. Thomas Stone did not declare any kin or relations in all his official documents, including his Bank Deposit paperwork in my Bank

[44]Παραδείγματα Νιγηριανών επιστολών http://www.419legal.org/# (Ημερομηνία Πρόσβασης: 12/07/09)

This sum of US$25m is still sitting in my Bank and the interest is being rolled over with the principal sum at the end of each year. No one will ever come forward to claim it. According to Laws of United Arab Emirates, at the expiration of 8 (eight) years, the money will revert to the ownership of the (U.A.E) Government if nobody applies to claim the fund. Consequently, my proposal is that I will like you as a foreigner to stand in as the next of kin to Mr. Thomas Stone so that the fruits of this old man 92s labor will not get into the hands of some corrupt government officials This is simple, I will like you to provide immediately your full names and address so that the attorney will prepare the necessary documents and affidavits that will put you in place as the next of kin.
We shall employ the services of an attorney for drafting and notarization of the WILL and to obtain the necessary documents and letter of probate administration in your favor for the transfer. A bank account in any part of the world that you will provide will then facilitate the transfer of this money to you as the beneficiary/next of kin.
The money will be paid into your account for us to share in the ratio of 60% for me and 40% for you. There is no risk at all as all the paperwork for this transaction will be done by the attorney and my position as the Branch Manager guarantees the successful execution of this transaction.
If you are interested, please reply immediately via the private email address above.
Upon your response, I shall then provide you with more details and relevant documents that will help you understand the transaction. Please send me your confidential telephone and fax numbers for easy communication. Please observe utmost confidentiality, and rest assured that this transaction would be mostprofitable for both of us because I shall require your assistance to invest my share in your country.
Awaiting your urgent reply
Regards
Mr, Abbas Abdulla Esmail

Στην δεύτερη περίπτωση, που είναι παρόμοια με τις Νιγηριανές επιστολές, Αφρικανοί υπήκοοι, κάτοικοι Ισπανίας, αποστέλλουν e-mails σε ανυποψίαστους χρήστες, ζητώντας τους προσωπικά στοιχεία και αριθμούς τραπεζικών λογαριασμών, προκειμένου, να τους μεταβιβάσουν τα κέρδη από την υποτιθέμενη νίκη τους στο ισπανικό ΛΟΤΤΟ. Στη συνέχεια, εφόσον τα θύματα έχουν πεισθεί ότι έχουν κερδίσει, ζητούν να τους καταβληθούν χρήματα για διαδικαστικά έξοδα. Με τον τρόπο αυτό, κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά.[45]

[45] http://419.bittenus.com/lotteries.htm (Ημερομηνία πρόσβασης: 13/07/09)

From: Euro Award <infoeuromailer@web.de>
To: undisclosed-recipients:
Sent: Monday, March 13, 2006 6:22 PM
Subject: (Your E-Mail Address Have Won A Lottery Prize !!!.)

FROM THE DESK OF VICE PRESIDENT
EURO MILLONES LOTTERY
MADRID - SPAIN
www.loteria.com

Dear Beneficiary

We are pleased to announce you as one of the 10 lucky winners in the Euro Millones Lottery International Email Address draw on the 15th of January due to the mixture of names and address the result was released on the 12th march, 2006. All 10 winning addresses were randomly selected from a batch of 50,000,000 international email addresses. Your
email address emerged alongside 9 others as a category 2 winner in the Euro Millones Lottery Draw.
Consequently, you have therefore been approved for a total pay out of US$950,0! 00:00 (Nine Hundred And Fifty Thousand United States Dollars
Only).The! following particulars are attached to your lotto payment order:
(I) Batch No: TTOW/1989/TAC
(ii) Ticket No: 777-312-009
(iii) Lucky No: 01-10-22-33-54
(iv) Ref No: WUMT/XX43/9000/LAES
(V) Serial No: MMUEU/U423/876
The Euro Millones Lottery Program internet draw is held once in a year and is so organized to encourage the use of the internet and computers worldwide. We are proud to say that over 200 Million Euros are won annually in more than 150 countries worldwide.
To claim your winning prize you are to contact the appointed agent as soon as possible for the immediate release of your winnings:

MR.Pedro Rodrigo.
Heritage Agencies Madrid-Spain.
E-mail: heritageconsults@netscape.net

N.B:Steps to claiming your prize;
1.Please quote! your Reference number in all correspondence with the claims office r! .

2. You must contact the appointed agent with your Full Names, Contact Telephone Numbers (Home, Office and Mobile Number and also Fax Number)
via email to process the immediate payment of your prize.

3. Be informed that the appointed agent will be required to swear an Affidavits of Lotto Claim and also obtain Approval Legal Clearance Certificate from the Court here in Spain which is in accordance with the European Union Financial Act 2004 on payment of International Lottery Winners.

Please be aware that the PAYING BANK will Effect Payment Swiftly upon satisfactory Report, Verifications and validation provided by this fiduciary agent.
For security reasons, you are advised to keep your winning information confidential till your claims is processed and your money remitted to you.

Once again congratulations!!!
Best regards,
Mrs.Suzan Zeeman

3.3.1.2. Απάτη με πιστωτικές κάρτες

Η χρήση πιστωτικών καρτών στο Διαδίκτυο, για να διεκπεραίωση πάσης φύσεως συναλλαγών (π.χ. μέσω του ηλεκτρονικού εμπορίου), έχει δημιουργήσει νέες δυνατότητες για τη διάπραξη εγκλημάτων. Η μη αυτοπρόσωπη παρουσία του αγοραστή και η άγνωστη ταυτότητα του πωλητή (ή υποψήφιου απατεώνα) έχουν συμβάλει στην αύξηση των περιπτώσεων απάτης, με την χρήση πιστωτικών καρτών στο Διαδίκτυο.

Με τη χρήση την σύγχρονων τεχνολογιών δεν απαιτείται, πλέον, ιδιαίτερη δεξιότητα για να αποκτήσει κάποιος τον αριθμό μιας πιστωτικής κάρτας και να πραγματοποίηση αγορές μέσω του Διαδικτύου. Με την τεχνολογία «websniffer», παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα δεκαεξαψήφιοι αριθμοί πιστωτικών καρτών. Επιπλέων, είναι δυνατή η αγορά μέσω του Διαδικτύου, αριθμών πιστωτικών καρτών που έχουν υποκλαπεί. Τέλος, υπάρχουν και εφαρμογές λογισμικού, που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών,[46] χρησιμοποιώντας διαφόρους λογάριθμους.

3.3.2. Κλοπή ταυτότητας

Η κλοπής ταυτότητας, 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. Είναι εύκολο για τον καθένα, να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών.

Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δύο στάδια[47] : Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους, συμβατικούς και ψηφιακούς και το δεύτερο είναι η χρησιμοποίηση

---

[46] Τα εργαλεία λογισμικού που δημιουργούν αυτόματα τυχαίους αριθμούς πιστωτικών καρτών και επιβεβαιώνουν την γνησιότητα τους, διατίθενται ελεύθερα στο Διαδίκτυο. Στους περισσότερους δικτυακούς τόπους που προσφέρονται τέτοια εργαλεία, υπάρχει σχετική προειδοποίηση ότι η χρήση των αριθμών πιστωτικών καρτών που δημιουργούνται για διεκπεραίωση on-line συναλλαγών είναι παράνομη. Βλ. http://www.whatprice.co.uk/financial/credit-card-generator.html (Ημερομηνία πρόσβασης: 13/07/2009)

[47] New Man, R. 2004 (Ημερομηνία πρόσβασης: 14/07/09)

των κλεμμένων στοιχείων. Ένα πρόσφατο συμβάν κλοπής ταυτότητας[48] είναι η επίθεση που δέχτηκε το Facebook από hacker.

Οι άγνωστοι επιχείρησαν να έχουν πρόσβαση στα προσωπικά δεδομένα των περίπου 200 εκατομμυρίων χρηστών και κατάφεραν να αποσπάσουν τους κωδικούς αρκετών εξ αυτών. Ο εκπρόσωπος του Facebook, Barry Schnitt δήλωσε ότι βρίσκεται στη διαδικασία αποκατάστασης της βλάβης που υπέστη το δίκτυο από την επίθεση των χάκερ και πως έχουν μπλοκαριστεί οι λογαριασμοί των χρηστών από τους οποίους υπέκλεψαν στοιχεία. Ωστόσο απέφυγε να πει πόσοι ακριβώς ήταν οι λογαριασμοί αυτοί. Οι χάκερ απέσπασαν προσωπικά δεδομένα και κωδικούς πρόσβασης μέσω της τεχνικής «phishing»: αρχικά κατάφεραν να αποκτήσουν πρόσβαση σε ορισμένους λογαριασμούς μελών του Facebook και στη συνέχεια έστειλαν μηνύματα στους φίλους τους, προκαλώντας τους να ανοίξουν links που οδηγούσαν σε ψεύτικες ιστοσελίδες.

Οι ιστοσελίδες αυτές είχαν σχεδιαστεί ώστε να μοιάζουν με την αρχική σελίδα του Facebook. Τα θύματα δέχθηκαν οδηγίες να δώσουν και πάλι τα στοιχεία εγγραφής, ωστόσο αντί να κάνουν log in στο Facebook, έμπαιναν στην ιστοσελίδα που είχαν υπό τον έλεγχό τους οι χάκερ, δίνοντας τους κωδικούς ασφαλείας. Στόχοι επιθέσεων όπως αυτή είναι συνήθως η κλοπή ταυτότητας και η διαρροή ανεπιθύμητων ηλεκτρονικών μηνυμάτων (spam). Μεταξύ των ψεύτικων ιστοσελίδων που χρησιμοποιήθηκαν ήταν οι www.151.im , www.121.im και www.123.im. Το Facebook διέγραψε κάθε αναφορά στα sites αυτά.

Όπως δήλωσε ο Schnitt, οι υπεύθυνοι για θέματα ασφάλειας στο Facebook εκτιμούν ότι οι δράστες είχαν στόχο να συλλέξουν όσο το δυνατόν περισσότερους κωδικούς πρόσβασης και αργότερα να τους χρησιμοποιήσουν για να στείλουν spam και να προωθήσουν πλαστά φαρμακευτικά προϊόντα και άλλα καταναλωτικά αγαθά. Το κοινωνικό δίκτυο Facebook και ο βασικός ανταγωνιστής του, το δίκτυο MySpace απαιτεί από τους αποστολείς μηνυμάτων εντός δικτύου να είναι μέλη του και κρύβει τα προσωπικά δεδομένα μελών από επισκέπτες που δεν είναι εγγεγραμμένα μέλη. Λόγω της τακτικής αυτής, οι χρήστες έχουν την τάση να είναι λιγότερο καχύποπτοι απέναντι στα μηνύματα που λαμβάνουν και αυτό επιχείρησαν να εκμεταλλευτούν οι χάκερ.

3.3.3. Πορνογραφία

Πορνογραφικό υλικό

Η είσοδος αυτού του μαγαζιού βρίσκεται στην μεγάλη Λεωφόρο της Πληροφορίας, όμως είναι καλά κρυμμένη. Πάνω απ΄ αυτήν την πόρτα κρέμεται πάντα μια πινακίδα με τη μαγική λέξη «sex». Είναι ένα μαγαζί που πουλάει φωτογραφίες, ταινίες σε ψηφιακή μορφή, λέξεις και αντικείμενα που έχουν σχέση με την ανθρώπινη σάρκα σε κάθε μορφή

[48] http://treloparea.forumn.net/-f46/--facebook-t265.htm?highlight=facebook (Ημερομηνία πρόσβασης: 13/09/2009)

της και σε κάθε χρονική της περίοδο. Ένας αμύητος που μπαίνει για πρώτη φορά στο μαγαζί, δεν μπορεί να φανταστεί πόσες εικόνες και πόσα κείμενα πουλιούνται εκεί ή, πιο σωστά, σε ποιό βαθμό και σε πόσο ζήλο γίνεται η πώληση. Διαρκώς νέα πρόσωπα έρχονται στο μαγαζί και άλλα, παλιοί πελάτες, εξαφανίζονται, χωρίς κανένας να γνωρίζει που πάνε. Διαρκώς ξεπροβάλλουν πίσω από τα ράφια καινούργιοι πελάτες. Το κούνημα των κεφαλιών, οι αγχωμένες χειρονομίες των πρωτάρηδων, το σούρσιμο των ποδιών στον συνωστισμό, το θρόισμα διαλεγμένων φωτογραφιών στα χέρια ενός αμήχανου πιτσιρικά, τα ατελείωτα παζάρια, οι φασαρίες, δημιουργούν μια αλλόκοτη ατμόσφαιρα. Μια περίεργη, σχεδόν συνωμοτική κίνηση επικρατεί εδώ μέσα. Το ταμείο δεν έχει και πολλή δουλειά, όπως θα περίμενε κανείς. Δεν πληρώνουν όλοι οι πελάτες μετρητά. Ελάχιστοι πληρώνουν έτσι. Υπάρχουν προφανώς κι άλλες δυνατότητες διακανονισμού. Αρκεί να ξέρεις τον τρόπο να φέρεις κι εσύ εμπόρευμα στο μαγαζί. Φέρνεις κάτι καινούριο και το ανταλλάσεις με κάτι που δεν έχεις. Δίνεις και παίρνεις. Συλλέγεις.... **Αυτή είναι σήμερα η σημερινή απεικόνιση της πορνογραφίας στο δίκτυο.** Έτσι μεταφέρεται από το ένα σημείο του πλανήτη στο άλλο.[49]

Ένας δικηγόρος στη Λάρισα, ένας φοιτητής στην Κρήτη, ένας μπάρμαν στη Μύκονο, ένας πανεπιστημιακός στη Θεσσαλονίκη, αλλά και ο επιστάτης του τμήματος στο οποίο εργαζόταν, ένας συνταξιούχος στα βόρεια προάστια της Αθήνας, ένας επισμηνίας του υπουργείου Εθνικής Άμυνας, ένας καθηγητής ξένων γλωσσών στα Γιαννιτσά, ένας φωτογράφος στην Αθήνα, ένας ιδιωτικός υπάλληλος στη Ρόδο, ένας μαθητής και πάλι στην Αθήνα και άλλοι πολλοί. Κοινό χαρακτηριστικό όλων τους και άλλων πολλών που συνελήφθησαν τα τελευταία χρόνια, η διακίνηση υλικού παιδικής πορνογραφίας μέσω του Διαδικτύου[50].

3.3.3.1. Ορισμός του πορνογραφικού υλικού ανηλίκων και η νομική αντιμετώπιση των δραστών κατά το Ελληνικό δίκαιο

Η πορνογραφία ανηλίκων συνιστά μία μορφή οικονομικής εκμετάλλευσης της γενετήσιας ζωής, που στρέφεται με βάναυσο τρόπο ενάντια στην ατομική τους αξιοπρέπεια και τραυματίζει την εξέλιξή τους. Το άρθρο 348 Α του ελληνικού Ποινικού Κώδικα, όπως τροποποιήθηκε πρόσφατα με το Ν. 3625/2007, δίνει τον ακόλουθο ορισμό σχετικά: «Υλικό παιδικής πορνογραφίας συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο». Αξιοσημείωτο είναι, πάντως, ότι οι νομικοί ορισμοί που δίδονται από τις επιμέρους εθνικές νομοθεσίες για την παιδική πορνογραφία διαφοροποιούνται μεταξύ τους σε σημαντικό βαθμό. Σε γενικές γραμμές, όμως, φαίνεται να συγκλίνουν, οι περισσότερες τουλάχιστον, στην ευρεία παραδοχή ότι παιδική πορνογραφία αποτελεί οποιαδήποτε αναφορά γενετήσιας δραστηριότητας που αναμειγνύει ένα πρόσωπο προεφηβικής ηλικίας.

---

[49] Αναστασία Ζάννη 2005 σελ.69

[50] http://pacific.jour.auth.gr/emmeis/issues/21/21maties3.htm (Ημερομηνία πρόσβασης: 13/08/2009)

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

3.3.3.2. Οι διαστάσεις του εγκλήματος σε διεθνές και ελληνικό επίπεδο

Για να γίνουν αντιληπτές οι διαστάσεις του προβλήματος, παρατίθενται μερικά στατιστικά στοιχεία που έχουν δοθεί στη δημοσιότητα:

- Ο τζίρος της βιομηχανίας παιδικής πορνογραφίας στο διαδίκτυο υπερβαίνει τα τρία δισεκατομμύρια ευρώ ετησίως.

- Ο αριθμός των ιστοσελίδων που φιλοξενούν πορνογραφικό περιεχόμενο με πρωταγωνιστές ανηλίκους, ακόμη και βρέφη, υπολογίζεται ότι αυξήθηκε την τελευταία δεκαετία κατά 345%.

- Η ημερήσια επισκεψιμότητα ορισμένων τέτοιου περιεχομένου ιστοσελίδων είναι περίπου 150.000, αριθμός ιδιαίτερα υψηλός, δεδομένου των υπέρογκων ποσών που απαιτείται να διαθέσει κανείς για την πρόσβαση σε αυτές.

- Επίσης, έχει υπολογιστεί, παρά το γεγονός ότι η εκτίμηση της έκτασης της διαδικτυακής παιδικής πορνογραφίας είναι ιδιαίτερα δυσχερής, ότι περισσότερες από ένα εκατομμύριο πορνογραφικές εικόνες ανηλίκων διακινούνται στο ίντερνετ και διακόσιες καινούργιες εικόνες ταχυδρομούνται ηλεκτρονικά ημερησίως.

- Σε ότι αφορά την Ελλάδα, σύμφωνα με στατιστικά στοιχεία του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής, από τις αρχές του 2004 μέχρι τον Οκτώβριο του 2005 εξιχνιάστηκαν 48 υποθέσεις διακίνησης υλικού παιδικής πορνογραφίας, συνελήφθησαν 68 άτομα, ενώ κατηγορήθηκαν συνολικά 90. Και, όπως χαρακτηριστικά αναφέρει ο διευθυντής του Τμήματος, Μ. Σφακιανάκης, «η συγκεκριμένη μορφή εγκληματικότητας συνεχώς φουντώνει, παρουσιάζονται συνεχώς νέες υποθέσεις, ιστοσελίδες ξεφυτρώνουν από παντού. Στο παρελθόν θα θεωρούσαμε πολύ σημαντικό να βγάλουμε δύο-τρεις τέτοιες υποθέσεις μέσα σε μια χρονιά και τώρα απαριθμούμε δεκάδες». Επιχειρώντας μια προσέγγιση σε επίπεδο στατιστικής, ο κ. Σφακιανάκης αναφέρει ότι σύμφωνα με μια καταγραφή που έχει γίνει, οι ιστοσελίδες με ανάλογο περιεχόμενο αυξάνονται από το 2001 και έπειτα κατά 150% ανά έτος.

Έχει χαρακτηριστεί «παράδοξο» το πώς μια από τις μεγαλύτερες επιτεύξεις του περασμένου αιώνα, το ίντερνετ, από δημοκρατικό «forum ελεύθερης ανταλλαγής απόψεων» κατέστη φορέας σεξουαλικής κακοποίησης παιδιών και παιδοφιλίας. Είναι,

όμως, αναγκαία η επισήμανση ότι η δημιουργία του ίντερνετ δε συνιστά σε καμία περίπτωση το μόνο λόγο της ύπαρξης του φαινομένου της παιδικής πορνογραφίας.

Επιπρόσθετα, άξιο αναφοράς είναι ότι η πορνογραφία ανηλίκων συνιστά στις μέρες μας εγκληματική δραστηριότητα που εντάσσεται στο πλαίσιο του οργανωμένου εγκλήματος και ειδικότερα με αυτή ασχολούνται κυκλώματα που είτε την έχουν ως αποκλειστικό τομέα της δραστηριότητάς τους είτε ασχολούνται με το human trafficking εν γένει.

3.3.3.3. Το προφίλ του δράστη της παιδικής πορνογραφίας στο διαδίκτυο

Οι προσπάθειες που έχουν σημειωθεί ως σήμερα για την αντιμετώπιση του ειδεχθούς εγκλήματος του υπό εξέταση φαινομένου είναι επίμονες. Ωστόσο, τα κρούσματα πορνογραφίας ανηλίκων αυξάνουν με γοργούς ρυθμούς. Η τεχνολογική ανάπτυξη των τελευταίων ετών και πιο συγκεκριμένα η εισαγωγή των ηλεκτρονικών υπολογιστών και του διαδικτύου στην καθημερινή ζωή, έχει συμβάλλει σε αυτό, καθώς η χρήση του διαδικτύου παρέχει την ευκαιρία για πρόσβαση στις τεράστιες ποσότητες πορνογραφικών εικόνων που διακινούνται στον πλανήτη. Επίσης, καθιστά την παιδική πορνογραφία εύκολα προσβάσιμη άμεσα, σε οποιονδήποτε χρόνο και τόπο, παρέχοντας επίσης ανωνυμία στους χρήστες της. Άξιο αναφοράς είναι ότι καθιστά ευχερέστερη την άμεση επικοινωνία και τη διανομή των εικόνων ανάμεσα στους χρήστες, με ιδιαίτερα μικρό χρηματικό κόστος. Η χρήση του διαδικτύου προσφέρει, ακόμη, εικόνες υψηλής ψηφιακής ποιότητας, κρατά αναλλοίωτη την ποιότητα του αναπαριστώμενου υλικού και «παρέχει μια ποικιλία σχηματικών απεικονίσεων (εικόνων, βίντεο, φωνής), καθώς επίσης τη δυνατότητα πορνογραφικής απόλαυσής τους σε πραγματικό χρόνο και με διαντιδραστικές εμπειρίες».

Εάν κανείς περιπλανηθεί στους διάφορους διαδικτυακούς τόπους του κυβερνοχώρου, ενδέχεται να έρθει αντιμέτωπος με έναν πραγματικό «θησαυρό», δεδομένου του κόστους του πορνογραφικού υλικού εν γένει. Ο αριθμός των πορνογραφικού περιεχομένου φωτογραφιών και βίντεο είναι ανυπολόγιστος, ενώ ανάμεσά τους υπάρχει και απέραντο υλικό για τους παιδόφιλους. Η πλειονότητα του τελευταίου απεικονίζει ανήλικους, ακόμη και βρέφη, από 8 μηνών μέχρι 17 ετών, σε άσεμνες στάσεις και ερωτικές περιπτύξεις είτε μεταξύ τους είτε με ενήλικα πρόσωπα, ενώ υφίσταται υλικό ακόμη και για εντελώς αρρωστημένα μυαλά. Οι επισκέπτες των ιστοσελίδων άσεμνου περιεχομένου ακολουθούν, κυρίως, δύο τακτικές: Είτε «κατεβάζουν» τα αρχεία στο σκληρό δίσκο του υπολογιστή τους ή σε CD – ROM και δισκέτες είτε αρκούνται στην παρατήρηση του εν λόγω υλικού. Οι ενδιαφερόμενοι λαμβάνουν γνώση για τους διαδικτυακούς τόπους με παιδικό πορνογραφικό υλικό μέσω των λεγόμενων δωματίων επικοινωνίας που υφίστανται στο διαδίκτυο (chat rooms), ηλεκτρονικού ταχυδρομείου (e-mail) και των ομάδων συζήτησης (newsgroups), ενώ σπάνια θα ανακαλύψει ένας απλός χρήστης του διαδικτύου φωτογραφίες και βίντεο με ανηλίκους σε άσεμνες πράξεις ή πόζες στις μηχανές αναζήτησης (search engines).

Αξιοσημείωτο είναι, επιπρόσθετα, το γεγονός ότι οι επιτήδειοι του είδους κάνουν χρήση παραπλανητικών κειμένων ή φωτογραφιών, ώστε να προσελκύσουν τους χρήστες του διαδικτύου στις ιστοσελίδες τους. Συνήθως, εμφανίζονται χαμογελαστά παιδιά να παίζουν ξέγνοιαστα, να επιδίδονται σε ερωτικές περιπτύξεις ή ακόμη και να ποζάρουν με νάζι, όπου, πατώντας απλώς ένα πλήκτρο, ο χρήστης μεταφέρεται στα «άδυτα» της ιστοσελίδας. Να σημειωθεί ακόμη πως αρκετοί από τους δημιουργούς των υπό αναφορά ιστοσελίδων χωρίζουν τα παιδιά ανά κατηγορίες και πιο συγκεκριμένα, ανάλογα με την

ηλικία τους ή το πόσο αποκαλυπτικές είναι οι πόζες και ερωτικές τους περιπτύξεις, με συνακόλουθη αύξηση του χρηματικού ποσού που πρέπει να καταβάλει ο χρήστης, ώστε να αποκτήσει πρόσβαση. Επιπρόσθετα, μέσω των chat rooms, ορισμένοι παιδεραστές ξεκινούν τη συνομιλία με τα υποψήφια θύματά τους, με στόχο τη δημιουργία ενός κλίματος εμπιστοσύνης και την πιο άνετη επικοινωνία. Ο ανωτέρω στόχος επιτυγχάνεται με αργούς ρυθμούς είτε μέσω της αποστολής φωτογραφιών παιδικής πορνογραφίας είτε με φράσεις όπως: «είναι κάτι το φυσιολογικό», «είναι κάτι το ωραίο», ή «δεν θα ήθελες κι εσύ να δεις το ωραίο γυμνό σου κορμάκι στο διαδίκτυο, όπως κάνουν και άλλα παιδιά;».

Σχετικά τώρα με το προφίλ των δραστών του εγκλήματος της παιδικής πορνογραφίας, είναι αναγκαίο να επισημανθεί ότι δεν υφίσταται ομοιογένεια ανάμεσα στους τελευταίους, ενώ επίσης διαφοροποιούνται συχνά ως προς τα κίνητρά τους. Επί παραδείγματι, στην κατηγορία των συλλεκτών και διαχειριστών πορνογραφικού υλικού παιδιών στο ίντερνετ ανήκουν άτομα που χαρακτηρίζονται από ψυχοσεξουαλική διαταραχή και ειδικότερα παιδοφιλία, «πελάτες» του διαδικτύου που επιζητούν την απόκτηση καινούργιων σεξουαλικών εμπειριών, αλλά και «επαγγελματίες» που αποσκοπούν στο κέρδος μέσω της διακίνησης και (ανα)παραγωγής του εν λόγω υλικού καθώς και άλλοι. Συνεπώς, οποιαδήποτε απόπειρα γενίκευσης αναφορικά με τα χαρακτηριστικά των δραστών χρήζει σημαντικής προσοχής.

Ιδιαίτερα ενδιαφέρουσα είναι η κατάταξη που έχει επιχειρήσει σε σχετική έρευνά του το **Ινστιτούτο Εγκληματολογίας της Αυστραλίας.** Εν προκειμένω, οι δράστες του εγκλήματος της πορνογραφίας ανηλίκων στο διαδίκτυο τίθενται σε κατηγορίες ανάλογα με τα κίνητρά τους, ξεκινώντας από αυτούς που δεν έχουν άμεση εμπλοκή με τον ανήλικο και καταλήγοντας σε αυτούς που επιδιώκουν τη σεξουαλική συναναστροφή με αυτόν. Ειδικότερα, στο πλαίσιο της συγκεκριμένης έρευνας, περιγράφονται οχτώ τύποι δραστών:

1) Ο πρώτος αποτελεί το άτομο που κάνει χρήση του διαδικτύου και δίχως τη θέλησή του (επί παραδείγματι με τη μέθοδο του spamming) συναντά παιδικό πορνογραφικό υλικό και, παρά το γεγονός ότι δε το επιδίωξε, δέχεται να το κρατήσει,

2) Ο δεύτερος τύπος χρήστη περιγράφει το άτομο που φαντασιώνεται σεξουαλικά ανηλίκους, αποτυπώνει σε ψηφιακής μορφής κείμενα τις συγκεκριμένες του φαντασιώσεις στον υπολογιστή του ή κάνει προσωπική χρήση ψηφιακών φωτογραφιών, δίχως, όμως, να προτίθεται να τις διανέμει σε άλλους,

3) Τον τρίτο τύπο αποτελεί ο «αλιευτής», που επιζητεί υλικό παιδικής πορνογραφίας ενεργά, επικοινωνώντας για το σκοπό αυτό και με άλλους χρήστες με συναφείς προτιμήσεις,

4) Τον τέταρτο τύπο χαρακτηρίζει η ανασφάλεια και για τον λόγο αυτό αποτελεί τον «επισφαλή» συλλέκτη, ο οποίος κάνει χρήση πορνογραφικού υλικού το οποίο περιέχεται σε διαδικτυακούς τόπους ή chat rooms, όπου δεν απαιτούνται κωδικοί ασφαλείας, εγγραφές και οτιδήποτε άλλο σχετικό για να αποκτήσει πρόσβαση. Ο συγκεκριμένος χρήστης λαμβάνει ιδιαίτερα υψηλό ρίσκο ως προς την αποκάλυψη των στοιχείων του,

5) Ο επόμενος τύπος, εν αντιθέσει με τον προηγούμενο, χρησιμοποιεί πάντα εχέγγυα. Επί παραδείγματι, ορισμένα δίκτυα ανταλλαγής υλικού απαιτούν, προτού ολοκληρωθεί η διαδικασία εγγραφής καινούργιων μελών, να κατατεθεί από τα τελευταία μερίδα των προσωπικών τους συλλογών, «κλειδώνοντας» με τον τρόπο αυτό τα μέλη τους,

6) Ο έκτος τύπος αποτελεί τον λεγόμενο groomer, ο οποίος προσελκύει μέσω του ίντερνετ ανηλίκους, ώστε να τους κακοποιήσει σεξουαλικά. Η χρήση παιδικού πορνογραφικού υλικού υλοποιείται εν προκειμένω, ώστε ο ανήλικος να προετοιμαστεί για την ειδική περίσταση και να αμβλυνθεί η συστολή του,

7) Ο έβδομος τύπος τελεί σεξουαλικά εγκλήματα εις βάρος ανηλίκων. Για τον συγκεκριμένο, η παιδική πορνογραφία χρησιμοποιείται ως πλαίσιο της εν λόγω δραστηριότητάς του, καθώς ο ίδιος παράγει το υλικό με την κακοποίηση του παιδιού και εν συνεχεία το διακινεί στο διαδίκτυο. Δεν αποκλείεται να πείθει και τα ίδια τα παιδιά να διαθέσουν τις φωτογραφίες τους,

8) Ο τελευταίος τύπος περιγράφει αυτόν που πωλεί το πορνογραφικό υλικό στο σύνολο των ανωτέρω, επιδιώκει δηλαδή μέσω αυτής του της πράξεις να αποκομίσει οικονομικό όφελος. Ο ίδιος ενδέχεται να έχει σεξουαλικό ενδιαφέρον για παιδιά, αλλά αυτό μπορεί κιόλας να μη συμβαίνει.

Αν και από τα παραπάνω συνάγεται το συμπέρασμα ότι οι δράστες παρουσιάζουν αρκετές διαφορές μεταξύ τους, υφίστανται ορισμένα στοιχεία που εμφανίζουν πολλοί από αυτούς, όπως ότι τα συγκεκριμένα άτομα δυσκολεύονται στο να συμμεριστούν τον πόνο του άλλου (στην «ενσυναίσθηση» όπως χαρακτηριστικά ονομάζεται). Επιπρόσθετα, πολλοί παιδόφιλοι είχαν υποστεί στο παρελθόν σεξουαλική κακοποίηση. Η ψυχολογική ανωριμότητα, ανάλογη τα παιδιά – θύματα, αποτελεί, επίσης, ένα σύνηθες χαρακτηριστικό τους. Σημαντικό, επιπλέον, ότι οι χρήστες παιδικής πορνογραφίας είναι πολύ πιθανό να έχουν κάποια ερωτική σχέση, ορισμένο επάγγελμα, υψηλό δείκτη νοημοσύνης, πανεπιστημιακή μόρφωση, καθώς και λευκό ποινικό μητρώο και για το λόγο αυτό είναι ιδιαίτερα δυσχερής η σκιαγράφηση του εγκληματικού τους στερεοτύπου. Εκείνοι που έχουν κατηγορηθεί για τέλεση εγκλημάτων παιδικής πορνογραφίας στο διαδίκτυο είναι οδοντίατροι, δάσκαλοι, ακαδημαϊκοί καθηγητές, σταρ του ροκ, επαγγελματίες στρατιώτες και αξιωματικοί της αστυνομίας κ.ά.

Είναι αξιοσημείωτο, τέλος, ότι, από πορίσματα ερευνών που διεξήχθησαν σε δείγμα ανδρών που είχαν κατηγορηθεί για κατοχή παιδικού πορνογραφικού υλικού, προέκυψε ότι μέσω της συλλογής παιδικής πορνογραφίας δεν επιδιωκόταν η σεξουαλική διέγερση και ικανοποίηση. Έχει προκύψει, λοιπόν, ότι σε κάποιες περιπτώσεις ο συλλέκτης επιδιώκει τον εμπλουτισμό της συλλογής του με κάτι πρωτόγνωρο. Από τη συγκεκριμένη συμπεριφορά αναδεικνύεται ο ρόλος που διαδραματίζει η πορνογραφία ανηλίκων ως προϊόν προς πώληση και ταυτόχρονα ως «τρόπαιο».[51]

3.3.4. Διαδικτυακή τρομοκρατία

Η τρομοκρατία είναι ένα φαινόμενο, που παρουσιάζει ιδιαίτερη έξαρση τα τελευταία χρόνια. Η ιστορία έχει καταγράψει αιματηρές τρομοκρατικές επιθέσεις με χιλιάδες αθώα θύματα. Τα μέσα, που χρησιμοποιούν οι τρομοκράτες για τις επιθέσεις τους, συνεχώς εκσυγχρονίζονται, με το Διαδίκτυο να διαδραματίζει πλέον σημαντικό ρόλο. Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) ως την «προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι άμαχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες».

---

[51] http://pacific.jour.auth.gr/emmeis/issues/21/21maties3.htm (Ημερομηνία πρόσβασης: 13/08/2009)

Η χρήση του διαδικτύου αποτελεί βασικό εργαλείο των τρομοκρατών, γιατί τους προσφέρει μια σειρά από πλεονεκτήματα[52]: είναι φθηνότερο από τις παραδοσιακές τρομοκρατικές μεθόδους, οι ενέργειες τους είναι δύσκολο να εντοπιστούν, μπορούν να αποκρύψουν την τοποθεσία τους, δεν υπάρχουν φυσικά εμπόδια ή σημεία ελέγχου τα οποία πρέπει να διέλθουν, μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και μπορούν να επιτεθούν, ταυτόχρονα, σε πολλούς στόχους.

Η μεγαλύτερη τρομοκρατική απειλή παγκοσμίως, θεωρείται η οργάνωση Al-Kaida. Η έρευνα για το χτύπημα στους δίδυμους πύργους της 11ης Σεπτεμβρίου 2001, κατέληξε στο συμπέρασμα, ότι οι τρομοκράτες είχαν αναπτύξει ένα ευρύτατο δίκτυο επικοινωνίας με την χρήση του Διαδικτύου, το οποίο βοήθησε τα μέγιστα στο συντονισμό των ενεργειών τους. Η επίθεση αυτή δημιούργησε διάφορα σενάρια για τη νέα μορφή κυβερνοτρομοκρατίας που απειλεί την ανθρωπότητα. Για παράδειγμα, οι τρομοκράτες με τη χρήση του Διαδικτύου, θα έχουν τη δυνατότητα να παραβιάσουν τα συστήματα ελέγχου κρίσιμων υποδομών μιας χώρας, όπως οι ενεργειακές εγκαταστάσεις, το δίκτυο διανομής νερού και τα τηλεπικοινωνιακά συστήματα.[53] Εκτιμάται ότι, το βασικότερο όπλο των τρομοκρατών του μέλλοντος θα είναι ο ηλεκτρονικός υπολογιστής.

3.3.5. Επιθέσεις παρενόχλησης

Με τους όρους cyberstalking και harassment ή γενικότερα παρενόχληση, περιγράφεται μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών κ.α. Η συμπεριφορά αυτή υπήρξε και στο συμβατικό περιβάλλον, όμως με την διάδοση του Διαδικτύου και την δυνατότητα άμεσης επικοινωνίας, που προσφέρουν υπηρεσίες όπως το e-mail το chat, τα newsgroup κ.λπ. έχει λάβει τεράστιες διαστάσεις, με αποτέλεσμα το μεγαλύτερο ποσοστό των εγκλημάτων αυτών, να διαπράττονται μέσω του Διαδικτύου.[54]

Την παρενόχληση, που διαπράττεται μέσω του Διαδικτύου, μπορούμε να την διακρίνουμε σε δύο κατηγορίες:[55]

- Την άμεση παρενόχληση, που συντελείται όταν ο επιτιθέμενος αποστείλει απευθείας στο θύμα μηνύματα με προσβλητικό ή απειλητικό περιεχόμενο, άσχετα με το γεγονός, εάν οι απειλές πραγματοποιηθούν.
- Την έμμεση παρενόχληση, όταν το μήνυμα δεν στέλνεται αμέσως στο θύμα, αλλά, σε τυχαίους χρήστες του Διαδικτύου και περιλαμβάνει προσβλητικό ή απειλητικό για το θύμα περιεχόμενο.

---

[52] M.Elmusharaf (2004) Cyber terrorism, a new kind of terrorism. http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/ (Ημερομηνία πρόσβασης: 27/07/2009)

[53] B. Collin, The future of Cyberterrorism: Where the Physical and Virtual Words Converge http://afgen.com/terrorism1.html (Ημερομηνια πρόσβασης: 27/07/2009)

[54] Εξαιρετικό ενδιαφέρον παρουσιάζουν τα στατιστικά στοιχεία της οργανισμού Working to Halt Online Abuse. Τα ετήσια στατιστικά που δημοσιεύει ο οργανισμός, προέρχονται από καταγγελίες ατόμων που έχουν πέσει θύματα παρενόχλησης. Ειδικότερα: Από τα συγκεντρωτικά στοιχεία για τα έτη 2000 έως 2005, προκύπτει ότι το μεγαλύτερο ποσοστό των θυμάτων (38%) ήταν ηλικίας 18-30 ετών, το 74% των θυμάτων ήταν γυναίκες, το 54% των επιτιθέμενων άνδρες και, τέλος, το συντριπτικό ποσοστό των επιθέσεων πραγματοποιήθηκε on-line (66%). http://www.haltabuse.org/resources/stats/index.shtml 27/07/09

[55] Maxwell, A. 2001(Ημερομηνία πρόσβασης: 07/09/2009)

3.3.6. Διαδικτυακό ξέπλυμα Χρήματος

Εκτός από απάτες υπάρχουν και τα παραδοσιακά εγκλήματα που διεξάγονται μέσω του ηλεκτρονικού υπολογιστή και πλέον, και μέσω του Διαδικτύου[56]. Ένα από αυτά είναι ο εκβιασμός. Πολλοί crackers αντιγράφουν αρχεία και στη συνέχεια απειλούν τις εταιρείες προκειμένου να μη τα πουλήσουν στους οικονομικούς τους αντίπαλους. Το πιο συνηθισμένο και κερδοφόρο παραδοσιακό έγκλημα που διεξάγεται online είναι το ξέπλυμα χρήματος. Υπάρχουν διαδικτυακές ιστοσελίδες που διαφημίζουν το κυβερνο-ψηφιακό τρόπο ξεπλύματος (cyberlaudering) και υπόσχονται ανωνυμία .

Το ξέπλυμα του χρήματος, στην παραδοσιακή του μορφή, είναι, σύμφωνα με τον Bortner, «η τέχνη της απόκρυψης της ύπαρξης, της παράνομης πηγής ή της παράνομης κατανάλωσης του εισοδήματος και μετά η μεταμφίεση του, έτσι ώστε το τελευταίο να εμφανίζεται μόνιμο». Στο εικονικό σύμπαν του κυβερνοχώρου η καθιέρωση του ηλεκτρονικού χρήματος παρέχει τη δυνατότητα της ανωνυμίας, την ηλεκτροποιημένη ευκολία, ασφάλεια και ιδιωτικότητα/προσωπικό απόρρητο. Αυτός που επιθυμεί να ξεπλύνει χρήμα προσλαμβάνει ανθρώπους ή καταθέτει ο ίδιος, μέσω του διαδικτύου, σε τράπεζες που αποδέχονται ηλεκτρονικό χρήμα (e-cash). Για να υπάρχει μια σχετική ασφάλεια το ύψος των χρηματικών καταθέσεων δεν ανέρχεται σε υψηλά ποσά. Η μετατροπή του χρήματος σε e-cash προσφέρει στον παραβάτη την ανωνυμία του (μέσω ψηφιακών κωδικοποιημένων υπογραφών, και κοινού κλειδάριθμου) και την πρόσβαση σε νόμιμο ηλεκτρονικό χρήμα. Για να συλληφθεί κάποιος για ξέπλυμα χρήματος , μέσω διαδικτύου θα πρέπει η τράπεζα να καλύπτεται από νομοθετικές διατάξεις που θα επιτρέπουν τον έλεγχο των λογαριασμών ή να πιαστεί επ' αυτοφώρω κάτι που θεωρείται αδύνατο. Οι περισσότερες τράπεζες, όμως, ανά τον κόσμο δεν επιδιώκουν την υπαγωγή τους σε νομοθετικές διατάξεις γιατί χάνουν πελατεία.

3.3.7. Κινητή τηλεφωνία

Μια άλλη μορφή ηλεκτρονικού εγκλήματος είναι οι απάτες μέσω κινητής τηλεφωνίας. Η πρόσφατη εμπειρία στην χώρα μας σχετικά με την εξαπάτηση ανυποψίαστων θυμάτων μέσω τηλεφώνου, κατέδειξε το μέγεθος του προβλήματος. Ένα παράδειγμα τέτοιας μορφής εγκλήματος παρουσιάζεται παρακάτω[57]:

«Σε είδα στην καφετέρια το Σάββατο και μου άρεσες πολύ. Μου το έδωσε το τηλέφωνο ο φίλος σου! Είσαι ακόμη διαθέσιμος; Μαριάννα». Αυτό το φαινομενικά αθώο ή... πικάντικο μήνυμα κυκλοφορεί το τελευταίο χρονικό διάστημα σε εκατοντάδες κινητά, προκαλώντας τεράστια οικονομικά προβλήματα, αλλά και ομηρικούς συζυγικούς καβγάδες. Ακόμη και η απλή απάντηση: «Λάθος» θα έχει ως αποτέλεσμα να λάβετε έναν «φουσκωμένο» λογαριασμό. Αν πάλι η ανταπόκρισή σας στην «πρόκληση» είναι θετική, το μπουγιουρντί θα είναι αντίστοιχο της θέρμης με την οποία απαντήσατε. Σύμφωνα με πληροφορίες από την Αστυνομία, δεν είναι ούτε μία ούτε δύο οι περιπτώσεις ανθρώπων που κλήθηκαν να πληρώσουν ακόμη και 1.500 ευρώ, ενώ κάποιοι χρεώθηκαν 5.000

---

[56] Αναστασία Ζάννη 2005 σελ.102

[57] http://www.enet.gr/?i=news.el.article&id=80256 (Ημερομηνία πρόσβασης: 15/09/09)

ευρώ. Τα θύματα που κατήγγειλαν την κινητή απάτη έχουν ήδη ξεπεράσει τα 250, ενώ εκτιμάται πως ο αριθμός των εξαπατημένων είναι πολύ μεγαλύτερος.

Πώς λειτουργεί το κόλπο; Οι εταιρείες αυτές, που συνήθως έχουν έδρα τα νησιά Κέιμαν και άλλες χώρες στις οποίες δεν υπάρχει δυνατότητα ελέγχου και ελλιπές νομικό πλαίσιο. αλιεύουν τα υποψήφια θύματά τους με δυο τρόπους. Είτε στέλνουν sms σε τυχαίους αριθμούς και όποιος πέσει στην παγίδα, είτε βρίσκουν τους αριθμούς των τηλεφώνων από διάφορα κουίζ, τεστ και άλλα «λογισμικά» στο Διαδίκτυο, στα οποία κάποιος καταχωρεί οικειοθελώς τον αριθμό του. Η χρέωση κυμαίνεται από 3 έως 4 ευρώ ανά sms, ενώ σε κάποιες περιπτώσεις ο κάτοχος χρεώνεται με ακόμη 2 ευρώ και για το μήνυμα που άθελά του έλαβε. Στον μηνιαίο λογαριασμό τελικά η χρέωση από την απάτη κυμαίνεται από 30 έως και 300 ευρώ. Ουσιαστικά με μια απάντηση ο παραλήπτης «αποδέχεται» τη συμμετοχή του σε κεκαλυμμένα «παιχνίδια» ή dating services (τηλεφωνικά ραντεβού).

4. ΕΡΕΥΝΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

Ο βαθμός εισχώρησης του φαινομένου του ηλεκτρονικού εγκλήματος στη σύγχρονη κοινωνία, αποτελεί αντικείμενο μελέτης πολλών επιστημονικών κλαδών. Στην Ελλάδα, ο κίνδυνος από ηλεκτρονικές επιθέσεις κρίνεται σχετικά μικρός, όμως σε άλλες χώρες(π.χ. ΗΠΑ), αποτελεί μια καθημερινή πραγματικότητα. Δυστυχώς δεν μπορούμε να έχουμε μια επαρκή εικόνα για το βαθμό εξάπλωσης του ηλεκτρονικού εγκλήματος, καθώς η συλλογή στατιστικών στοιχείων είναι δυσκολότερη από κάθε άλλη μορφή εγκλήματος.

Προβλήματα κατά τη συλλογή στατιστικών δεδομένων

Τα στατιστικά στοιχεία που διαθέτουμε για το ηλεκτρονικό έγκλημα και προέρχονται από διωκτικές αρχές, δεν μπορούν να χαρακτηριστούν αξιόπιστα. Υπάρχουν δύο βασικά εμπόδια που δεν μας επιτρέπουν να έχουμε ακριβή στοιχεία[58]

- Η δυσκολία εντοπισμού του ηλεκτρονικού εγκλήματος : Το πρόβλημα της λεγόμενης «κρυφής» εγκληματικότητας, που το συναντάμε σε όλες τις μορφές εγκλημάτων, παρουσιάζει μεγάλη συχνότητα στην περίπτωση των ηλεκτρονικών εγκλημάτων. Ο όρος αναφέρεται σε εγκλήματα που έχουν τελεσθεί, χωρίς να το έχουν αντιληφθεί τα θύματα.
- Η διστακτικότητας αναφοράς από τα θύματα : Ακόμη κι αν το θύμα αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, διστάζει να την αναφέρει στις διωκτικές αρχές, με αποτέλεσμα, να μην είναι δυνατή η συστηματική συλλογή στατιστικών στοιχείων. Οι λόγοι για τη μη αναφορά των ηλεκτρονικών εγκλημάτων ποικίλλουν με κυρίαρχο τον φόβο της εταιρείας, που δέχθηκε την επίθεση, ότι αν αποκαλυφθεί το γεγονός θα έχει αρνητικές συνέπειες στην εικόνα της προς τους πελάτες της.

Εκτιμάται ότι τα στατιστικά στοιχεία που διαθέτονται από τις διωκτικές αρχές, αντιπροσωπεύουν μόνον το 10% της πραγματικής έκτασης του φαινομένου. Για το λόγο αυτό, η μέτρηση του ηλεκτρονικού εγκλήματος, γίνεται με εναλλακτικές μεθόδους όπως συνεντεύξεις και έρευνες σε συγκεκριμένες κατηγορίες ατόμων.

4.1. 2005 FBI Computer Crime Survey[59]

Η πλέον αξιόπιστη έρευνα στην Αμερική, πραγματοποιείται κάθε χρόνο από το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau of Investigation – FBI) των Ηνωμένων πολιτειών. Τα αποτελέσματα της έρευνας για το έτος 2005, βασίζονται στις απαντήσεις

---

[58] Kabay M. 2001 (Ημερομηνία πρόσβασης: 11/07/09)

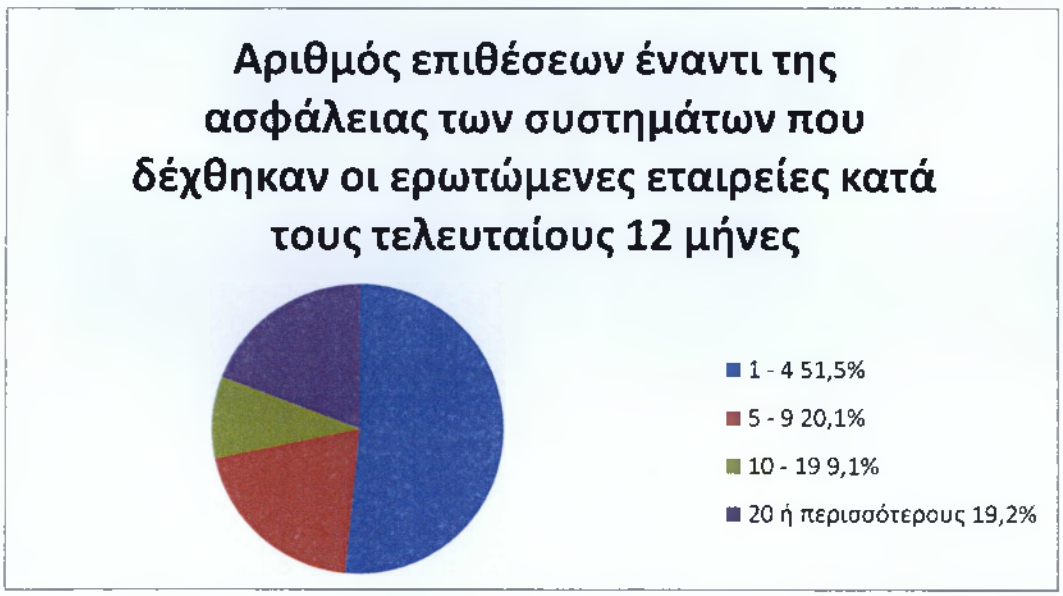
[59] www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf (Ημερομηνία πρόσβασης: 26/07/09)

2066 οργανισμών και σκοπός της έρευνας είναι, να διαπιστωθεί το είδος των εγκλημάτων που διαπράττονται σε όλο το εύρος των οργανισμών, που δραστηριοποιούνται στις ΗΠΑ.

Η έρευνα βασίζεται σε ένα ερωτηματολόγιο 23 ερωτήσεων, που σχετίζεται με πλήθος θεμάτων όπως ασφάλεια υπολογιστών, χρησιμοποιούμενη τεχνολογία, είδος επιθέσεων και τρόποι αντιμετώπισης αυτών. Οι ερωτώμενοι απαντούν διατηρώντας την ανωνυμία τους.

Από την έρευνα αυτή συνάγονται ουσιαστικά συμπεράσματα για το φαινόμενο του ηλεκτρονικού εγκλήματος. Ας δούμε, τις απαντήσεις ορισμένων χαρακτηριστικών ερωτήσεων σχετικά με την έκταση του φαινομένου:

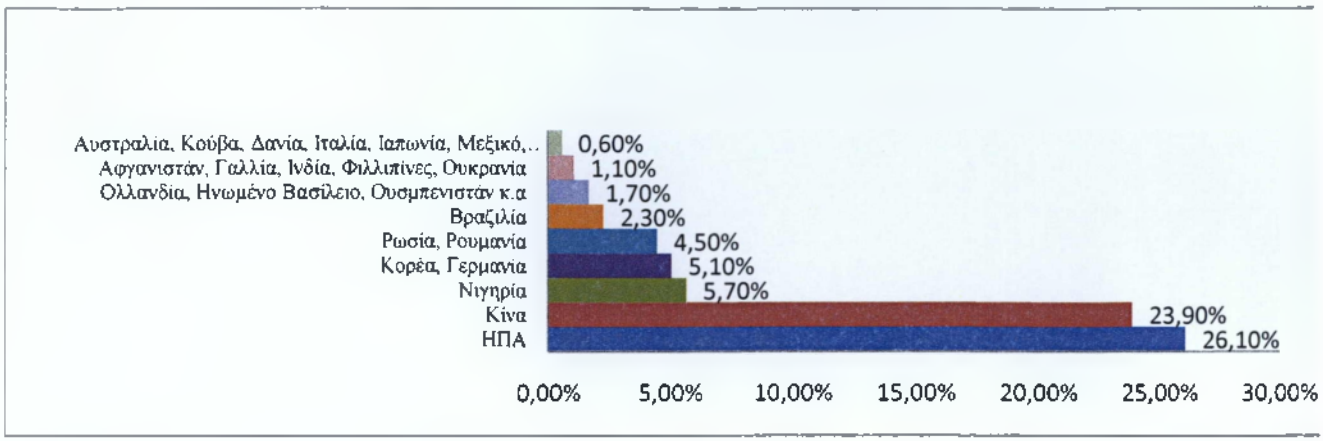
a) Στην ερώτηση «Πόσα συμβάντα παραβίασης της ασφάλειας των υπολογιστών έλαβαν χώρα τους τελευταίους 10 μήνες» το 51,5% απάντησε από 1 – 4, το 20,1% από 5 – 9, το 9,1% από 10 – 19 και το 19,2% από 20 και πάνω. Διαφαίνεται ότι οι απειλές έναντι της ασφάλειας των υπολογιστών, είναι σύνηθες φαινόμενο για το 87% των επιχειρήσεων που ερωτήθηκαν και μάλιστα το 50% από αυτές, έχει δεχθεί περισσότερες από 5 επιθέσεις. Εντυπωσιακό είναι επίσης το ποσοστό των επιχειρήσεων που δέχθηκαν πάνω από 20 επιθέσεις (19,2%).



Εικόνα 4.1. Αριθμός επιθέσεων έναντι της ασφάλειας των συστημάτων που δέχθηκαν οι ερωτώμενες εταιρείες κατά τους τελευταίους 12 μήνες

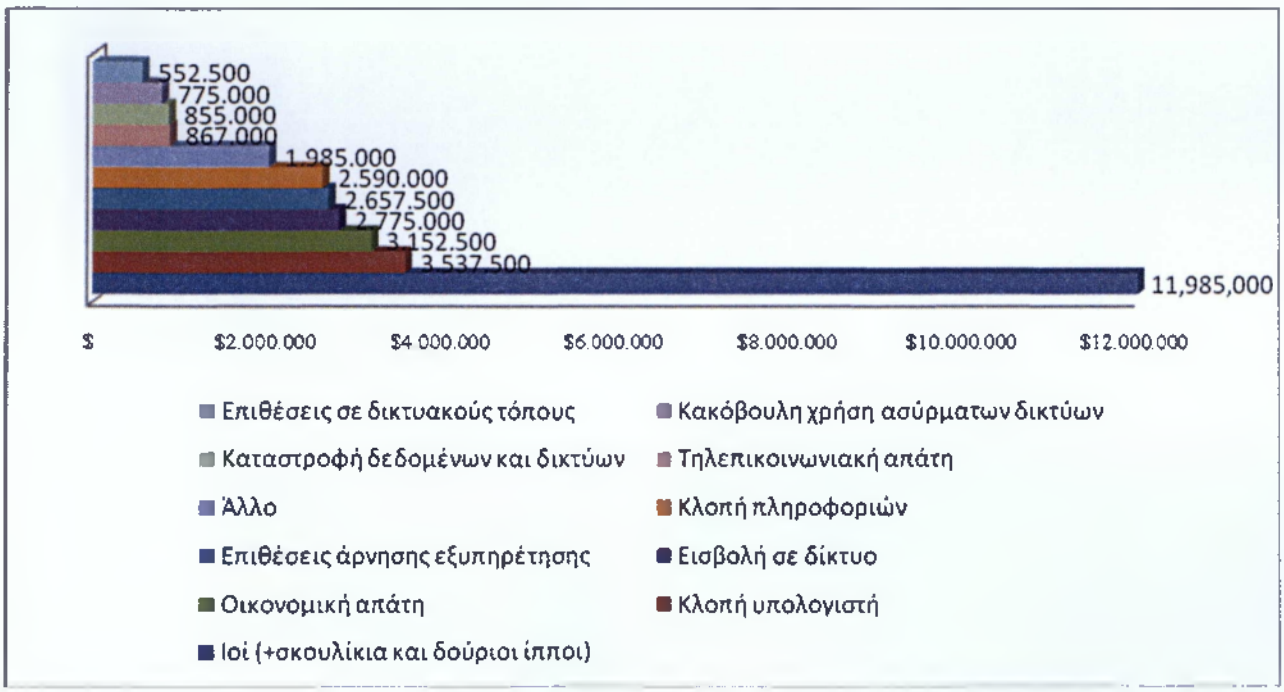
b) Ένας μύθος που θεωρεί ότι οι περισσότερες επιθέσεις προέρχονται από τις είπα ΗΠΑ καταρρίφθηκε από τις απαντήσεις στην αντίστοιχη ερώτηση. Ναι μεν η έρευνα έδειξε ότι το μεγαλύτερο ποσοστό επιθέσεων προέρχεται από τις ΗΠΑ(26,1%), όμως είναι πολύ μικρό από αυτό που κάποιος θα περίμενε. Στην δεύτερη θέση ακολουθεί η Κίνα με ποσοστό 23,9%. Συνολικά εμφανίζονται 36

χώρες από τις οποίες προέρχεται το 75% των επιθέσεων, καταδεικνύοντας, ότι το ηλεκτρονικό έγκλημα είναι φαινόμενο παγκόσμιας κλίμακας.

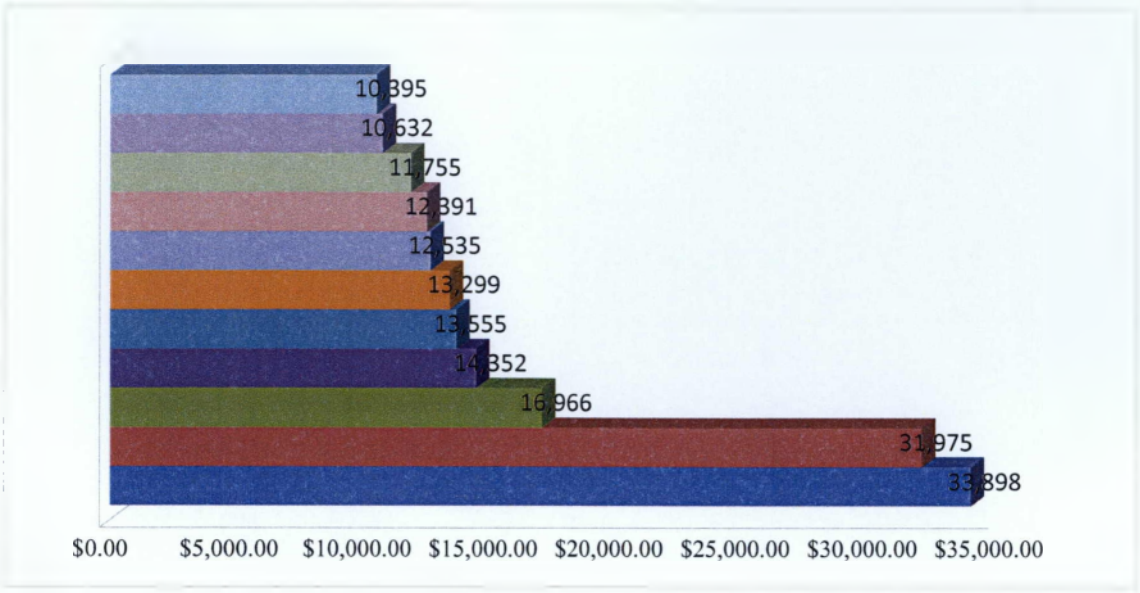


Εικόνα 4.2:Οι χώρες από τις οποίες προέρχονται οι επιθέσεις εναντίον της ασφάλειας των υπολογιστικών συστημάτων.

c) Όσον αφορά τις οικονομικές συνέπειες από τις επιθέσεις που υπέστησαν οι οργανισμοί, παρατηρούμε ότι, το συνολικό κόστος ανήλθε περίπου στα 30.000.000 δολάρια, δηλαδή 170.000 δολάρια κατά μέσο όρο.

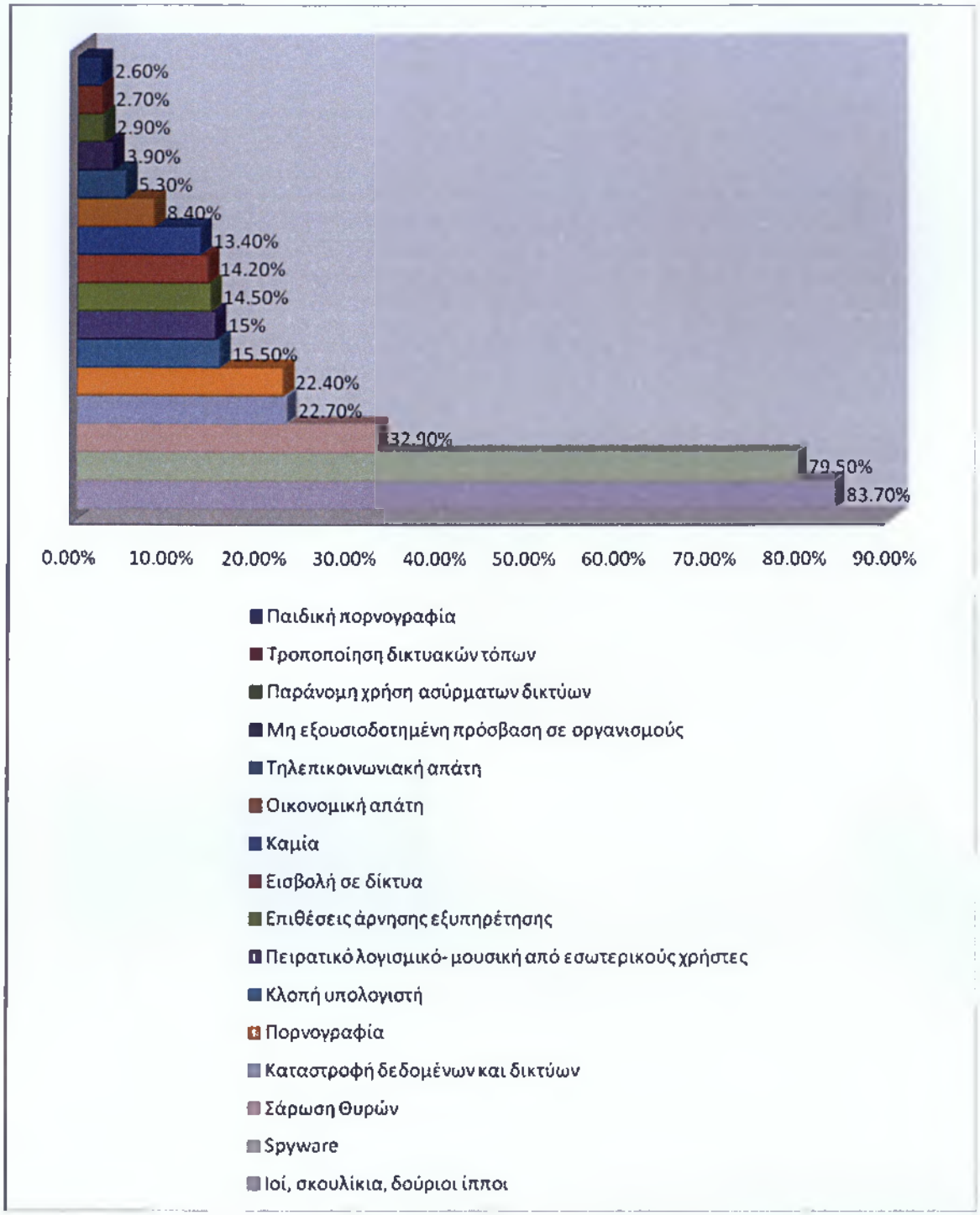


Εικόνα 4.3: Συνολικές οικονομικές απώλειες.



Εικόνα 4.4: Μέσος όρος οικονομικών απωλειών.

Σύμφωνα με την FBI Computer Crime Survey (2005), η διασπορά κακόβουλου λογισμικού κατέχει την πρώτη θέση και μάλιστα με υψηλό ποσοστό (83,7% οι ιοί και 79,5% τα spyware). Σημαντικό ποσοστό, επίσης, καταλαμβάνουν οι επιθέσεις, που έχουν σκοπό την καταστροφή δεδομένων ή δικτύου (22,7%) και άρνησης εξυπηρέτησης, ενώ, μικρότερα ποσοστά παρατηρούμε στις οικονομικές και τηλεπικοινωνιακές απάτες (8,4% και 5,3% αντιστοίχως).



Εικόνα 4.5: Μορφές των επιθέσεων έναντι της ασφάλειας υπολογιστικών συστημάτων

Η e-Crime Watch Survey (2005), όπως φαίνεται και από τον παρακάτω πίνακα, παρουσίασε παρόμοια αποτελέσματα. Αίσθηση όμως προκαλεί το υψηλό ποσοστό των επιθέσεων phising (57%). Τέλος, υψηλά ποσοστά παρατηρούνται σε όλες τις μορφές επιθέσεων που έχουν αν κάνουν με την κακόβουλη εισβολή σε δίκτυα.

Which of the following electronic crimes were committed against your organization in 2004? (base: among those experiencing electronic crimes)	2005 (base:777)	2004 (base:342)
Virus or other malicious code	82%	77%
Spyware	61%	N/A
Phising	57%	31%
Illegal generation of spam email	48%	38%
Unauthorized access to information, systems of networks	43%	47%
Denial of service attack	32%	44%
Rogue Wireless access point	21%	N/A
Exposure of private of sensitive information	19%	N/A
Fraud	19%	22%
(2004: Emplyee) Identity theft	17%	12%
Password sniffing	16%	N/A
Theft of intellectual property	14%	20%
Zombie machines on organization's network	13%	N/A
Theft of other (proprietary) info	12%	16%
Sabotage	11%	18%
Web site defacement	9%	N/A
Extortion	2%	5%
Other	4%	11%
Don't Know/not sure	3%	8%

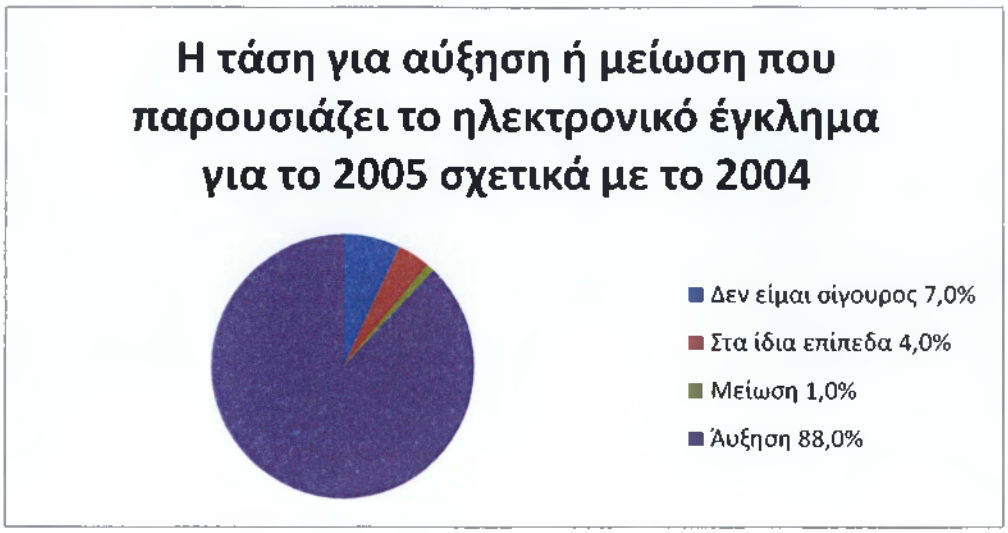
Πίνακας 4.6: Οι συχνότερες μορφές ηλεκτρονικών εγκλημάτων.

4.2. 2005 e – Crime Watch Survey [60]

Η E – Crime Watch Survey πραγματοποιήθηκε το 2005 από το περιοδικό CSO(Chief Security Officers) σε συνεργασία με δύο πολύ σημαντικούς οργανισμούς: (α) The US Secret Service Electronic Crimes Task Force και (β) Carnegie Mellon University Software Engineering Institute's CERT Coordination Center. Η έρευνα, σκιαγραφεί τις τάσεις που υπάρχουν στο φαινόμενο του ηλεκτρονικού εγκλήματος. Πραγματοποιήθηκε on-line, κατά το χρονικό διάστημα από 3 έως 14 Μαρτίου 2005. Οι ερωτώμενοι, ο συνολικός αριθμός των οποίων ανερχόταν στους 819, αποτελούνταν μόνο από μέλη του περιοδικού CSO ή της US Secret Service's Electronic Crimes TaskForce. Ας δούμε ορισμένα βασικά αποτελέσματα της έρευνας:

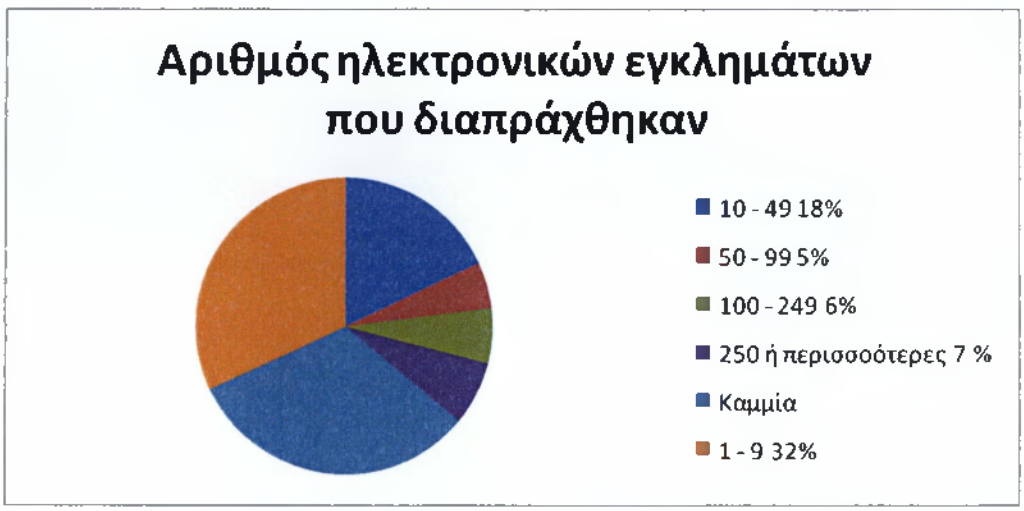
a) Στην ερώτηση εάν το ηλεκτρονικό έγκλημα θα αυξηθεί κατά το έτος 2005 το 85% απάντησε θετικά ενώ μόλις το 1% απάντησε αρνητικά.

[60] www.cert.org/archive/pdf/ecrimesummary05.pdf (Ημερομηνία πρόσβασης: 26/07/2009)



Εικόνα 4.7. Η τάση για αύξηση ή μείωση που παρουσιάζει το ηλεκτρονικό έγκλημα για το 2005 σχετικά με το 2004

b) Στην κρίσιμη ερώτηση σχετικά με τον αριθμό των ηλεκτρονικών εγκλημάτων, που διαπράχθηκαν το έτος 2005, το 68% των ερωτώμενων απάντησαν ότι δέχθηκε τουλάχιστον μια επίθεση, ενώ το 36% ότι δέχθηκε παραπάνω από 10 επιθέσεις.



Εικόνα 4.8. Αριθμός ηλεκτρονικών εγκλημάτων που διαπράχθηκαν

c) Τέλος, όσον αφορά το κόστος που υπέστησαν οι επιχειρήσεις από τις επιθέσεις που δέχθηκαν, το 62% από αυτές δεν κατέστη δυνατόν να προσδιορίσει έστω και κατά προσέγγιση το χρηματικό ποσό, το 19% δεν είχε καθόλου χρηματικές απώλειες, ενώ ένα ποσοστό της τάξης του 16%, είχε ζημιές που ανέρχονται στο ένα εκατομμύριο δολάρια. Αν και τα οικονομικά δεδομένα που παρουσιάζονται από την έρευνα αυτή δεν είναι πολύ υψηλά, το ποσοστό 62% που δεν μπορεί να προσδιορίσει το ακριβές ποσό είναι το πλέον ανησυχητικό στοιχείο, καθώς

ενισχύει την αβεβαιότητα για τις οικονομικές απώλειες του ηλεκτρονικού εγκλήματος.

Οι οικονομικές απώλειες από το ηλεκτρονικό έγκλημα	**Έτος 2005**
$10 million or more	1%
$1 million - $9.9 million	2%
$500.000 - $999.999	1%
$100.000 - $499.999	4%
$1 - $499.999	12%
Zero	19%
Mean	$506,670
Median	$0
Sum	$150,000,000
Don't Know/not sure	62%

Πίνακας 4.9: Οικονομικές απώλειες του ηλεκτρονικού εγκλήματος.

4.3. Γραφείο καταπολέμησης ηλεκτρονικού εγκλήματος Κύπρου

Παρακάτω βλέπουμε στοιχεία που αφορούν καταγγελίες για παιδική πορνογραφία για τα έτη 2004 έως τον Οκτώβριο του 2008 όπου αντλήθηκαν από το γραφείο καταπολέμησης ηλεκτρονικού εγκλήματος:

ΕΤΟΣ	ΚΑΤΑΓΓΕΛΙΕΣ	ΠΟΙΝΙΚΗ ΔΙΩΞΗ	ΜΗ ΠΟΙΝΙΚΗ ΔΙΩΞΗ	ΚΑΤΑΔΙΚΕΣ	ΥΠΟ ΔΙΕΡΕΥΝΗΣ	ΥΠΟ ΕΚΔΙΚΑΣΗ
2004	8	2	6	1		
2005	16	6	10	5		
2006	24	8	16	6		1
2007	34	8	26	2		1
2008	60	7	39		14	

Πίνακας 4.10: Καταγγελίες παιδικής πορνογραφίας Κύπρος 2004-2008

Τα πιο πάνω στοιχεία αφορούν **καταγγελίες** κυρίως για την κατοχή παιδικού πορνογραφικού υλικού είτε σε ηλεκτρονική ή άλλη μορφή κατά παράβαση του Νόμου 22(iii)/2004 και 87(i)/2007 οι οποίες διερευνήθηκαν από την Αστυνομία. Επίσημα στατιστικά στοιχεία για την παιδική πορνογραφία άρχισαν να τηρούνται μετά την ίδρυση του Γ.Κ.Η.Ε τον Σεπτέμβριο του 2007.

4.4 Διακίνηση πορνογραφικού υλικού

Η διακίνηση πορνογραφικού υλικού, δεν είναι έγκλημα νέο. Η εξάπλωση, όμως, του Διαδικτύου, έχει διευκολύνει την διάπραξη του. Στατιστικές μελέτες έχουν καταδείξει, ότι η διακίνηση υλικού πορνογραφίας μέσω του Διαδικτύου, αποτελεί μια από τις πιο συχνές μορφές εγκλήματος.[61]

Ειδικότερα:

» Δικτυακοί τόποι με πορνογραφικό υλικό: 4,2 Εκατομμύρια
» Σελίδες με πορνογραφικό υλικό: 372 Εκατομμύρια
» Αιτήματα για πορνογραφικό υλικό σε μηχανές αναζήτησης (ανά ημέρα)(25% του συνόλου): 68 Εκατομμύρια
» E-mail με πορνογραφικό περιεχόμενο: 4,5 ανά χρήστη
» Δικτυακοί τόποι που προσφέρουν παιδική πορνογραφία: 100 Χιλιάδες
» Μέσος όρος ηλικίας πρώτης επαφής με τη πορνογραφία: 11 ετών
» Μεγαλύτερη κατανάλωση πορνογραφίας: 12-17 Ετών
» Ποσοστό παιδιών ηλικίας 7-17 ετών που δίνουν ελεύθερα την διεύθυνση κατοικίας τους: 20%
» Σεξουαλική παρενόχληση νέων σε δωμάτια συζητήσεων: 89 %

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

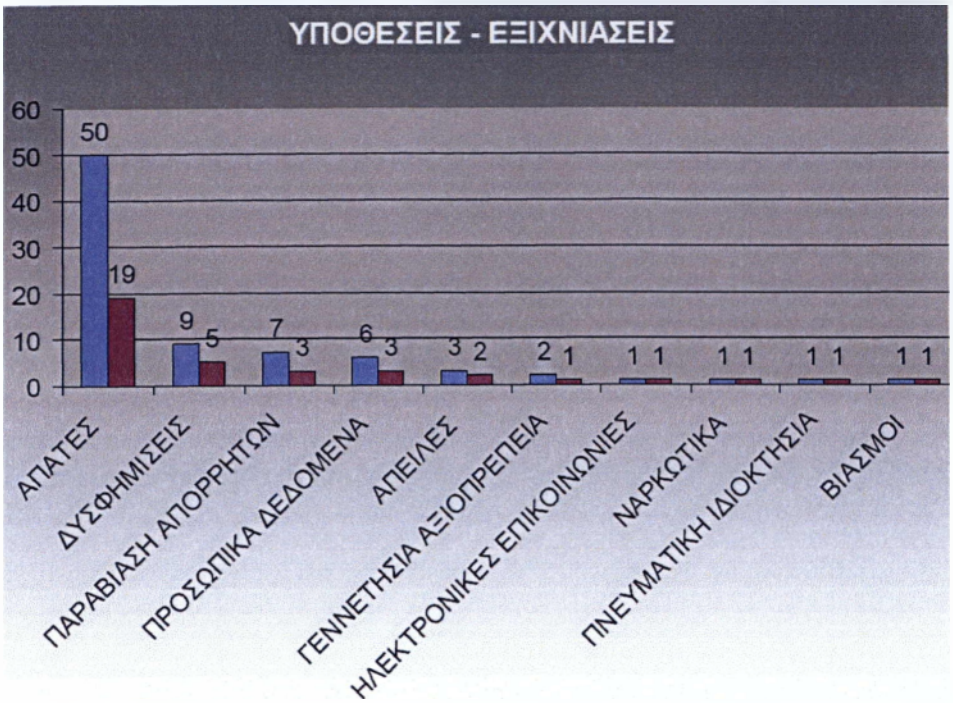
Το πορνογραφικό υλικό, που διακινείται μέσω του Διαδικτύου, μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή και οποιοδήποτε άλλης μορφής πολυμέσων. Ο καθένας μπορεί εύκολα να το «κατεβάσει» στον υπολογιστή του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητα του. Τέτοιου είδους υλικό, βρίσκεται σε διάφορους 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.

Παρακάτω παρουσιάζονται στατιστικά στοιχεία ηλεκτρονικής εγκληματικότητας και ηλεκτρονικής απάτης στην Ελλάδα.

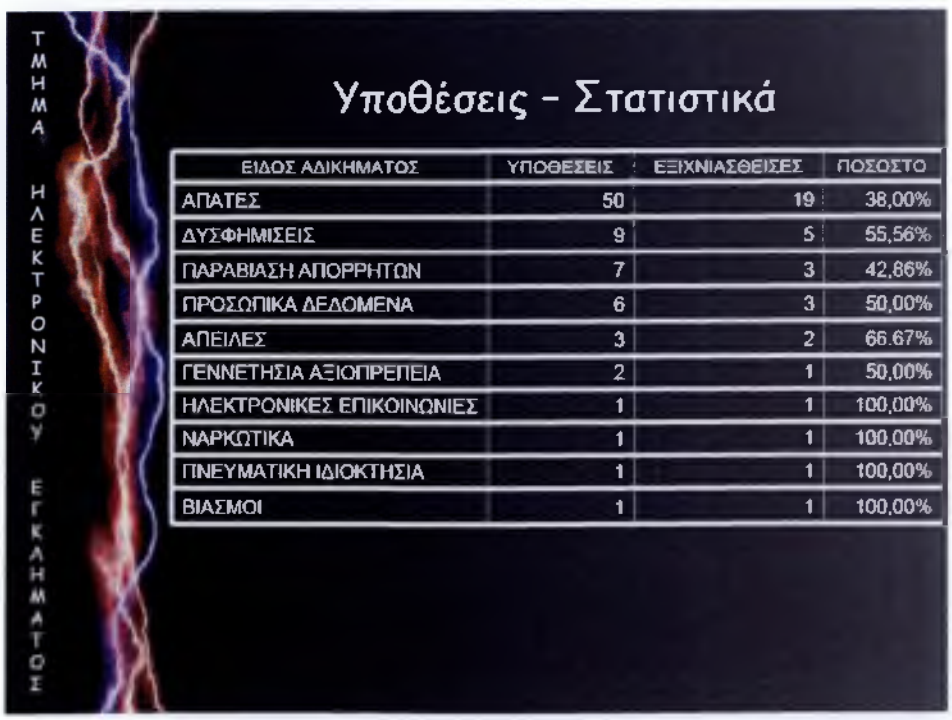
---

[61] http://familysafemedia.com/pornography_statistics.html (Ημερομηνία Πρόσβασης: 26/07/2009)

4.5. Τμήμα δίωξης ηλεκτρονικού εγκλήματος Ελλάδος



Εικόνα 4.11: Υποθέσεις και εξιχνιάσεις για το τμήμα δίωξης ηλεκτρονικού εγκλήματος Ελλάδα.



ΕΙΔΟΣ ΑΔΙΚΗΜΑΤΟΣ	ΥΠΟΘΕΣΕΙΣ	ΕΞΙΧΝΙΑΣΘΕΙΣΕΣ	ΠΟΣΟΣΤΟ
ΑΠΑΤΕΣ	50	19	38,00%
ΔΥΣΦΗΜΙΣΕΙΣ	9	5	55,56%
ΠΑΡΑΒΙΑΣΗ ΑΠΟΡΡΗΤΩΝ	7	3	42,86%
ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ	6	3	50,00%
ΑΠΕΙΛΕΣ	3	2	66,67%
ΓΕΝΝΕΤΗΣΙΑ ΑΞΙΟΠΡΕΠΕΙΑ	2	1	50,00%
ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ	1	1	100,00%
ΝΑΡΚΩΤΙΚΑ	1	1	100,00%
ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ	1	1	100,00%
ΒΙΑΣΜΟΙ	1	1	100,00%

Εικόνα 4.12. Στοιχεία από το τμήμα δίωξης ηλεκτρονικού εγκλήματος.

5. ΑΣΦΑΛΕΙΑ ΚΑΙ ΜΕΤΡΑ ΠΡΟΛΗΨΗΣ

5.1. Ασφάλεια στο Διαδίκτυο

Η ευρύτατη χρήση της τεχνολογίας της πληροφορικής και των επικοινωνιών, αποτελούν το βασικό χαρακτηριστικό τη σημερινή εποχή. Οι υπολογιστές, χρησιμοποιούνται σε όλες τις εκφάνσεις της ανθρώπινης δραστηριότητας, όπως στο εμπόριο, την εκπαίδευση, την ενημέρωση και την ψυχαγωγία. Ως αποτέλεσμα, η ασφάλεια των δεδομένων, που περιέχονται σε αυτούς, αποτελεί πρωταρχικό ζήτημα, καθότι οι κίνδυνοι καταστροφών, αλλοιώσεων ή μη εξουσιοδοτημένης χρήσης των δεδομένων και των υπολογιστικών πόρων πολλαπλασιάζονται.

Ο όρος ασφάλεια, χρησιμοποιείται συχνότατα στην καθημερινή μας ζωή. Προσδιορίζει μια ποικιλία από έννοιες. Στον τομέα των πληροφοριακών συστημάτων, η ασφάλεια σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του, από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με:

- την πρόληψη μη εξουσιοδοτημένων ενεργειών έναντι ενός συστήματος,
- την ανίχνευση κάθε είδους επιθέσεως και τέλος
- την αντίδραση δηλαδή την λήψη μέτρων για την αποκατάσταση της ζημιάς, που προκλήθηκε από τον επιτιθέμενο.

Η πρόληψη, η ανίχνευση και η αντίδραση περιλαμβάνονται στο γενικότερο σχεδιασμό της ασφάλειας ενός οργανισμού, που έχει επικρατήσει να ονομάζεται πολιτική ασφάλειας. Η πολιτική ασφάλειας καθορίζει τις διαδικασίες, που πρέπει να ακολουθούνται, για να μειωθούν οι κίνδυνοι επιθέσεων και τα αποτελέσματα αυτών.

5.1.1. Βασικές έννοιες της ασφάλειας

Η ασφάλεια των πληροφοριακών συστημάτων, προσδιορίζεται με τρεις βασικές έννοιες, οι οποίες είναι κοινά αποδεκτές:

» Εμπιστευτικότητα
» Ακεραιότητα
» Διαθεσιμότητα

Εμπιστευτικότητα

Η εμπιστευτικότητα σχετίζεται με την προστασία των δεδομένων, ώστε μη εξουσιοδοτημένα άτομα να μην έχουν πρόσβαση σ' αυτά. Η έννοια της εμπιστευτικότητας δεν προστατεύει μόνο τα ίδια τα δεδομένα, αλλά, και το γεγονός ότι αυτά υπάρχουν. Για παράδειγμα, η ύπαρξη του φακέλου ενός εγκληματία, τυχαίνει της ίδιας προστασίας και με τα περιεχόμενα του φακέλου.

Ακεραιότητα

Η ακεραιότητα αναφέρεται στην πρόσληψη μη εξουσιοδοτημένης μεταβολής των πληροφοριών. Η μεταβολή περικλείει τις έννοιες της προσθήκης, διαγραφής αλλά και μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Διαθεσιμότητα

Η διαθεσιμότητα περιλαμβάνει την δυνατότητα άμεσης προσπέλασης, χωρίς καθυστερήσεις, των πληροφοριών και υπηρεσιών ενός πληροφοριακού συστήματος. Ο μεγαλύτερος κίνδυνος, έναντι της διαθεσιμότητας, είναι οι επιθέσεις άρνησης εξυπηρέτησης, κατά τις οποίες, ο επιτιθέμενος στερεί από τους χρήστες την πρόσβαση στους πόρους τους συστήματος ή του δικτύου.

5.2. Μέτρα πρόληψης

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

5.2.1. Διαδικασίες αυθεντικοποίησης

Στον κόσμο της τεχνολογίας της πληροφορίας, με τον όρο αυθεντικοποίηση, νοείται η διαδικασία κατά την οποία διαπιστώνεται, ότι η ταυτότητα ενός χρήστη είναι αυθεντική. Για τον προσδιορισμό της ταυτότητας ενός ατόμου, υπάρχουν τρεις βασικές προσεγγίσεις:

- Κάτι που ο χρήστης γνωρίζει π.χ. ένας κωδικός πρόσβασης, ένα PIN κ.λπ.
- Κάτι που ο χρήστης έχει στην κατοχή του, π.χ. μια έξυπνη κάρτα.
- Κάτι που ο χρήστης έχει ως προσωπικό φυσικό χαρακτηριστικό π.χ. το δακτυλικό αποτύπωμα.

Κάθε μια από τις προσεγγίσεις αυτές, φέρει τα προτερήματα και ελαττώματα της. Για παράδειγμα, ένας χρήστης μπορεί να ξεχάσει τον κωδικό πρόσβασης ή να τον αποκαλύψει από λάθος σε μη εξουσιοδοτημένα άτομα. Μια κάρτα εισόδου, μπορεί εύκολα να χαθεί. Ασφαλέστερη θεωρείται η χρήση προσωπικών χαρακτηριστικών, όμως για ένα σύστημα που απαιτεί υψηλό επίπεδο ασφαλείας, χρησιμοποιείται ένας συνδυασμός όσο το δυνατόν περισσότερων τεχνικών.

5.2.1.1.Κωδικοί πρόσβασης

Τα συστήματα, που χρησιμοποιούν κωδικούς, απαιτούν την εισαγωγή από το χρήστη ενός ονόματος χρήστη και ενός κωδικού πρόσβασης για να προστατέψουν την είσοδο. Μετά την εισαγωγή των στοιχείων, το σύστημα κάνει έλεγχο των κωδικών με την 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 απλότητας της αλλά και της μεγάλης ασφάλειας που προσφέρει τυχαίνει 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[62]. 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 εντός συστήματος, που βασίζεται στην χρήση κωδικών πρόσβασης, είναι:

» **Η επιλογή κωδικών πρόσβασης:** Η ορθή επιλογή του κωδικού πρόσβασης είναι πολύ σημαντική. Όταν οι χρήστες αφήνονται μόνοι τους να επιλέξουν του κωδικούς που επιθυμούν, προτιμούν κωδικούς που μπορούν εύκολα να θυμούνται , 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 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 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 κινδύνους προερχόμενους, κυρίως, από τους κοινωνικούς μηχανικούς, οι οποίοι προσποιούμενοι ότι είναι υπάλληλοι μιας π.χ. θυγατρικής εταιρείας, επιτυγχάνουν 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, ο επιτιθέμενος μπορεί να ανακτήσει και να έχει, πλέον, στην κατοχή του όλους τους κωδικούς ενός οργανισμού.

5.2.1.2. Βιομετρικές τεχνικές

Βιομετρία είναι η επιστήμη που χρησιμοποιεί ψηφιακή τεχνολογία, για να αναγνωρίσει την ταυτότητα ατόμων, βάση κάποιων ιδιαίτερων και μοναδικών φυσιολογικών ή συμπεριφοριστικών χαρακτηριστικών τους.

---

[62] Π.χ. εργαλεία σπασίματος κωδικών όπως το Ophcrack http://ophcrack.sourceforge.net/ (Ημερομηνία πρόσβασης: 30/08/09)

Η χρήση των βιομετρικών τεχνικών στον τομέα της ασφάλειας των πληροφοριακών συστημάτων στοχεύει:

- Στην επαλήθευση ταυτότητας ενός χρήστη, η οποία επιτυγχάνεται με την σύγκριση ενός χαρακτηριστικού του, με ένα χαρακτηριστικό μιας βάσης δεδομένων με σκοπό να βρεθεί ταίριασμα.
- Στην ταυτοποίηση ενός χρήστη, η οποία επιτυγχάνεται με τη σύγκριση ενός χαρακτηριστικού του, με το σύνολο των χαρακτηριστικών μιας βάσης δεδομένων με σκοπό να βρεθεί ταίριασμα.

Οι σημαντικότερες βιομετρικές τεχνικές είναι οι ακόλουθες:

Σάρωση δακτυλικού αποτυπώματος

Η ταυτοποίηση δύο ατόμων με την χρήση δακτυλικών αποτυπωμάτων, αποτελεί μια από τις πλέον κλασικές και αξιόπιστες μεθόδους ταυτοποίησης. Χρησιμοποιείται, ευρέως , από τις περισσότερες αστυνομικές υπηρεσίες του κόσμου. Έχει αποδειχτεί, ότι η πιθανότητα δύο άτομα να έχουν το ίδιο δακτυλικό αποτύπωμα είναι μία στο δισεκατομμύριο.

Η λήψη δακτυλικών αποτυπωμάτων γινόταν, παραδοσιακά, με την επικάλυψη των δακτύλων με μελάνη και την εναπόθεση τους σε λευκή κόλλα χαρτί. Στη συνέχεια, πραγματοποιούνταν σάρωση του σάρωση του δακτυλικού αποτυπώματος. Σήμερα, η μέθοδος αυτή, τείνει να ξεπεραστεί, καθώς αρχίζουν ευρέως να χρησιμοποιούνται ευρέως οπτικοί αναγνώστες, υπέρυθρες ακτίνες και τεχνολογίες σιλικόνης για τη λήψη των αποτυπωμάτων.

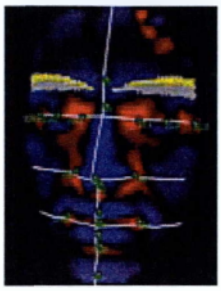
Εικόνα 5.1: Σάρωση δακτυλικού αποτυπώματος με υπέρηχο

Αναγνώριση προσώπου

Η αναγνώριση προσώπου, αποτελεί μια από τις πλέον ταχύτατα αναπτυσσόμενες βιομετρικές τεχνικές. Τα πλεονεκτήματα της μεθόδου αυτής είναι, ότι βρίσκεται πιο κοντά στον τρόπο που, καθημερινά, οι άνθρωποι αναγνωρίζουμε τους συνανθρώπους μας. Επιπλέον, με τα σύγχρονα μηχανήματα είναι δυνατή η λήψη φωτογραφιών από μεγάλη απόσταση.

Στην αναγνώριση προσώπου δίνεται έμφαση σε σημεία του προσώπου, που είναι λιγότερο ευάλωτα στην αλλαγή, όπως τα παραπάνω περιγράμματα του ματιού , οι περιοχές που περιβάλλουν τα ζυγωματικά και η όψη του στόματος καθώς και σε

γεωμετρικά χαρακτηριστικά όπως η απόσταση από τα μάτια έως την μύτη, το κενό ανάμεσα στα φρύδια κ.ά. Τα περισσότερα συστήματα δεν αντιμετωπίζουν πρόβλημα σε αλλαγές κόμμωσης και για καλύτερα αποτελέσματα δεν χρησιμοποιούν περιοχές του προσώπου κοντά στα μαλλιά. Όλα τα βασικά συστήματα είναι σχεδιασμένα, ώστε, να είναι αρκετά ισχυρά, για να διεξάγουν αναζητήσεις ένα-προς-πολλά, δηλαδή, να μπορούν να βρίσκουν ένα πρόσωπο, μέσα σε μια βάση δεδομένων χιλιάδων ή ακόμα και εκατοντάδων χιλιάδων προσώπων. Όμως, πολλά συστήματα αντιμετωπίζουν δυσκολίες στο να πετύχουν μεγάλα επίπεδα απόδοσης, όταν το μέγεθος της βάσης δεδομένων αυξάνεται σε δεκάδες χιλιάδες ή και περισσότερο.



Εικόνα 5.2. Εξαγωγή γεωμετρικών χαρακτηριστικών προσώπου

Σάρωση φωνής

Τα συστήματα σάρωσης φωνής λειτουργούν, αναγνωρίζοντας το μοναδικό ηχητικό σήμα, που παράγει ο χρήστης, λέγοντας μια συγκεκριμένη φράση κλειδί. Το βασικό προτέρημα αυτής της τεχνολογίας, είναι η δυνατότητα εξ αποστάσεως ταυτοποίηση. Δηλαδή, δεν είναι αναγκαίο ο χρήστης να βρίσκεται μπροστά σε κάποιο μηχάνημα ή συσκευή του συστήματος, όπως γίνεται κατά την αναγνώριση δακτυλικού αποτυπώματος ή προσώπου, αλλά μπορεί να βρίσκεται χιλιόμετρα μακριά, χρησιμοποιώντας το τηλέφωνο του ή να βρίσκεται σπίτι και να χρησιμοποιεί ένα κοινό μικρόφωνο.

Σάρωση ίριδας ματιού και αμφιβληστροειδή χιτώνα

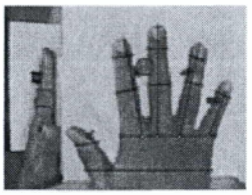
Η ίριδα είναι το έγχρωμο μέρος, που περιβάλλει την κόρη του ματιού και έχει πλούσια και μοναδικά χαρακτηριστικά, όπως ραβδώσεις, νεύρα, δακτύλιοι, ιστοί, αυλάκια, αγγεία και το δίκτυο των κυττάρων. Σύμφωνα με μελέτες, η ανθρώπινη ίριδα έχει σχεδόν 250 χαρακτηριστικά και καθένα απ' αυτά είναι μοναδικό σε κάθε άτομο. Ο αριθμός των χαρακτηριστικών είναι δέκα φορές πάνω από τον αριθμό των γνωρισμάτων, που διαθέτουν τα δακτυλικά αποτυπώματα. Αυτό σημαίνει, ότι η πιθανότητα ο γενετικός κώδικας της ίριδας ενός ατόμου να ταιριάζει απόλυτα με το γενετικό κώδικα της ίριδας κάποιου άλλου ατόμου είναι τόσο απίθανη, σαν να είναι σχεδόν αδύνατο. Η αναγνώριση ίριδας είναι ακόμα πιο αξιόπιστη και από την εξέταση DNA.

Μαζί με τη σάρωση ίριδας, η σάρωση αμφιβληστροειδούς είναι η πιο ακριβής και αξιόπιστη βιομετρική τεχνολογία, όμως είναι και μεταξύ των πιο δύσκολων στη χρήση. Διάφορες έρευνες έχουν δείξει, ότι η μορφή των αγγείων αίματος στο πίσω μέρος του ανθρώπου ματιού είναι διαφορετική από άτομο σε άτομο, ακόμα και σε δίδυμα αδέρφια.

Επίσης, ο αμφιβληστροειδής παραμένει ίδιος σε όλη τη ζωή του ανθρώπου, με την εξαίρεση ορισμένων τύπων εκφυλιστικών ασθενειών του ματιού, ή περιπτώσεις σοβαρών τραυμάτων στο κεφάλι.

Σάρωση χεριού

Η σάρωση χεριού είναι γνωστή και ως γεωμετρία χεριού. Είναι μια αυτοματοποιημένη μέτρηση πολλών μεγεθών του χεριού και των δακτύλων. Η τεχνολογία αυτή χρησιμοποιεί το ύψος των δαχτύλων, την απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων, για να πιστοποιήσει την ταυτότητα του χρήστη. Παρόλο, που δεν είναι η πιο ακριβής τεχνολογία, η σάρωση χεριού έχει αποδειχτεί, ως η ιδανική λύση για χαμηλού επιπέδου εφαρμογές ασφάλειας.



Εικόνα 5.3: Γεωμετρία χεριού

Σάρωση υπογραφής

Η σάρωση υπογραφής είναι γνωστή και ως Δυναμική Εξακρίβωση Υπογραφής. Επειδή κάθε άτομο έχει τον προσωπικό του γραφικό χαρακτήρα, το σύστημα παίρνει τα χαρακτηριστικά του τρόπου γραφής και αναλύει τη δυναμική του χτυπήματος, την ταχύτητα και την πίεση. Ενώ με εξάσκηση κάποιος, ίσως μπορέσει να αντιγράψει την οπτική εικόνα της υπογραφής κάποιου άλλου, είναι πολύ δύσκολο, έως αδύνατο, να αντιγράψει τον τρόπο με τον οποίο το άτομο αυτό υπογράφει. Ακόμα και αν η υπογραφή είναι τέλεια σχεδιασμένη, η ταχύτητα, η δύναμη και η πίεση θα διαφέρουν. Η σάρωση υπογραφής δεν τυγχάνει ακόμη ευρείας χρήσης, αναμένεται όμως πολύ σύντομα να βοηθήσει στην πιστοποίηση επίσημων εγγράφων.

Σάρωση πατήματος πλήκτρου

Η δυναμική πατήματος πλήκτρου είναι γνωστή και ως ρυθμός δακτυλογράφησης. Η μέθοδος αυτή, εξετάζει τον τρόπο με τον οποίο ένα άτομο δακτυλογραφεί ή πιέζει τα πλήκτρα σε ένα πληκτρολόγια. Τα χαρακτηριστικά που αναλύονται, είναι η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος, που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα ενός άλλου.

Άλλες τεχνικές

Εκτός των ανωτέρω, υπάρχουν και μια σειρά από βιομετρικές τεχνικές που είτε βρίσκονται στο στάδιο της έρευνας είτε στο στάδιο της ανάπτυξης. Οι βασικότερες από αυτές, είναι το σχήμα του αυτιού, η οσμή, η σάρωση φλέβας, η γεωμετρία δακτύλου, η σάρωση νυχιού και η αναγνώριση βηματισμού.

5.2.2. Χρήση λογισμικού Ασφαλείας

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 τα firewalls.

5.2.2.1. Λογισμικό Antivirus

Οπως 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:** Πρώτη και βασική λειτουργία του λογισμικού είναι η ανίχνευση του συστήματος, για να εξακριβωθεί, εάν έχει μολυνθεί από ιούς. Η διαδικασία αυτή, μπορεί να γένει 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 μας έχει προσβληθεί από κάποιο ιό, το λογισμικό θα μας ενημερώσει για την ταυτότητα του. Η δυνατότητα αυτή είναι πολύ σημαντική, γιατί μας επιτρέπει να εκτίσουμε το μέγεθος της ζημιάς που έχει προκληθεί, όσο και να εκτελέσουμε τις 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 πρέπει να κάνει. Ο 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

Μέθοδοι εντοπισμού ιών

Η βασικότερη λειτουργία ενός λογισμικού αντιμετώπισης ιών, είναι ο εντοπισμός των ιών. Λόγω καθημερινής δημιουργίας νέων ιών με ιδιαίτερα χαρακτηριστικά, ένα λογισμικό μπορεί να εντοπίσει μόνο τους ιούς, οι οποίοι του είναι γνωστοί. Γι' αυτό, όλες οι εταιρείες που προσφέρουν λογισμικό ανίχνευσης ιών, δίνουν τη δυνατότητα στους χρήστες να κάνουν on-line ενημέρωση της βάσης δεδομένων του προγράμματος με τους νέους ιούς, προκειμένου, να είναι δυνατός ο εντοπισμός και η απομάκρυνση τους.

Πως όμως ένα λογισμικό εντοπίζει τους ιούς σε ένα σύστημα; Όπως αναφέρθηκε, κάθε ιός είναι διαφορετικός. Το στοιχείο που τον κάνει μοναδικό ονομάζεται αποτύπωμα ή υπογραφή του ιού. Στη βάση δεδομένων ενός προγράμματος antivirus, τηρείται μια λίστα

με όλες τις υπογραφές, που είναι γνωστές. Κατά τον έλεγχο ενός συστήματος, όταν βρεθεί κάποιο ταίριασμα της υπογραφής του αρχείου με την υπογραφή που έχει αποθηκευτεί στη βάση δεδομένων του antivirus, ενημερώνεται άμεσα ο χρήστης, ότι έχει μολυνθεί από κάποιο ιό.

Προηγμένες δυνατότητες εφαρμογών antivirus

Το μεγαλύτερο μειονέκτημα των εφαρμογών antivirus, είναι ότι για να εντοπίσει ένας ιός θα πρέπει , πρωταρχικά να έχει ενημερωθεί η Β.Δ. του προγράμματος με την υπογραφή του. Οι εταιρείες λογισμικού έχουν βελτιώσει, κατά πολύ, τη διαδικασία αυτή και μόλις λίγες ώρες μετά την εμφάνιση ενός νέου ιού ενημερώνουν, άμεσα, τις βάσεις τους με το απαιτούμενο λογισμικό απομάκρυνσης του. Όμως, μέσα σε αυτό το μικρό, σχετικά, χρονικό διάστημα, ο ιός, θα έχει προλάβει να προξενήσει ζημιά σε αρκετές χιλιάδες υπολογιστές. Για το λόγο αυτό, οι εταιρείες λογισμικού αναζητούν νέες τεχνικές και μεθόδους για την αντιμετώπιση των προβλημάτων αυτών. Οι σχετικές τεχνολογίες, που τυγχάνουν ευρείας ανάπτυξης τα τελευταία χρόνια, είναι η ευρετική ανάλυση και ο έλεγχος ακεραιότητας.

- **Ευρετική Ανάλυση:** Κατά τη χρήση ευρετικής ανάλυσης το πρόγραμμα δεν αναζητά τις υπογραφές των ιών, αλλά, ελέγχει τα εκτελέσιμα αρχεία και προσπαθεί να προσδιορίσει, εάν στον κώδικα τους περιέχεται εντολή ή εντολές, οι οποίες πιθανώς να αποτελούν ιούς. Τα ποσοστά επιτυχίας, με τη χρήση της μεθόδου αυτής, ανέρχονται στο 60% με 90%. Το μεγάλο πλεονέκτημα είναι ότι στην περίπτωση αυτή, δεν απαιτείται η ενημέρωση της Β.Δ. του προγράμματος, ενώ , αν υπάρχει η δυνατότητα εφαρμογής και των δύο τεχνικών τότε έχουμε ακόμη μεγαλύτερη προστασία.
- **Έλεγχος ακεραιότητας:** Είναι μία τεχνική που χρησιμοποιείται για την ανίχνευση μόνο των ιών, χωρίς να δίνει τη δυνατότητα προσδιορισμού της ταυτότητας τους. Η τεχνική αυτή ολοκληρώνεται σε δύο στάδια: Στο πρώτο στάδιο, για κάθε αρχείο του συστήματος υπολογίζεται ένα άθροισμα ελέγχου. Το άθροισμα αυτό είναι ένας αριθμός, που προσδιορίζει μοναδικά ένα αρχείο, ενώ, κάθε τροποποίηση, έστω και ενός bit, του αρχείου προκαλεί μεταβολή του αθροίσματος. Τα αθροίσματα αυτά αποθηκεύονται σε μια βάση δεδομένων (απαιτείται βέβαια σε αυτό το στάδιο το σύστημα να είναι καθαρό). Στο δεύτερο στάδιο, γίνεται επανυπολογισμός των αθροισμάτων και αυτά συγκρίνονται με τα περιεχόμενα της βάσης δεδομένων. Εφόσον διαπιστωθεί διαφορά, πιθανολογείται ότι αυτή οφείλεται στην επίδραση ενός ιού.

Κριτήρια επιλογής λογισμικού ανίχνευσης ιών

Σήμερα, στην παγκόσμια αγορά, κυκλοφορούν πολλά πακέτα ανίχνευσης ιών. Τα κριτήρια, με τα οποία θα επιλέξουμε το λογισμικό, εξαρτώνται άμεσα, από τις ανάγκες που θέλουμε να καλύψουμε. Οι βασικότερες προϋποθέσεις είναι οι ακόλουθες:

- Εύχρηστο Interface & χαμηλή κατανάλωση πόρων.
- Προστασία σε πραγματικό χρόνο.
- Αυτόματη ενημέρωση.

» Προστασία Ηλεκτρονικής Αλληλογραφίας.
» Προγραμματισμένος Έλεγχος.
» Δισκέτα Εκκίνησης.
» Καταγραφή Συμβάντων (event logging).

5.2.2.2. Firewalls

Ο όρος firewalls, έχει αρχικά χρησιμοποιηθεί από τις κατασκευαστικές εταιρείες, για να προσδιορίσουν τον τοίχο που χτιζόταν σε ένα κτίριο, ο οποίος, χώριζε δυο σημεία με σκοπό, σε περίπτωση πυρκαγιάς, να μην επεκταθεί η φωτιά. Ο όρος, επίσης, χρησιμοποιήθηκε για να περιγράψει τα περιβλήματα στα ντεπόζιτα καυσίμων των αγωνιστικών αυτοκινήτων, τα οποία εμπόδιζαν τη διείσδυση της φωτιάς στα καύσιμα.

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

Τα περισσότερα firewalls επιτελούν δύο βασικές λειτουργίες ασφάλειας:

a) 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 υιοθετούμενη πολιτική ασφάλειας και
b) Πύλες εφαρμογών (Application proxy gateways), που προσφέρουν υπηρεσίες στους εσωτερικούς χρήστες και ταυτόχρονα προστατεύουν τους hosts από εξωτερικές απειλές.

Η επιλογή της λειτουργίας, που θα χρησιμοποιηθεί σε ένα firewall, σχετίζεται άμεσα με την πολιτική ασφαλείας ενός οργανισμού. Οι βασικότερες πολιτικές ασφαλείας, που εφαρμόζονται, είναι δύο:

a) Πολιτική προκαθορισμένης αδείας χρήσης (Allow- everything-not-specifically-denied) όπου η κυκλοφορία πακέτων και η εκτέλεση εφαρμογών επιτρέπεται ελεύθερα, εκτός των περιπτώσεων που υπάρχει ρητή απαγόρευση
b) Πολιτική προκαθορισμένης απαγόρευσης χρήσης (Deny-everything-not-specifically-denied), στην οποία το firewall ρυθμίζεται, έτσι ώστε, να μην επιτρέπει καμιά κυκλοφορία πακέτων και καμιά εκτέλεση εφαρμογής, εφόσον, δεν έχουν εκ των προτέρων καθοριστεί. Στην περίπτωση αυτή, έχουμε μεγαλύτερη ασφάλεια από την πρώτη, όμως, η έντονη «παρουσία» του firewall ενδέχεται να δυσανασχετήσει τους χρήστες.

Βασικές τεχνικές προστασίας με χρήση firewalls

Με την ραγδαία ανάπτυξη του ηλεκτρονικού εγκλήματος, η χρήση των firewalls είναι περισσότερο αναγκαία από ποτέ. Η τεχνολογία, στο συγκεκριμένο τομέα, αναπτύσσεται με γοργούς ρυθμούς και έχουν δημιουργηθεί firewalls, τα οποία επιτελούν πολλές

εργασίες ταυτόχρονα. Επιχειρώντας ένα διαχωρισμό των firewalls, με κριτήριο την χρησιμοποιούμενη τεχνική, μπορούμε να διακρίνουμε τρεις βασικές τεχνικές προστασίας:

» Πύλες φιλτραρίσματος πακέτων (Packet filtering gateways)
» Πύλες εφαρμογών (application gateways)
» Υβριδικές πύλες (Hybrid gateways)

Πύλες φιλτραρίσματος πακέτων: Οι πύλες φιλτραρίσματος πακέτων είναι η πιο απλή τεχνική, που χρησιμοποιείται στα firewalls. Όλα τα πακέτα που διακινούνται στο δίκτυο και διέρχονται από το firewall φιλτράρονται, με βάση κάποιους προκαθορισμένους κανόνες, που τίθενται από το διαχειριστή. Οι επιλογές είναι δύο: είτε να επιτραπεί η διέλευση του πακέτου (permit,allow) είτε να απορριφθεί (block, deny). Οι παράμετροι, που προσδιορίζουν τα κριτήρια επιλογής των πακέτων που θα εισέλθουν ή εξελιχθούν είναι:

» Η διεύθυνση IP του αποστολέα και του παραλήπτη, με δυνατότητα ομαδοποίησης των διευθύνσεων με τη χρήση μάσκας (address masks)
» Η θυρίδα (port) προέλευσης και προορισμού
» Το χρησιμοποιούμενο πρωτόκολλο επικοινωνίας

Το μεγαλύτερο μειονέκτημα των firewall, που χρησιμοποιούν την τεχνική αυτή, είναι ότι το περιεχόμενο των IP-πακέτων δεν λαμβάνεται υπόψη, καθώς εξετάζονται μόνο οι IP-επικεφαλίδες, από τις οποίες λαμβάνονται οι πληροφορίες δρομολόγησης, που στη συνέχεια αξιολογούνται και αναλόγως επιτρέπεται ή απαγορεύεται η διέλευση του πακέτου.

Πύλες εφαρμογών: Οι πύλες εφαρμογών λειτουργούν στο υψηλότερο στρώμα επικοινωνίας, γνωστό και ως επίπεδο εφαρμογής. Κύριο χαρακτηριστικό των πυλών εφαρμογής είναι η ύπαρξη μιας υπηρεσίας διαμεσολάβησης, που πραγματώνεται με τη χρήση ενός πακέτου λογισμικού proxy server. Η υπηρεσία proxy έχει τη δυνατότητα να ενεργεί, ταυτόχρονα, ως πελάτης και διακομιστής. Όσον αφορά στους εσωτερικούς χρήστες λειτουργεί ως διακομιστής, ενώ, όσον αφορά στους εξωτερικούς, λειτουργεί ως πελάτης. Το λογισμικό αυτό παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας και έχει, ως βασικό σκοπό, τον έλεγχο των επικοινωνιών. Για παράδειγμα , ένας εξωτερικός χρήστης για να αποκτήσει πρόσβαση σε μια υπηρεσία του προστατευμένου δικτύου, θα πρέπει πρώτα να συνδεθεί σε μια υπηρεσία του προστατευμένου δικτύου, θα πρέπει πρώτα να συνδεθεί με την proxy εφαρμογή, η οποία θα προβεί στην αναγνώριση και πιστοποίηση του και έπειτα, θα του επιτρέψει την πρόσβαση στην υπηρεσία που ζήτησε. Η αντίστροφη διαδικασία πραγματοποιείται, όταν ένας εσωτερικός χρήστης αιτείται τη χρήση μιας εξωτερικής υπηρεσίας.

Με τον τρόπο αυτό, οι πύλες εφαρμογών ελέγχουν και το περιεχόμενο των πακέτων που δρομολογούνται, όχι μόνο τις επικεφαλίδες, γι' αυτό και έχουν τη δυνατότητα να ανατρέπουν επιθέσεις IP και DNS spoofing. Σε σχέση, όμως, με τις πύλες φιλτραρίσματος πακέτων υστερούν στην ταχύτητα.

Υβριδικές πύλες: Τα firewalls που τείνουν να επικρατήσουν σήμερα, είναι τα υβριδικά. Συνδυάζουν την ταχύτητα ελέγχου, που προσφέρουν οι πύλες φιλτραρίσματος και την αξιοπιστία των πυλών εφαρμογής. Ακόμη και τα καθαρά proxy firewalls διαθέτουν λογισμικό, που λειτουργεί ως πύλη φιλτραρίσματος πακέτων.

Η νεότερη τεχνολογία των υβριδικών firewalls, η Stateful Inspection, συμπληρώνει το IP-φιλτράρισμα από μια υπηρεσία ελέγχου του εσωτερικού των πακέτων, λαμβάνοντας υπόψη προηγούμενες επικοινωνίες. Οι πληροφορίες αυτές, καταχωρούνται σε μια βάση δεδομένων που συνεχώς ανανεώνεται και η σύγκριση των δεδομένων της με τα πακέτα, που επιχειρούν να διέλθουν το firewall, επιτρέπει ή απαγορεύει την επικοινωνία.

5.2.3. Κρυπτογραφία και Ασφάλεια

Η κρυπτογραφία αποτελεί μέρος της κρυπτολογίας, της επιστήμης που ασχολείται με τη μελέτη της ασφαλής επικοινωνίας. Ο έτερος κλάδος της κρυπτολογίας, είναι η κρυπτανάλυση, που ασχολείται με την ανάλυση και το σπάσιμο των αλγόριθμων κρυπτογράφησης. Η κρυπτογραφία, σύμφωνα με τον ορισμό που δίνεται στη Βικιπαίδεια[63], 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 (Confidentially), η αυθεντικοποίηση (authentication), η ακεραιότητα (integrity) και η μη αποποίηση παραλαβής-αποστολής (non repudiation).

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 στη αρχική του μορφή και η πληροφορία μπορεί να αναγνωστεί. Η κρυπτογραφία, ως επιστήμη, είναι γνωστή από την αρχαιότητα. Τα πρώτα κρυπτογραφικά συστήματα βασιζόταν στην χρήση κωδικών συμβόλων, αντί, για τα σύμβολα της αλφαβήτου.

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

a) Το αρχικό μήνυμα (plaintext).
b) Το κρυπτογραφικό σύστημα, το οποίο αποτελείται από ένα αλγόριθμο κρυπτογράφησης και ένα αλγόριθμο αποκρυπτογράφησης.
c) Το κρυπτογραφημένο κείμενο (ciphertext), το οποίο αποτελεί το αποτέλεσμα της εφαρμογής του αλγόριθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη.
d) Ένα κλειδί, το οποίο είναι μια συμβολοσειρά, η οποία χρησιμοποιείται από τους αλγόριθμους στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.

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

---

[63] www.wikipedia.gr

» 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.

5.2.3.1. Συμμετρική κρυπτογραφία

Στην 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.

5.2.3.2. 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 (public key) και είναι γνωστό σε όλους, ενώ το κλειδί με το οποίο γίνεται η αποκρυπτογράφηση, ονομάζεται ιδιωτικό (private key) και το κατέχει μόνο 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 κλειδιών. Όταν ένας χρήστης θέλει να λάβει ένα κρυπτογραφημένο μήνυμα, δίνει στο 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 ασφάλειας.

Χρησιμοποιώντας την συμμετρική κρυπτογραφία λίγο διαφορετικά, μπορούμε να επιτύχουμε την 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 ο οποιοσδήποτε, αλλά η αρχική κρυπτογράφηση με το ιδιωτικό κλειδί, που συνηθίζει να λέγεται ψηφιακή υπογραφή, προσδιορίζει τον αποστολέα αυτού.

5.2.3.3. Υβριδική κρυπτογράφηση

Όπως είδαμε παραπάνω, στην συμμετρική κρυπτογράφηση, το πρόβλημα είναι η εύρεση ασφαλούς καναλιού επικοινωνίας για την ανταλλαγή των μυστικών κλειδιών, ενώ στην ασύμμετρη κρυπτογράφηση, απαιτούνται μεγαλύτερα κλειδιά που καθιστούν την

διαδικασία κρυπτογράφησης – αποκρυπτογράφησης χρονοβόρα. Για την υπερκέραση των προβλημάτων αυτών, έχει επικρατήσει σε ένα υβριδικό σύστημα το οποίο φέρει στοιχεία και από τις δύο μεθόδους. Ειδικότερα, χρησιμοποιείται αρχικά η ασύμμετρη κρυπτογράφηση για να γίνει ανταλλαγή του μυστικού κλειδιού. Όταν ολοκληρωθεί η ανταλλαγή του μυστικού κλειδιού, το οποίο οι χρήστες παραλαμβάνουν μέσω ασφαλούς καναλιού επικοινωνίας, η επικοινωνία πραγματοποιείται με συμμετρική κρυπτογράφηση των δεδομένων.

5.2.3.4. Διαχείριση δημόσιων κλειδιών - πιστοποιητικά

Ο αλγόριθμος του Καίσαρα

Ένας από τους πρώτους αλγόριθμους κρυπτογράφησης, είναι ο «Αλγόριθμος του Καίσαρα» (Ceasar cipher), ο οποίος χρησιμοποιούσε την μέθοδο της αντικατάστασης. Για να γίνει η κρυπτογράφηση και αντιστοίχως η αποκρυπτογράφηση του μηνύματος, κάθε γράμμα αντικαθιστούνταν από το επόμενο κατά τρεις θέσεις γράμμα, σύμφωνα με τον ακόλουθο πίνακα.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y	Z	A	B	C

Με βάση τον παραπάνω πίνακα η λέξη SECURE κρυπτογραφείται σε VHFXUH.

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 υποτιθέμενα 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 διακρίβωσης 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.

5.2.3.5. Επιθέσεις σε συστήματα κρυπτογράφησης

Η χρήση της κρυπτογράφησης οδήγησε στην ανάπτυξη μιας σχετικά παράλληλης, απλά αντίθετης, θα λέγαμε, επιστήμης της κρυπτανάλυσης, που ασχολείται με την αποκρυπτογράφηση του κρυπτογραφημένου κειμένου. Οι μέθοδοι και οι τεχνικές της κρυπτανάλυσης αποτελούν τα βασικά εργαλεία των επιτιθέμενων, έναντι των συστημάτων κρυπτογράφησης. Πολύ σημαντικό ρόλο διαδραματίζει το υλικό, που έχει στα χέρια του ο κρυπταναλυτής. Αν για παράδειγμα κατέχει μόνο το κρυπτογραφημένο κείμενο, είναι πολύ δύσκολο έως αδύνατο να βρει το μη κρυπτογραφημένο. Αν όμως έχει

στα χέρια του το κρυπτογραφημένο αλλά και το αντίστοιχο αρχικό, είναι πιο εύκολο να βρει το κλειδί για τις κρυπτογραφήσεις και αποκρυπτογραφήσεις.

Η κυρίαρχη ιδέα ενός συστήματος κρυπτογράφησης είναι ο φόρτος εργασίας (wordload), που απαιτείται από έναν κρυπταναλυτή για βρει το κλειδί. Όσο περισσότερος κόπος, αλλά και χρόνος απαιτείται για τη εύρεση ενός κλειδιού σε ένα κρυπτογραφικό σύστημα, τόσο ασφαλέστερο αυτό θεωρείται.

Οι αλγόριθμοι κρυπτογράφησης μπορούν πολύ δύσκολα να σπάσουν. Όμως, αν υπάρχει αρκετός χώρος και υπομονή, ένα πρόγραμμα, που θα δοκιμάζει όλα τα πιθανά κλειδιά, κάποια στιγμή θα βρει το σωστό[64]. Το κρίσιμο ζήτημα είναι ο χρόνος που θα απαιτηθεί για να ολοκληρωθεί αυτή η διαδικασία, έστω και αν χρησιμοποιούν υπερυπολιστές για την διεκπεραίωση της. Ο χρόνος αυτός, όπως επίσης και το μήκος του κλειδιού, αποτελεί τα στοιχεία που αποτρέπουν τους επιτιθέμενου, συνεπώς καθορίζουν το βαθμό αξιοπιστίας του συστήματος κρυπτογράφησης.

Η κρυπτογράφηση χρησιμοποιείται ευρέως για την ασφάλεια των ηλεκτρονικών συναλλαγών. Τα πρωτόκολλα SSL, PNG, και SET, αποτελούν τις πιο διαδεδομένες εφαρμογές της κρυπτογραφίας στον τομέα αυτό.

5.2.4. Φυσική ασφάλεια

Ένας από τους πιο σημαντικούς τομείς, που αφορά την ασφάλεια του πληροφοριακού συστήματος ενός οργανισμού, είναι η φυσική ασφάλεια. Οι περισσότεροι οργανισμοί, κατά την κατάρτιση της πολιτικής ασφάλειας τους, έχουν την τάση να παραμελούν τον πολύ σημαντικό αυτό τομέα, θεωρώντας τον δευτερεύοντα, κυρίως διότι το κόστος είναι αρκετό υψηλό. Οι διαχειριστές των δικτύων θέτουν, ως πρώτη προτεραιότητα, τον εξοπλισμό του οργανισμού με σύγχρονο και εξελιγμένο υλικό και λογισμικό, αγνοώντας ότι οι διακομιστές, οι δρομολογητές, τα καλώδια των δικτύων και τόσες ακόμη συσκευές κινδυνεύουν από απ' ευθείας προσβολή.

Με τον όρο φυσική ασφάλεια, αναφερόμαστε σε όλα εκείνα τα μέτρα, που είναι απαραίτητο να ληφθούν, προκειμένου, να προστατευθεί η φυσική υπόσταση των συσκευών που απαρτίζουν ένα υπολογιστή ή ένα δίκτυο υπολογιστών. Όσο και αν προστατεύουμε ένα διακομιστή με εργαλεία λογισμικού θα έχουμε αποτύχει παντελώς, αν κάποιος εισβολέας καταφέρει να φτάσει στην φυσική τοποθεσία όπου αυτός φυλάσσεται και να αφαιρέσει το σκληρό δίσκο, που περιέχει όλα τα ευαίσθητα και σημαντικά δεδομένα του οργανισμού.

Ο τομέας της φυσικής ασφάλειας, που παραμελείται περισσότερο από όλους, είναι η προστασία από φυσικές καταστροφές. Πλημμύρες, σεισμοί και φωτιές μπορεί να προκαλέσουν ανεπανόρθωτες ζημιές. Η σωστή συντήρηση των κτηρίων, ο συχνός έλεγχος των υδραυλικών και ηλεκτρολογικών εγκαταστάσεων και η ύπαρξη συστήματος

---

[64] Η μέθοδος αυτή ονομάζεται brute force. Βλ. http://www.cl.cam.ac.uk/~rnc1/brute.html (Ημερομηνία πρόσβασης: 30/08/09)

πυρόσβεσης, τουλάχιστον στους χώρους όπου έχουν τοποθετηθεί ηλεκτρονικοί υπολογιστές, μπορούν να αποσοβήσουν τους κινδύνους αυτούς.

Εκτός όμως από τους ηλεκτρονικούς υπολογιστές, ιδιαίτερη σημασία, πρέπει να δίνεται και στον βοηθητικό εξοπλισμό. Για παράδειγμα, τα καλώδια κινδυνεύουν από απευθείας παρέμβαση, η οποία μπορεί να στοχεύει είτε στην καταστροφή του δικτύου είτε στην παρεμβολή συσκευών για την υποκλοπή δεδομένων. Επίσης, οι αφαιρούμενες αποθηκευτικές μονάδες, καθώς και τα δεδομένα που τυπώνονται, δύναται να περιέχουν σημαντικές πληροφορίες για την ασφάλεια του συστήματος, γι' αυτό πρέπει να προστατεύονται με την ίδια επιμέλεια.

Τέλος, οι μέθοδοι και τα συστήματα αυθεντικοποίησης μπορούν, επίσης, να χρησιμοποιηθούν για την φυσική ασφάλεια του εξοπλισμού. Ένα σύστημα αναγνώρισης φωνής ή ίριδας, μπορεί να εμποδίσει την μη εξουσιοδοτημένη πρόσβαση ατόμων στους χώρους όπου φυλάσσονται οι διακομιστές ενός δικτύου ή άλλα ευπαθή μέρη του εξοπλισμού.

5.3. Ανίχνευση επιθέσεων

Τα μέτρα πρόληψης, που προαναφέρθηκαν, έχουν ως σκοπό την αποτροπή μιας επίθεσης έναντι της ασφάλειας ενός συστήματος και την παρεμπόδιση εκδήλωση της. Τι γίνεται όμως όταν ο επιτιθέμενος καταφέρει να παραβιάσει τα μέτρα πρόληψης; Στην περίπτωση αυτή, το σύστημα θα πρέπει να έχει τη δυνατότητα να εντοπίσει την επίθεση, προκειμένου, να επιχειρήσει είτε να αποτρέψει είτε να προβεί στην αποκατάσταση του συστήματος.

5.3.1. Συστήματα Ανίχνευσης Επιθέσεων (ΣΑΕ)

Για την ανίχνευση μιας επίθεσης, χρησιμοποιούνται τα Συστήματα Ανίχνευσης Επιθέσεων (Intrusion Detection Systems – IDS). Τα συστήματα ανίχνευσης επιθέσεων τοποθετούνται από το διαχειριστή ενός δικτύου, για να εντοπίσουν μια προσπάθεια μη εξουσιοδοτημένης πρόσβασης σε αυτό.

Υπάρχουν τρία βασικά μοντέλα συστημάτων ανίχνευσης επιθέσεων:

- Ανίχνευσης ανωμαλιών (anomaly-based detection)
- Ανίχνευσης υπογραφών (signature-based detection)
- Υβριδικό μοντέλο (hybrid detection)

Ανίχνευση ανωμαλιών: Τα συστήματα ανίχνευσης ανωμαλιών αυτοεκπαιδεύονται, υπό την έννοια ότι, καταγράφουν ροές και διαδικασίες δεδομένων προσπαθώντας, να κάνουν ένα είδος τυποποίησης. Οι τυποποιημένες αυτές διαδικασίες, χρησιμοποιούνται για να εντοπιστούν ανωμαλίες, που πιθανώς θα αποτελούν εισβολή, σύμφωνα με τα όσα έχουν ήδη καταγραφεί. Κατά την ανίχνευση ανωμαλιών, υπάρχει η δυνατότητα να καταγράφονται δραστηριότητες, που ξεφεύγουν πέρα των συνηθισμένων, που έχουν, νομίμως, δοθεί σε μια ομάδα χρηστών.

Για την δημιουργία του γνωστικού τους περιεχομένου, τα συστήματα της κατηγορίας αυτής, χρησιμοποιούν ευρετικές μεθόδους, αξιοποιώντας με στατιστικά κριτήρια τα δεδομένα του συστήματος. Κατά συνέπεια, υπάρχει η πιθανότητα τα συστήματα αυτά, εφόσον δεν έχουν ρυθμιστεί κατάλληλα, να δίνουν λάθος συναγερμούς (false alarms) ή στην αντίθετη περίπτωση να μην εντοπίζουν μια επίθεση. Το κρίσιμο σημείο ισορροπίας (threshold) πάνω ή κάτω από το οποίο, το σύστημα αποφαίνεται θετικά ή αρνητικά είναι υποκειμενικό, στηρίζεται στην πολιτική ασφάλειας και στην έμπνευση του διαχειριστή, για το λόγο αυτό η σχετική τεχνολογία θεωρείται ότι θα ωριμάσει έπειτα από πολλά χρόνια.

Ανίχνευση υπογραφών: Τα συστήματα αυτά στηρίζονται στο γεγονός, ότι για κάθε επίθεση υφίσταται μια μοναδική μέθοδος ή υπογραφή η οποία και μπορεί να εντοπιστεί. Έστω και αν υπάρχει μια μικρή διαφορά, μεταξύ δυο υπογραφών και πάλι υπάρχει δυνατότητα εντοπισμού. Για την ταυτοποίηση των υπογραφών, απαιτείται μια βάση δεδομένων, στην οποία θα αποθηκεύονται οι υπογραφές των επιθέσεων, προκειμένου να υπάρχει η δυνατότητα σύγκρισης.

Η λειτουργία των συστημάτων ανίχνευσης επιθέσεων της κατηγορίας αυτής, μπορεί να παρομοιαστεί με τη λειτουργία ενός λογισμικού ανίχνευσης ιών, καθώς απαιτείται να είναι ενημερωμένη η βάση δεδομένων για να εντοπιστούν νέες επιθέσεις. Εφόσον η βάση των υπογραφών δεν είναι ενημερωμένη, δεν μπορεί να εντοπιστεί μια νέα μορφή επίθεσης.

Υβριδικό μοντέλο ανίχνευσης επιθέσεων: Λόγω των μειονεκτημάτων, που παρουσιάζουν τα ανωτέρω συστήματα, αρχίζουν να αναπτύσσονται υβριδικά μοντέλα, τα οποία δανείζονται χαρακτηριστικά από ήδη υπάρχοντα. Η τεχνολογία των υβριδικών μοντέλων βρίσκεται ακόμα σε πρώτο στάδιο.

Περαιτέρω, τα συστήματα ανίχνευσης επιθέσεων, ανάλογα με το μέσο το οποίο παρακολουθούν, μπορούμε να τα διακρίνουμε σε συστήματα που:

a) συλλέγουν πληροφορίες από το δίκτυο (Network based IDS)
b) συλλέγουν πληροφορίες από υπολογιστές (Host based IDS) και
c) συλλέγουν πληροφορίες από εφαρμογές (Application based IDS).

ΣΑΕ που συλλέγουν πληροφορίες από το δίκτυο: Τα συστήματα αυτά παρακολουθούν την κίνηση στο δίκτυο, με σκοπό να εντοπίσουν επιθέσεις. Είναι υπεύθυνα, για τον εντοπισμό ανωμαλιών, δυσλειτουργιών, καθώς και δεδομένων, που πιθανώς να είναι κακόβουλα και επιβλαβή για το δίκτυο. Αν και εκ πρώτης όψεως, τα συστήματα αυτά θυμίζουν τα firewalls υπάρχουν σημαντικές διαφορές μεταξύ τους, με σημαντικότερη ότι τα ΣΑΕ λειτουργούν παθητικά, απλά παρακολουθούν την κίνηση στο δίκτυο και δεν επεμβαίνουν για να την διακόψουν ή αλλοιώσουν. Για το λόγο αυτό, είναι πολύ δύσκολο να εντοπιστούν από τον επιτιθέμενο, σε αντίθεση με τα firewalls.

ΣΑΕ που συλλέγουν πληροφορίες από υπολογιστές: Η δημιουργία των συστημάτων της κατηγορίας αυτής προήλθε από ανάγκη επιτήρησης μεμονωμένων υπολογιστών, που βρίσκονται στο εσωτερικό δίκτυο ενός οργανισμού. Οι απειλές έναντι της ασφάλειας ενός

συστήματος δεν είναι μόνο εξωτερικές, αλλά, είναι και εσωτερικές προερχόμενες από τους ίδιους τους υπαλλήλους και χρήστες των συστημάτων του οργανισμού.

Τα συστήματα αυτά, επικεντρώνονται στην παρακολούθηση ενός και μόνο υπολογιστή, στον οποίο τοποθετείτε κατάλληλο λογισμικό που παρακολουθεί συγκεκριμένα αρχεία καταγραφής (log files). Όταν διαπιστωθεί οποιαδήποτε μεταβολή, θεωρείτε, ότι έχει υπεισέλθει κακόβουλη δραστηριότητα.

ΣΑΕ που συλλέγουν πληροφορίες από εφαρμογές: Αποτελούν μια υποκατηγορία των ΣΑΕ που συλλέγουν πληροφορίες από υπολογιστές. Χρησιμοποιούν τα αρχεία καταγραφής των εφαρμογών για να εντοπίσουν πιθανές επιθέσεις, που επιχειρούνται στο επίπεδο της εφαρμογής. Η χρήση των συστημάτων αυτών, είναι λιγότερο συχνή από της ανωτέρω δύο κατηγορίες. Προτιμούνται όταν θέλουμε να προστατεύσουμε μια πολύ σημαντική εφαρμογή, όπως π.χ. μια βάση δεδομένων με σημαντικές πληροφορίες.

5.3.1.1. Η αντίδραση των ΣΑΕ σε μια επίθεση

Ένα σύστημα ανίχνευσης επιθέσεων δεν περιορίζεται, μόνο, στην παρακολούθηση ενός δικτύου ή υπολογιστή. Όταν αντιληφθεί μια επίθεση, εκτελεί σε μια σειρά εντολές, ανάλογα με τις ρυθμίσεις που έχει επιλέξει ο διαχειριστής. Τις αντιδράσεις των ΣΑΕ μπορούμε να τις διακρίνουμε σε δύο κατηγορίες: ενεργητικές και παθητικές.

Ενεργητικές αντιδράσεις: Όταν το σύστημα εντοπίσει μια επίθεση, προβαίνει σε μια σειρά από ενέργειες για την παρεμπόδιση της. Κάθε επίθεση και ο πιθανός κίνδυνος αξιολογείται. Εάν το ΣΑΕ δεν είναι σίγουρο για το πόσο επικίνδυνη είναι η επίθεση, μπορεί να μην αντιδράσει, αλλά, να περιμένει για να συγκεντρώσει περισσότερες πληροφορίες και να επαναξιολογήσει την κατάσταση. Όταν αποφανθεί ότι η επίθεση είναι σοβαρή, έχει τη δυνατότητα να αντιδράσει π.χ. ενεργοποιώντας το firewall, με το οποίο και «συνεργάζεται» για να αποτρέψει την είσοδο του επιτιθέμενου στο δίκτυο.

Παθητικές αντιδράσεις: Το ΣΑΕ δεν προβαίνει σε καμιά ενέργεια. Ειδοποιεί το διαχειριστή ή τον υπεύθυνο ασφαλείας του συστήματος ότι υπάρχει πρόβλημα. Και στην περίπτωση αυτή, γίνεται η αξιολόγηση της σοβαρότητας της επίθεσης και τα μέσα και τρόποι ειδοποίησης του διαχειριστή εξαρτώνται άμεσα και από τον παράγοντα αυτό.

5.3.1.2. Ειδικές κατηγορίες ΣΑΕ

Εκτός των βασικών κατηγοριών ΣΑΕ, υπάρχουν και επιμέρους συστήματα, τα οποία λόγω της απλότητας λειτουργίας τους, θα μπορούσαμε να τα ονομάσουμε εργαλεία ανίχνευσης εισβολών. Μερικά από τα εργαλεία αυτά είναι τα ακόλουθα:

a) **Συστήματα ελέγχου ακεραιότητας (System Integrity Verifiers):** Τα συστήματα αυτά παρακολουθούν κρίσιμα αρχεία, όπως τα αρχεία συστήματος (system files), προκειμένου να εντοπίσουν τυχόν μεταβολές. Έχουν, επίσης τη δυνατότητα να παρακολουθούν τους λογαριασμούς των χρηστών και να εντοπίζουν, εάν, κάποιος απλός χρήστης έχει αποκτήσει δικαιώματα διαχειριστή.
b) **Συστήματα παρακολούθησης αρχείων καταγραφής (Log File Monitors):** Τα συστήματα αυτά, δημιουργούν έναν φάκελο από αρχεία καταγραφής, τα οποία

προέρχονται από τις υπηρεσίες του δικτύου. Στη συνέχεια, παρακολουθούν τα αρχεία, καταγράφουν τις συνηθισμένες λειτουργίες του συστήματος και βασιζόμενα σε αυτές, προσπαθούν να εντοπίσουν πιθανές επιθέσεις.

c) **Honeypots:** Τα Honeypots είναι εικονικά συστήματα, τα οποία προσπαθούν να ξεγελάσουν τον επιτιθέμενο, δίνοντας του την εντύπωση ότι είναι πολύ εύκολο να εισβάλει στο σύστημα. Όταν πραγματοποιηθεί η εισβολή το σύστημα θα καταγράψει όλες τις μεθόδους και τεχνικές που χρησιμοποίησε ο επιτιθέμενος.

5.3.2. Έλεγχος (audit) συστημάτων

Ο έλεγχος των αρχείων καταγραφής (log files) του συστήματος, μπορεί να αποβεί πολύ σημαντικός και να βοηθήσει στον εντοπισμό μιας επίθεσης.

Τα εργαλεία ελέγχου υπάρχουν σε κάθε λειτουργικό σύστημα. Στις επαγγελματικές εκδόσεις των πρόσφατων λειτουργικών συστημάτων της Microsoft υπάρχουν τα ακόλουθα τρία βασικά αρχεία καταγραφής:

- Application log, τα οποία περιέχουν μηνύματα, πληροφορίες κατάστασης και άλλα γεγονότα που αναφέρονται από ζωτικές υπηρεσίες των WINDOWS.
- System log, τα οποία καταγράφονται σφάλματα αρχείων, προειδοποιήσεις και γεγονότα, τα οποία δημιουργούνται από το ίδιο το λειτουργικό σύστημα και σχετίζονται με υπηρεσίες του συστήματος.
- Security log στο οποίο καταγράφονται αρχεία που σχετίζονται με την πολιτική ελέγχου που έχει καθοριστεί από το διαχειριστή του λειτουργικού συστήματος.

Το τι θα παρακολουθείται και τι όχι είναι υποκειμενικό και υπόκειται σε μεταβολές. Ένας καλός διαχειριστής πρέπει να βρει τη χρυσή τομή και να παρακολουθεί μόνο τα δεδομένα και τις διαδικασίες που απαιτούνται για την επίτευξη του σκοπού του. Εξάλλου, το να παρακολουθούμε τα πάντα είναι ισοδύναμο με το να μην παρακολουθούμε τίποτα, καθώς εάν έχουμε να ελέγξουμε ένα τεράστιο πλήθος πληροφοριών από αρχεία και διαδικασίες, πιθανώς δεν θα μπορέσουμε να εντοπίσουμε το πρόβλημα.

5.4. Αντιμετώπιση καταστροφών

Στην περίπτωση που αποτύχουμε είτε να αποτρέψουμε είτε να αντιμετωπίσουμε μια επίθεση, ο επιτιθέμενος, θα προκαλέσει κάποιου είδους ζημιά, όπως απώλεια πληροφοριών και δεδομένων, καταστροφή του συστήματος κ.λπ. Η απώλεια δεδομένων ενός οργανισμού μπορεί να έχει απρόβλεπτες συνέπειες και να οδηγήσει σε ολοκληρωτική οικονομική καταστροφή.

Για τους λόγους αυτούς, είναι απαραίτητο ο κάθε οργανισμός, αλλά και κάθε μεμονωμένος χρήστης που αποθηκεύει σημαντικά δεδομένα σε ένα υπολογιστικό σύστημα, να έχει την προνοητικότητα να εξασφαλίσει ότι σε περίπτωση που δεχθεί οποιαδήποτε επίθεση ή ακόμη και υποστεί τις συνέπειες μιας φυσικής καταστροφής, θα έχουν τηρηθεί σε ασφαλές μέρος εφεδρικά αρχεία, τα οποία θα αποτελούν μέρος ή και το σύνολο των αποθηκευμένων δεδομένων που χάθηκαν.

Για την λήψη των εφεδρικών αντιγράφων (back-up files) χρησιμοποιούνται μια σειρά από τεχνικές.

5.4.1. Συστήματα ανάνηψης από καταστροφές

Τα Συστήματα από Καταστροφές (Disaster Recovery Systems), αποτελούν αναπόσπαστο κομμάτι της πολιτικής ασφάλειας κάθε μεγάλου οργανισμού. Ένα σύστημα ανάνηψης από καταστροφές αποτελείται από αρκετά υποσυστήματα, τα οποία στοχεύουν στην εξασφάλιση της ακεραιότητας των δεδομένων του οργανισμού από διάφορους κινδύνους, που μπορεί να προκύψουν, όπως φυσικά φαινόμενα, κακόβουλες επιθέσεις μέσω διαδικτύου, σφάλματα υλικού και λογισμικού, λάθη των χρηστών κ.λπ.

Οι λειτουργίες ενός συστήματος ανάνηψης από καταστροφές είναι υποκειμενικές και εξαρτώνται από τις ανάγκες του οργανισμού. Τα κρίσιμα σημεία σχεδιασμού του συστήματος είναι:

- το είδος των δεδομένων που θα αποθηκευτούν,
- κάθε πότε θα γίνεται η αποθήκευση και
- που θα αποθηκευτούν τα δεδομένα.

Τα δεδομένα, που θα αποθηκευτούν, εξαρτώνται από τις ανάγκες που θέλουμε να καλύψουμε αλλά και το κεφάλαιο, που θα διαθέσουμε για την εργασία αυτή. Σε μικρές έως μεσαίες επιχειρήσεις αποθηκεύονται μόνο τα ζωτικής σημασίας αρχεία, σε μεγαλύτερες αποθηκεύεται το σύνολο των δεδομένων, ενώ μεγάλοι οργανισμοί αποθηκεύουν και περαιτέρω δεδομένα, όπως πληροφορίες συστήματος και εφαρμογών, ρυθμίσεις δικτύου κ.λπ.

Το χρονικό διάστημα, που μεσολαβεί για την αποθήκευση των δεδομένων, εξαρτάται από μια σειρά από παράγοντες, όπως πόσο συχνά τα δεδομένα αλλάζουν, η ποσότητα των δεδομένων για τα οποία απαιτείται η λήψη εφεδρικών αντιγραφών (backup files), το χρονικό διάστημα στο οποίο μπορεί να λειτουργήσει ο οργανισμός χωρίς δεδομένα και το μέσο στο οποίο θα γίνει η αποθήκευση των εφεδρικών αντιγραφών. Κατά την εξέταση των προηγουμένων παραγόντων και την λήψη αποφάσεων, το κρίσιμο σημείο είναι αυτό μεταξύ των αναγκών, που θα πρέπει να καλυφθούν και τους κόστους που απαιτείται για την κάλυψη τους.

Το χρονικό διάστημα, που μεσολαβεί για την αντιμετώπιση των δεδομένων, εξαρτάται από μια σειρά από παράγοντες, όπως πόσο συχνά τα δεδομένα αλλάζουν, η ποσότητα των δεδομένων για τα οποία απαιτείται η λήψη εφεδρικών αντιγραφών (backup files), το χρονικό διάστημα στο οποίο μπορεί να λειτουργήσει ο οργανισμός χωρίς δεδομένα και το μέσο στο οποίο θα γίνει η αποθήκευση των εφεδρικών αντιγραφών. Κατά την εξέταση των προηγούμενων παραγόντων και την λήψη αποφάσεων, το κρίσιμο σημείο είναι αυτό μεταξύ των αναγκών, που θα πρέπει να καλυφθούν και τους κόστους που απαιτείται για την κάλυψη τους.

Η αποθήκευση των δεδομένων επηρεάζεται από το είδος του φυσικού μέσου αποθήκευσης και την δυνατότητα για περαιτέρω διατήρηση του σε άρτια κατάσταση. Τα μέσα, που χρησιμοποιούνται για την αποθήκευση εφεδρικών δεδομένων, ποικίλουν. Η

αποθήκευση των δεδομένων μπορεί να γίνει σε μαγνητικά μέσα, όπως η μαγνητικές ταινίες και σε άλλους τοπικούς ή απομακρυσμένους δίσκους[65]. Αν υπάρχει οικονομική δυνατότητα, μπορούν να εγκατασταθούν εφεδρικοί υπολογιστές, στους οποίους θα γίνετε πλήρη αποθήκευση (disk mirroring) των δεδομένων που χρησιμοποιούνται στους βασικούς υπολογιστές.

5.4.2. Λήψη εφεδρικών αντιγραφών

Η λήψη εφεδρικών αντιγραφών (back-up files) αποτελεί, όπως είδαμε παραπάνω, ένα μέρος του συστήματος ανάνηψης καταστροφών. Μια επιχείρηση ή ένας οργανισμός που αδυνατεί να διαθέσει τα κεφάλαια για την προμήθεια ενός πλήρους συστήματος ανάνηψης καταστροφών, είναι απαραίτητο να εξασφαλίσει τα δεδομένα, με την λήψη εφεδρικών αντιγραφών. Η διαδικασία αυτή, μπορεί να ολοκληρωθεί με τη χρήση διαφόρων εφαρμογών, που κυκλοφορούν στο εμπόριο για το σκοπό αυτό. Κάθε εφαρμογή φέρει τα δικά της χαρακτηριστικά και μπορεί να χρησιμοποιηθεί για την κάλυψη διαφορετικών αναγκών. Για παράδειγμα η εφαρμογή snapshot επιτρέπει την πλήρη αντιγραφή του σκληρού δίσκου χωρίς να απαιτείται ο τερματισμός του λειτουργικού συστήματος. Παράλληλα, είναι δυνατή η συνέχιση των εργασιών του χρήστη καθ' όλη την διάρκεια της αντιγραφής. Σε περίπτωση καταστροφής του πρωτότυπου δίσκου, γίνεται πλήρης αποκατάσταση και ο νέος δίσκος περιέχει ακριβώς, τα δεδομένα που ήταν αποθηκευμένα στον παλαιό.

Τη διαδικασία λήψης αντιγράφων, μπορούμε να τη διακρίνουμε με τρείς βασικές κατηγορίες: Την πλήρη λήψη αντιγραφών (full backup), κατά την οποία λαμβάνονται εφεδρικά αντίγραφα από όλα τα αρχεία του συστήματος, την λήψη τροποποιημένων αντιγράφων (incremental backup), κατά την οποία λαμβάνονται αντίγραφα μόνο από τα αρχεία, που έχουν τροποποιηθεί από την προηγούμενη χρονικά λήψη αντιγράφων και λήψη διαφοροποιημένων αντιγράφων (differential backup), κατά την οποία γίνεται λήψη εφεδρικών αντιγραφών των αρχείων, που έχουν διαφοροποιηθεί από την τελευταία πλήρη λήψη αντιγράφων ασφαλείας.

5.5. Άλλα θέματα που σχετίζονται με την ασφάλεια

5.5.1. Ασφάλεια Ηλεκτρονικού Ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο είναι, αδιαμφισβήτητα, το πιο διαδεδομένο μέσο επικοινωνίας στο Διαδίκτυο. Οι επιθέσεις, με τη χρήση του ηλεκτρονικού ταχυδρομείου, αποτελούν καθημερινή πραγματικότητα. Τα ζητήματα ασφαλείας, που σχετίζονται με το ηλεκτρονικό ταχυδρομείο ανάγονται στις έννοιες της εμπιστευτικότητας, της ακεραιότητας του μηνύματος και της αυθεντικότητας του αποστολέα. Παράλληλα, το ηλεκτρονικό ταχυδρομείο γίνεται στόχος και άλλων επιθέσεων, όπως άρνησης εξυπηρέτησης ενώ χρησιμοποιείται και για τη μετάδοση κακόβουλου λογισμικού. Τέλος

[65] Πολλές εταιρείες στο Διαδίκτυο, προσφέρουν την δυνατότητα on-line αποθήκευσης δεδομένων, διαθέτοντας τεράστιους αποθηκευτικούς χώρους, που τους διαθέτουν στους χρήστες. Μάλιστα, με την ανάπτυξη των ευρυζωνικών συνδέσεων η δυνατότητα αυτή γίνεται όλο και πιο δημοφιλής.

η μαζική αποστολή ανεπιθύμητων μηνυμάτων, το λεγόμενο spamming αποτελεί επίσης σημαντικό πρόβλημα,

Για την αντιμετώπιση του προβλήματος των ιών, απαιτείται η χρήση μιας εφαρμογής antivirus, η οποία ελέγχει όλα τα εισερχόμενα και εξερχόμενα μηνύματα. Παράλληλα, οι χρήστες δεν πρέπει να ανοίγουν επικίνδυνα συννημένα αρχεία(κυρίως αυτά με καταλήξεις .com, .exe, .dll, .bat) εφόσον δεν έχουν ελεγχθεί από το antivirus και δεν έχει εξακριβωθεί η ταυτότητα του αποστολέα.

Όσο αφορά την ενοχλητική αλληλογραφία, μερικοί βασικοί κανόνες ασφαλείας συνιστούν να μη δίνεται ποτέ σε άγνωστους δικτυακούς τόπους, η ηλεκτρονική διεύθυνση και να μην απαντώνται μηνύματα τέτοιου τύπου. Στο εμπόριο κυκλοφορούν εργαλεία λογισμικού για την αντιμετώπιση του spamming[66], τα οποία μπορούν να χρησιμοποιηθούν, εφόσον υπάρχει σημαντικό πρόβλημα. Τα εργαλεία αυτά ρυθμίζονται ανάλογα με τις επιθυμίες του χρήστη.

Τέλος, θα πρέπει να σημειωθεί, ότι η επικοινωνία μέσω e-mail παρέχει ελάχιστη ασφάλεια, γι' αυτό και δεν πρέπει με το μέσο αυτό να διακινούνται ευαίσθητα δεδομένα, όπως αριθμοί πιστωτικών καρτών και λογαριασμών. Ειδικότερα, στους λογαριασμούς web-mail το πρόβλημα ασφαλείας είναι ακόμη εντονότερο, γι' αυτό και προτείνεται να γίνεται σε τακτά χρονικά διαστήματα αλλαγή του κωδικού πρόσβασης. Ένας αποτελεσματικός τρόπος ασφαλούς επικοινωνίας, μέσω ηλεκτρονικής αλληλογραφίας, είναι η χρήση κρυπτογράφησης με το πρωτόκολλο SSL.

5.5.2. Ασφάλεια ηλεκτρονικών συναλλαγών

Το Διαδίκτυο και ιδιαίτερα ο παγκόσμιος ιστός, έχει μεταφέρει μεγάλο μέρος των καθημερινών αγορών μας στα ηλεκτρονικά καταστήματα. Ως αποτέλεσμα, αναπτύχθηκαν μια σειρά από εργαλεία, για την πληρωμή αγαθών και υπηρεσιών μέσω του Διαδικτύου. Οι ηλεκτρονικές πληρωμές στο Διαδίκτυο, σήμερα, πραγματοποιούνται με τη χρήση πιστωτικών ή χρεωστικών καρτών, ηλεκτρονικού χρήματος και επιταγών, αυτόματης μεταφοράς κεφαλαίων κ.ά.

Η νέα αυτή μορφή συναλλαγών, πολύ γρήγορα, έγινε στόχος κακόβουλων επιθέσεων, δημιουργώντας την ανάγκη για όσο το δυνατό ασφαλέστερα συστήματα συναλλαγών (π.χ. αριθμούς πιστωτικών καρτών), που διακινούνται στο Διαδίκτυο. Για το λόγο αυτό, δημιουργήθηκαν μια σειρά από πρωτόκολλα επικοινωνίας, τα οποία στοχεύουν στην προστασία των δεδομένων αυτών. Τα πιο σημαντικά από αυτά, από άποψη ευρύτητας χρήσεως είναι το SSL και το SET, τα οποία και εξετάζουμε στην συνέχεια.

5.5.2.1. Το πρωτόκολλο SSL

Το πρωτόκολλο SSL, σχεδιάστηκε με σκοπό την ασφαλή μεταφορά δεδομένων στο Διαδίκτυο και γενικότερα μεταξύ δύο συσκευών, που είναι συνδεδεμένες στο Διαδίκτυο.

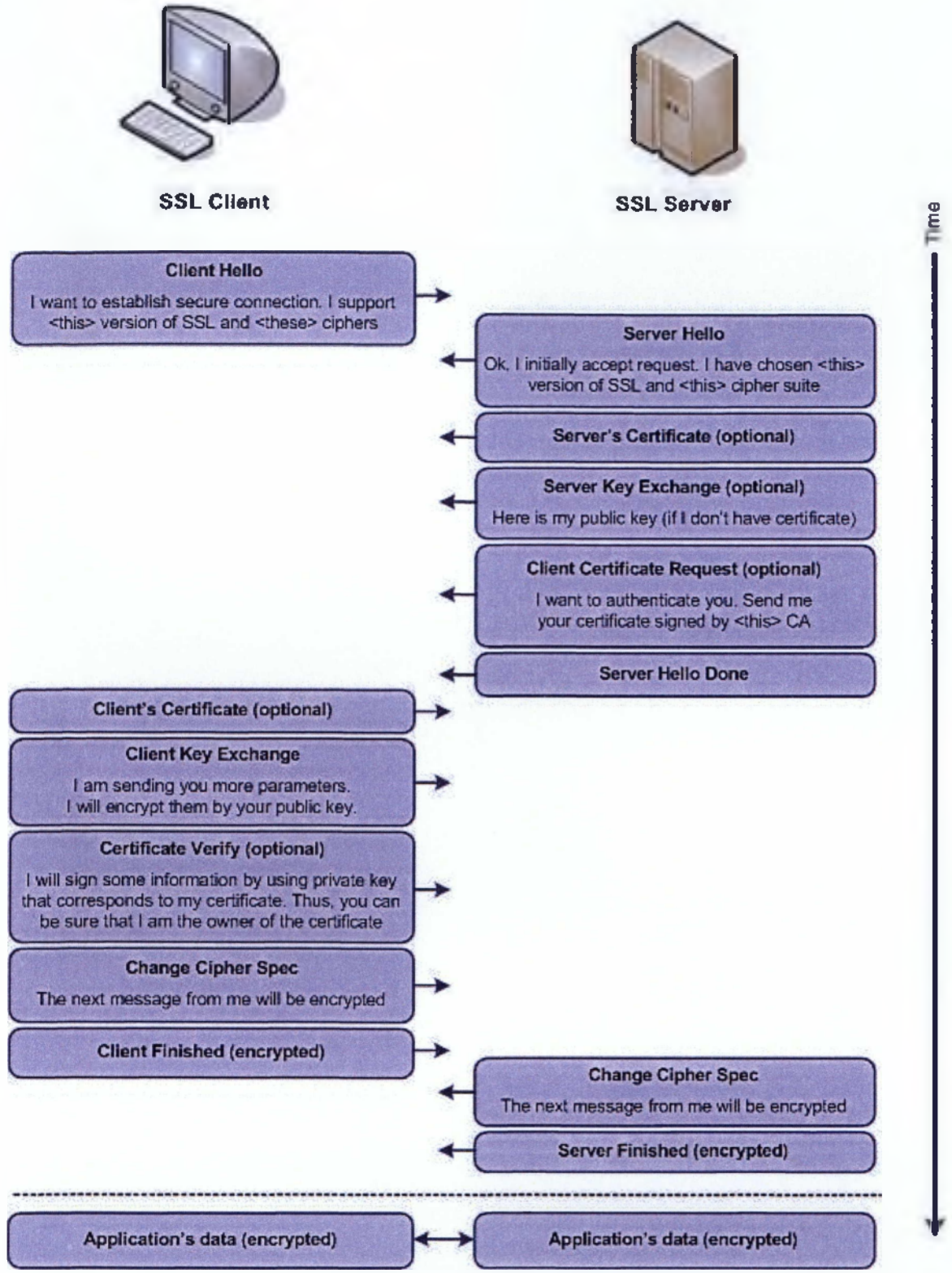
---

[66] Μια πλήρης λίστα με εργαλεία λογισμικού για την αντιμετώπιση του spamming, είναι διαθέσιμη στη διεύθυνση http://spam.abuse.net/userhelp/#filter (Ημερομηνία πρόσβασης: 30/08/09)

Εκμεταλλεύεται στο έπακρο, τα πλεονεκτήματα τόσο της συμμετρικής όσο και της ασύμμετρης κρυπτογράφησης. Από άποψη ασφάλειας, το SSL εξασφαλίζει τρεις βασικούς παραμέτρους των μεταδιδόμενων μηνυμάτων: την κρυπτογράφηση των δεδομένων, την αυθεντικοποίηση των μερών επικοινωνίας και την ακεραιότητα των μεταδιδόμενων μηνυμάτων.

Το πρωτόκολλο SSL λειτουργεί ως εξής: Τη στιγμή, που ο φυλλομετρητής συνδέεται με μια «υψηλής ασφαλείας» σελίδα του Διαδικτύου, ο απομακρυσμένος διακομιστής στέλνει ένα μήνυμα καλωσορίσματος. Για να ξεκινήσει η σύνδεση ασφάλειας, ο φυλλομετρητής πρέπει να απαντήσει με ένα μήνυμα «client hello» και ο διακομιστής με ένα «server hello». Κατά την αρχική αυτή φάση, ο φυλλομετρητής και ο διακομιστής διαπραγματεύονται τις παραμέτρους ασφαλείας χρησιμοποιώντας το πρωτόκολλο χειραψίας (handshake), το πρώτο τμήμα του SSL. Το μήνυμα «client hello», περιέχει έναν αριθμό, που ονομάζεται ταυτότητα συνδέσεως (session ID) και χαρακτηρίζει το τύπο της client-server σύνδεσης. Το μήνυμα περιέχει ακόμα πληροφορίες σχετικά με τους αλγόριθμους κρυπτογράφησης, την έκδοση του SSL και τις μεθόδους συμπίεσης δεδομένων, που υποστηρίζει ο φυλλομετρητής. Τέλος περιέχει και ένα τυχαίο αριθμό, που δημιουργεί ο φυλλομετρητής. Το μήνυμα «server hello» απαντά με τη μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης, που επέλεξε με βάση τις προτάσεις του φυλλομετρητή (πελάτης), την έκδοση του SSL, ένα νέο τυχαίο αριθμό και μια αποδεκτή ταυτότητα σύνδεσης.

Στη συνέχεια, πελάτης και διακομιστής ανταλλάσσουν ψηφιακά πιστοποιητικά που επιβεβαιώνουν ότι τα δυο μέρη είναι στην πραγματικότητα αυτά που ισχυρίζονται. Το πιστοποιητικό του διακομιστή μπορεί να περιέχει και ένα δημόσιο κλειδί για τον αλγόριθμο κρυπτογράφησης ιδιωτικού-δημόσιου κλειδιού, που έχει επιλεγεί κατά το handshake. Το κλειδί αυτό ωστόσο, θα χρησιμοποιηθεί για μικρό χρονικό διάστημα. Η συναλλαγή (π.χ. αποστολή αριθμού πιστωτικής κάρτας από το χρήστη θα κωδικοποιηθεί με χρήση ενός συμβατικού αλγόριθμου κρυπτογράφησης (με ιδιωτικό μόνο κλειδί).



Εικόνα 5.4: Συνοπτική αναπαράσταση του SSL

Το βασικότερο μειονέκτημα του πρωτοκόλλου SSL είναι, ότι δημιουργείται μεγάλος όγκος πρόσθετων δεδομένων, τα οποία και περιορίζουν την ταχύτητα μετάδοσης τους μέσω του Διαδικτύου. Για το λόγο αυτό, το πρωτόκολλο χρησιμοποιείται μόνο σε συγκεκριμένες σελίδες ενός δικτυακού τόπου οι οποίες σχετίζονται με τα στοιχεία των συναλλαγών και χρήζουν πρόσθετης ασφάλειας.

5.5.2.2. Το πρωτόκολλο SET

Οι μεγαλύτερες εταιρείες πιστωτικών καρτών όπως η MasterCard και Visa, έχουν αναπτύξει ένα άλλο πρωτόκολλο, το SET (Secure Electronic Transaction Standard-Πρωτόκολλο Ασφαλών Ηλεκτρονικών Συναλλαγών). Το SET δεν ανταγωνίζεται το SSL, αλλά εστιάζει πάνω στις εμπιστευτικές συναλλαγές, με παράλληλη ανάγκη πιστοποίησης της ταυτότητας των συναλλασσομένων μερών. Έτσι, το SET επιχειρεί να εξασφαλίσει, ότι κανείς δε θα μπορέσει να χρησιμοποιήσει ένα κλεμμένο αριθμό πιστωτικής κάρτας, αλλά και ότι ο πωλών δε θα δει ποτέ τον αριθμό αυτό και θα αρκεστεί σε μια επιβεβαίωση, ότι η κάρτα είναι εντάξει. Αμέσως οι πληροφορίες στέλνονται στην εταιρεία της κάρτας, η οποία της αποκρυπτογραφεί και κάνει τη χρέωση. Πάντως, τα επιμέρους τεχνικά στοιχεία του και κυρίως το μήκος των κλειδιών που χρησιμοποιεί, χαρακτηρίζουν το SET ως πρωτόγονο και ίσως ανεπαρκές σε σύγκριση με την ασφάλεια που παρέχουν πακέτα όπως το PGP[67].

5.5.3. Ασφάλεια βάσεων δεδομένων

Οι βάσεις δεδομένων, σήμερα αποτελούν το κύριο συστατικό, σχεδόν του συνόλου των πληροφοριακών συστημάτων. Υπολογίζεται ότι το 90% των υπολογιστικών συστημάτων, που λειτουργούν παγκοσμίως, χρησιμοποιούν κάποιο σύστημα βάσεως δεδομένων. Οι απαιτήσεις ασφάλειας μιας βάσεως δεδομένων, όσον αφορά την γενικότερη φιλοσοφία, δεν απέχουν και πολύ από την ασφάλεια οποιουδήποτε πληροφοριακού συστήματος. Εξετάζουμε όμως χωριστά την ασφάλεια των βάσεων δεδομένων, για δυο βασικούς λόγους: Κατά πρώτον, μια βάση δεδομένων έχει ιδιαίτερη δομή και μηχανισμούς διαχείρισης, που απαιτούν τη χρήση εξειδικευμένων και πολύπλοκων εργαλείων για να επιτευχθεί ικανοποιητικό επίπεδο ασφαλείας και κατά δεύτερον τα δεδομένα, που αποθηκεύονται στις βάσεις δεδομένων, είναι ιδιαίτερα σημαντικά, συνήθως και ευαίσθητα, η δε προστασία τους αποτελεί πρωτεύον στόχο κάθε οργανισμού.

5.5.3.1. Γενικές απαιτήσεις ασφάλειας συστήματος βάσης δεδομένων

Όπως ήδη αναφέραμε, οι βασικές απαιτήσεις ασφάλειας ενός συστήματος βάσης δεδομένων δε διαφέρουν κατά πολύ από τις γενικότερες απαιτήσεις ενός πληροφοριακού συστήματος. Οι κυριότερες εκφάνσεις είναι οι ακόλουθες:

- **Φυσική ακεραιότητα της βάσης δεδομένων (physical database integrity):** Αναφέρεται στην φυσική ασφάλεια της βάσεως και ιδιαίτερα στην προστασία των υπολογιστικών συστημάτων, στα οποία έχει εγκατασταθεί, από φυσικά προβλήματα όπως πτώση της τάσεως του ρεύματος, πυρκαγιά, πλημμύρα κ.λπ.
- **Λογική ακεραιότητα τη βάσης δεδομένων (logical database security):** Η λογική ακεραιότητα αναφέρεται στην εξασφάλιση της λογικής δομής της βάσης. Τα προβλήματα ασφαλείας της λογικής ακεραιότητας μπορούν να ξεπεραστούν, εφόσον

[67] Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της.

εξ αρχής έχει γίνει σωστός σχεδιασμός. Κλασικό πρόβλημα ασφαλείας λογικής ακεραιότητας μιας βάσης, έχουμε όταν η μεταβολή της τιμής ενός πεδίου επηρεάζει και τις τιμές άλλων πεδίων, χωρίς αυτό να έχει προβλεφτεί.

- **Ακεραιότητα των πεδίων βάσης δεδομένων (element integrity):** Η παράμετρος αυτή εγγυάται, ότι οι τιμές των πεδίων της βάσης είναι σωστές.
- **Έλεγχος προσπέλασης (access control):** Σε κάθε βάση δεδομένων υπάρχουν διάφοροι χρήστες, στον καθένα από τους οποίους εκχωρούνται συγκεκριμένα δικαιώματα χρήσης και προσπέλασης της βάσης. Ο έλεγχος προσπέλασης εγγυάται, ότι όλοι οι χρήστες της βάσης θα προσπελάσουν μόνο τα δεδομένα, για τα οποία έχουν λάβει σχετική εξουσιοδότηση (π.χ. μόνο ανάγνωση)
- **Αυθεντικοποίηση των χρηστών (user authentication):** Κάθε βάση, πριν δεχθεί ένα χρήστη, θα πρέπει να πιστοποιήσει την ταυτότητα του. Ήδη σε προηγούμενη ενότητα παρουσιάστηκαν οι διαδικασίες αυθεντικοποίησης. Στις βάσεις δεδομένων χρησιμοποιούνται κωδικοί πρόσβασης, ενώ σε πιο εξελιγμένα συστήματα είναι δυνατή και η ενσωμάτωση βιομετρικών μεθόδων.
- **Διαθεσιμότητα (availability):** Η διαθεσιμότητα έχει, ακριβώς, την ίδια έννοια που περιγράψαμε στην αρχή της ενότητας, δηλαδή, ότι τα δεδομένα της βάσης θα είναι ανά πάσα στιγμή άμεσα προσπελάσιμα. Η παράμετρος αυτή είναι ιδιαίτερα σημαντική στις βάσεις δεδομένων, γιατί ενδέχεται να περιέχουν ευαίσθητα δεδομένα και απόρρητες πληροφορίες.

5.5.3.2. Σχεδιασμός ασφαλών συστημάτων βάσεων δεδομένων

Τα σημαντικότερα προβλήματα ασφάλειας, που παρουσιάζουν οι βάσεις δεδομένων, οφείλονται στον λανθασμένο σχεδιασμό. Τόσο οι εταιρείες που εμπορεύονται το συγκεκριμένο λογισμικό, όσο και οι οργανισμοί που το προμηθεύονται, παραμελούν το σωστό σχεδιασμό για λόγους, κυρίως, οικονομικούς αλλά και πίεσης χρόνου. Όταν βέβαια, στη συνέχεια, παρουσιαστούν προβλήματα ασφάλειας αντιλαμβάνονται το τεράστιο λάθος, στο οποίο είχαν υποπέσει.

Οι σημαντικότερες φάσεις, από πλευράς ασφάλειας, κατά το σχεδιασμό ενός συστήματος βάσεων δεδομένων είναι οι ακόλουθες:

α) Προκαταρτική ανάλυση: Στο στάδιο αυτό, προσδιορίζονται οι στόχοι σχετικά, με την ασφάλεια της βάσης δεδομένων και εξετάζονται οι πιθανοί κίνδυνοι, όπως οι μη εξουσιοδοτημένες προσπελάσεις, τα κακόβουλα προγράμματα, η φυσική ασφάλεια, η συμβατότητα με τα υπάρχοντα συστήματα ασφαλείας, η θέση της βάσης στην πολιτική ασφάλειας του οργανισμού κ.λπ.

β) Ανάλυση απαιτήσεων ασφαλείας: Κατά τη φάση αυτή του σχεδιασμού προσδιορίζονται οι χρήστες της βάσης και τα δικαιώματα, που καταχωρούνται στον καθένα από αυτούς. Οι κρισιμότεροι παράγοντες, στη φάση αυτή, είναι το επίπεδο εξουσιοδότησης του χρήστη και ο βαθμός ευαισθησίας των δεδομένων.

γ) Σχεδιασμός λογικού μοντέλου: Στη φάση αυτή, καθορίζεται επακριβώς, η πολιτική ασφάλειας της βάσης με τη χρήση ενός λογικού μοντέλου. Το μοντέλο αυτό, περιλαμβάνει τα υποκείμενα της βάσης (π.χ. χρήστες), τα αντικείμενα (π.χ. δεδομένα), τις

διαδικασίες (π.χ. τρόπος ενημέρωσης των δεδομένων) και τους επιτρεπτούς τρόπους προσπέλασης στην βάση (π.χ. απαγόρευση προσπέλασης από το Διαδίκτυο).

δ) Λογικός σχεδιασμός: Το επόμενο βήμα, είναι η ενσωμάτωση του λογικού μοντέλου στο γενικότερο μοντέλο δεδομένων, που υποστηρίζει το σύστημα βάσης δεδομένων. Κατά τον τρόπο αυτό, ο γενικότερος σχεδιασμός της βάσης στηρίζεται στο λογικό μοντέλο ασφαλείας.

ε) Φυσικός σχεδιασμός: Ο φυσικός σχεδιασμός είναι το τελευταίο στάδιο σχεδιασμού. Ο σχεδιαστής ασφαλείας καθορίζει τις τελευταίες λεπτομέρειες και ειδικότερα τους παραμέτρους του συστήματος, που σχετίζονται με την απόδοση, την αντίδραση σε περίπτωση υπερφόρτωσης, την ευελιξία και την προσαρμοστικότητα.

5.6. Πολιτικές ασφάλειας

Οι μέθοδοι και τεχνικές, που χρησιμοποιούνται για την ασφάλεια των πληροφοριακών συστημάτων και τα σύγχρονα εργαλεία υλικού και λογισμικού δεν μπορούν από μόνα τους να επιτύχουν το επίπεδο ασφαλείας, που απαιτούν οι ανάγκες ενός σύγχρονου οργανισμού. Τα εργαλεία υλικού και λογισμικού, που αναλύσαμε στα προηγούμενα μέρη της ενότητας, δεν λειτουργούν αυτόβουλα, είναι συμπληρωματικά και επιπλέον δύναται να παραμετροποιηθούν, ανάλογα με τις υπάρχουσες ανάγκες. Παράλληλα, σε κάθε σύστημα ασφαλείας, σημαντικό ρόλο διαδραματίζουν και οι ίδιοι οι χρήστες, οι οποίοι μπορούν με τις πράξεις και παραλείψεις τους, να αποτελέσουν πηγή σημαντικών κινδύνων ασφαλείας.

Για την αντιμετώπιση του συνόλου των κινδύνων ασφαλείας, κάθε οργανισμός εφαρμόζει μια πολιτική ασφαλείας η οποία υλοποιεί τους στόχους ασφαλείας, που έχει θέσει η διοίκηση του οργανισμού. Η πολιτική ασφαλείας, είναι το γραπτό κείμενο το οποίο καθορίζει τους κανόνες, που θα πρέπει να ακολουθούνται, για την ασφάλεια του πληροφοριακού συστήματος του οργανισμού από υφιστάμενους πληροφοριακούς κινδύνους. Η σύνταξη του κειμένου αυτού πραγματοποιείται σε δυο βασικά βήματα:

Στο πρώτο βήμα και πριν την σύνταξη του κειμένου της πολιτικής ασφάλειας, προσδιορίζονται οι κίνδυνοι ασφάλειας που διατρέχει ο οργανισμός. Ειδικότερα καθορίζεται:

- Το είδος των κινδύνων ασφαλείας, έναντι των οποίων είναι ευάλωτος ο οργανισμός.
- Η πιθανότητα να προκύψει κίνδυνος.
- Το κόστος, που θα έχει ο οργανισμός σε περίπτωση, που αυτός πραγματοποιηθεί.

Η προσέγγιση αυτή ονομάζεται ποσοτική ανάλυση κινδύνου, καθώς τα κριτήρια που λαμβάνονται υπ' όψιν και αξιολογούνται ανάγονται στην ψυχρή γλώσσα των αριθμών. Εκτός όμως από την ποσοτική ανάλυση, η χρήση της οποίας είναι περιορισμένη, ευρέως χρησιμοποιείται η ποιοτική ανάλυση κινδύνου. Στην ποιοτική ανάλυση δεν εφαρμόζεται η λογική των πιθανοτήτων, αλλά εξετάζονται άλλοι παράγοντες, όπως οι πιθανές απειλές

και ρα χαρακτηριστικά του συστήματος που το καθιστούν ευάλωτο έναντι των απειλών αυτών.

Στο δεύτερο βήμα, γίνεται η σύνταξη του κειμένου της πολιτικής ασφάλειας. Το άτομο που θα αναλάβει να διεκπεραιώσει την απαιτητική αυτή διαδικασία, εκτός από προηγούμενη συναφή εμπειρία και γνώση, θα πρέπει να ακολουθήσει και μια σειρά από βασικούς κανόνες. Κατ' αρχήν, το κείμενο θα πρέπει να χωρίζεται σε δυο βασικά έγγραφα: Το πρώτο, περιγράφει τις γενικές πολιτικές, οι οποίες και αλλάζουν σπανιότερα, ενώ το δεύτερο περιγράφει συγκεκριμένες διαδικασίες, οι οποίες αλλάζουν πιο συχνά, λόγω της αλματώδης εξέλιξης της τεχνολογίας, της εμφάνισης νέων πακέτων λογισμικού ασφάλειας κ.λπ. Πολύ σημαντικό στοιχείο είναι η γλώσσα γραφής, η οποία πρέπει να είναι απλή, χωρίς ειδικευμένους τεχνικούς όρους που το μόνο που θα επιτύχουν είναι να μπερδέψουν αυτούς που θα κληθούν να την εφαρμόσουν.

Τέλος, για κάθε πολιτική η οποία θα υιοθετηθεί, θα πρέπει να γίνεται σαφής η σημασία της, καθώς σε αντίθετη περίπτωση, κάποιοι υπάλληλοι μπορεί να την θεωρήσουν περιττή.

5.6.1. Βασική δομή πολιτικής ασφάλειας

Η πολιτική ασφάλειας είναι ένα κείμενο ογκώδες, με πολλές παραμέτρους και έννοιες, που απαιτεί αρκετό χρόνο από τους χρήστες για εξοικείωση και εφαρμογή. Για το λόγο αυτό, είναι ιδιαίτερα σημαντικό να έχει σωστή δομή, που θα καθοδηγεί τον αναγνώστη. Παράλληλα, η σωστή δομή βοηθά και στην ευκολότερη αναθεώρηση της, διαδικασία αναγκαία με βάση τους ρυθμούς ανάπτυξης των πληροφοριακών κινδύνων. Το μοντέλο, που έχει κυριαρχήσει, σήμερα είναι το ιεραρχικό, όπου στο υψηλότερο επίπεδο συναντάμε τις γενικές αρχές, ακολουθούν οι πολιτικές ειδικού σκοπού και στο τελευταίο επίπεδο συναντάμε συγκεκριμένες διαδικασίες ασφαλείας, οδηγίες και τεχνικά εγχειρίδια.

Γενική πολιτική ασφάλειας

Στο επίπεδο αυτό, περιλαμβάνονται οι γενικές αρχές για την ασφάλεια του οργανισμού και καθορίζονται οι στρατηγικοί στόχοι, αλλά και οι πόροι για την επίτευξη τους,

Ειδικού σκοπού ή επιμέρους πολιτικές

Στο επίπεδο αυτό, γίνεται διαχωρισμός της γενικής πολιτικής ασφαλείας του οργανισμού δε επιμέρους πολιτικές π.χ. ασφάλειας δικτύων, χρηστών, ηλεκτρονικής αλληλογραφίας, φυσικής ασφάλειας κ.λπ. Και εδώ κινούμαστε και πάλι σε υψηλό επίπεδο, καθώς δεν καθορίζονται επιμέρους πρακτικές.

Διαδικασία ασφάλειας

Ο τρόπος υλοποίησης της πολιτικής ασφάλειας, που έχει θέσει ο οργανισμός περιγράφεται στο στάδιο αυτό. Το κείμενο αναλύει, με λεπτομέρεια, τι πρέπει να γίνει σε συγκεκριμένες περιπτώσεις. Παράλληλα καθορίζονται οι ρόλοι, τα δικαιώματα και οι υποχρεώσεις του κάθε χρήστη, όσον αφορά στα θέματα ασφάλειας.

Οδηγίες ασφάλειας και τεχνικά εγχειρίδια

Στο τελευταίο αυτό στάδιο, παρέχονται ακόμη πιο λεπτομερής περιγραφή, ειδικότερες οδηγίες και κατευθύνσεις για πάσης φύσεως θέματα, κυρίως τεχνικής φύσεως, π.χ. εγχειρίδιο ρυθμίσεως του firewall, του web server κ.λπ.

5.6.2. Ο ρόλος των χρηστών

Ο ρόλος των χρηστών στην πολιτική ασφάλειας ενός οργανισμού είναι πολύ σημαντικός. Στη πράξη έχει αποδειχτεί, ότι τα τελειότερα συστήματα ασφαλείας, που χρησιμοποιούν την τελευταία τεχνολογία, δεν κατάφεραν να προστατεύσουν ένα οργανισμό λόγω λάθους ή παράλειψης ενός χρήστη. Ο παράγων άνθρωπος είναι ο πιο αδύναμος κρίκος στην αλυσίδα, που καθορίζει την ασφάλεια του οργανισμού. Όπως ήδη είδαμε, στις επιθέσεις κοινωνικής μηχανικής, οι επιτιθέμενοι δεν αναλώνονται στη σπατάλη χρόνου με τη χρήση προγραμμάτων λογισμικού για την εύρεση π.χ. κωδικών πρόσβασης αλλά εκμεταλλεύονται τις αδυναμίες του παράγοντα άνθρωπος.

Είναι, λοιπόν, πολύ σημαντικό, στην πολιτική ασφάλειας ενός οργανισμού να προβλέπεται η εκπαίδευση αλλά και συνεχής επιμόρφωση του προσωπικού. Μόνο ο συνδυασμός τεχνολογικών μέτρων προστασίας και εκπαίδευσης των χρηστών μπορεί να αποδώσει το μέγιστο (όχι όμως απόλυτο) επίπεδο ασφαλείας κάθε οργανισμό.

Ο κύριος στόχος ενός προγράμματος εκπαίδευσης είναι να πείσει τους εργαζόμενους για την ανάγκη προστασίας του οργανισμού, ώστε και οι ίδιοι να θέλουν να ακολουθήσουν τους κανόνες της πολιτικής ασφάλειας. Ο μεγαλύτερος κίνδυνος είναι ο εφησυχασμός, γι' αυτό οι εργαζόμενοι πρέπει να κατανοήσουν, ότι ο οργανισμός μπορεί να δεχθεί επίθεση ανά πάσα στιγμή και αυτοί αυτή αποτελούν την βασική μονάδα άμυνας και όχι το firewall ή το antivirus. Οι επιτιθέμενοι εκμεταλλεύονται το φορτίο εργασίας ενός υπαλλήλου ή την κόπωση από συνεχόμενη εργασία και καταφέρνουν να αποσπάσουν ευαίσθητες πληροφορίες. Το πρόγραμμα εκπαίδευσης οφείλει να τονίσει τον κίνδυνο αυτό και να παράσχει οδηγίες για την αντιμετώπιση του. Τέλος, το συνολικό πρόγραμμα εκπαίδευσης και η εφαρμογή του, θα πρέπει να αποτελεί πρώτη προτεραιότητα για τους υπαλλήλους, οι οποίοι θα πρέπει να κατανοήσουν, ότι η ασφάλεια των πληροφοριών στον οργανισμό αποτελεί μέρος της δουλειάς τους.

6. ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΗΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

6.1. Το πρόβλημα της νομοθεσίας για το ηλεκτρονικό έγκλημα

Το ηλεκτρονικό έγκλημα είναι μια νέα μορφή εγκλήματος, που οριοθετείται από δύο βασικά στοιχεία: τους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο. Η προσέγγιση των νομικών θεμάτων που αφορούν το ηλεκτρονικό έγκλημα ενέχει τη δυσκολία ότι προϋποθέτει όχι μόνο νομικές, αλλά και σε ένα βαθμό τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών και Διαδικτύου. Τα προβλήματα της νομοθεσίας επικεντρώνονται στην διαμόρφωση της κατάλληλης ορολογίας, στην αρτιότερη εφαρμογή του Ποινικού και Δικονομικού Δικαίου, καθώς και σε ειδικότερα θέματα που άπτονται της διεθνούς συνεργασίας, όπως η διεθνής δικαιοδοσία.

Έως σήμερα, οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα προέρχονται κυρίως από την τεχνολογία. Ο τεχνικός, λόγω έλλειψης νομικών γνώσεων, προσδιορίζει τους όρους με βάση τις επιστημονικές του γνώσεις και τα τεχνολογικά χαρακτηριστικά κάθε αντικειμένου. Στη νομική επιστήμη, ο προσδιορισμός των όρων είναι τελείως διαφορετικός. Για το νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο που με ακρίβεια καθορίζει ο νόμος. Σε περίπτωση που δεν υπάρχει νόμος ερευνάται η σχετική νομολογία, η ανάλυση ανάγεται στους γενικούς κανόνες του ισχύοντος δικαίου για να βρεθεί κάποια θεωρητική λύση του ζητήματος. Στην πράξη, ο νομοθέτης αποφεύγει να δημιουργήσει ειδική ορολογία για το ηλεκτρονικό έγκλημα και δανείζεται την χρησιμοποιημένη από την τεχνολογία,[68] η οποία μπορεί να είναι ασαφής, γενική, αόριστη ή έλλειπες, κατά τρόπο που να εμποδίζει την ορθή απονομή της δικαιοσύνης.

Όπως αναφέρθηκε στο Κεφάλαιο 1, το ηλεκτρονικό έγκλημα φέρει κάποια ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το συμβατικό έγκλημα. Τα χαρακτηριστικά αυτά, απαιτούν την υιοθέτηση ειδικών νομοθετικών ρυθμίσεων για την αντιμετώπιση του, τόσο στον τομέα του Ποινικού, όσο και στον τομέα του Δικονομικού Δικαίου, το ηλεκτρονικό έγκλημα σε πολλές χώρες αντιμετωπίζεται με τις υπάρχουσες διατάξεις του κοινού Ποινικού Δικαίου, γεγονός που πολλές φορές καθιστά αδύνατη τη δίωξη του. Στον τομέα του δικονομικού δικαίου, οι παρεμβάσεις στην ισχύουσα νομοθεσία παγκοσμίως, είναι ελάχιστες, με αποτέλεσμα να δημιουργούνται ανυπέρβλητα προβλήματα, όπως η δυσκολία ασφαλούς καθορισμού της δικαιοδοσίας των δικαστηρίων και της αρμοδιότητας των διωκτικών αρχών.

Με δεδομένο ότι η τεχνολογία προχωρά πολύ πιο γρήγορα από τη νομοθεσία, κάθε νομοθετική ρύθμιση υπόκειται πολύ γρήγορα σε αμφισβήτηση. Αυτό που σήμερα ορίζουμε ως ηλεκτρονικό έγκλημα, πολύ σύντομα δεν θα υπάρχει ως συμπεριφορά ή θα έχει τροποποιηθεί κατά τρόπο ουσιαστικό, που θα καθιστά ανίσχυρο τον υπάρχοντα νόμο. Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος δεν αρκεί μόνο ειδική νομοθεσία, αλλά απαιτείται συνεχής ενημέρωση της, λαμβάνοντας υπ' όψιν τις

---

[68] Σε πολύ σημαντικά κείμενα διεθνώς, όπως για παράδειγμα στη Σύμβαση για τον Κυβερνοχώρο του Συμβουλίου της Ευρώπης, αναφέρονται μόνο τέσσερις όροι: υπολογιστικό σύστημα, ηλεκτρονικά δεδομένα, παροχέας υπηρεσιών και μεταδιδόμενα δεδομένα. Πολύ σημαντικοί όροι, για τη νέα αυτή μορφή εγκλήματος όπως π.χ. ο κυβερνοχώρος, δεν αναφέρεται.

τεχνολογικές εξελίξεις. Επιπλέον, για ένα άρτιο σύστημα απονομής δικαιοσύνης, όλοι όσοι εμπλέκονται στη δίωξη του ηλεκτρονικού εγκλήματος όπως αστυνομικοί, εισαγγελείς, δικαστές και δικηγόροι, πρέπει να κατέχουν τόσο νομικές, όσο και τεχνικές γνώσεις, για τη νέα αυτή μορφή εγκληματικής δραστηριότητας.

Τέλος, τα σημαντικότερα νομοθετικά προβλήματα για το ηλεκτρονικό έγκλημα οφείλονται στον παγκόσμιο χαρακτήρα του. Ο τόπος διάπραξης των συμβατικών εγκλημάτων, προσδιορίζεται από ένα συγκεκριμένο γεωγραφικό χώρο. Στα ηλεκτρονικά εγκλήματα, ο τόπος διάπραξης πολλές φορές είναι αδύνατο να προσδιοριστεί, οι δε συνέπειες της εγκληματικής συμπεριφοράς, μπορούν να είναι ορατές σε περισσότερες από μια χώρες, στις οποίες ισχύει διαφορετικό νομικό πλαίσιο. Η δικαιοδοσία, η συνεργασία μεταξύ των κρατών σε διεθνείς έρευνες ηλεκτρονικών εγκλημάτων και η διαδικασία έκδοσης όσων έχουν διαπράξει ηλεκτρονικά εγκλήματα με διεθνικό χαρακτήρα, είναι μερικά μόνο από τα ζητήματα που επιτείνουν τους νομοθετικούς προβληματισμούς.

6.2. Νομοθετικοί προβληματισμοί

6.2.1. Νομική προσέγγιση του Διαδικτύου

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου, ενός «χώρου» τεραστίου και αχανούς, με δυσδιάκριτα όρια και απεριόριστες δυνατότητες ανταλλαγής πληροφοριών. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω Διαδικτύου, υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιαδήποτε προσπάθειας ρύθμισης του Διαδικτύου[69].

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 η 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.

---

[69] Αναστασία Ζάννη 2005

- Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.[70]
- 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 τον χρονικό σημείο που άρχισε να αναπτύσσεται και να επεκτείνεται. Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπολικά από τον ΟΤΕ. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες. Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία με δύο οδηγίες την 90/387[71] και την 90/388[72], 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 τις Ευρωπαϊκής Κοινότητας, προήλθε, καταρχήν, με τον Ν.2075/92. Ο νόμος αυτός, πολύ σύντομα καταργήθηκε με τον νέο Ν.2246/94 και στη συνέχεια 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 πάροχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους.

6.2.2. Παγκόσμιος χαρακτήρας του Ηλεκτρονικού Εγκλήματος

Το κύριο χαρακτηριστικό γνώρισμα του ηλεκτρονικού εγκλήματος είναι ο παγκόσμιος χαρακτήρας του. Το ηλεκτρονικό έγκλημα έχει υπερβεί τα στενά γεωγραφικά όρια των κρατών, παρουσιάζοντας ένα « πρόσωπο» παγκόσμιο, το οποίο οφείλεται κυρίως στην ανάπτυξη του Διαδικτύου.

Σε νομοθετικό επίπεδο, η παγκοσμιότητα αυτή δημιουργεί μια σειρά από ερωτήματα. Τι γίνεται όταν ένα έγκλημα διαπράττεται σε δύο ή περισσότερες χώρες ταυτόχρονα, στις οποίες ισχύει διαφορετικό νομικό πλαίσιο ή όταν σε μια από τις χώρες αυτές δεν υπάρχει καθόλου νομοθετικό πλαίσιο για τη συγκεκριμένη συμπεριφορά; Σε περίπτωση διεθνών ερευνών για ένα ηλεκτρονικό έγκλημα, πως θα γίνουν οι απαιτούμενες ενέργειες σε μια χώρα, που δεν διαθέτει σχετική νομοθεσία;

Οι αποσπαστικές νομοθετικές παρεμβάσεις συγκεκριμένων κρατών για την αντιμετώπιση των προβλημάτων αυτών δεν επαρκούν. Απαιτείται πρωταρχικά εναρμόνιση της διεθνούς

---

[70] Οι έννοιες αυτές αναφέρονται στο «Declaration of the Independence of Cyberspace» του John Perry Barlow. http://www.lafraze.net/nbernard/misc/Declaration-Final.html (Ημερομηνία πρόσβασης: 21/08/09)

[71] 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.

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

νομοθεσίας σχετικά με το ηλεκτρονικό έγκλημα, μέσω συμβάσεων ή άλλων επίσημων εγγράφων. Η διαδικασία αυτή, βέβαια, είναι ιδιαίτερα πολύπλοκη. Ενδεικτικά, αναφέρεται ότι σε κάποιες χώρες δεν έχει καν φθάσει η τεχνολογία των υπολογιστών και του Διαδικτύου, ενώ το ηλεκτρονικό έγκλημα, όπως και πολλές άλλες μορφές εγκλήματος , αντιμετωπίζεται με διαφορετικό τρόπο σε κάθε χώρα, ανάλογα με το συγκεκριμένο κοινωνικοπολιτιστικό καθεστώς, τα ήθη, τα έθιμα και τις παραδόσεις κάθε λαού.

Όσον αφορά τον καθαυτό νομικό τομέα, μια τέτοια επιχειρούμενη προσπάθεια θα συναντούσε περισσότερα προβλήματα. Για παράδειγμα, σε κάποιες χώρες απαιτείται συνταγματική αναθεώρηση για να ισχύσουν παγκόσμιοι νομοθετικοί κανόνες, οι οποίοι, ενδεχομένως, να μην γίνουν αποδεκτοί, αλλά και στην περίπτωση που γίνουν, θα απαιτηθεί μεγάλο χρονικό διάστημα για να ολοκληρωθούν οι συνταγματικές αναθεωρήσεις.

Εκτός όμως από τον τομέα του ποινικού δικαίου, σημαντικά προβλήματα προκύπτουν και κατά την εφαρμογή του δικονομικού δικαίου. Η διερεύνηση ηλεκτρονικών εγκλημάτων , απαιτεί εξειδικευμένες δυνατότητες έρευνας από τις αρμόδιες αρχές, που έρχονται σε σύγκρουση με θεμελιώδεις αξίες, όπως η προστασία του απορρήτου και της ιδιωτικότητας του ατόμου. Παράλληλα, ο παγκόσμιος χαρακτήρας του επιβάλλει την άμεση και συνεχή συνεργασία μεταξύ των χωρών για την αναζήτηση και αποκάλυψη των δραστών.

Μέχρι σήμερα, διάφοροι οργανισμοί, όπως το Συμβούλιο της Ευρώπης και τα Ηνωμένα Έθνη, έχουν επιχειρήσει να πρωτοστατήσουν στην προσπάθεια εναρμόνισης της διεθνούς νομοθεσίας για το ηλεκτρονικό έγκλημα.

6.3. Παγκόσμια νομοθεσία για το Ηλεκτρονικό Έγκλημα

6.3.1. Ηνωμένες Πολιτείες της Αμερικής

Το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα θεσπίστηκε στις Ηνωμένες Πολιτείες της Αμερικής, το 1984.[73] Ο νόμος Computer Fraud and Abuse Act, προσπάθησε, ανεπιτυχώς θα λέγαμε, να θέσει ένα βασικό νομικό πλαίσιο για την νέα αυτή μορφή εγκλήματος. Η έλλειψη όρων σχετιζόμενων με τη νέα τεχνολογία των ηλεκτρονικών υπολογιστών, αλλά και η αποτυχία προσδιορισμού των ορίων δικαιοδοσίας των δικαστηρίων, ήταν από τα σημαντικότερα προβλήματα[74]. Επιπλέον, ο νόμος περιοριζόταν, στην προστασία κρατικών υπολογιστικών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, με σκοπό την απόκτηση απόρρητων πληροφοριών που θα μπορούσαν να βλάψουν τις ΗΠΑ.

Τα προβλήματα αυτά, οδήγησαν πολύ γρήγορα στην πρώτη αναθεώρηση, το 1986, στην οποία προστέθηκε μια ακόμα ενότητα, που προέβλεπε ότι «όποιος σκόπιμα αποκτά πρόσβαση σε ομοσπονδιακό υπολογιστικό σύστημα χωρίς εξουσιοδότηση και συνέπεια της πρόσβασης αυτής τροποποιεί, προκαλεί ζημιά ή καταστρέφει πληροφορίες που είναι αποθηκευμένες σε έναν ηλεκτρονικό υπολογιστή κρατικού ενδιαφέροντος ή εμποδίζει

---

[73] Κωνσταντίνος Βλαχόπουλος 2007 σελ.129
[74] Colombell, M. 2002 (Ημερομηνία πρόσβασης: 25/07/09)

την εξουσιοδοτημένη χρήση ενός υπολογιστή ή των πληροφοριών που είναι αποθηκευμένες σε αυτών τιμωρείται» Στην τροποποίηση αυτή χρησιμοποιήθηκε πιο σαφής ορολογία, ενώ διαφαίνεται και η πρώτη προσπάθεια αντιμετώπισης περιπτώσεων άρνησης εξυπηρέτησης με τη φράση «εμποδίζει την εξουσιοδοτημένη χρήση ενός υπολογιστή». Και πάλι όμως, η συγκεκριμένη τροποποίηση αναφέρονταν μόνο σε κρατικά υπολογιστικά συστήματα.

Η πιο σημαντική τροποποίηση του νομοθετήματος αυτού έγινε το 1994, η οποία επέφερε αλλαγές σε τρία σημαντικά σημεία:

1. Η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικούς υπολογιστές, που χρησιμοποιούνται στο διαπολιτειακό εμπόριο
2. Αναφέρθηκε ο όρος, «με εξουσιοδοτημένη πρόσβαση», που σημαίνει ότι οι υπάλληλοι εταιρειών (insiders) και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχθούν και
3. Συγκεκριμένες μορφές επικίνδυνων και σκόπιμων ενεργειών θεωρούνταν, πλέον, παράνομες, όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης (denial of service attacks).

Τέλος, το 1996 συμπληρώθηκε ο νόμος αυτός με τη National Information Infrastructure Protection Act (NIIPA), η οποία αναφέρεται στους « προστατευμένους υπολογιστές»[75]. Η πιο σημαντική διάταξη του νομοθετήματος αυτού προβλέπει ότι κάθε μεμονωμένος χρήστης, που εισέρχεται σε ένα προστατευμένο υπολογιστή, είναι υπεύθυνος όχι μόνο για τις πράξεις του αλλά και για τις συνέπειες αυτών, ενώ εάν η πρόσβαση του είναι εξουσιοδοτημένη, είναι ποινικά υπεύθυνος μόνο εάν έχει πρόθεση να προξενήσει ζημιά στο θύμα. Οι διατάξεις αυτές, με μικρές τροποποιήσεις που έχουν επέλθει στη συνέχεια, ισχύουν και σήμερα, ενσωματωμένες στο κεφάλαιο 18, παράγραφος 1030 του ποινικού κώδικα των Η.Π.Α.

Εκτός των ανωτέρω, σε κάθε πολιτεία υπάρχουν σε ισχύ διάφορες διατάξεις, που αντιμετωπίζουν το ηλεκτρονικό έγκλημα με διαφορετικό τρόπο. Η απουσία ενιαίων διατάξεων σε όλα τα μήκη και πλάτη των Η.Π.Α., αποτελεί τη μεγαλύτερη πληγή του δικαϊκού συστήματος.

6.3.2. Αυστραλία

Η Αυστραλία είναι η χώρα που έχει δώσει την μεγαλύτερη, μετά τις Η.Π.Σ, προσοχή στην αντιμετώπιση του ηλεκτρονικού εγκλήματος. Ο νόμος «Crime Act 1914» προβλέπει τέσσερις βασικές μορφές ηλεκτρονικού εγκλήματος:

- Παράνομη πρόσβαση σε δεδομένα αποθηκευμένα σε κρατικό ηλεκτρονικό υπολογιστή.
- Καταστροφή δεδομένων αποθηκευμένων σε κρατικό ηλεκτρονικό υπολογιστή
- Πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης και τέλος

[75] Ο Αγγλικός όρος «protected computers» αναφέρεται σε Η/Υ που α) προορίζονται για χρήση από ένα οικονομικό ίδρυμα ή την κυβέρνηση των ΗΠΑ ή β) χρησιμοποιούνται σε διαπολιτειακό ή εμπόριο με χώρες της αλλοδαπής και επικοινωνίες.

- Καταστροφή δεδομένων σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.

Ο νόμος που σήμερα είναι σε ισχύ στην Αυστραλία, αναφέρεται ως The Cybercrime Act 2001[76], ο οποίος προήλθε από την τροποποίηση του νόμου Crime Act και του Ποινικού Κώδικα που ψηφίστηκε το 1995. Ο νόμος προβλέπει τρεις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων:

- Μη εξουσιοδοτημένη πρόσβαση, μετατροπή και φθορά δεδομένων, πε σκοπό την διάπραξη σοβαρού εγκλήματος. Στην περίπτωση αυτή, η ποινή είναι ισοδύναμη της αντίστοιχης που επιβάλλεται στο συμβατικό έγκλημα.
- Μη εξουσιοδοτημένη τροποποίηση δεδομένων, που οδηγεί σε φθορά δεδομένων.
- Μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών, για την οποία προβλέπεται ποινή έως δέκα ετών.

Παράλληλα, ο νόμος δημιούργησε τέσσερις νέες μορφές εγκλημάτων:

- Μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευομένων δεδομένων.
- Παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ.
- Κατοχή ή έλεγχος δεδομένων, με σκοπό την διάπραξη ηλεκτρονικών αδικημάτων.
- Παραγωγή, προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος.

Στο νόμο περιλαμβάνονται ακόμη, διατάξεις για τον τρόπο έρευνας ηλεκτρονικών αδικημάτων από τις διωκτικές αρχές και τους μεθόδους εξέτασης δεδομένων, που είναι αποθηκευμένα σε ηλεκτρονικά μέσα.

6.3.3. Αγγλία

Στην Αγγλία, το πρώτο νομοθέτημα για το ηλεκτρονικό έγκλημα ψηφίστηκε το 1990. Πρόκειται για τον νόμο « Computer Misuse Act»[77] ένα από τα πλέον σημαντικά νομοθετικά κείμενα για το ηλεκτρονικό έγκλημα, το οποίο αποτέλεσε οδηγό για τις νομοθεσίες άλλων χωρών, όπως ο Καναδάς και η Ιρλανδία.

Η νομοθετική, αυτή, πράξη καλύπτει σε μεγάλος εύρος το νομοθετικό κενό για το ηλεκτρονικό έγκλημα. Διακρίνει τρεις βασικές κατηγορίες αδικημάτων, που σχετίζονται με ηλεκτρονικό υπολογιστή:

- Μη εξουσιοδοτημένη πρόσβαση, σε πληροφορίες που είναι αποθηκευμένες σε ηλεκτρονικό υπολογιστή.
- Μη εξουσιοδοτημένη πρόσβαση με σκοπό τη διάπραξη αδικημάτων.
- Μη εξουσιοδοτημένη τροποποίηση πληροφοριών, αποθηκευμένων σε υπολογιστικό σύστημα.

---

[76] The cybercrime Act 2001, Corporate & Technology Group of Freehills, διαθέσιμο από: http://www.findlaw.com.au/article/1408.htm (Ημερομηνία πρόσβασης: 25/08/09)

[77] Το κείμενο του νόμου είναι διαθέσιμο στην διεύθυνση http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm (Ημερομηνία πρόσβασης: 19/08/09)

Στο νομοθέτημα περιλαμβάνονται διατάξεις σχετικά με τη δικαιοδοσία και τον τρόπο απονομής της δικαιοσύνης, όσο αφορά στα ηλεκτρονικά εγκλήματα.

Αν και πλήρης σε πολλά σημεία, λαμβάνοντας υπόψη τη χρονική περίοδο κατά την οποία τέθηκε σε ισχύ, ο νόμος αυτός χρειάζεται αναθεώρηση, γιατί δεν έχει λάβει υπόψη ένα πολύ σημαντικό παράγοντα, το Διαδίκτυο. Η ανάπτυξη του Διαδικτύου δημιούργησε μια σειρά από νέα αδικήματα και μεθόδους τέλεσής τους που ήταν αδύνατον να προβλεφθούν την εποχή εκείνη. Μάλιστα, ο νομοθέτης απέφυγε να ορίσει τι είναι ηλεκτρονικός υπολογιστής (και σωστά), καθώς δεν ήταν δυνατό να προβλεφθεί, τότε, η σημερινή μορφή των ηλεκτρονικών υπολογιστών.

6.3.4. Αργεντινή

Στην Αργεντινή, δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για το ηλεκτρονικό έγκλημα. Η ποινική αντιμετώπιση των εγκλημάτων της μορφής αυτής προέρχεται από τον κοινό Ποινικό Κώδικα, ο οποίος δεν περιλαμβάνει συγκεκριμένες διατάξεις για τη δίωξη αδικημάτων, που τελούνται με τη χρήση υπολογιστών και Διαδικτύου. Τα εγκλήματα αυτά είναι δυνατόν να διωχθούν μόνο με διασταλτική ερμηνεία των ισχυουσών διατάξεων. Για παράδειγμα, τα άρθρα 128 και 129 του Ποινικού Κώδικα, σχετικά με την παιδική πορνογραφία , καθιστούν παράνομη τη δημοσίευση, δημιουργία, αναπαραγωγή και διάθεση τέτοιου υλικού χωρίς να προσδιορίσουν το μέσο με το οποίο θα πραγματοποιηθούν οι ενέργειες αυτές[78].

6.3.5. Κίνα

Η Κίνα, αντιμετωπίζει το ηλεκτρονικό έγκλημα με ειδική νομοθεσία που έχει θεσπιστεί για το σκοπό αυτό. Το άρθρο 23 του Νομοθετικού Διατάγματος 147, καθιστά παράνομη οποιαδήποτε δραστηριότητα σχετίζεται με τη διασπορά ιών ή άλλου είδους «κακόβουλου» λογισμικού, σε ηλεκτρονικούς υπολογιστές. Παράνομη, επίσης, είναι η πώληση συστημάτων προστασίας υπολογιστών χωρίς άδεια. Οι κυρώσεις που τη προβλέπονται για την παραβίαση των παραπάνω διατάξεων, περιλαμβάνουν χρηματικό πρόστιμο, που κυμαίνεται από 5.000 έως 15.000 γιέν ανάλογα με τη σοβαρότητα του εγκλήματος.

Το ζήτημα της πορνογραφίας αντιμετωπίζεται με την υπάρχουσα νομοθεσία, όπως συμβαίνει στις περισσότερες χώρες στο κόσμο. Το Διαδίκτυο, με το οποίο διακινούνται τεράστιες ποσότητες πορνογραφικού υλικού, αποτελεί ένα ακόμη μέσο τέλεσης του εγκλήματος.

Εξαιρετικό ενδιαφέρον παρουσιάζουν ορισμένες διατάξεις της νομοθεσίας στην Κίνα, τις οποίες δεν συναντάμε σε άλλες χώρες. Για παράδειγμα, θεωρείται παράνομη η δημιουργία, αναπαραγωγή, ανάκτηση και διάδοση πληροφοριών, που μπορούν να βλάψουν την εθνική ενότητα. Επίσης απαγορεύεται η παραποίηση της αλήθειας και η διάδοση φημών που μπορούν να βλάψουν τη συνοχή της κοινωνίας, η διάδοση προλήψεων, υλικού σχετικά με τη βία κ.ά.., δημιουργώντας σαφή ερωτήματα για τα όρια της ελευθερίας του λόγου στο Διαδίκτυο.

---

[78] Shinder, D. and Tittel, E. 2002 page:700

6.3.6. Ελλάδα

Στην Ελλάδα ισχύει ο νόμος 2928 του 2001 για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων.

Οι διάφορες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και στην Ευρωπαϊκή Ένωση. Ειδικότερα αναλύονται οι εξής μορφές[79]:

Κυβερνοσφετερισμός – Προστασία των Domain names

Κυβερνοσφετερισμός (cybersquatting) είναι το ηλεκτρονικό αδίκημα κατά το οποίο κάποιος χρήστης του Διαδικτύου για εμπορικούς σκοπούς κατοχυρώνει και χρησιμοποιεί ηλεκτρονική διεύθυνση (domain name) που περιέχει είτε την επωνυμία γνωστών επιχειρήσεων είτε σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νόμιμων δικαιούχων αλλά και αποκλεισμός τους από τη χρήση του Διαδικτύου με την επωνυμία τους.

Η προστασία των domain name παρέχεται ανάλογα με το περιεχόμενο του δεύτερου μέρους τους. Αν τη διαδικτυακή διεύθυνση αποτελεί ένα όνομα, τότε παρέχεται η προστασία των άρθρων 57 και 58 ΑΚ. Αν πρόκειται για εμπορική επωνυμία, δηλαδή ένα όνομα με το οποίο ο έμπορος διεξάγει τις συναλλαγές του ή για διακριτικό τίτλο τότε μαζί με την προστασία του άρθρου 58 ΑΚ παρέχεται και η προστασία του άρθρου 13 του νόμου 146/1914. Το άρθρο 13 του νόμου 1146/1914 εφαρμόζεται και όταν ένα domain name αποτελεί εικονικό κατάστημα που είναι γνωστό και επικρατεί στις ηλεκτρονικές συναλλαγές. Αν η ηλεκτρονική διεύθυνση ταυτίζεται με το σήμα και υπάρχει κίνδυνος σύγχυσης στις συναλλαγές παρέχεται η προστασία των άρθρων 4, 18 και 26 του νόμου 2239/1994 περί σημάτων.

Παράνομη διείσδυση σε δεδομένα (hacking, cracking)- Προστασία του απορρήτου στο Διαδίκτυο

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ.

Cracking είναι η αλλαγή των κωδίκων πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους. Η χωρίς δικαίωμα διείσδυση –πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του Ποινικού κώδικα. Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Αυτά είναι:

---

[79] http://www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=90 (Ημερομηνία Πρόσβασης: 01/09/09)

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

Ιοί - Προστασία των δεδομένων από ιούς

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί των υπολογιστών είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται από μόνα τους. Διακρίνονται σε δύο μορφές: στους ιούς των προγραμμάτων και στους ιούς των συστημάτων. Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ. Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

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

Παράνομο και βλαβερό περιεχόμενο που θίγει την προσωπικότητα και την ηθική των ατόμων αποτελούν η δυσφήμηση μέσω του διαδικτύου και η διάδοση πορνογραφικού υλικού. Ο προσβληθείς στην προσωπικότητα του από κάποιο μήνυμα που διακινείται στο Διαδίκτυο προστατεύεται από τις διατάξεις 361, 362, 366 και 367 του Π.Κ. Δυσχερέστερο είναι το ζήτημα της διάδοσης πορνογραφικού υλικού στο διαδίκτυο ιδιαίτερα σε σχέση με τους ανηλίκους και την προστασία τους από την έκθεση σε αυτό.

Στην Ευρωπαϊκή Ένωση έχουν ληφθεί και ισχύουν αρκετά μέτρα για την αντιμετώπισης αυτού του είδους εγκληματικότητας.

1. Η Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06 που περιέχει προτροπές του Συμβουλίου προς τα κράτη μέλη και την Επιτροπή ώστε να ληφθούν μέτρα για την προστασία των ανηλίκων στα οπτικοακουστικά μέσα και στο Ιντερνετ,
2. Η Σύσταση με αριθμό 98/560/ΕΚ όπου αναφέρονται οι συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης ,
3. Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ όπου γίνεται λόγος για τα μέτρα που λαμβάνουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης ώστε οι χρήστες του διαδικτύου να βοηθήσουν στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα παιδιά,
4. Η Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301 όπου υπάρχουν οι προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων σε όλα τα οπτικοακουστικά μέσα και για την προστασία των ανηλίκων στο ψηφιακό περιβάλλον και με την συμμετοχή των γονέων,
5. Η Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06 όπου αναφέρεται ότι τα κράτη μεταξύ τους πρέπει να συνεργάζονται ώστε να διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη ποινικών αδικημάτων που αφορούν την παιδική πορνογραφία στο Ίντερνετ,
6. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών
7. Η Απόφαση 276/1999/ΕΚ για την έγκριση, την διάρκεια, τη χρηματοδότηση και τους στόχους προγράμματος για την προώθηση της ασφαλέστερης χρήσης του Ίντερνετ,
8. Η Απόφαση 1151/2003/ΕΚ που τροποποιεί την απόφαση αριθ. 276/1999/ΕΚ και
9. Η Ανακοίνωση της Επιτροπής COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου (Ιντερνετ) μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα

Ένα ακόμα ζήτημα που τίθεται σχετικά με την χρήση του διαδικτύου από τους ανήλικους είναι η πραγματοποίηση συναλλαγών με ηλεκτρονικά μέσα. Είναι γνωστό ότι οποιαδήποτε συναλλαγή με ανήλικο είναι άκυρη και μπορεί να επισύρει ποινή για τον αντισυμβαλλόμενο εφόσον το περιεχόμενό της δεν απευθύνεται σε παιδία και εφήβους. Στην περίπτωση όμως των ηλεκτρονικών συναλλαγών δεν είναι πάντα δυνατή η εξακρίβωση των στοιχείων του καταναλωτή. Για την προστασία των προμηθευτών που δραστηριοποιούνται μέσω κάποιας ιστοσελίδας είναι απαραίτητη η αναγραφή στους όρους χρήσης του site ότι δεν επιτρέπονται οι συναλλαγές με ανηλίκους και ότι η ιστοσελίδα δεν φέρει καμία ευθύνη.

Προστασία δεδομένων προσωπικού χαρακτήρα

Η συγκέντρωση και επεξεργασία ηλεκτρονικών δεδομένων αντιμετωπίστηκε από πολύ νωρίς ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική και προσωπική σφαίρα. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση υπάρχει νομοθεσία που ρυθμίζει τα σχετικά με την επεξεργασίας δεδομένων όπως η Οδηγία 2002/58 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και η Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού.

Απάτη μέσω του Διαδικτύου

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α). Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών .

Spamming

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming, δηλαδή η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο σε χιλιάδες καταναλωτές-χρήστες του διαδικτύου . Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι « η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους» καθώς και από άλλα νομοθετήματα. Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο.

Προστασία της Πνευματικής Ιδιοκτησίας

Η εμφάνιση των βάσεων δεδομένων σε συνδυασμό με τη διάδοση του Διαδικτύου έχει κάνει την αντιγραφή και την ηλεκτρονική διάδοση των πνευματικών δημιουργημάτων αποτελεσματική και εξαιρετικά απλή. Με τον τρόπο αυτό όμως καταστρατηγούνται τα δικαιώματα της πνευματικής ιδιοκτησίας των δημιουργών πάνω στα δημιουργήματά τους. Η κύρια πηγή του δικαίου της πνευματικής ιδιοκτησίας στην Ελλάδα αποτελεί ο Νόμος 2121/1993 με τίτλο «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα.» Με την έναρξη της ισχύς αυτού του νόμου όλοι σχεδόν οι προγενέστεροι νόμοι, που αφορούσαν την πνευματική ιδιοκτησία καταργήθηκαν.

Δικαιοδοσία στο Ιντερνετ

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες.

A. Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.
B. Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
C. Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.
D. Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.

Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται αναρίθμητες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται με νέες εκφάνσεις και καθίσταται σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις. Για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών όπως αναφέρεται σε πολλά νομοθετικά κείμενα.

6.3.7. Διεθνείς προσπάθειες

Σε διεθνές επίπεδο, η Interpol προσέγγισε πρώτη το ζήτημα του ηλεκτρονικού εγκλήματος, στο Τρίτο Διεθνές Συμπόσιο για την Απάτη (3rd Interpol Symposium on International Fraud), στο Παρίσι, το 1979. Διάφορες άλλες προσεγγίσεις έλαβαν χώρα κατά τα χρόνια που ακολούθησαν, με πιο σημαντικές αυτές που αναπτύχθηκαν από το OECD, τα Ηνωμένα Έθνη και την «Ομάδα των Οκτών» (Group of Eight).

i)Organization for Economic Cooperation and Development (OECD)

Ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α.) διόρισε στο Παρίσι, το 1983, μια επιτροπή, για το ζήτημα του ηλεκτρονικού εγκλήματος και την ανάγκη, που αυτό δημιουργεί, για την τροποποίηση των ποινικών διατάξεων στα κράτη-μέλη του οργανισμού. Η επιτροπή, αφού εξέτασε τις ισχύουσες νομοθετικές διατάξεις των κρατών- μελών, κατέληξε σε ένα κείμενο για το ηλεκτρονικό έγκλημα, που λειτουργούσε ως κοινός παρανομαστής μεταξύ των διαφορετικών νομικών προσεγγίσεων, που εξετάστηκαν στα κράτη-μέλη. Οι διατάξεις του κειμένου αυτού απαγόρευαν την εισαγωγή, τροποποίηση, διαγραφή και απόκρυψη δεδομένων, με σκοπό την παράνομη μεταφορά κεφαλαίων, τη διάπραξη πλαστογραφίας και την παρεμπόδιση λειτουργίας ενός υπολογιστή ή δικτύου. Επίσης, απαγόρευαν την πρόσβαση σε συστήματα Η/Υ χωρίς άδεια, ενώ προστάτευαν και την παράνομη αντιγραφή και διάθεση πακέτων λογισμικού.

ii) Οργανισμός Ηνωμένων Εθνών

Τα Ηνωμένα Έθνη παρουσίασαν ένα ψήφισμα, σχετικά με τη νομοθεσία για το ηλεκτρονικό έγκλημα, στο 8° Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος,[80] εκδόθηκε το 1994. Το Εγχειρίδιο αυτό αντιμετωπίζει συνολικά το ζήτημα του ηλεκτρονικού εγκλήματος, παρουσιάζοντας την έκταση του φαινομένου, τις μορφές του και την υπάρχουσα νομοθεσία σε διάφορες χώρες, και καταλήγει σε προτάσεις για την καλύτερη αντιμετώπιση του. Το συγκεκριμένο κείμενο, πρέπει να αναθεωρηθεί, λόγω των τεχνολογικών εξελίξεων που συντελέστηκαν μετά την έκδοση του. Αποτελεί, όμως, την πρώτη συστηματική διεθνή προσπάθεια νομοθετικής προσέγγισης του ηλεκτρονικού εγκλήματος. Για τον λόγο αυτό, θεωρείται η βάση πάνω στην οποία μπορούν να στηριχθούν μελλοντικές προσπάθειες.

iii) Ομάδα των Οκτώ - Group of Eight (G8)

Οι Οκτώ ισχυρότερες χώρες του κόσμου,[81] δημιούργησαν το 1997 μια Υποομάδα για το Έγκλημα Υψηλής Τεχνολογίας (Hi-tech crime Subgroup). Η Υποομάδα αυτή σε μια συνάντηση που πραγματοποιήθηκε τον ίδιο χρόνο στην Ουάσινγκτον, με την συμμετοχή των υπουργών Εσωτερικών και Δικαιοσύνης των οκτώ χωρών, κατέληξε σε «Δέκα Αρχές» (Ten Principles) και «Δέκα Τομείς Δράσης» (Ten Action Items) για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. [82]Οι αρχές αυτές είχαν ως σκοπό τη διασφάλιση της ενιαίας αντιμετώπισης του εγκληματικού φαινομένου, σε όλες τις χώρες του κόσμου.

Εκτός από τις Αρχές και Δράσεις, η Υποομάδα ίδρυσε ένα δίκτυο επικοινωνίας, το οποίο λειτουργούσε όλο το εικοσιτετράωρο, επτά ημέρες την εβδομάδα[83], με αποστολή τη

---

[80] United Nations Manuals on the prevention and control of Computer Related crime http://www.uncjin.org/Documents/EighthCongress.html (Ημερομηνία πρόσβασης:19/08/09)

[81] Η Ομάδα των Οκτώ, είναι ένας οργανισμός που αποτελείται από τις οκτώ οικονομικά ισχυρότερες χώρες του κόσμου: Γαλλία, Γερμανία, Ιταλία, Ιαπωνία, Μεγάλη Βρετανία, Ρωσία, Καναδάς και Η.Π.Α. Οι χώρες αυτές αντιπροσωπεύουν το 65% της παγκόσμιας οικονομίας.

[82] Οι Αρχές και Δράσεις, είναι διαθέσιμες στην διεύθυνση http://www.jya.com/g8crime-doj.htm#action (Ημερομηνία πρόσβασης: 19/08/09)

[83] 24-Hour-Contact-Group http://www.jya.com/g8-charney.htm (Ημερομηνία πρόσβασης: 08/09/09)

συνεργασία μεταξύ των χωρών σε επίπεδο ερευνών για εγκλήματα υψηλής τεχνολογίας. Στο δίκτυο επικοινωνίας συμμετέχουν σήμερα πάνω από σαράντα χώρες.[84]

6.4. Η Ευρώπη απέναντι στο ηλεκτρονικό έγκλημα

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 Εγκληματολογικές 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 συμπεράσματα της συμπεριλήφθησαν στη Σύσταση του 1989, η οποία όριζε εγκληματικές 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 περιλάμβανε 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 νομοθεσίας για το ηλεκτρονικό έγκλημα το 1996, εκδίδοντας δύο Συστάσεις α) τη Σύσταση No R(89)9 σχετικά με το έγκλημα που διαπράττεται με τη χρήση ηλεκτρονικού υπολογιστή και την β) τη Σύσταση No R(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 το Κυβερνοχώρο του 2001[85]

6.4.1. Η Σύμβαση για τον Κυβερνοχώρο[86]

Οι εργασίες για τη δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο (Convention on Cybercrime) ξεκίνησαν το 1997, όταν συστήθηκε μια επιτροπή ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με σκοπό να εξετάσει τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα, που αναπτύσσεται και συνεχώς διευρύνεται στον κυβερνοχώρο. Αν και αρχικά η περαίωση των εργασιών της επιτροπής, είχε προσδιοριστεί για το 1999, τα ιδιαίτερα προβλήματα που συνάντησαν τα μέλη της, έθεσαν νέα προθεσμία το έτος 2000.

Τελικά, το κείμενο της «Σύμβασης για το Έγκλημα στον Κυβερνοχώρο», υπογράφηκε στις 23 Νοεμβρίου 2001, στη Βουδαπέστη, από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου και από τις Ηνωμένες Πολιτείες, τον Καναδά, την Νότιο Αφρική και την Ιαπωνία.

---

[84] Η λειτουργία του δικτύου αυτού, συνεχίζεται στα πλαίσια εφαρμογής της Συνθήκης για το Κυβερνοχώρο που παρουσιάζεται στην επόμενη ενότητα. Η Ομάδα των Οκτών, προτρέπει όλες τις χώρες του κόσμου , να υιοθετήσουν τις αρχές που θέτει η Σύμβαση για το Κυβερνοχώρο, για την ενιαία αντιμετώπιση του ηλεκτρονικού εγκλήματος και της τρομοκρατίας. Βλ. σχετικά
http://www.usdoj.gov/ag/events/g82004/Communique_2004_G8_JHA_Ministerial_051204.pdf
(Ημερομηνία πρόσβασης: 19/08/09)

[85] Akdeniz,Y. 2004 (Ημερομηνια πρόσβασης: 20/08/09)

[86] http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (Ημερομηνία πρόσβασης: 23/08/09)

Η σύμβαση έχει υπογραφεί ως σήμερα από τις ακόλουθες χώρες:
2001: Αλβανία, Αρμενία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρος, Εσθονία, Φιλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ισλανδία, Ιταλία, Μολδαβία, Ολλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Ισπανία, Σουηδία, Ελβετία, Σκόπια, Ουκρανία, Αγγλία, Καναδάς, Ιαπωνία, Νότια Αφρική, Ηνωμένες Πολιτείας Αμερικής.
2002: Ιρλανδία, Μάλτα, Σλοβενία
2003: Δανία, Λιθουανία, Λουξεμβούργο
2004: Λετονία
2005: Βοσνία-Ερζεγοβίνη, Τσεχία, Σερβία, Σλοβακία, Μαυροβούνιο.

Η Σύμβαση έχει, ως στόχο, την εναρμόνιση των εθνικών νομοθεσιών, σχετικά με το ηλεκτρονικό έγκλημα και την παροχή νομοθετικού πλαισίου στον τομέα του δικονομικού δικαίου για την διερεύνηση και δίωξη εγκλημάτων, που σχετίζονται με τον κυβερνοχώρο. Επιχειρεί, επίσης, να θέσει τις βάσεις για άμεση και αποτελεσματική διεθνή συνεργασία για τα ηλεκτρονικά εγκλήματα. Το κείμενο της Σύμβασης χωρίζεται σε τέσσερα κεφάλαια:

Στο πρώτο κεφάλαιο, παρατίθενται οι όροι που χρησιμοποιούνται στη Σύμβαση. Δεν επιχειρήθηκε να καταρτίσει ένας μεγάλος κατάλογος όρων. Περιλήφθησαν μόνο τέσσερις: υπολογιστικό σύστημα(computer system), ηλεκτρονικά δεδομένα (computer data), παροχέας υπηρεσιών (service provider) και μεταδιδόμενα δεδομένα (traffic data). Πιθανώς, οι συντάκτες αντιλήφθησαν ότι ένας μεγάλος κατάλογος ορών θα ήταν ανούσιος, αναλογιζόμενοι τις ραγδαίες τεχνολογικές εξελίξεις, που σύντομα θα καθιστούσαν τη σχετική ορολογία ελλιπή και ανίσχυρη.

Το δεύτερο κεφάλαιο της Σύμβασης ορίζει τα νομοθετικά μέτρα, που θα πρέπει να ληφθούν σε εθνικό επίπεδο, για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Χωρίζεται σε τρία μέρη : Στο πρώτο μέρος, καθορίζονται τέσσερις βασικές μορφές του ηλεκτρονικού εγκλήματος:

Α) Αδικήματα ενάντια στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων

1. Παράνομη πρόσβαση (Illegal Acces)

Σύμφωνα με το άρθρο 2 της Σύμβασης, ποινικοποιείται η από πρόθεση πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα. Το αδίκημα διαπράττεται με την παραβίαση των μέτρων ασφαλείας με σκοπό την απόκτηση ηλεκτρονικών δεδομένων.

2. Αθέμιτη παγίδευση- Υποκλοπή (Illegal interception)

Συμφώνα με το άρθρο 3 της Συμβάσεως , καθίσταται παράνομη η από πρόθεση, παγίδευση- υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σε ένα σύστημα υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που «μεταφέρει» τέτοια στοιχεία.

Η διάταξη αυτή, μπορεί να εφαρμοστεί σε κάθε μορφή υποκλοπής ηλεκτρονικών δεδομένων, είτε αυτά διακινούνται μέσω του κυβερνοχώρου με μεταφορά αρχείων, είτε με ηλεκτρονικό ταχυδρομείο, ή τηλεομοιοτυπία.

3. Επέμβαση σε δεδομένα (Data interference)

Ως επέμβαση σε δεδομένα, νοείται η από πρόθεση καταστροφή, διαγραφή, χειροτέρευση, μεταβολή ή απόκρυψη δεδομένων χωρίς δικαίωμα.

4. Επέμβαση σε σύστημα (System Interference)

Ως επέμβαση σε σύστημα θεωρείται η από πρόθεση σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση, μεταφορά, καταστροφή, διαγραφή, χειροτέρευση, μεταβολή, ή απόκρυψη δεδομένων χωρίς δικαίωμα.

5. Κακή χρήση συσκευών (Misuse of devises)

Σύμφωνα με το άρθρο 6 της Συμβάσεως, απαγορεύεται η από πρόθεση και χωρίς δικαίωμα παραγωγή, πώληση, προετοιμασία για χρήση, εισαγωγή, διανομή ή με οποιαδήποτε άλλο τρόπο διάθεση μιας συσκευής, συμπεριλαμβανομένου προγράμματος υπολογιστή, που έχει σχεδιαστεί ή προσαρμοστεί με σκοπό, τη διάπραξη οποιουδήποτε από τα αδικήματα που περιγράφονται στα άρθρα 2-5 της Συμβάσεως.

Β) Αδικήματα σχετικά με τους ηλεκτρονικούς υπολογιστές

1. Πλαστογραφία σχετιζόμενη με ηλεκτρονικούς υπολογιστές (Computer related Forgery)

Αυτό το αδίκημα διαπράττει όποιος με πρόθεση και χωρίς δικαίωμα προβαίνει στην εισαγωγή, μεταβολή, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικών υπολογιστών, με σκοπό τα δεδομένα αυτά να θεωρούνται ή να χρησιμοποιούνται για νόμιμους σκοπούς, σαν να ήταν αυθεντικά.

2. Απάτη σχετιζόμενη με ηλεκτρονικούς υπολογιστές (Computer-related Fraud)

Αυτό το αδίκημα διαπράττει όποιος με πρόθεση και χωρίς δικαίωμα, προκαλεί απώλεια περιουσίας σε κάποιον άλλον με οποιαδήποτε εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικού υπολογιστή, με σκοπό να επιφέρει οικονομικό όφελος στον εαυτό του ή σε άλλον.

Γ) Αδικήματα σχετικά με το περιεχόμενο

Το άρθρο 9 της Συμβάσεως, ασχολείται αποκλειστικά, με το αδίκημα της διακίνησης πορνογραφικού υλικού μέσω του Διαδικτύου. Θεωρείται παράνομη η από πρόθεση:

- Παραγωγή υλικού παιδικής πορνογραφίας, με σκοπό την διακίνηση πορνογραφικού υλικού με τη χρήση ηλεκτρονικού υπολογιστή.
- Προσφορά ή διακίνηση υλικού παιδικής πορνογραφίας, με τη χρήση ηλεκτρονικού υπολογιστή

- Απόκτηση υλικού παιδικής πορνογραφίας, με τη χρήση ηλεκτρονικού υπολογιστή για ιδία χρήση ή για χρήση άλλου ατόμου.
- Κατοχή υλικού παιδικής πορνογραφίας, αποθηκευμένου σε ηλεκτρονικό υπολογιστή η οποιαδήποτε άλλη μονάδα αποθήκευσης δεδομένων.

Ο όρος παιδική πορνογραφία περιλαμβάνει υλικό, στο οποίο απεικονίζεται ανήλικος ή άτομο που εμφανίζεται ως ανήλικος και συμμετέχει σε σεξουαλικές επαφές καθώς επίσης και φωτογραφικό υλικό που απεικονίζει παρόμοιο περιεχόμενο. Ως ανήλικος θεωρείται αυτός που δεν έχει συμπληρώσει το 18^{ο} έτος της ηλικίας του.

Δ) Αδικήματα σχετικά με την πνευματική ιδιοκτησία και συναφή δικαιώματα

Το άρθρο 10 προστατεύει την πνευματική ιδιοκτησία και τα συναφή δικαιώματα για τα οποία παραπέμπει στη Σύμβαση της Βέρνης, αλλά και την Πράξη των Παρισίων.

Το άρθρο 13 αναφέρεται στις ποινές που θα πρέπει να επιβάλλονται στους παραβάτες των παραπάνω διατάξεων. Ειδικότερα, προτείνεται να επιβάλλονται αυστηρές κυρώσεις όπως στερητικές της ελευθερίας ποινές για μεμονωμένα άτομα σε συνδυασμό με χρηματικές ποινές, ιδιαίτερα στις περιπτώσεις που τα αδικήματα τελούνται από νομικά πρόσωπα.

Στο δεύτερο μέρος καθορίζονται οι δικονομικές διατάξεις σχετικά με τη δίωξη του ηλεκτρονικού εγκλήματος. Οι πιο σημαντικές διατάξεις αναφέρονται:

α) Στην υποχρέωση όσων υπογράψουν και θέσουν σε ισχύ τη σύμβαση, να προστατεύουν τα ανθρώπινα δικαιώματα και ελευθερίες, συμπεριλαμβανόμενων και των υποχρεώσεών τους που απορρέουν από 1) τη Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των Ανθρωπίνων Δικαιωμάτων και θεμελιωδών Ελευθεριών (1950), 2) το διεθνές σύμφωνο των Ηνωμένων Εθνών για τα Αστικά και Πολιτικά Δικαιώματα (Άρθρο 15).

β) Στην υποχρέωση ενός ατόμου, κατόπιν παραγγελίας των αρμοδίων διωκτικών αρχών, να διατηρεί δεδομένα, που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του για όσο χρονικό διάστημα απαιτείται, (το οποίο όμως δεν μπορεί να υπερβαίνει τις 90 ημέρες) προκειμένου να βοηθήσουν η σχετικές έρευνες και

γ) Στη δυνατότητα των διωκτικών αρχών να έχουν πρόσβαση και δυνατότητα αναζήτησης δεδομένων, που είναι αποθηκευμένα σε ένα σύστημα Η/Υ ή σε φορητά μέσα, όπως, επίσης, να υποχρεώσουν ένα άτομο που κατέχει ειδικές γνώσεις για τη διατήρηση των δεδομένων σε ένα Η/Υ, να παράσχει στις διωκτικές αρχές όλες τις απαραίτητες πληροφορίες (Άρθρο 19).

Το τρίτο μέρος αναφέρεται στο ζήτημα της δικαιοδοσίας (άρθρο 22) η οποία ορίζεται από το γεωγραφικό χώρο κάθε χώρας και επεκτείνεται στα πλοία που φέρουν τη σημαία της και τα αεροσκάφη, τα οποία υπόκεινται στους νόμους της. Η προσωπική δικαιοδοσία εφαρμόζεται, όταν το διαπραττόμενο έγκλημα τιμωρείται με τους νόμους της χώρας στην οποία διαπράχθηκε ή όταν διαπράχθηκε σε τόπο που δεν εφαρμόζεται καμιά δικαιοδοσία. Η εφαρμογή των ανωτέρω κανόνων, επαφίεται στην ελεύθερη κρίση κάθε χώρας, η οποία δύναται να εφαρμόσει και την εθνική της νομοθεσία. Σε περίπτωση που μπορεί να τύχουν εφαρμογής παραπάνω από μια δικαιοδοσία, η καταλληλότερη καθορίζεται κατόπιν συνεννόησης των εμπλεκόμενων μερών.

Το τρίτο κεφάλαιο, προσεγγίζει στο ζήτημα της διεθνούς συνεργασίας. Στο άρθρο 24 θίγεται το ζήτημα της έκδοσης, για το οποίο προβλέπεται η επιβολή της μικρότερης ποινής, που επιβάλλεται για ένα αδίκημα σε δύο χώρες, εφόσον απαιτηθεί η έκδοση του κατηγορουμένου από την μία στην άλλη. Το άρθρο 25, αναφέρεται στην υποχρέωση για αμοιβαία συνεργασία κατά το μεγαλύτερο δυνατό, για την διευκόλυνση των ερευνών για ηλεκτρονικά εγκλήματα. Το άρθρο 29 υποχρεώνει μια χώρα να διατηρήσει δεδομένα, αποθηκευμένα σε Η/Υ ή άλλα μέσα, εφόσον της ζητηθεί από άλλη χώρα, για τα οποία αναμένεται να υποβληθεί αίτημα για πρόσβαση και έρευνα. Στο τελευταίο άρθρο της ενότητας αυτής (άρθρο 35) προβλέπεται η δημιουργία ενός κέντρου επικοινωνίας, σχετικά με την έρευνα του ηλεκτρονικού εγκλήματος, το οποίο θα λειτουργεί 24 ώρες το 24ωρο, επτά ημέρες την εβδομάδα, με κύριες αρμοδιότητες την παροχή τεχνικών συμβούλων, τη διατήρηση δεδομένων, που προβλέπονται από τη σύμβαση, τη συλλογή δεδομένων, την παροχή νομικών πληροφοριών και τον εντοπισμό υπόπτων.

Στο τέταρτο και τελευταίο μέρος, περιλαμβάνονται οι τελικές διατάξεις, σχετικά με τον χρόνο στον οποίο θα τεθεί σε ισχύ η σύμβαση, η γεωγραφική εφαρμογή της, η ακολουθούμενη διαδικασία που θα απαιτηθεί για πιθανή τροποποίησή της στο μέλλον και άλλες διατάξεις.

Το κυρίως κείμενο της Σύμβασης για το Κυβερνοχώρο, συνοδεύεται και από μια Επεξηγηματική Αναφορά[87] (Explanatory Report), στην οποία αναλύονται όλα τα άρθρα της Σύμβασης, παρέχοντας συμπληρωματικές πληροφορίες, καθώς και αιτιολόγηση των επιλογών των συντακτών της Σύμβασης, για συγκεκριμένες διατάξεις που περιλήφθηκαν.

Τέλος, η Σύμβαση συμπληρώθηκε το 2002 από ένα Πρόσθετο Πρωτόκολλο, σχετικά με την Ποινικοποίηση Πράξεων Ρατσισμού και Ξενοφοβίας που διαπράττονται μέσω ηλεκτρονικού υπολογιστή. Σχετικές διατάξεις για το θέμα αυτό δεν είχαν περιληφθεί στο τελικό κείμενο της αρχικής Σύμβασης, λόγω της πολυπλοκότητας του ζητήματος. Το Πρόσθετο Πρωτόκολλο, προτρέπει όσους το υπογράψουν να το θέσουν σε ισχύ, να υιοθετήσουν τέτοια νομοθετικά μέτρα ώστε να ποινικοποιηθεί:

1) η διάδοση ρατσιστικού και ξενοφοβικού υλικού, με τη χρήση ηλεκτρονικών υπολογιστών,
2) η διάδοση ρατσιστικών και ξενοφοβικών απειλών ή υβριστικών συνθημάτων, μέσω τέτοιων συστημάτων και
3) η χρησιμοποίηση τέτοιων συστημάτων, για τη διάδοση υλικού το οποίο αρνείται, ελαχιστοποιεί, εγκρίνει ή δικαιολογεί πράξεις γενοκτονίας ή εγκλημάτων ενάντια στην ανθρωπότητα, όπως αυτά ορίζονται από τη διεθνή νομοθεσία.

6.4.2. Κριτική Αξιολόγηση της Σύμβασης

Αν και η Σύμβαση για το Κυβερνοχώρο είχε χαρακτηριστεί από πολλούς ως το πιο σημαντικό βήμα που έγινε παγκόσμιος για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, δεν λείπουν οι επικριτές της, που έθεσαν νέους προβληματισμούς, για το κατά πόσο μια τέτοια Σύμβαση μπορεί να εφαρμοστεί ευρέως και αν αυτό συμβεί, κατά πόσο μπορεί στην πράξη να βοηθήσει στη δίωξη του ηλεκτρονικού εγκλήματος.

---

[87] Το πλήρες κείμενο, είναι διαθέσιμο στην διεύθυνση
http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (Ημερομηνία πρόσβασης: 20/08/09)

Η Jones (2005)[88] υποστηρίζει ότι η Σύμβαση δεν μπορεί να εφαρμοστεί παγκοσμίως, καθότι, ναι μεν είναι ανοιχτή προς υπογραφή σε μη μέλη του Συμβουλίου της Ευρώπης,, η προσχώρηση όμως των κρατών αυτών, μπορεί να πραγματοποιηθεί, εφόσον συμφωνήσουν τα κράτη- μέλη του Συμβουλίου, διαδικασία ιδιαίτερα χρονοβόρα. Επιπλέον, πολλά από τα εγκλήματα που προβλέπονται, τιμωρούνται ήδη από τη διεθνή νομοθεσία (π.χ. πορνογραφία), για το λόγο αυτό δεν θα έπρεπε να περιληφθούν στη Σύμβαση, η οποία έπρεπε να περιοριστεί μόνο στα « γνήσια εγκλήματα» του κυβερνοχώρου. Ακόμη, εκφράζει τους προβληματισμούς της σχετικά με την αδυναμία μικρών χώρων να εφαρμόζουν όσα αναφέρονται στη Σύμβαση, την αναξιόπιστη προστασία της ιδιωτικότητας και των ανθρωπίνων δικαιωμάτων και τη μη πρόβλεψη του κόστους που προκαλείται για τους παρόχους υπηρεσιών Διαδικτύου από την υποχρέωση τους για διατήρηση συγκεκριμένων δεδομένων. Για όσα από τα παραπάνω θέματα, καθώς και πολλά άλλα, υπάρχουν περαιτέρω οδηγίες στην Επεξηγηματική Αναφορά, η Jones υποστηρίζει ότι αυτή δεν είναι δεσμευτικό νομοθετικό κείμενο, παρά μόνο συμβουλευτικό.

Ο Hopkins (2003) πιστεύει ότι η Σύμβαση δεν περιέχει λεπτομερείς διατάξεις και διαδικασίες, για τη δίωξη του ηλεκτρονικού εγκλήματος. Επικεντρώνει την κριτική του σε τέσσερα βασικά στοιχεία:

- Οι ορισμοί, που δίνονται στο πρώτο κεφάλαιο της Σύμβασης, έχουν ευρεία έννοια με αποτέλεσμα να είναι ασαφείς, αδυνατώντας να προσδιοριστούν τι είδους επαφή συνάγει με συγκεκριμένο όρο. Για παράδειγμα, ο ορισμός του ηλεκτρονικού υπολογιστή είναι τόσο ευρύς, με αποτέλεσμα να μπορούν να θεωρήσουν ως υπολογιστές συσκευές, όπως παιδικά παιχνίδια και μονάδες καλωδιακής τηλεόρασης.
- Ο κατάλογος με τα εγκλήματα που περιλαμβάνονται στο δεύτερο κεφάλαιο, δεν καθορίζει, επακριβώς τα συστατικά στοιχεία κάθε παράνομης δραστηριότητας. Ως αποτέλεσμα, ενδέχεται από χώρα σε χώρα, να διαφέρουν οι επιμέρους διατάξεις, που θα θεσμοθετηθούν για τη δίωξη συγκεκριμένης παράνομης συμπεριφοράς. Το πρόβλημα αυτό, εκτείνεται και στον τομέα της διεθνούς συνεργασίας, η οποία δεν θα είναι εφικτή στην περίπτωση που μια συμπεριφορά αποτελεί έγκλημα σε μια χώρα και όχι σε κάποια άλλη.
- Η Σύμβαση δεν περιλαμβάνει διαδικασίες για την έρευνα και δίωξη του ηλεκτρονικού εγκλήματος. Οι συντάκτες σκόπιμα δεν συμπεριέλαβαν συγκεκριμένες διατάξεις, σεβόμενοι το νομικό σύστημα αλλά και την κουλτούρα κάθε χώρας, στην πράξη όπως προκύπτουν πολλά προβλήματα. Για παράδειγμα, χώρες με διαφορετική νομοθεσία για τα ανθρώπινα δικαιώματα και την προστασία προσωπικών δεδομένων, δεν θα μπορούσαν να ανταλλάξουν πληροφορίες για παράνομη δραστηριότητα στο Διαδίκτυο.
- Το θέμα της δικαιοδοσίας αντιμετωπίζεται επιφανειακά, αφήνοντας την επίλυση τέτοιων ζητημάτων στις εθνικές νομοθεσίες και τη μεταξύ των χωρών συνεργασία.

Η κριτική που ασκήθηκε είναι φυσιολογική και αναμενόμενη, λαμβάνοντας υπόψη, ότι ένα νομοθετικό κείμενο για ένα τόσο περίπλοκο ζήτημα, όπως το ηλεκτρονικό έγκλημα, δεν είναι δυνατό να επιτύχει την απόλυτη συναίνεση όλων των μερών, από την στιγμή που επιζητά παγκόσμια εφαρμογή. Περιθώρια βελτίωσης σίγουρα υπάρχουν, καθώς κανένας νόμος οπουδήποτε στο κόσμο δεν είναι τέλειος. Όμως, η συμμετοχή πολλών κρατών στη σύνταξη του κειμένου της Σύμβασης και μάλιστα με τη βοήθεια και

[88] Κωνσταντίνος Βλαχόπουλος 2007 σελ.143

συμμετοχή των Ηνωμένων Πολιτειών της Αμερικής, υποδηλώνει ότι για τη Σύμβαση έχει πράγματι επιτευχθεί η, όσο το δυνατόν, ευρύτερη παγκόσμια συναίνεση.

6.5. Η ισχύουσα στην Ελλάδα νομοθεσία για το Ηλεκτρονικό έγκλημα.

Στην ελληνική νομοθεσία, δεν υπάρχουν ειδικές διατάξεις για τα ηλεκτρονικά εγκλήματα. Ο όρος, «ηλεκτρονικό έγκλημα», δεν αναφέρεται πουθενά στο ελληνικό δίκαιο. Οι περισσότερες υποθέσεις που έχουν προκύψει μέχρι σήμερα, έχουν διωχθεί με τις διατάξεις του Ν.1805/1988, ο οποίος πρόσθεσε τα άρθρα 370Β, 370Γ και 386Α στον Ποινικό Κώδικα, τα οποία αναφέρονται στα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές. Επίσης το άρθρο 370Α αναφέρεται στην παραβίαση του απορρήτου των τηλεφωνημάτων και το άρθρο 348Α στην πορνογραφία ανηλίκων.[89]

Τα άρθρα αυτά του Ποινικού Κώδικα δεν επαρκούν για να καλύψουν τις ανάγκες δίωξης των σύγχρονων ηλεκτρονικών εγκλημάτων, κυρίως γιατί δεν έχουν προβλέψει την ύπαρξη του Διαδικτύου. Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης, δεν μπορούν να τιμωρηθούν με βάση το ισχύον νομοθετικό πλαίσιο.

Όπως συμβαίνει και σε πολλές άλλες χώρες, το κενό στην νομοθεσία για τα ηλεκτρονικά εγκλήματα, αντιμετωπίζεται με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, η οποία προσαρμόζεται στο εικονικό κόσμο του Διαδικτύου, θεωρώντας το, ως ένα άμεσο μέσο για την διάπραξη εγκλημάτων.

Ειδικότερες διατάξεις για θέματα, που σχετίζονται με το ηλεκτρονικό έγκλημα, περιλαμβάνονται μόνο στο Π.Δ. 131/2003, το οποίο θεσπίστηκε σε εφαρμογή κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο και αναφέρεται στην ανεπιθύμητη αλληλογραφία και στην ευθύνη των παροχών υπηρεσιών Διαδικτύου για πράξεις των χρηστών τους. Επίσης, ο Ν.2867/2000 για την «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών», οι Ν.2774/99 και 2472/97 «περί προσωπικών δεδομένων» και ο Ν.2225/94 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας» προσεγγίζουν κάποιες πτυχές του ηλεκτρονικού εγκλήματος.

Αν και η χώρα μας έχει υπογράψει την Ευρωπαϊκή Σύμβαση για το έγκλημα στο Κυβερνοχώρο, δεν την έχει θέσει ακόμη σε ισχύ. Η θέση, σε ισχύ της Σύμβασης θα καλύψει ένα πολύ μεγάλο κενό της ελληνικής νομοθεσίας, όχι μόνο, στον τομέα του Ποινικού αλλά και του Δικονομικού Δικαίου.

---

[89] Βλ.το πλήρες κείμενο των άρθρων 348Α, 370Α, 370Β, 370Γ και 386Α στο παράρτημα Β'.

7. ΔΙΕΡΕΥΝΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ. ΕΡΓΑΛΕΙΑ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΕΣ

7.1.Εισαγωγή

Η διερεύνηση του εγκλήματος από τις αρμόδιες αρχές, έχει ως σκοπό, την ανακάλυψη του δράστη και την νομική και επιστημονική τεκμηρίωση της υπόθεσης, προκειμένου να καταστεί δυνατή η απόδειξη της αλήθειας. Με το πέρασμα των χρόνων, τα μέσα διάπραξης του εγκλήματος μεταβάλλονται. Η τεχνολογική εξέλιξη αποτελεί σύμμαχο των κακοποιών, οι οποίοι χρησιμοποιούν την τεχνολογία για την πραγμάτωση των εγκληματικών τους προθέσεων. Παράλληλα όμως, η τεχνολογία έχει συνδράμει και στο έργο των διωκτικών αρχών, οι οποίες χρησιμοποιούν νέους μεθόδους διερεύνησης των εγκλημάτων, που βοηθούν στην ανεύρεση των ενόχων.

Η Εγκληματολογική Επιστήμη (Forensic Science), ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο, ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία. Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες της επιστήμης αυτής.

Πολλές φορές έχει αναφερθεί, ότι οι Η/Υ συμμετέχουν, ποικιλοτρόπως, στο εγκληματικό φαινόμενο. Τα υπολογιστικά συστήματα μπορούν να χρησιμοποιηθούν για την διάπραξη εγκλημάτων, να περιέχουν πληροφορίες για το έγκλημα ή να αποτελούν το στόχο του εγκλήματος. Οι αρμόδιες διωκτικές αρχές για να εξιχνιάσουν ένα έγκλημα, στο οποίο συμμετέχει με οποιαδήποτε μορφή ένας, Η/Υ, θα πρέπει να εξετάσουν τις πληροφορίες που βρίσκονται αποθηκευμένες σε αυτόν και σε άλλα φορητά μέσα αποθήκευσης ή διακινούνται σε ένα δίκτυο.

Η Ηλεκτρονική Εγκληματολογία (Computer Forensic Science), είναι « η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό». Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε ένα υπολογιστή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπιστούν αποδείξεις, αλλά και να τις συγκεντρώσουν με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορούμενου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατάστρεψε αποδείξεις σχετικά με την αθωότητα του κατηγορουμένου.

7.2. Ψηφιακές αποδείξεις και δεδομένα

Οι ψηφιακές αποδείξεις αποτελούν το πιο σπουδαίο αποδεικτικό μέσο, κατά την εξέταση μιας υπόθεσης ηλεκτρονικού εγκλήματος και γενικά κατά την εξέταση οποιουδήποτε στοιχείου έχει ψηφιακή μορφή. Ο SWGDE[90] (Scientific Working Group on Digital

[90] www.swgde.org (Ημερομηνία πρόσβασης: 24/08/09)

Evidence), μια κοινοπραξία διεθνών οργανισμών, που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή, διαχωρίζοντας τις σε :

- **Ψηφιακές αποδείξεις (digital evidence):** Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.
- **Αντικείμενα δεδομένων (data objects):** Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.
- **Φυσικά αντικείμενα (physical items):** τα φυσικά μέσα όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.
- **Γνήσιες ψηφιακές αποδείξεις (original digital evidence):** φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.
- **Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence):** Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
- **Αντίγραφο(copy):** Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό,

Οι ψηφιακές αποδείξεις μπορεί να είναι αποθηκευμένες σε οποιαδήποτε συσκευή, όπως ηλεκτρονικό υπολογιστή, palmtop, κινητό τηλέφωνο κ.ά., καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως δισκέτες, CDs, DVDs, κάρτες μνήμης κ.ά.

Βασικό χαρακτηριστικό των ψηφιακών αποδείξεων είναι ο μεγάλος βαθμός μεταβλητότητας τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν με τη χρήση διάφορων εργαλείων και μεθόδων. Ο ερευνητής, λοιπόν, πρέπει να αναζητεί και να μεταχειρίζεται τις πληροφορίες αυτές με ιδιαίτερη δεξιότητα.

Οι ψηφιακές αποδείξεις αποτελούνται από ψηφιακά δεδομένα. Μια πολύ σημαντική διάκριση των ψηφιακών δεδομένων είναι σε μεταβλητά δεδομένα και σε διαρκή δεδομένα. Τα μεταβλητά, είναι δεδομένα που αποθηκεύονται στην μνήμη του συστήματος (π.χ. μητρώο συστήματος, cache, μνήμη RAM) και χάνονται αν σταματήσει η τροφοδοσία του υπολογιστή με ρεύμα, αν γίνει τερματισμός της λειτουργίας του ή επανεκκίνηση. Τα διαρκή δεδομένα είναι αποθηκευμένα στους σκληρούς δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης, όπως οδηγοί USB, CDs και κάρτες μνήμης. Τα δεδομένα αυτά δεν χάνονται, όταν τερματιστεί η λειτουργία του υπολογιστή ή γίνει επανεκκίνηση. Κατά τη συλλογή των δεδομένων αυτών, χρησιμοποιούνται διαφορετικές τεχνικές, τις οποίες και θα εξετάσουμε στην συνέχεια.

7.3. Η έρευνα της σκηνής διάπραξης του εγκλήματος

Η έρευνα της σκηνής διάπραξης του εγκλήματος, αποτελεί το σημαντικότερο κομμάτι της προανακριτικής διαδικασίας, που διεξάγετε από τις αρμόδιες διωκτικές αρχές. Η χρήση τεχνολογικά εξελιγμένων εργαλείων από τις διωκτικές αρχές, έχει διευρύνει τις πληροφορίες, που μπορούν να αποκτηθούν και να αξιοποιηθούν από τη σκηνή διάπραξης του εγκλήματος. Για το λόγο αυτό, οι εξερευνητές πρέπει να διαθέτουν τις απαραίτητες γνώσεις και εμπειρία, προκειμένου να μην χαθούν πολύτιμα στοιχεία.

Ο ρόλος των εξερευνητών

Οι εξερευνητές κατέχουν ειδικότερες εξειδικευμένες γνώσεις για τη μεθοδολογία εξέτασης της σκηνής του εγκλήματος και τη συγκέντρωση του απαραίτητου, για περαιτέρω εξέταση, υλικού. Στην περίπτωση διαπράξεως ενός εγκλήματος, με το οποίο σχετίζεται με οποιονδήποτε τρόπο ένας Η/Υ ή παρόμοια συσκευή, ο εξερευνητής πρέπει να ακολουθήσει συγκεκριμένες διαδικασίες, προκειμένου να μην χαθούν ψηφιακά δεδομένα,

Βασικός κανόνας για τον εξερευνητή, όταν φτάσει στη σκηνή του εγκλήματος, είναι να εντοπίσει τις διάφορες συσκευές που περικλείονται στο χώρο. Ο εντοπισμός δεν περιορίζεται μόνο στους ηλεκτρονικούς υπολογιστές, αλλά περιλαμβάνει: λογισμικό, αποθηκευτικά μέσα πάσης φύσεως, γραπτές σημειώσεις, εγχειρίδια χρήσεως των συσκευών, περιφερειακές συσκευές κ.ά.

Εντοπίζοντας τις συσκευές, ο εξερευνητής θα ξεκινήσει την διαδικασία συλλογής των δεδομένων, που πιθανώς σχετίζονται με την υπόθεση. Πρώτη εργασία είναι η συλλογή των μεταβλητών δεδομένων. Τα μεταβλητά δεδομένα, στα οποία αναφερθήκαμε παραπάνω, είναι αυτά που βρίσκονται αποθηκευμένα στην μνήμη RAM και στην cache ενός συστήματος, και χάνονται όταν διακοπεί η τροφοδοσία του συστήματος με ρεύμα. Η συλλογή τους, μπορεί να γίνει με την χρήση κατάλληλων εργαλείων λογισμικού. Ορισμένα από τα εργαλεία αυτά, αναλύονται στην συνέχεια.

Η επόμενη εργασία είναι η συλλογή των διαρκών δεδομένων, αυτών δηλαδή που βρίσκονται αποθηκευμένα σε σκληρούς δίσκους. Συνηθίζεται τα δεδομένα αυτά, να αντιγράφονται στη σκηνή του εγκλήματος με την χρήση ενός λογισμικού imaging ή άλλου παρόμοιου εργαλείου. Τα αντίγραφα των σκληρών δίσκων ή άλλων συσκευών αποθήκευσης αποστέλλονται για αναλυτική εξέταση στο εργαστήριο, έχοντας ως εφεδρικά τα αρχικά αποθηκευτικά μέσα.

Η αποσύνδεση και συσκευασία των συσκευών είναι το βήμα, που ακολουθεί. Για τον τερματισμό ενός υπολογιστή, οι απόψεις διίστανται. Κάποιοι προτείνουν να γίνεται κανονικά με την διαδικασία που προβλέπεται για το υπό εξέταση λειτουργικό σύστημα, ενώ άλλοι υποστηρίζουν ότι ο τερματισμός πρέπει να γίνεται τραβώντας το καλώδιο από την πρίζα, προκειμένου να αποφευχθεί το ενδεχόμενο διαγραφής δεδομένων κατά τον τερματισμό του υπολογιστή. Η επιλογή της κατάλληλης μεθόδου έγκειται στην εμπειρία και την γενικότερη εκτίμηση της κατάστασης από τον εξερευνητή.

Η αποσύνδεση των καλωδίων του υπολογιστή πρέπει, επίσης, να γίνεται με επιμέλεια. Όλα τα καλώδια και οι συνδέσεις τους θα πρέπει να καταγραφούν με ιδιαίτερη προσοχή. Καλό θα ήταν να φωτογραφηθούν ή να βιντεοσκοπηθούν οι συνδέσεις, προκειμένου να μην γίνει κάποιο λάθος κατά την επανασύνδεση των μηχανημάτων.

Τέλος, η μεταφορά των υλικών θα πρέπει να πραγματοποιηθεί, αφού προηγουμένως έχουν συσκευαστεί κατάλληλα για να αποφευχθούν φθορές κατά την μεταφορά. Τα ψηφιακά δεδομένα είναι ευαίσθητα σε μαγνητικά πεδία, υψηλές θερμοκρασίες και υγρασία. Οι παράγοντες αυτοί, θα πρέπει να ληφθούν σοβαρά υπόψη κατά την μεταφορά τους αλλά και την αποθήκευση τους.

7.4. Οι μέθοδοι εξέτασης των ψηφιακών τεκμηρίων

Η εργαστηριακή εξέταση των ψηφιακών αποδείξεων που συλλέγονται από τη σκηνή διάπραξης του εγκλήματος, είναι μια από τις σημαντικότερες εργασίες της προανακριτικής διαδικασίας. Τα ιδιαίτερα χαρακτηριστικά των ψηφιακών αποδείξεων, όπως για παράδειγμα μεγάλος βαθμός μεταβλητότητας, απαιτούν την εφαρμογή ειδικών τεχνικών για τη συλλογή πληροφοριών με αποδεικτική αξία.

7.4.1. Ανάκτηση διαγεγραμμένων δεδομένων

Στα λειτουργικά συστήματα της Microsoft, η διαγραφή ενός αρχείου σημαίνει την μεταφορά του στον Κάδο Ανακύκλωσης. Από εκεί, είναι δυνατή η επαναφορά του αρχείου στην αρχική του θέση ή η οριστική διαγραφή του. Πολλοί χρήστες ηλεκτρονικών υπολογιστών, ακόμη και έμπειροι, πιστεύουν ότι διαγράφοντας ένα αρχείο από τον Κάδο Ανακύκλωσης, χάνεται οριστικά. Ωστόσο, η διαγραφή δεν επηρεάζει το αποθηκευμένο αρχείο, που παραμένει αποθηκευμένο έως ότου ένα καινούριο αρχείο εγγραφεί στον ίδιο αποθηκευτικό χώρο.

Τα αρχεία, σε ένα σκληρό δίσκο, αποθηκεύονται σε συστοιχίες, οι οποίες είναι μονάδες αποτελούμενες από ένα συγκεκριμένο αριθμό bits. Κάθε αρχείο μπορεί να είναι αποθηκευμένο σε πολλές συστοιχίες, διάσπαρτες στην επιφάνεια του δίσκου. Η θέση των συστοιχιών, προσδιορίζεται από ένα δείκτη που χρησιμεύει για την ανάκληση του αρχείου. Ο δείκτης είναι αποθηκευμένος σε ένα μέρος του δίσκου, που ονομάζεται Κύριος Πίνακας Αρχείων (Master File Table – MFT)[91]. Όταν διαγράφεται ένα αρχείο δεν διαγράφονται τα ψηφιακά δεδομένα που το αποτελούν. Το σύστημα διαχείρισης αρχείων, επεμβαίνει στο δείκτη του αρχείου, ο οποίος επισημάνει τις συστοιχίες στις οποίες παραπέμπει, ως διαθέσιμο χώρο (unallocated space), που σημαίνει ότι στις συστοιχίες αυτές μπορεί να αποθηκευτεί ένα νέο αρχείο. Αν ο σκληρός δίσκος έχει μεγάλη χωρητικότητα, ενδέχεται να περάσει πολύ χρονικό διάστημα ώσπου να εγγραφούν νέα αρχεία στο συγκεκριμένο διαθέσιμο χώρο και να σβήσουν τα παλιά. Το διαγραμμένο αρχείο εξακολουθεί να υπάρχει στο σκληρό δίσκο, δεν μπορεί όμως να το εντοπίσει το λειτουργικό σύστημα.[92]

Η ανάκτηση των αρχείων αυτών, είναι δυνατή με τη χρήση μιας σειράς από εργαλεία λογισμικού, που κυκλοφορούν στο εμπόριο. Σε κάποια από αυτά θα αναφερθούμε στη συνέχεια.

7.4.2. Ανάκτηση κρυπτογραφημένων δεδομένων

Η κρυπτογράφηση, εκτός από εργαλείο ασφάλειας των πληροφοριακών συστημάτων, αποτελεί ταυτόχρονα και βασικό εργαλείο των ηλεκτρονικών εγκλημάτων, για την απόκρυψη της παραβατικής συμπεριφοράς τους. Δεδομένα, που εμπεριέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, συμπιεσμένους φακέλους, αρχεία PDF,

---

[91] Οι πληροφορίες αυτές ισχύουν για το σύστημα διαχείρισης αρχείων NTFS, που χρησιμοποιείται στα νεότερα λειτουργικά συστήματα της Microsoft και κυρίως στα Windows XP. Ωστόσο, οι τεχνικές που χρησιμοποιούνται για άλλα συστήματα αρχείων όπως το FAT είναι παρόμοιες.

[92] Η ανάκτηση αρχείων είναι επίσης δυνατή και από ένα σκληρό δίσκο που έχει διαμορφωθεί με την εντολή format. Η διαμόρφωση πάντα αφήνει κατάλοιπα αποθηκευμένων αρχείων, τα οποία μπορούν να ανακτηθούν.

λογιστικά φύλλα κ.λπ., ενδέχεται να έχουν κρυπτογραφηθεί. εφόσον περιέχουν σημαντικές πληροφορίες σχετικές με εγκληματική δραστηριότητα. Η ανάκτηση των δεδομένων αυτών, γίνεται με τη χρήση ειδικών πακέτων λογισμικού, που χρησιμοποιούν κυρίως τη μέθοδο της εξαντλητικής αναζήτησης (brute force). Τα προγράμματα αυτά, δοκιμάζουν όλους τους πιθανούς συνδυασμούς γραμμάτων, αριθμών και συμβόλων για να βρουν τον αλγόριθμο κρυπτογράφησης.[95]

7.4.3. Η ανάκτηση κρυφών δεδομένων

Η απόκρυψη δεδομένων στο σκληρό δίσκο ενός υπολογιστή είναι μια τεχνική, που χρησιμοποιείται πολύ συχνά από τους ηλεκτρονικούς εγκληματίες. Υπάρχουν πολλά σημεία στα οποία μπορούν να κρυφτούν δεδομένα σε ένα Η/Υ.

Μαγνητικοί δίσκοι

Οι σκληροί δίσκοι είναι χωρισμένοι σε τομείς (sectors), μεγέθους συνήθως 512 bytes, που αποτελούν και το μικρότερο κομμάτι στο οποίο μπορούμε να έχουμε πρόσβαση. Λόγω της κατασκευής των δίσκων, ενδέχεται να παραμείνει κάποιο κενό ανάμεσα στους τομείς (sector gap), στο οποίο μπορούν να αποθηκευτούν δεδομένα. Ορισμένες εφαρμογές ανάκτησης αρχείων έχουν την δυνατότητα να εντοπίζουν και να ανακτούν τα δεδομένα που είναι αποθηκευμένα σε αυτό το κενό.

Οι τομείς του σκληρού δίσκου ομαδοποιούνται σε συστοιχίες (clusters). Το μέγεθος κάθε συστοιχίας διαφέρει. Ένα αρχείο που αποθηκεύεται, δεν έχει ποτέ το ίδιο μέγεθος με τη συστοιχία στην οποία τοποθετείται. Ο κενός χώρος που απομένει, ονομάζεται slack area και σε αυτόν μπορεί να αποθηκευτούν διάφορα δεδομένα, η ανάκτηση των οποίων είναι δυνατή μόνο με την έρευνα του σκληρού δίσκου με εξειδικευμένα εργαλεία λογισμικού.

Τέλος, οι μηχανικές κεφαλές, που γράφουν στα μαγνητικά μέσα, δεν είναι πάντα απόλυτα στοιχισμένες και ευθυγραμμισμένες. Ενδέχεται, λοιπόν, ακόμη και όταν γράφονται δεδομένα σε ένα σκληρό δίσκο πάνω σε παλιά, να παραμείνουν κάποια δείγματα των παλιών αρχείων, τα οποία με τα κατάλληλα εργαλεία μπορούν να ανακτηθούν και να επανασυσταθούν.

Στενογραφικά δεδομένα

Η στενογραφία είναι μια τεχνική, με την οποία είναι δυνατόν να κρυφτούν δεδομένα μέσα σε άλλα δεδομένα. Η διαδικασία εντοπισμού των δεδομένων που έχουν στεγανογραφηθεί, ονομάζεται στεγανάλυση. Στο ψηφιακό περιβάλλον είναι δυνατή η ενσωμάτωση στεγανογραφικών δεδομένων σε αρχεία της μορφής jpg, gif, bmp, wav, voc, gz και txt. Η συχνότερα χρησιμοποιημένη μέθοδος, είναι η απόκρυψη ενός μηνύματος μέσα σε μια φωτογραφία. Αυτό επιτυγχάνεται με την αλλαγή στο ελάχιστο ενός εικονοστοιχείου (pixel), τέτοιας που δεν είναι δυνατόν να εντοπιστεί από το ανθρώπινο μάτι (για παράδειγμα το κόκκινο γίνεται ελάχιστα πιο ανοιχτό με την μεταβολή ενός δυαδικού ψηφίου στο συγκεκριμένο pixel). Αν λοιπόν σε μια φωτογραφία πραγματοποιηθούν μια σειρά από τέτοιες μεταβολές είναι δυνατός ο σχηματισμός ενός ολόκληρου μηνύματος με τα μεταβαλλόμενα εικονοστοιχεία. Στο παρακάτω παράδειγμα.

---

[95] Σχετικά με την ανάκτηση κρυπτογραφημένων δεδομένων βλ. E.Casey, 2002 Practical Approaches to Recovering Encrypted Digital Evidence.(27/07/09)

στην πρώτη εικόνα 7.1. έχουν μετατραπεί κάποια εικονοστοιχεία. Η δεύτερη εικόνα 7.2. είναι το αποτέλεσμα της εξαγωγής των μεταβαλλόμενων εικονοστοιχείων[94].

Εικόνα 7.1.

Εικόνα 7.2.

Ο εντοπισμός τέτοιων δεδομένων από τις διωκτικές αρχές μπορεί να πραγματοποιηθεί με τη χρήση κατάλληλου λογισμικού[95]. Το δυσκολότερο σημείο δεν είναι η εξαγωγή των κρυμμένων δεδομένων, αλλά η ανακατασκευή του μηνύματος.

7.4.4. Ανάκτηση «ξεχασμένων» δεδομένων

Μεγάλο πλήθος δεδομένων αποθηκεύεται σε ένα Η/Υ αυτόματα από διάφορες εκτελούμενες εφαρμογές, είτε εν γνώσει είτε χωρίς να το γνωρίζει ο χρήστης. Τα δεδομένα αυτά, ενδέχεται να αποτελέσουν σημαντικό αποδεικτικό υλικό σε μια διαδικτυακή έρευνα.

Μνήμη cache και ιστορικό

Κατά την περιήγηση στο Διαδίκτυο, οι φυλλομετρητές αποθηκεύουν στην μνήμη cache διάφορα αρχεία, τα οποία λαμβάνουν από τις ιστοσελίδες που επισκέπτεται ο χρήστης, προκειμένου την επόμενη φορά που θα την επισκεφτεί, να μπορούν να την εμφανίσουν πιο γρήγορα, χωρίς να χρειάζεται η πρόσβαση σε όλο το περιεχόμενο, μέσω των αργών δικτυακών ταχυτήτων. Τα αρχεία αυτά αποθηκεύονται στο φάκελο Temporary Internet Files και ενδέχεται να εμπεριέχουν σημαντικές πληροφορίες για την υπό εξέταση υπόθεση.[96]

Πληροφορίες, επίσης, μπορούν να ανακτηθούν από το ιστορικό του φυλλομετρητή. Στο ιστορικό αποθηκεύονται οι διευθύνσεις (όχι το περιεχόμενο) όλων των σελίδων, που επισκέφτηκε πρόσφατα ο χρήστης. Οι πληροφορίες αυτές μπορεί να είναι ιδιαίτερα χρήσιμες, κατά την εξέταση αδικημάτων όπως π.χ. πορνογραφία.

---

[94] Το παράδειγμα προέρχεται από τη διεύθυνση www.petitcolas.net/fabien/steganography (Ημερομηνία πρόσβασης: 27/08/09) στην οποία επίσης παρατίθετνται περισσότερες πληροφορίες για την τεχνική της στενογραφίας.

[95] Στην διεύθυνση http://www.jjtc.com/Security/stegtools.htm (Ημερομηνία πρόσβασης: 25/08/09) παρατίθενται μια σειρά από εργαλεία λογισμικού για τον εντοπισμό στενογραφικών δεδομένων.

[96] Ιδιαίτερη αξία κατά την έρευνα διαδικτυακών εγκλημάτων έχουν τα αρχεία index.dat, τα οποία περιέχουν όλες τις πληροφορίες που σχετίζονται με τις σελίδες που έχει επισκεφτεί ένας χρήστης, η δε διαγραφή του από έναν Η/Υ δεν είναι εύκολη.

Προσωρινά αρχεία

Πολλές εφαρμογές, ιδιαίτερα αυτές της Microsoft Office, κατά την δημιουργία ενός αρχείου από το χρήστη αποθηκεύουν, κατά τακτά χρονικά διαστήματα, προσωρινά αντίγραφα στο δίσκο, για να ανακτηθούν σε περίπτωση που το πρόγραμμα τερματιστεί με σφάλμα. Τα αρχεία αυτά διαγράφονται, όταν ο χρήστης τερματιστεί με σφάλμα. Τα αρχεία αυτά διαγράφονται, όταν ο χρήστης τερματίσει το πρόγραμμα με την κατάλληλη διαδικασία. Στην ουσία όμως, τα αρχεία αυτά, όπως αναφέρθηκε παραπάνω δεν διαγράφονται οριστικά από τον σκληρό δίσκο, έως ότου κάποιο άλλο αρχείο εγγραφεί στο σημείο που ήταν αποθηκευμένα. Ο εξερευνητής μπορεί να ανακτήσει από τα αρχεία αυτά σημαντικές πληροφορίες.

Αρχεία σελιδοποίησης

Τα σύγχρονα λειτουργικά συστήματα χρησιμοποιούν την εικονική μνήμη για να «ξεγελάσουν» το σύστημα, το οποίο «νομίζει» ότι έχει μεγαλύτερη μνήμη RAM. Η εικονική μνήμη, χρησιμοποιεί ένα μέρος του σκληρού δίσκου, στον οποίο αποθηκεύονται δεδομένα, που προορίζονται για την πραγματική φυσική μνήμη. Τα δεδομένα αυτά, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία κειμένου, ιστοσελίδες κ.α. αποθηκεύονται στα αρχεία σελιδοποίησης (page files). Τα αρχεία αυτά, δημιουργούνται αυτόματα από το λειτουργικό σύστημα. Πολλοί χρήστες Η/Υ δεν γνωρίζουν την ύπαρξη των αρχείων ή ποια δεδομένα αποθηκεύονται σε αυτά. Τα δεδομένα που θα ανακτηθούν από τα page files, ενδέχεται να έχουν σημαντική αποδεικτική αξία.

Κάδος ανακύκλωσης

Οι περισσότεροι χρήστες Η/Υ γνωρίζουν ότι , διαγράφοντας ένα αρχείο, μετακινείται αρχικά στον Κάδο Ανακύκλωσης. Έχει παρατηρηθεί, ότι πολλοί χρήστες ξεχνούν τα δεδομένα στον Κάδο Ανακύκλωσης. Έχει παρατηρηθεί, ότι πολλοί χρήστες ξεχνούν τα δεδομένα αυτά στον Κάδο Ανακύκλωσης, δίνοντας εύκολα αποδεικτικά στοιχεία στους εξερευνητές. Άλλες φορές, δεν γνώριζαν καν ότι τα αρχεία που διέγραψαν τοποθετήθηκαν στον Κάδο Ανακύκλωσης, ιδιαίτερα στις περιπτώσεις που το εικονίδιο του Κάδου Ανακύκλωσης δεν εμφανιζόταν στην Επιφάνεια Εργασίας. Επομένως, είναι πολύ σημαντικό, για τον εξερευνητή να ελέγξει τον Κάδο Ανακύκλωσης, καθώς μπορεί να αποκτήσει σημαντικά δεδομένα εύκολα και άμεσα.

Ανάκτηση δεδομένων από εφεδρικά αρχεία

Ένας χρήστης, εφόσον θέλει να εξαφανίσει δεδομένα που είναι αποθηκευμένα σε ένα Η/Υ, μπορεί να τα διαγράψει με τη χρήση κατάλληλου λογισμικού[97] ώστε να μην παραμείνουν υπολείμματα αυτών στο σκληρό δίσκο. Στις περιπτώσεις αυτές, ο εξερευνητής θα πρέπει να αναζητήσει τυχόν εφεδρικά αρχεία, που ενδέχεται να έχει αποθηκεύσει ο χρήστης σε φορητά μέσα ή σε άλλους σκληρούς δίσκους και έχει ξεχάσει να διαγράψει.

---

[97] Π.χ. με το XL Delete 1.5, όταν διαγράφεται ένα αρχείο, το λογισμικό επανεγγράφει τυχαία δεδομένα στις συστοιχίες όπου είναι αποθηκευμένο, έτσι ώστε προγράμματα ανάκτησης αρχείων να μην μπορούν πλέον να το ανακτήσουν. Βλ. http://www.xldevelopment.net/xldelete.php (Ημερομηνία πρόσβασης: 25/08/09)

7.5. Ο εντοπισμός του ηλεκτρονικού εγκλήματία στο Διαδίκτυο

7.5.1. Αρχεία καταγραφής (log files)

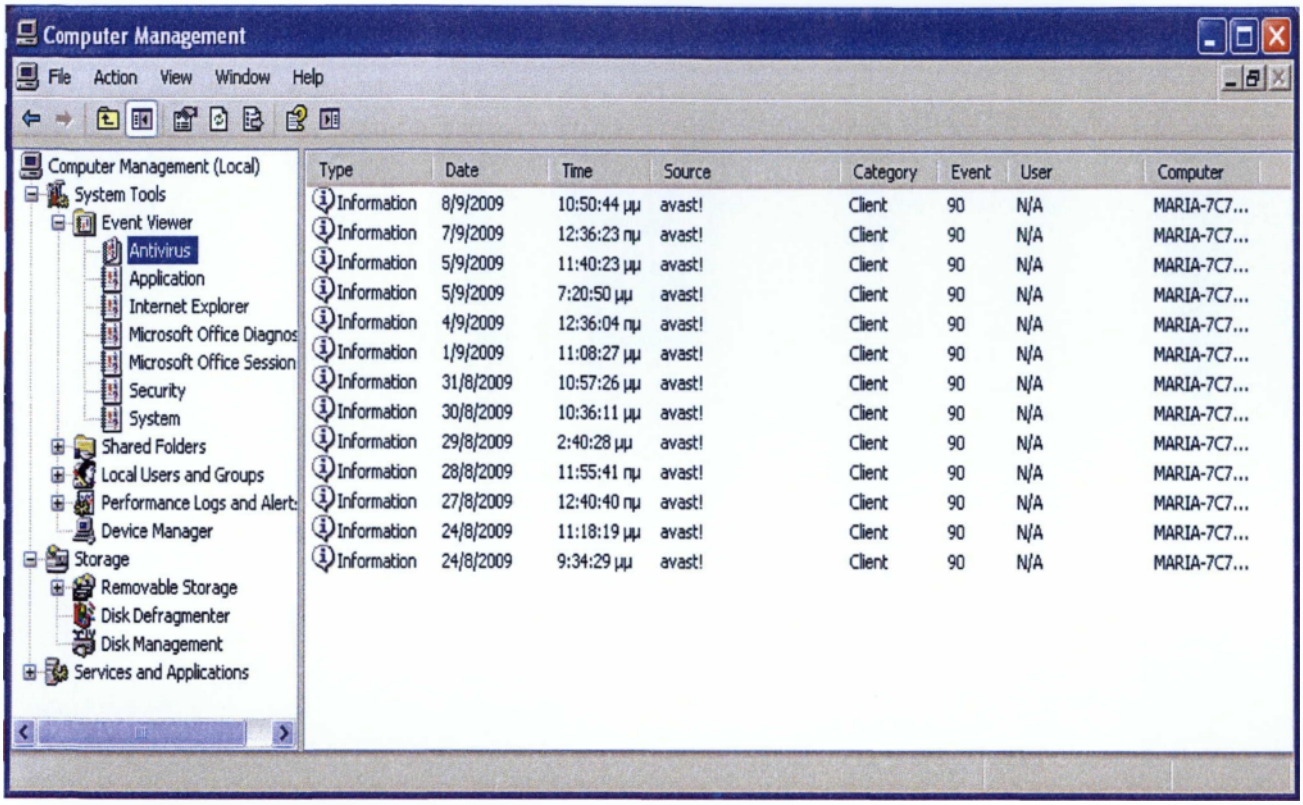
Τα αρχεία καταγραφής διαδραματίζουν σημαντικό ρόλο, καθώς σε αυτά αποθηκεύονται πληροφορίες, που αφορούν τη λειτουργία του συστήματος. Στα λειτουργικά συστήματα της οικογένειας Windows, υπάρχουν τρία βασικά είδη αρχείων καταγραφής: Application log, System log και Security log.

Ο εντοπισμός όλων των πληροφοριών, που αποθηκεύονται τα αρχεία καταγραφής, μπορεί να πραγματοποιηθεί μέσω της κονσόλας διαχείρισης των Windows

Η χρησιμότητα των αρχείων καταγραφής των Windows μεγιστοποιείται, όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές ομάδων (group policies). Τα Security logs είναι κενά, εάν δεν έχει οριστεί συγκεκριμένη πολιτική ασφάλειας για μια ομάδα χρηστών. Η ευθύνη ορισμού πολιτικών ασφάλειας ανήκει στο διαχειριστή και υπεύθυνο ασφαλείας ενός συστήματος.

Από τα αρχεία καταγραφής, ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί να διαπιστώσει εάν χρησιμοποιήθηκε συγκεκριμένη εφαρμογή από ένα χρήστη, εάν κάποιος μη εξουσιοδοτημένος χρήστης απέκτησε πρόσβαση στο σύστημα, εάν χρησιμοποιήθηκε κάποια περιφερειακή συσκευή και πλήθος άλλων σημαντικών πληροφοριών.

Εκτός από το λειτουργικό σύστημα, αρχεία καταγραφής δημιουργούνται και από άλλες εφαρμογές. Το firewall, ως βασικό εργαλείο, που ελέγχει την κίνηση από και προς ένα προστατευόμενο δίκτυο ή υπολογιστή, αποθηκεύει σημαντικές πληροφορίες στα αρχεία καταγραφής του. Οι πληροφορίες των αρχείων αυτών, αποτελούν σημαντικό προανακριτικό αλλά και αποδεικτικό υλικό, σε περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε δίκτυα.



Εικόνα 7.3: Πληροφορίες για τα συμβάντα του λογισμικού ανίχνευσης ιών από την κονσόλα διαχείρισης Windows

7.5.2. Συναγερμοί, προειδοποιήσεις, αναφορές

Τα αρχεία καταγραφής είναι ένα μόνο είδος δεδομένων, που μπορούν να αντληθούν από το firewall. Τα firewalls μπορούν να προσφέρουν και άλλου είδους πληροφορίες:

Συναγερμοί (Alarms): Τα firewalls έχουν την δυνατότητα να αποστέλλουν μηνύματα υψηλής προτεραιότητας σε συγκεκριμένους παραλήπτες, σε περίπτωση που διαπιστωθεί κάποια ύποπτη δραστηριότητα. Ένα τέτοιο μήνυμα μπορεί να αποσταλεί με e-mail στο διαχειριστή του συστήματος, ή ακόμη να γίνει τηλεφωνική κλήση και παράλληλα η ύποπτη δραστηριότητα να αποθηκευτεί στα αρχεία καταγραφής. Η λειτουργία αυτή είναι πολύ σημαντική, καθώς μπορεί μια επίθεση να αποφευχθεί στη γέννηση της.

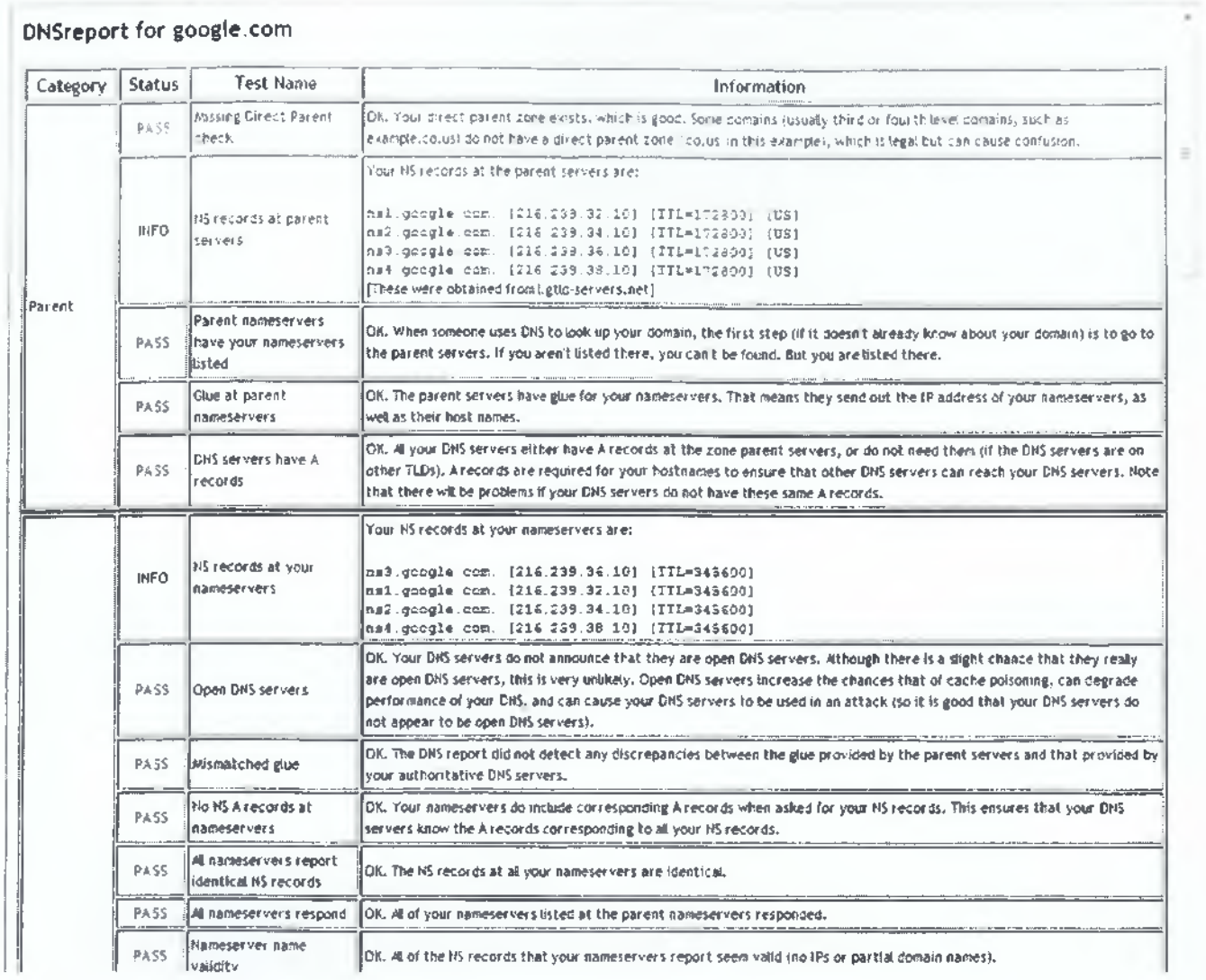
Προειδοποιήσεις (Alerts): Αποτελούν μια πιο ήπια μορφή συναγερμού. Η ενημέρωση του διαχειριστή, μπορεί να γίνει με τους τρόπους που αναφέρθηκαν παραπάνω. Η βασική διαφορά είναι, ότι τα μηνύματα δεν έχουν το χαρακτήρα του άμεσου κινδύνου, όπως στην προηγούμενη περίπτωση, αλλά προειδοποιούν για το ενδεχόμενο εκδήλωσης επίθεσης.

Αναφορές (Reports): Αν και οι πληροφορίες ασφάλειας από το firewall αποθηκεύονται στα αρχεία καταγραφής, οι αναφορές μπορούν να δώσουν επιπρόσθετα δεδομένα, όπως την συχνότητα αποτυχημένων προσπαθειών απόκτησης μη εξουσιοδοτημένης πρόσβασης, την συχνότητα σφαλμάτων κ.ά.

Οι πληροφορίες, που μπορεί να συλλέξει ο ερευνητής από τα firewalls, όπως το χρονικό σημείο στο οποίο συνέβη μια δραστηριότητα, η IP διεύθυνση από την οποία προήλθε μια επίθεση, το πρωτόκολλο που χρησιμοποιήθηκε από τον επιτιθέμενο, το είδος του μηνύματος που στάλθηκε, η θύρα που χρησιμοποιήθηκε κ.ά. μπορούν να βοηθήσουν στον εντοπισμό του επιτιθέμενου.

7.5.3. Εντοπισμός ονόματος χώρου και διεύθυνσης IP

Ο εντοπισμός της διεύθυνσης IP, αποτελεί βασική ενέργεια των διωκτικών αρχών για την εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε ένα σε ένα δίκτυο. Στις επιθέσεις αυτές οι εισβολείς χρησιμοποιούν πλαστές διευθύνσεις IP, προκειμένου να παραπλανήσουν τις διωκτικές αρχές. Κάθε διεύθυνση στο Διαδίκτυο έχει έναν αντίστοιχο αριθμό IP. Το σύστημα, που έχει αναλάβει την διατήρηση των αντιστοιχιών μεταξύ μιας ηλεκτρονικής διεύθυνσης και του αντίστοιχου IP, είναι το DNS (Domain Name System). Κατά την εκδήλωση μιας επίθεσης, ο επιτιθέμενος πλαστογραφεί την διεύθυνση του για να φαίνεται ότι είναι νόμιμος χρήστης, δεν πλαστογραφεί όμως (ή δεν μπορεί να πλαστογραφήσει) τον αντίστοιχο αριθμό IP. Συνήθως, συσκευές, όπως τα firewalls, έχουν την δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να επιτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη. Εφόσον το firewall δεν έχει ρυθμιστεί κατάλληλα, ο ερευνητής θα κληθεί να ελέγξει τις διευθύνσεις όλων όσων απέκτησαν πρόσβαση, προκειμένου να εξακριβώσει από ποιόν προήλθε η κακόβουλη επίθεση. Η εργασία αυτή μπορεί να διεκπεραιωθεί με διάφορα εργαλεία λογισμικού, τα οποία ελέγχουν αν οι ηλεκτρονικές διευθύνσεις, αναλογούν σε σωστούς αριθμούς IP. Επίσης, υπάρχουν και δικτυακοί τόποι που επιτελούν on-line την εργασία αυτή. Για παράδειγμα στο www.dnsreport.com μπορεί να δοθεί μια ηλεκτρονική διεύθυνση ή διεύθυνση ηλεκτρονικού ταχυδρομείου και να ληφθούν διάφορες πληροφορίες για αυτή όπως το IP ο server κ.α.



DNSreport for google.com

Category	Status	Test Name	Information
Parent	PASS	Missing Direct Parent check	OK. Your direct parent zone exists, which is good. Some domains (usually third or fourth level domains, such as example.co.us) do not have a direct parent zone (co.us in this example), which is legal but can cause confusion.
	INFO	NS records at parent servers	Your NS records at the parent servers are: ns1.google.com. [216.239.32.10] [TTL=172800] (US) ns2.google.com. [216.239.34.10] [TTL=172800] (US) ns3.google.com. [216.239.36.10] [TTL=172800] (US) ns4.google.com. [216.239.38.10] [TTL=172800] (US) [These were obtained from l.gtld-servers.net]
	PASS	Parent nameservers have your nameservers listed	OK. When someone uses DNS to look up your domain, the first step (if it doesn't already know about your domain) is to go to the parent servers. If you aren't listed there, you can't be found. But you are listed there.
	PASS	Glue at parent nameservers	OK. The parent servers have glue for your nameservers. That means they send out the IP address of your nameservers, as well as their host names.
	PASS	DNS servers have A records	OK. All your DNS servers either have A records at the zone parent servers, or do not need them (if the DNS servers are on other TLDs). A records are required for your hostnames to ensure that other DNS servers can reach your DNS servers. Note that there will be problems if your DNS servers do not have these same A records.
	INFO	NS records at your nameservers	Your NS records at your nameservers are: ns3.google.com. [216.239.36.10] [TTL=345600] ns1.google.com. [216.239.32.10] [TTL=345600] ns2.google.com. [216.239.34.10] [TTL=345600] ns4.google.com. [216.239.38.10] [TTL=345600]
	PASS	Open DNS servers	OK. Your DNS servers do not announce that they are open DNS servers. Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances that of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack (so it is good that your DNS servers do not appear to be open DNS servers).
	PASS	Mismatched glue	OK. The DNS report did not detect any discrepancies between the glue provided by the parent servers and that provided by your authoritative DNS servers.
	PASS	No NS A records at nameservers	OK. Your nameservers do include corresponding A records when asked for your NS records. This ensures that your DNS servers know the A records corresponding to all your NS records.
	PASS	All nameservers report identical NS records	OK. The NS records at all your nameservers are identical.
	PASS	All nameservers respond	OK. All of your nameservers listed at the parent nameservers responded.
	PASS	Nameserver name validity	OK. All of the NS records that your nameservers report seem valid (no IPs or partial domain names).

Εικόνα 7.4: Πληροφορίες για το google.com από το DNS Report

7.5.4. Μηνύματα ηλεκτρονικού ταχυδρομείου

Τα μηνύματα ηλεκτρονικού ταχυδρομείου, εκτός από μέσο άμεσης επικοινωνίας μεταξύ των χρηστών, χρησιμοποιούνται για την διάπραξη πολλών αδικημάτων, όπως μετάδοση ιών και άλλου κακόβουλου κώδικα, επιθέσεις άρνησης εξυπηρέτησης, απάτες, απειλές, δυσφήμηση κ.α.

Για τους λόγους αυτούς, η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου, αποτελεί βασική εργασία στην αναζήτηση των ηλεκτρονικών ιχνών του επιτιθέμενου. Αν ο αποστολέας αναγράψει στο μήνυμα το όνομα του και την διεύθυνση του (και τα στοιχεία είναι αληθή) τότε ο εντοπισμός τους είναι εύκολος. Αυτό, όμως, δεν συμβαίνει σχεδόν ποτέ. Ο μόνος τρόπος για την εύρεση του αποστολέα του μηνύματος,

στις περιπτώσεις αυτές, είναι η ανάγνωση και κατανόηση των επικεφαλίδων[98] του μηνύματος.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου, κατά την μετάβαση τους από τον αποστολέα στον παραλήπτη, διέρχονται από πολλούς ενδιάμεσους υπολογιστές. Κάθε ένας από αυτούς, προσθέτει τις δικές του πληροφορίες στην επικεφαλίδα του μηνύματος. Οι πληροφορίες στην επικεφαλίδα του μηνύματος καταγράφονται σε διάφορα πεδία, που αφορούν τις επικεφαλίδες του αποστολέα και του παραλήπτη, τις επικεφαλίδες ημερομηνίας και διάφορες άλλες. Κατά την αναζήτηση του αποστολέα κακόβουλων μηνυμάτων, οι σημαντικότερες πληροφορίες περιλαμβάνονται στις επικεφαλίδες του αποστολέα. Από αυτές μπορούμε να συλλέξουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου στην οποία μπορούν να αποστέλλονται πιθανές απαντήσεις, το μονοπάτι (διεύθυνση) προς τον αποστολέα και, τέλος, τους διακομιστές από τους οποίους διήλθε το μήνυμα για να φτάσει στον τελικό του παραλήπτη. Η πρόσβαση στις πληροφορίες αυτές, είναι δυνατή μέσω των χρησιμοποιούμενων εφαρμογών ηλεκτρονικού ταχυδρομείου.[99]

Ο εντοπισμός του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι μια εξαιρετικά δύσκολη διαδικασία. Οι επιτιθέμενοι έχουν ανακαλύψει μια σειρά από μεθόδους για την απόκρυψη της ταυτότητας τους. Για παράδειγμα, με την χρήση anonymous remailers είναι δυνατή η αποστολή μηνυμάτων χωρίς να φαίνεται η ταυτότητα του αποστολέα. Επίσης, στο Διαδίκτυο είναι δυνατή η εύρεση αναλυτικών οδηγιών με την χειροκίνητη δημιουργία ψευδών επικεφαλίδων των διακινούμενων μηνυμάτων.

7.5.5. Honeypots και honeynets

Τα Honeypots και honeynets αποτελούν τα πλέον σύγχρονα εργαλεία των διωκτικών αρχών, για την αντιμετώπιση ηλεκτρονικού εγκλήματος. Τα honeypots είναι μια συλλογή από τα συστήματα, τα οποία «προσποιούνται» ότι είναι αληθινοί στόχοι, προκειμένου να ξεγελάσουν τον επιτιθέμενο και να τον ωθήσουν στην παραβίαση τους. Ένα honeynet είναι μια συλλογή από συστήματα honeypots, τα οποία συνεργάζονται μεταξύ τους.

Βασικός σκοπός των honeypots είναι η παρακολούθηση των ενεργειών του επιτιθέμενου και η καταγραφή τους, προκειμένου να αναλυθεί η μεθοδολογία της επιθέσεως τους. Σε αντίθεση με τα firewalls, τα honeypots λειτουργούν παθητικά, δηλαδή αναμένουν την επίθεση του χρήστη και δεν ενεργούν για την παρεμπόδιση της, απλά καταγράφουν τις ενέργειες του.

---

[98] Ένας πλήρης οδηγός ανάγνωσης των επικεφαλίδων μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι διαθέσιμος στη διεύθυνση http://www.stopspam.org/index.php?option=com_content&view=article&id=45&Itemid=56 (Ημερομηνία πρόσβασης: 25/08/09).

[99] Για παράδειγμα το Outlook Express εφόσον έχουμε ανοίξει ένα μήνυμα, μπορούμε να επιλέξουμε από το μενού Αρχείο> ιδιότητες, καρτέλα Λεπτομέρειες και να δούμε τις πληροφορίες που αφορούν τις επικεφαλίδες του μηνύματος.

Ευκαιρία ή Παγίδευση;

Οι αστυνομικοί που επιχειρούν να εξιχνιάσουν ένα έγκλημα, πολλές φορές καλούνται να εμφανιστούν ως έμποροι ναρκωτικών, τοξικομανείς, κλεπταποδόχοι κ.ά., με σκοπό ύποπτοι τέλεσης ποινικών αδικημάτων να συλληφθούν επ'αυτοφώρο. Τέτοιου είδους ενέργειες, αντιμετωπίζονται με διαφορετικό νομικό πλαίσιο σε κάθε χώρα. Η σχεδιαζόμενη «παγίδευση» κάποιου ατόμου από τις διωκτικές αρχές, θεωρείται παράνομη σε πολλές πολιτείες των Η.Π.Α.

Ωστόσο, το να δίνεται απλά μια «ευκαιρία» σε ένα άτομο να διαπράξει ένα έγκλημα δεν συνιστά παγίδευση. Σε κάθε περίπτωση, το κριτήριο με το οποίο η δικαιοσύνη αποφαίνεται αν έγινε παγίδευση ή όχι, είναι αν κατηγορούμενος με την πειθώ, την απειλή βίας ή άλλου ψυχολογική πίεση, εξαναγκάστηκε να διαπράξει ένα έγκλημα, που διαφορετικά δεν θα τελούσε.

Η χρησιμοποίηση των honeypots και honeynets από τις διωκτικές αρχές, αποτελεί ένα είδος παγίδευσης με βάση την παραπάνω έννοια. Για το λόγο αυτό, οι αιτιάσεις που προαναφέρθηκαν, θα πρέπει να λαμβάνονται σοβαρά υπόψη, όταν χρησιμοποιείται μια τέτοια μέθοδος για την εξιχνίαση ενός εγκλήματος.

Υπάρχουν δύο βασικές κατηγορίες honeypots[100]: Τα πραγματικά και τα εικονικά. Ένα πραγματικό honeypot, είναι ακριβώς αυτό που φαίνεται, π.χ. ένας διακομιστής. Ένα εικονικό honeypot ένας συνδυασμός υλικού και λογισμικού, που προσομοιάζει σε ένα πραγματικό διακομιστή.

Αρχιτεκτονική honeynets

Ένα honeynet αποτελείται από διαφορετικού τύπου honeypots, δηλαδή συστήματα ,με διαφορετικές υπηρεσίες και λειτουργικά συστήματα, ώστε να συγκεντρώνονται ταυτόχρονα δεδομένα από διαφορετικά συστήματα αλλά και να αποτελούν ένα περισσότερο αληθοφανές δίκτυο. Μερικές φορές σχεδιάζονται έτσι, ώστε να αποτελούν ολοκληρωμένα αντίγραφα δικτύων ή παραγωγικών συστημάτων. Ο στόχος ενός honeynet είναι να συλλέγει δεδομένα από κάθε δυνατή πηγή.

7.6. Μοντέλα Ηλεκτρονικής Εγκληματολογίας (Digital Forensic Models)

Η Ηλεκτρονική Εγκληματολογία (Computer Forensic Science) βρίσκεται στα πρώιμα στάδια της ανάπτυξης της, σε σχέση με άλλους τομείς της Εγκληματολογικής Επιστήμης. Έως τώρα, δεν έχει υιοθετηθεί μια κοινά αποδεκτή μεθοδολογία που να καθορίζει τα στάδια της έρευνας σε μια υπόθεση ηλεκτρονικού εγκλήματος. Η ύπαρξη ενός ολοκληρωμένου μοντέλου ερευνών είναι πάρα πολύ σημαντική, γιατί θα βοηθούσε το έργο των ερευνητών, παρέχοντας ένα βασικό σκελετό ενεργειών και μεθόδων έρευνας, ανεξαρτήτως του περιβάλλοντος στο οποίο αυτή διεξάγεται. Επιπλέον θα βοηθούσε στην ανάπτυξη κατάλληλων εργαλείων για την υποβοήθηση του έργου των ερευνητών[101], στην υιοθέτηση κοινής ορολογίας, ενώ θα αποτελούσε ένα βασικό μέσο εκπαίδευσης και

[100] http://articles.techrepublic.com.com/5100-22_11-5758218.html (Ημερομηνία πρόσβασης: 28/08/09)
[101] Ciardhuain, S. 2004 (Ημερομηνία πρόσβασης: 28/07/09)

επιμόρφωσης του προσωπικού, που ασχολείται με την έρευνα του ηλεκτρονικού εγκλήματος.

Οι πρώτες προσπάθειας δημιουργίας ενός μοντέλου διαδικτυακών ερευνών, επικεντρώθηκαν στην παροχή ενός αναλυτικού πλαισίου οδηγιών για τον τρόπο έρευνας της σκηνής διάπραξης του εγκλήματος. Ο Lee κ.α. πρότειναν ένα μοντέλο έρευνας της σκηνής διάπραξης του εγκλήματος, αποτελούμενο από 4 βασικά βήματα[102]:

- **Αναγνώριση (Recognition):** Η αναχώρηση περιλαμβάνει τον εντοπισμό των αντικειμένων, που πιθανώς έχουν αποδεικτική αξία. Ο ερευνητής, στο στάδιο αυτό, θα πρέπει να γνωρίζει τι πρέπει να αναζητήσει και που μπορεί να το βρει. Η αναγνώριση οδηγεί στην τεκμηρίωση, συλλογή και διατήρηση των αποδεικτικών στοιχείων
- **Ταυτοποίηση (Identification):** Στο στάδιο αυτό περιλαμβάνεται, η ταξινόμηση των αποδεικτικών στοιχείων και η μεταξύ τους σύγκριση με γνωστά πρότυπα.
- **Εξατομίκευση (Individualization)**: Εξετάζεται, εάν τα αποδεικτικά στοιχεία φέρουν συγκεκριμένα μοναδικά χαρακτηριστικά, που μπορούν να τα συνδέσουν με κάποιο άτομο. Βασική αρχή αποτελεί η αξιολόγηση όλων των αντικειμένων.
- **Συμπέρασμα (Reconstruction):** Το τελευταίο αυτό στάδιο περιλαμβάνει, την συγκέντρωση όλων των αποδεικτικών στοιχείων και σχετικών πληροφοριών και την σύνταξη και παρουσίαση λεπτομερής αναφοράς, για τα ευρήματα από τη σκηνή του εγκλήματος.

Το παραπάνω μοντέλο επικεντρώνεται στην έρευνα της σκηνής διάπραξης του εγκλήματος, για την εύρεση αποδεικτικών στοιχείων, που έχουν φυσική υπόσταση. Η μη αναφορά των ψηφιακών αποδείξεων μειώνει την αξία του μοντέλου, όμως δεν θα έπρεπε να παραβλεφτεί, ότι πολλά από τα στάδια έρευνας που περιγράφηκαν, μπορούν να χρησιμοποιηθούν και σε ένα μοντέλο έρευνας σε ψηφιακό περιβάλλον.

Ο DFRW[103] (Digital Forensic Research Workshop), είναι ένας από τους πλέον σημαντικούς οργανισμούς, που ασχολούνται με την ανάπτυξη μοντέλων για την έρευνα του ηλεκτρονικού εγκλήματος. Η κοινοπραξία αποτελείται περισσότερο από τα μέλη της ακαδημαϊκής κοινότητας. Το 2001 πρότεινε ένα μοντέλο ερευνών αποτελούμενο από επτά βήματα:

1) Identification (Αναγνώριση)
2) Preservation (Διατήρηση)
3) Collection (Συλλογή)
4) Examination (Εξέταση)
5) Analysis (Ανάλυση)
6) Presentation (Παρουσίαση)
7) Decision (Απόφαση)

Το μοντέλο αυτό προτάθηκε, με το σκοπό να αποτελέσει τη βάση για την ανάπτυξη στο μέλλον ενός πιο πλήρους μοντέλου, καθώς η έρευνα, το συγκεκριμένο χρονικό σημείο, ήταν περιορισμένη.

---

[102] Κωνσταντίνος Βλαχόπουλος 2007σελ.178
[103] http://www.dfrws.org/ (Ημερομηνία πρόσβασης: 28/08/09)

Ένα από τα πιο πλήρη μοντέλα δικτυακών ερευνών, προτάθηκε το 2004, από τον Ciardjuain. Αξιολογώντας, αλλά και συνθέτοντας τα υπάρχοντα μοντέλα, ο Ciardjuain κατέληξε σε ένα πλήρες μοντέλο ερευνών, αποτελούμενο από δεκατρία βήματα. Ο Ciardjuain θέλησε στο μοντέλο του, να συμπεριλάβει όλες τις πτυχές της έρευνας του ηλεκτρονικού εγκλήματος και να μην περιοριστεί μόνο στην σκηνή διάπραξης, όπως συνέβαινε με τα προηγούμενα μοντέλα. Τα βήματα, που προτείνει, είναι τα ακόλουθα:

- **Awareness (Επίγνωση):** Το βήμα αυτό δεν υπήρχε σε προηγούμενα μοντέλα. Αναφέρεται στην ενημέρωση ενός αρμοδίου φορέα (π.χ. της αστυνομίας), ότι έχει προκύψει η ανάγκη για την διεξαγωγή μιας έρευνας. Θεωρείται σημαντικό γιατί τα γεγονότα, που προκάλεσαν μια έρευνα μπορούν να επηρεάσουν σημαντικά τον τύπο αυτής.
- **Authorization (Εξουσιοδότηση):** Στο βήμα αυτό, αποκτάται η εξουσιοδότηση για την διεξαγωγή της έρευνας. Για παράδειγμα, η αστυνομία θα πρέπει να αποκτήσει εξουσιοδότηση για την διεξαγωγή της έρευνα μέσω ενός εντάλματος του αρμόδιου εισαγγελέα.
- **Planning (Σχεδιασμός):** Ο σχεδιασμός της έρευνας είναι το επόμενο βήμα. Κατά το σχεδιασμό μπορεί να προκύψουν διάφορα προβλήματα, όπως ανάγκη για περαιτέρω εξουσιοδότηση, για το λόγο αυτό θα πρέπει να διεξάγεται με ιδιαίτερη προσοχή και επιμέλεια.
- **Notification (Ενημέρωση):** Αναφέρεται στην ενημέρωση ενός οργανισμού ή προσώπου ότι πρόκειται να διεξαχθεί η έρευνα. Το βήμα αυτό είναι δυνατόν να παραληφθεί σε περιπτώσεις, που η έρευνα απαιτεί το στοιχείο του αιφνιδιασμού.
- **Search for and identify evidence (Αναζήτηση και αναγνώριση αποδεικτικών στοιχείων):** Η δραστηριότητα αυτή περιλαμβάνει τον εντοπισμό και αναγνώριση των αποδεικτικών στοιχείων (π.χ. υπολογιστές, αποθηκευτικά μέσα κ.λπ.), που θα χρησιμοποιηθούν στο επόμενο βήμα.
- **Collection of Evidence (Συλλογή αποδεικτικών στοιχείων):** Αποτελεί το πλέον σημαντικό βήμα της όλης διαδικασίας. Ο ερευνητής καλείται να συλλέξει όλα τα αποδεικτικά στοιχεία, που θα συναντήσει στην σκηνή του εγκλήματος, π.χ. αντίγραφα των σκληρών δίσκων, φορητά μέσα αποθήκευσης, συσκευές κ.α.
- **Transport of Evidence (Μεταφορά των αποδεικτικών στοιχείων):** Αποτελεί εξίσου σημαντικό βήμα με την συλλογή των αποδείξεων, καθώς η λανθασμένη συσκευασία και μεταφορά τους μπορεί να οδηγήσει σε καταστροφή ή απώλεια σημαντικών πληροφοριών.
- **Storage of Evidence (Αποθήκευση αποδείξεων):** Η αποθήκευση των αποδείξεων είναι μια διαδικασία, που μπορεί να απαιτηθεί σε περίπτωση, που δεν είναι δυνατή η άμεση εξέταση τους. Και στο βήμα αυτό θα πρέπει να ληφθεί μέριμνα, για να διατηρηθούν αναλλοίωτα τα αποδεικτικά στοιχεία.
- **Examination of Evidence (Εξέταση Αποδείξεων):** Στο στάδιο αυτό, απαιτείται η χρησιμοποίηση ποικίλων τεχνικών για την ανάκτηση σημαντικών δεδομένων. Εργαλεία υλικού και λογισμικού ενδέχεται να χρησιμοποιηθούν για την ανάκτηση δεδομένων από κατεστραμμένους δίσκους, για τον εντοπισμό ηλεκτρονικών ιχνών και για την τελική επεξεργασία μεγάλων ποσοτήτων δεδομένων.
- **Hypothesis (Υπόθεση):** Η υπόθεση αποτελεί το συμπέρασμα της εξέτασης των ψηφιακών αποδείξεων. Στις αστυνομικές έρευνες, η υπόθεση έχει την μορφή της έκθεσης πραγματογνωμοσύνης, στην οποία καταγράφονται όλα τα γεγονότα και αποδεικτικά στοιχεία που εξετάστηκαν κατά τη διάρκεια της έρευνας. Το κείμενο

της υπόθεσης, βοηθά τον ερευνητή να κατανοήσει καλύτερα τα αποτελέσματα της έρευνας του.

- **Presentation of hypothesis (Παρουσίαση της υπόθεσης):** Η παρουσίαση της υπόθεσης σε μια αστυνομική έρευνα, ενεργείται, συνήθως ενώπιον του αρμόδιου δικαστηρίου.
- **Proof/ defence of hypothesis (Απόδειξη- υποστήριξη της υπόθεσης):** Στις περισσότερες περιπτώσεις η υπόθεση θα αμφισβητηθεί στο ακροατήριο από τα μέρη τα οποία θίγονται από αυτή. Στο στάδιο αυτό, ο ερευνητής καλείται να υποστηρίξει προφορικά, όλα όσα έχει αναφέρει στην έκθεση του, στηρίζοντας τα σε επιστημονικά στοιχεία.
- **Dissemination of Information (Διανομή των πληροφοριών):** Η διανομή των αποτελεσμάτων της έρευνας είναι το τελευταίο στάδιο του μοντέλου, που προτείνει ο Ciardjuain. Στοχεύει στην χρησιμοποίηση της τεχνογνωσία που αποκτήθηκε από μια έρευνα, σε παρεμφερείς περιπτώσεις, που ενδεχομένως προκύψουν στο μέλλον.

Ο Ciardjuain επισημαίνει ότι, η σειρά των βημάτων που περιλαμβάνονται στο μοντέλο δεν είναι αυστηρή και απόλυτη. Ενδέχεται κάποια από τα βήματα να παραληφθούν, να μεταβληθεί η σειρά τους ή ακόμη το αποτέλεσμα ενός βήματος να έχει επιπτώσεις όχι μόνο στο επόμενο, αλλά και στο προηγούμενο. Ο ερευνητής πρέπει και οφείλει να καθοδηγείται από την ίδια την έρευνα και όχι από το μοντέλο το οποίο, απλά, βοηθά στην επίτευξη των στόχων της έρευνας,

Στα πλεονεκτήματα του μοντέλου, εκτός από αυτά που ήδη ισχύουν σε κάθε μοντέλο δικτυακών ερευνών, επισημάνει ότι ο τρόπος με τον οποίο οι διεργασίες διαδέχονται η μια την άλλη, θα βοηθήσει για την ανάπτυξη συγκεκριμένων εργαλείων εξέτασης και ελέγχου ψηφιακών τεκμηρίων. Αναγνωρίζει, όμως, ότι η γενικότητα του μοντέλου ενδέχεται να παρουσιάσει ορισμένες δυσκολίες, όσο αφορά την εφαρμογή του στο συγκεκριμένο περιβάλλον ενός οργανισμού.

7.7. Νομικά ζητήματα

Η διερεύνηση μιας υπόθεσης ηλεκτρονικού εγκλήματος εκτός από τεχνικής απόψεως πρέπει να είναι και σύννομη, συμβαδίζοντας με τους ισχύοντες σε κάθε χώρα νόμους και κανονισμούς. Η Ηλεκτρονική Εγκληματολογία, ως μια σχετικά νέα επιστήμη, έχει προβληματίσει τους νομικούς κύκλους για το κατά πόσο αξιόπιστη είναι και σε πιο βαθμό οι ψηφιακές αποδείξεις μπορούν να τύχουν εφαρμογής σε μια δίκη. Οι νομικοί προβληματισμοί σχετίζονται με την έρευνα και κατάσχεση ψηφιακών αποδείξεων, το κατά πόσο οι γνώσεις ενός ερευνητή είναι επαρκείς για την διεκπεραίωση μιας έρευνας σε ένα Η/Υ και τέλος, αν η ανάλυση και διατήρηση των αποδείξεων έγινε σύμφωνα με τις προβλεπόμενες διαδικασίες.

Η έρευνα και κατάσχεση πληροφοριών είναι η πρώτη διαδικασία που αμφισβητείται σε μια δίκη. Σύμφωνα με το Ελληνικό Δίκαιο[104], μια έρευνα μπορεί να διενεργηθεί όταν διεξάγεται ανάκριση για κακουργήματα ή πλημμέλημα και μόνο με το μέσο αυτό μπορεί να κατορθώσει ή να διευκολυνθεί η βεβαίωση του εγκλήματος, η ανακάλυψη και σύλληψη των δραστών ή τέλος η βεβαίωση και αποκατάσταση της ζημιάς που

[104] Άρθρο 253 ΚΠΔ

προκλήθηκε. Επιπλέον, κατά την διεξαγωγή μιας έρευνας θα πρέπει να τηρούνται και οι βασικές αρχές της αναγκαίας αναλογίας, της αναγκαιότητας και της απαγορεύσεως του υπέρμετρου. Επειδή δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για τις διαδικτυακές έρευνες, οι ανωτέρω διατάξεις εφαρμόζονται κατ' αναλογία και σε περιπτώσεις ηλεκτρονικών εγκλημάτων. Επομένως, μια έρευνα στην οποία δεν έχουν τηρηθεί οι προβλεπόμενες προϋποθέσεις, θα επηρεάσει την αποδεικτικότητα των στοιχείων που συλλέχτηκαν.

Κατά την διεξαγωγή μιας έρευνας, το βασικό αγαθό, που διακυβεύεται, είναι η ιδιωτικότητα του ατόμου. Το Αμερικάνικο Σύνταγμα απαιτεί την ύπαρξη εντάλματος[105] για την διεξαγωγή μιας έρευνας, το οποίο εκδίδεται αν υπάρχει πιθανή αίτια, ότι διαπράχθηκε ένα έγκλημα. Το ένταλμα θα πρέπει να καθορίζει, επακριβώς, το μέρος και τα αντικείμενα που μπορούν να ερευνηθούν. Για παράδειγμα, εάν η πιθανή αιτία υποδεικνύει ότι τα αποδεικτικά στοιχεία είναι αποθηκευμένα σε ένα CD, η αστυνομία δεν έχει το δικαίωμα να ερευνήσει κάθε υπολογιστή που υπάρχει στο χώρο για την εύρεση συμπληρωματικών στοιχείων. Αν το πράξει, έστω κι αν βρει επιπρόσθετα αποδεικτικά στοιχεία, αυτά δεν θα έχουν αποδεικτική αξία στο δικαστήριο, γιατί παραβιάστηκε το ένταλμα.

Το δεύτερο νομικό ζήτημα, που σχετίζεται με υποθέσεις που εμπλέκονται αποδεικτικά στοιχεία σε ψηφιακή μορφή, είναι το κατά πόσο τα προσόντα ενός επιστημονικού ερευνητή επαρκούν για της διεκπεραίωση μιας ηλεκτρονικής έρευνας. Ο μεγαλύτερος προβληματισμός έγκειται στα χρησιμοποιούμενα από τον ερευνητή εργαλεία λογισμικού. Ο ερευνητής, απλά, γνωρίζει την χρήση ενός εργαλείου λογισμικού. Δεν μπορεί να έχει πρόσβαση στον πηγαίο κώδικα και έτσι δεν γνωρίζει τι εργασίες επιτελεί το λογισμικό. Πως λοιπόν μπορεί να βεβαιώσει ότι τα ψηφιακά δεδομένα, που συλλέχθηκαν, αποδεικνύουν την ενοχή ή την αθωότητα του κατηγορουμένου; Έως σήμερα, δεν υπάρχει απόφαση δικαστηρίου που να απέρριψε την επιστημονική άποψη ενός ερευνητή, τέτοιο ενδεχόμενο, όμως, δεν αποκλείεται να συμβεί στο μέλλον από τη στιγμή που τα εργαλεία λογισμικού εξελίσσονται με ραγδαίους ρυθμούς και γίνονται όλο και πιο πολύπλοκα.

Το τρίτο και τελευταίο ζήτημα αφορά την ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών, η αντιγραφή του μέσου αποθήκευσης, που θα εξεταστεί (π.χ. ενός σκληρού δίσκου) δημιουργώντας ένα ακριβές αντίγραφο (bit stream image), του πρωτοτύπου. Τα δικαστήρια έχουν αποδεχθεί, ότι εφόσον το αντίγραφο είναι ακριβές, τότε θεωρείται γνήσιο. Ωστόσο, πρέπει να λαμβάνεται κάθε απαραίτητο μέτρο για την άρτια διατήρηση του. Οι ψηφιακές πληροφορίες μπορούν να επηρεαστούν από μαγνητικά πεδία καιρικές συνθήκες κ.ά.. Για παράδειγμα, στην υπόθεση Ohio v. Cook[106], ο κατηγορούμενος προέβαλλε μια σειρά από ισχυρισμούς έναντι της μη ορθής συλλογής και διατήρησης των ψηφιακών αποδείξεων, που οδήγησαν στην αλλοίωση τους, όπως η μη τοποθέτηση του σκληρού δίσκου που αφαιρέθηκε σε αντιστατική θήκη. Το δικαστήριο λαμβάνοντας υπόψη τα παραπάνω, καθώς και μια σειρά από άλλες παραλήψεις των διωκτικών αρχών κατά την διατήρηση των ψηφιακών στοιχείων, έκρινε τον κατηγορούμενο αθώο λόγω αμφιβολιών.

---

[105] Μια έρευνα χωρίς ένταλμα, ενδέχεται να γίνει δεκτή από ένα δικαστήριο στην περίπτωση που ο ερευνούμενος, αποποιήσει το δικαίωμα της ιδιωτικότητας. Για παράδειγμα, εάν μεταφέρει τον υπολογιστή του σε ένα εργαστήριο για επισκευή, το δικαίωμα της ιδιωτικότητας μπορεί να χαθεί εφόσον διάφοροι τεχνικοί θα έχουν πρόσβαση στα δεδομένα που ειναι αποθηκευμένα στον υπολογιστή.

[106] Κωνσταντίνος Βλαχόπουλος 2007 σελ 183

7.8. Αστυνομία και ηλεκτρονικό έγκλημα

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος, από της υπηρεσίες επιβολής του νόμου και ιδιαίτερα την αστυνομία, αποτελεί πρωταρχικό ζήτημα. Ο παραδοσιακός τρόπος προσεγγίσεως του εγκλήματος, δηλαδή της περιγραφής του δράστη με την κατάθεση του θύματος, της συλλογής πληροφοριών από πληροφοριοδότες, της διεξαγωγής έρευνας, κατάσχεσης κ.λπ. δεν ισχύει στον κυβερνοχώρο. Για την έρευνα των ηλεκτρονικών εγκλημάτων, απαιτούνται εξειδικευμένες αστυνομικές υπηρεσίες με εκπαιδευμένο προσωπικό και σύγχρονα τεχνικά μέσα.

Οι πρώτες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, ιδρύθηκαν στις Ηνωμένες Πολιτείες της Αμερικής, καθότι από εκεί ξεκίνησε το hacking, στα μέσα της δεκαετίας του '70 και αναπτύχθηκε τόσο η τεχνολογία των ηλεκτρονικών υπολογιστών όσο και το Διαδίκτυο. Σήμερα, στις Η.Π.Α λειτουργούν υπηρεσίες αντιμετώπισης και δίωξης του ηλεκτρονικού εγκλήματος σε κάθε πολιτεία, οι οποίες έχουν τοπική αρμοδιότητα. Οι απειλές, όμως, που προβάλλουν από το οργανωμένο έγκλημα μέσω του κυβερνοχώρου, οδήγησαν στη σύσταση της US-CERT[107] (United States Computer Emergency Readness Team) μιας εθνικής υπηρεσίας που φέρει την κύρια ευθύνη για την ασφάλεια των Η.Π.Α από επιθέσεις που μπορεί να προκύψουν από τον κυβερνοχώρο. Η US-CERT αποτελεί το επιχειρησιακό κομμάτι της NCSD (National Cyber Security Division), η οποία με τη σειρά της υπάγεται στο Υπουργείο Εσωτερικών[108]. Οι κύριες αρμοδιότητες της US-CERT είναι:

- Η ανάλυση των πιθανών διαδικτυακών απειλών και ευπαθειών και η καταβολή προσπαθειών για τον περιορισμό τους.
- Η ενημέρωση των συναρμόδιων υπηρεσιών για πιθανές δικτυακές απειλές.
- Ο συντονισμός των ενεργειών αντιμετώπισης συμβάντων σχετικών με το Διαδίκτυο.

Σε επίπεδο εξέτασης ψηφιακών τεκμηρίων, το Ομοσπονδιακό Γραφείο Ερευνών[109] (Federal Bureau Of Investigation- FBI) διαθέτει το πιο σύγχρονο εργαστήριο στον κόσμο. Το εξειδικευμένο προσωπικό της Computer Analysis and Response Team[110], εξοπλισμένο με τα απαιτούμενα εργαλεία υλικού και λογισμικού, εξετάζει πάσης φύσεως ψηφιακά δεδομένα και υπολογιστικά συστήματα, έχοντας την δυνατότητα για ανάκτηση και ανάλυση αρχείων, σπάσιμο κωδικών, προσδιορισμό του χρόνου και σειράς δημιουργίας των αρχείων κ.ά.

Στην Αγγλία έχει ιδρυθεί Μονάδα Ηλεκτρονικού Εγκλήματος στην Μητροπολική Αστυνομία[111], για την αντιμετώπιση των απειλών με ηλεκτρονικούς υπολογιστές, που οριοθετούνται από το ισχύον νομικό πλαίσιο και, ειδικότερα τη Computer Misuse Act 1990. Επίσης, στον Καναδά έχει ιδρυθεί η Integrated Technological Crime Unit στην Royal Canadian Mounted Police[112].

---

[107] http://www.us-cert.gov
[108] http://www.dhs.gov
[109] http://www.fbi.gov
[110] http://www.fbi.gov/hq/lab/org/cart.htm
[111] http://www.met.police.uk/computercrime/
[112] http://www.rcmp-grc.gc.ca/notices-avis/index-eng.htm

Στην Αυστραλία έχει συνταθεί το Australian High Tech Crime Centre[113] υπαγόμενο στην Ομοσπονδιακή Αστυνομία. Σκοπός του είναι ο συντονισμός των εθνικών προσπαθειών για την πάταξη του ηλεκτρονικού εγκλήματος, καθότι αναγνωρίζει ότι, η αντιμετώπισή του δυσχεραίνεται από πλήθος εμποδίων νομικών και μη. Για το σκοπό αυτό συνεργάζεται και με άλλες υπηρεσίες στον κόσμο, με τις οποίες μπορεί από κοινού να ερευνήσουν υποθέσεις παράνομης δραστηριότητας στο Διαδίκτυο και να ανταλλάξουν τεχνογνωσία.

Στην Ελλάδα η αντιμετώπιση των υποθέσεων ηλεκτρονικού εγκλήματος από την Ελληνική Αστυνομία[114], ουσιαστικά αρχίζει με την ίδρυση του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος το 2004. Έως τότε, οι υποθέσεις που σχετίζονταν καθ' οποιονδήποτε τρόπο με ηλεκτρονικούς υπολογιστές αντιμετωπίζονταν από το Τμήμα Δίωξης Οικονομικού Εγκλήματος.

Το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής ιδρύθηκε με το Π.Δ. 100/2004, έχοντας αρμοδιότητα την δίωξη των εγκλημάτων, που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού εντός της περιοχής δικαιοδοσίας της Διεύθυνσης Ασφάλειας Αττικής, καθώς και την επί 24ώρου βάσεως παρακολούθηση του Διαδικτύου, προς διαπίστωση εγκληματικών πράξεων που τελούνται στη χώρα και την διαβίβαση όλων των απαραιτήτων συναφών στοιχείων στις αρμόδιες υπηρεσίες.

Επίσης με το Π.Δ. 48/2006 ιδρύθηκε το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος στην Υποδιεύθυνση Δίωξης Οικονομικού Εγκλήματος της Γενικής Αστυνομικής Διεύθυνσης Θεσσαλονίκης, με αρμοδιότητες της εντός της περιοχής δικαιοδοσίας της Διεύθυνσης Ασφαλείας Θεσσαλονίκης, δίωξη των εγκλημάτων που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού.

Οι υπηρεσίες αυτές, αν και βρίσκονται στο αρχικό στάδιο λειτουργίας έχουν να επιδείξουν σημαντικό έργο στην καταπολέμηση του ηλεκτρονικού εγκλήματος.

ΑΔΙΚΗΜΑ	ΥΠΟΘΕΣΕΙΣ	ΣΥΛΛΗΦΘΕΝΤΕΣ	ΚΑΤΗΓΟΡΟΥΜΕΝΟΙ
Πορνογραφία ανηλίκων	13	39	40
Απάτη με υπολογιστή	5	3	7
Παραβίαση απορρήτων σε υπολογιστή	3	0	8
Διαρροή διαβαθμισμένων πληροφοριών μέσω Διαδικτύου	1	0	1
Πνευματική δυσφήμηση	3	4	4

[113] http://www.ahtcc.gov.au/
[114] http://www.astynomia.gr/

Συκοφαντική δυσφήμηση	4	1	7
Εξύβριση	3	1	5
Σατανισμός	1	4	4
Απάτη με dialers	2	5	5
ΣΥΝΟΛΟ	**35**	**57**	**81**

Πίνακας 7.5: Στατιστικά στοιχεία εξιχνιασθέντων υποθέσεων Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος κατά το χρονικό διάστημα από 1/1/2004 έως 4/2/2005

7.8.1. Ελληνική Αστυνομική Πραγματικότητα

Η αυξανόμενη διάδοση του Διαδικτύου στη χώρα μας, η χρήση του για διεκπεραίωση καθημερινών εργασιών αλλά και η παροχή από κρατικούς και μη φορείς ηλεκτρονικών υπηρεσιών, έχουν οδηγήσει στην αλματώδη αύξηση των υποθέσεων που σχετίζονται με το ηλεκτρονικό έγκλημα. Ειδικότερα:

7.8.1.1. Case Studies[115]

Φεβρουάριος 2006

Μια 15άχρονη μαθήτρια πέφτει θύμα βιασμού από 28χρονο που γνώρισε σε δωμάτιο συνομιλιών (chat room) στο Internet.

Ιανουάριος 2006

Ένας 35χρονος κατηγορείται ότι σε συνεργασία με ουκρανικά κυκλώματα εφάρμοζε την απάτη του ψαρέματος (phishing), στο Διαδίκτυο. Έστελνε παραπλανητικά e-mail και μάζευε στοιχεία, με τα οποία διεκπεραίωναν ηλεκτρονικές συναλλαγές πελάτες ελληνικών τραπεζών, μεταξύ αυτών και της Εθνικής.

Ένας 67χρονος συνταξιούχος στρατιωτικός και ένας 50χρονος Νιγηριανός, κάτοικος Κύπρου, είχαν στήσει Λοταρία μέσω ιστοσελίδας και e-mails, που υποσχόταν μυθικά ποσά με την προϋπόθεση ότι, οι νικητές θα πλήρωναν τους φόρους. Μέχρι να συλληφθούν είχαν αποσπάσει από ανυποψίαστους χρήστες πάνω από 3,5 εκατομμύρια ευρώ.

Νοέμβριος 2005

Αστυνομικοί συλλαμβάνουν 57χρονο ιδιοκτήτη δύο ιστοσελίδων παιδικής πορνογραφίας, της οποίας οι συνδρομητές ξεπερνούσαν τους 1.000 (καταγράφηκαν πάνω από 360.000 επισκέψεις)

Οκτώβριος 2005

Σύλληψη ενός 40χρονου Δανού, ο οποίος έστελνε ηλεκτρονικά μηνύματα, υφάρπαζε προσωπικά δεδομένα και στη συνέχεια αποσπούσε μεγάλα χρηματικά ποσά από τραπεζικούς λογαριασμούς.

---

[115] Κωνσταντίνος Βλαχόπουλος σελ. 185

Ιούλιος 2005

Εξιχνιάζεται η πρώτη υπόθεση παράνομης κατασκευής όπλων, που διακινούταν μέσω Διαδικτύου. Οι πωλήσεις γινόταν μέσω ιστοσελίδας γνωστής εταιρείας δημοπρασιών και τα όπλα, πιστά αντίγραφα των αυθεντικών, παραδίδονταν στους ενδιαφερόμενους μέσω εταιρείας ταχυμεταφορών.

Το ίδιο διάστημα, συνελήφθη ένας 57χρονος, ο οποίος μαζί με έναν Ολλανδό συντηρούσαν ιστοσελίδα με γυμνές φωτογραφίες, βίντεο και άλλο υλικό με Ελληνίδες, που φωτογραφίζονταν σε ιδιωτικό στούντιο.

Μάιος 2005

Για απάτη χιλιάδων Ευρώ κατηγορήθηκε 32χρονος, ο οποίος συστηνόταν ως μεγαλοεπιχειρηματίας και είχε φτιάξει διάφορα κλειστά δωμάτια συζητήσεων στο Διαδίκτυο (chat rooms), υποσχόμενος στους επισκέπτες συμφέρουσες αγοραπωλησίες ανύπαρκτων φορητών υπολογιστών και αυτοκινήτων.

Απρίλιος 2005

Υπάλληλος ναυτιλιακής εταιρείας, 40 ετών, κατηγορήθηκε ότι κερδοσκοπούσε από τη διακίνηση σκληρότατου υλικού παιδικής πορνογραφίας, μέσω πλαστής πιστωτικής κάρτας.

Παράλληλα, συνελήφθη ένας 42χρονος δικηγόρος, από τη Λάρισα, που είχε πέντε ιστοσελίδες με ανάλογο υλικό, στις οποίες έβαζε φωτογραφίες, που έβρισκε σε άλλα sites στο Διαδίκτυο και στη συνέχεια τις μεταπωλούσε.

Την ίδια ηλικία, είχε και ο ιδιοκτήτης μπαρ στη Μύκονο, στην κατοχή του οποίου, οι αστυνομικοί βρήκαν χιλιάδες δισκέτες και cd-rom με πορνογραφικό υλικό, τις οποίες και εμπορευόταν μέσω internet.

Μάρτιος 2005

Τρία βιβλιάρια καταθέσεων, έξι πιστωτικές κάρτες, μεγάλος αριθμός CD-ROM και δισκετών με υλικό παιδικής πορνογραφίας και δύο «ειδικές» βιντεοκασέτες. Πρόκειται για ευρήματα της αστυνομίας στο σπίτι 39χρονου ιδιωτικού υπαλλήλου, που κατηγορείται ότι διακινούσε παιδοφιλικό υλικό στο Διαδίκτυο.

Φεβρουάριος 2005

Ένας 72χρονος, από την Αττική, κατηγορείται για διοχέτευση φωτογραφιών και βίντεο ιδιαίτερα σκληρής παιδικής πορνογραφίας σε ιστοσελίδα ανάλογου περιεχομένου.

Ιανουάριος 2005

Ένας 18χρονος αυτοκτονεί με οδηγίες που έδωσε ένας άγνωστος μέσω Διαδικτύου. Συγκεκριμένα, χρησιμοποίησε μήνυμα, το οποίο υποδείκνυε στον αυτόχειρα ως τρόπο αυτοκτονίας τη λήψη συγκεκριμένου γεωργικού φαρμάκου.

Περισσότερους από 1.000.000 επισκέπτες είχε η ιστοσελίδα ενός 29χρονου ιδιοκτήτη καταστήματος στον Βύρωνα που συνέλαβαν αστυνομικοί. Οι φωτογραφίες που πωλούσε, απεικόνιζαν 14χρονα γυμνά κορίτσια αλλά και ανυποψίαστους πολίτες την ώρα που ήταν σε κάποια τουαλέτα ή σε δοκιμαστήρια καταστημάτων ρούχων.

Δεκέμβριος 2004

Ο υπεύθυνος του γραφείου Τύπου της ΓΣΕΕ συλλαμβάνεται για μαστροπεία κατ' εξακολούθηση και για διακίνηση υλικού παιδικής πορνογραφίας. Στο σπίτι του βρέθηκαν και κατασχέθηκαν οκτώ πιστωτικές κάρτες διαφόρων τραπεζών και πλήθος αγγελιών κυρίως, κοριτσιών.

Για παράνομη διακίνηση λογισμικού συνελήφθη 35χρονος στους Αμπελόκηπους. Στο σπίτι του βρέθηκαν σκληροί δίσκοι τεράστιας χωρητικότητας με κάθε λογής προγράμματα, μουσική και ταινίες DVD, με τις οποίες πωλούσε μέσω Internet. Το πελατολόγιο του ξεπερνούσε τους 17.000 συνδρομητές.

Νοέμβριος 2004

Τέσσερα άτομα κατηγορούνται ότι, είχαν κατασκευάσει από το 2002 ιστοσελίδα πορνογραφικού περιεχομένου, στην οποία διακινούσαν βιντεοσκοπημένο υλικό από ζευγάρια σε ξενοδοχεία, καθώς και φωτογραφίες γυμνών γυναικών από δοκιμαστήρια καταστημάτων.

Για παράνομη διακίνηση μέσω Διαδικτύου παράνομων προγραμμάτων ηλεκτρονικών υπολογιστών, μεταξύ αυτών και μεγάλης αεροναυπηγικής βιομηχανίας με ευαίσθητες πληροφορίες, κατηγορείται ένας 50χρονος από την Αθήνα.

Σεπτέμβριος 2004

Ένας 27χρονος ομολογεί, ότι έβγαζε κρυφά φωτογραφίες μικρών παιδιών, που εντόπιζε στα αποδυτήρια παιδικών κατασκηνώσεων, ποδοσφαιρικών ομάδων και διαφόρων σχολείων, τις οποίες, στη συνέχεια, διακινούσε σε ξένες ιστοσελίδες αντί αμοιβής.

Τον ίδιο μήνα συνελήφθησαν δυο 32χρονοι, οι οποίοι διείσδυσαν στα υπολογιστικά προγράμματα ελληνικής τράπεζας και μετέφεραν χρήματα στους δικούς τους λογαριασμούς.

7.8.1.2. Case studies για social networks[116]

Προσωπικά δεδομένα που γίνονται αντικείμενο εκβιασμού, φωτογραφίες και βίντεο από προσωπικές στιγμές που γίνονται μέσο εκδίκησης για έναν χωρισμό, κυκλώματα πορνείας που παγιδεύουν ανυποψίαστους χρήστες, deal ναρκωτικών και παράνομων ουσιών, δημόσιος εξευτελισμός λόγω προσωπικής ή επαγγελματικής αντιζηλίας, ανακοίνωση διαζυγίου μέσα από χώρους κοινωνικής δικτύωσης, απολύσεις εξαιτίας σχολίων σε διάφορα social networks είναι ορισμένα από τα όσα αρνητικά συμβαίνουν το

---

[116] http://www.zougla.gr/news.php?id=24637 (Ημερομηνία πρόσβασης: 02/09/09)

τελευταίο διάστημα στην ιντερνετική σφαίρα των Facebook, My Space και άλλων παρόμοιων διαδικτυακών τόπων κοινωνικής δικτύωσης που μετρούν εκατομμύρια μέλη.

Εκβιασμοί

1. Η ηθοποιός Άννα-Ίρις Αγαθονικιάδη εκβίαζε μαζί με τον σύντροφο της έναν πολιτικό μηχανικό τον οποίο γνώρισαν σε chat γνωστού ιστότοπου και με τον οποίο είχαν σεξουαλικές επαφές επί πληρωμή. Η αστυνομία συνέλαβε επ' αυτοφώρω το ζευγάρι να λαμβάνει 2.000 ευρώ (αντί 6.000 ευρώ που αρχικά ζητούσαν) από τον πολιτικό μηχανικό προκειμένου να μην δημοσιοποιήσουν το ροζ DVD.
2. Δυο κοπέλες, μια 24χρονη υπάλληλος εταιρείας από τη Βόρειο Ελλάδα και μια 19χρονη φοιτήτρια κολεγίου από την Αθήνα έπεσαν θύματα εραστών που γνώρισαν μέσω του Facebook. Οι ανυποψίαστες κοπέλες έκαναν cyber sex με τους εραστές που γνώρισαν στο διαδίκτυο και οι οποίοι κατέγραψαν το ιντερνετικό σεξ εκβιάζοντάς τες στη συνέχεια ότι αν δεν έκαναν σεξ με δυο, τρεις ή και περισσότερους φίλους τους θα δημοσιοποιούσαν σε όλες τις "επαφές" των κοριτσιών τα εν λόγω βίντεο. Οι κοπέλες αρνήθηκαν να υποκύψουν και οι εκβιαστές τους έκαναν πράξη τις απειλές τους! Η άσχημη ψυχολογική κατάσταση των δυο γυναικών τις ώθησε να επικοινωνήσουν μεν με τη Δίωξη Ηλεκτρονικού Εγκλήματος, χωρίς όμως να υποβάλλουν μηνύσεις εναντίον των δυο εκβιαστών.
3. Περισσότερους από 30 συμμαθητές του εκβίαζε ένας 18χρονος από το Μιλγουόκι των ΗΠΑ για τουλάχιστον 2 χρόνια. Ο νεαρός είχε δημιουργήσει δύο λογαριασμούς στο Facebook –ως κορίτσι- με τα ονόματα Κάιλα και Έμιλυ και μέσω αυτών, προσέγγιζε τους συμμαθητές τους και τους έπειθε να του στέλνουν γυμνές φωτογραφίες τους. Όταν του έστελναν το υλικό, τους έλεγε ποιος ήταν και στη συνέχεια τους εκβίαζε ότι θα τους διασύρει στο διαδίκτυο αν δεν έχουν ερωτικές περιπτύξεις μαζί του.

Ερωτική εκδίκηση

1. Ένας 18χρονος έφηβος από τα Τρίκαλα ανέβασε στο facebook γυμνές φωτογραφίες της πρώην 20χρονης κοπέλας του, προκειμένου να την εκδικηθεί επειδή τον χώρισε. Ο 18χρονος μάλιστα δημιούργησε προφίλ με τα προσωπικά στοιχεία της κοπέλας όπου και ανέβασε τις φωτογραφίες. Συνελήφθη από τις αρχές ύστερα από την καταγγελία της 20χρονης.
2. Μια 25χρονη κοπέλα από το Παγκράτι, έπεσε θύμα εκδίκησης του πρώην 30χρονου συντρόφου της όταν αποφάσισε να τον χωρίσει. Ο πληγωμένος πρώην σύντροφος της, ανέβασε στο διαδίκτυο φωτογραφίες από προσωπικές τους στιγμές αλλά και βίντεο με ερωτικές περιπτύξεις, όχι όμως ολόκληρο αφού το "έκοψε" στο επίμαχο σημείο, λέγοντας στη συνέχεια στην κοπέλα ότι αν δεν ξαναγίνονταν ζευγάρι, θα δημοσιοποιούσε και το υπόλοιπο.

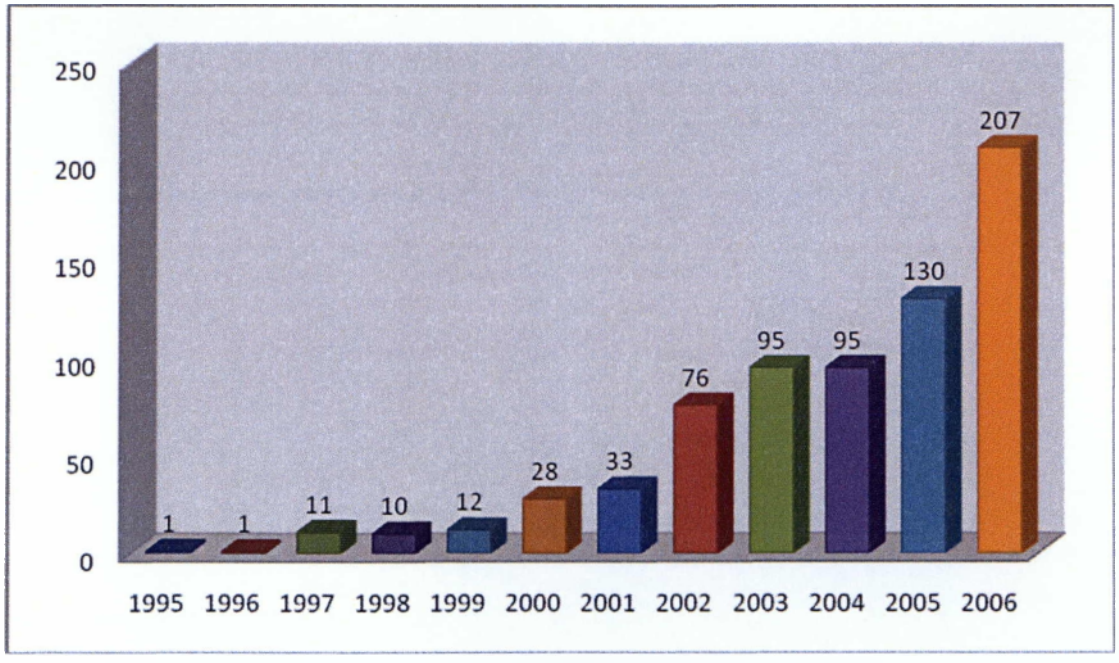
Ακραίες περιπτώσεις

1. Ο Βρετανός Έντουαρτ Ρίτσαρντσον καταδικάστηκε σε 18 χρόνια φυλάκιση για τη δολοφονία της εν διαστάσει γυναίκας του, η οποία είχε αλλάξει το status της στο Facebook. Ο 40χρονος που είχε χωρίσει από την 26χρονη Σάρα λίγες ημέρες νωρίτερα, είχε οργιστεί με την κίνησή της να βάλει πως δεν είναι παντρεμένη στη σελίδα της. Πήγε στο σπίτι των γονιών της, καθώς δεν του απαντούσε στα μηνύματα που της έστελνε και τη μαχαίρωσε μέχρι θανάτου, μην μπορώντας να δεχτεί πως ο γάμος τους είχε λάβει τέλος.

2. Η Emma Brady υποστηρίζει πως έμαθε ότι ο 6-χρονος γάμος της θα λάβει τέλος από ένα μήνυμα που δημοσίευσε ο σύζυγος της στην ιστοσελίδα του facebook! Το μήνυμα απλώς ανέφερε: «Ο Neil Brady θα διακόψει τον γάμο του με την Emma Brady.» Η 39-χρονη γυναίκα έμαθε ότι ο άντρας της τη χώρισε μέσα από το Facebook όταν μια φίλη της από την Δανία της τηλεφώνησε για να δει εάν είναι καλά.

Το έργο των παραπάνω υπηρεσιών, συνεπικουρείται από τα εργαστήρια της Διεύθυνσης Εγκληματολογικών Ερευνών. Ειδικότερα, στο Εργαστήριο Γραφολογίας λειτουργεί Τομέας Εξέτασης Ψηφιακών Τεκμηρίων[117], ο οποίος:

- Ενεργεί εξετάσεις, αναγνώσεις και συγκρίσεις ψηφιακών δεδομένων ή αρχείων, ευρισκόμενων σε αποθηκευτικούς χώρους Η/Υ ή σε περιφερειακά συστήματα.
- Ενεργεί εξετάσεις περί της γνησιότητας λογισμικού.
- Ενεργεί εξετάσεις σε κινητά τηλέφωνα ή άλλες ηλεκτρονικές συσκευές, οι οποίες περιέχουν ή αποθηκεύουν ψηφιακά δεδομένα.
- Ενεργεί εξετάσεις και αναγνώσεις δεδομένων σε μαγνητικές ταινίες πιστωτικών ή άλλων καρτών, καθώς και εξετάσεις άλλων σύγχρονων μέσων ψηφιακής αποθήκευσης δεδομένων σε ηλεκτρονικό κύκλωμα ή άλλης μορφής αποθηκευτικούς χώρους.
- Παρέχει τεχνική συνδρομή σε διαδικασίες κατάσχεσης, μεταφοράς, αποθήκευσης και αποστολής των ψηφιακών τεκμηρίων, που σχετίζονται με εγκληματική δραστηριότητα.
- Τηρεί αρχείο διενεργούμενων εργαστηριακών εξετάσεων καθώς και συλλογές ψηφιακών πειστηρίων, λογισμικών και συσκευών ψηφιακής αποθήκευσης, προς υποβοήθηση των συγκριτικών εξετάσεων.



Εικόνα 7.6: Υποθέσεις που απασχόλησαν το εργαστήριο εξέτασης ψηφιακών τεκμηρίων

[117] Η εξέταση ψηφιακών τεκμηρίων από τη διεύθυνση Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας, ξεκίνησε το 1995 με αφορμή την ανάγκη εξέτασης των προκηρύξεων της τρομοκρατικής οργάνωσης «17 Νοέμβρη» που γράφονταν πλέον με τη χρήση ηλεκτρονικού υπολογιστή.

Η πρώτη υπόθεση που ασχολήθηκε το εργαστήριο ήταν το 1995. Από κει και έπειτα, οι υποθέσεις πολλαπλασιάστηκαν με γεωμετρικούς ρυθμούς, όπως φαίνεται και από το παραπάνω γράφημα.

Σήμερα, το εργαστήριο διαθέτει εξειδικευμένο προσωπικό και τεχνικά μέσα για την διεκπεραίωση απαιτητικών εργασιών.

7.9. Λογισμικό διερεύνησης ηλεκτρονικού εγκλήματος

Η διερεύνηση του ηλεκτρονικού εγκλήματος, από τις αρμόδιες αρχές απαιτεί την χρήση κατάλληλου λογισμικού. Οι πληροφορίες, που αποθηκεύονται σε ένα υπολογιστή ή διακινούνται μέσω ενός δικτύου, δεν είναι δυνατόν να ανακτηθούν και να εξεταστούν με φυσικό τρόπο. Τα πακέτα λογισμικού, που δημιουργούνται για την κάλυψη αναγκών των διωκτικών αρχών και των εργαστηρίων εξέτασης ψηφιακών τεκμηρίων έχουν εξελιχθεί σημαντικά τα τελευταία χρόνια, επιτυγχάνοντας το συνδυασμό τριών βασικών στοιχείων: Την ακρίβεια των δεδομένων που ανακτούνται, την ταχύτητα ανάκτησής τους και την δυνατότητα επεξεργασίας μεγάλου όγκου δεδομένων για την εύρεση των αναγκαίων πληροφοριών.

EnCase Forensics

Το λογισμικό EnCase Forensics, της εταιρείας Guidance Software[118], χρησιμοποιείται από τις πιο σημαντικές υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, όπως το FBI και η Scotland Yard, καθώς και από κρατικές και στρατιωτικές υπηρεσίες και οργανισμούς. Το πολύ φιλικό με το χρήστη γραφικό περιβάλλον και οι πολυάριθμες δυνατότητες εύρεσης, ανάκτησης επεξεργασίας και παρουσίασης ψηφιακών δεδομένων, έχουν αναγάγει το EnCase στο κορυφαίο λογισμικό στο τομέα των Computer Forensics.

Το λογισμικό χρησιμοποιείται επίσης, από εργαστήρια εξέτασης ψηφιακών τεκμηρίων, καθώς εκτός από τις δυνατότητες ανάκτησης αρχείων, που έχουν διαγραφεί ή αποκρυφτεί σε ένα ηλεκτρονικό υπολογιστή, έχει τη δυνατότητα να επεξεργάζεται, σε πολύ λίγο χρόνο, τεράστιες ποσότητες δεδομένων.

Τα βασικά χαρακτηριστικά του λογισμικού EnCase είναι τα ακόλουθα:

- Υποστηρίζει όλα τα συστήματα αρχείων (FAT12, FAT16, FAT32, NTFS, Macintosh HFS, HFS+ κ.ά.) και όλα τα λειτουργικά συστήματα. Δίνεται ακόμη και η δυνατότητα αξιοποίησης του σε συστοιχίες δίσκων (RAIDS).
- Κατά τη διάρκεια της διαδικασίας δημιουργίας αντιγραφών των υπό εξέταση δίσκων και άλλων αποθηκευτικών μέσων (το αρχείο αποδείξεων – evidence file) γίνεται, επανειλημμένως, έλεγχος για την ακρίβεια των δεδομένων, στο τέλος δε πραγματοποιείται ένας ακόμη οριστικός έλεγχος με τον αλγόριθμο MD5[119], για να είναι βέβαιο ότι το αρχείο αποδείξεων είναι πιστό αντίγραφο του αρχικού δικαίου.

---

[118] Βλ. στον δικτυακό τόπο της εταιρείας http://www.guidancesoftware.com/computer-forensics-ediscovery-software-digital-evidence.htm ((Ημερομηνία πρόσβασης: 27/08/09)

[119] Ο αλγοριθμος MD5 είναι από τους πλέον αξιόπιστους καθώς παράγει αθροίσματα ελέγχου που διαφέρουν κατά πολύ μεταξύ τους έστω και εάν αλλάξει μόνο ένα γράμμα στη λέξη ή φράση. Για παράδειγμα, το hash της λέξης «e-banking» είναι το 8966f01c4a3f9a06ac 9dc99c658fe9c8, ενώ της λέξης «e-Banking» είναι το 4fa944c3c8520f5b6edc0516e7065f08 (εντελώς διαφορετικό).

- Τα αρχεία που εξετάζονται, μπορούν να ταξινομηθούν με βάση τριάντα διαφορετικά κριτήρια, όπως ημερομηνία πρόσβασης, ημερομηνία δημιουργίας, ημερομηνία τροποποίησης, όνομα, διαδρομή, άδεια χρήσης, άθροισμα ελέγχου κ.ά.. Επίσης, μπορούν να εφαρμοστούν φίλτρα και να γίνουν ερωτήματα για γρηγορότερη ανάκτηση των επιθυμητών δεδομένων.
- Μπορούν να ανακτηθούν διαγραμμένα αρχεία, swap και page files, να ερευνηθεί η slack area κ.ά.
- Υποστηρίζεται Unicode και έτσι μπορούν να αναγνωστούν αρχεία σε οποιαδήποτε γλώσσα.
- Το πρόγραμμα δημιουργεί αυτόματα ένα χάρτη με όλα τα αρχεία που συνδέονται μεταξύ τους, προκειμένου ο ερευνητής να μπορεί να ελέγξει την διαδρομή, που ακολουθούν τα στοιχεία σε ένα σύστημα.
- Αναγνωρίζει αυτόματα όλες τις συσκευές (hardware), που είναι συνδεδεμένες στο σύστημα, δίνοντας πρόσθετες πληροφορίες, όπως το είδος, η εταιρεία κατασκευής, η έκδοση κ,λπ.
- Ανακτά αυτόματα τα εφεδρικά αρχεία, που δημιουργούνται από εφαρμογές, όπως αυτές που περιλαμβάνονται στη σουίτα Microsoft Office.
- Παρέχει εξελιγμένες δυνατότητες αναζήτησης αρχείων.
- Έχει τη δυνατότητα να δημιουργεί αναλυτικές αναφορές για δικαστική χρήση, ανάλογα με τις επιθυμίες του χρήστη. Για παράδειγμα, μπορεί να δημιουργήσει μια αναφορά, που να περιλαμβάνει μια λίστα με τις διευθύνσεις, που επισκέφτηκε ο χρήστης στο Διαδίκτυο, ταξινομημένες κατά ημέρα και ώρα, έχοντας επισημάνει με έντονη γραφή αυτές που σχετίζονται άμεσα με την εξεταζόμενη υπόθεση.
- Περιέχει εξειδικευμένα εργαλεία για την έρευνα μηνυμάτων ηλεκτρονικού ταχυδρομείου και την δραστηριότητα στο Διαδίκτυο. Για παράδειγμα, εξετάζει το ιστορικό, την μνήμη cache, τα άμεσα μηνύματα κ.ά.
- Με την γλώσσα προγραμματισμού EnScript, που έχει ενσωματωθεί στο λογισμικό, ο ερευνητής μπορεί να δημιουργήσει δικά του σενάρια για να επιταχύνει κάποιες διαδικασίες ανάλογα με την έρευνα που επιτελεί.

Computer Incident Response Suite (CIRS)

Το CIRS[120] αποτελεί το κορυφαίο πακέτο λογισμικού της εταιρείας New Technologies Int., στον τομέα των Computer Forensics. Απευθύνεται σε οργανισμούς, κρατικούς ή μη και σε υπηρεσίες επιβολής του νόμου. Περιλαμβάνει εικοσιένα διαφορετικά προγράμματα, για την αντιμετώπιση κάθε ανάγκης κατά την έρευνα ενός ηλεκτρονικού υπολογιστή, όπως δημιουργία αντιγράφων δίσκων, δισκετών και άλλων αποθηκευτικών μέσων, εργαλείο αυτόματης αναγνώρισης αριθμών πιστωτικών καρτών, τηλεφωνικών αριθμών και τραπεζικών λογαριασμών, ανάκτηση διαγεγραμμένων αρχείων, αυτόματη αναγνώριση λογαριασμών Διαδικτύου, αναζήτηση αρχείων κ.ά.

LimeWire Investigator

Ο LimeWire Investigator, της εταιρείας λογισμικού Wetstone, αποτελεί ένα σύγχρονο εργαλείο στα χέρια των ερευνητών για τον έλεγχο υπολογιστικών συστημάτων. Το κύριο χαρακτηριστικό του είναι, ότι μπορεί να κάνει πλήρη ανάλυση του υπολογιστή- στόχου, χωρίς να απαιτηθεί να τερματιστεί η λειτουργία του. Η σύνδεση του με τον υπολογιστή-

[120] Κωνσταντίνος Βλαχόπουλος 2007 σελ.194

στόχο μπορεί να πραγματοποιηθεί είτε απευθείας, είτε απομακρυσμένα με τη χρήση ασφαλούς σύνδεσης τοπικού δικτύου, χωρίς να απαιτείται η εγκατάσταση ειδικού λογισμικού. Η εξέταση του υπολογιστή στόχου πραγματοποιείται, ενώ αυτός συνεχίζει να λειτουργεί κανονικά. Η δυνατότητα αυτή επιτρέπει στο λογισμικό:

- Να καταγράφει τις μεταβολές, που πραγματοποιούνται από τις τρέχουσες διαδικασίες στα αρχεία καταγραφής και το μητρώο του συστήματος..
- Να συλλέγει πληροφορίες για τα προγράμματα που εκτελούνται, τις συνδέσεις δικτύου και τις μεταδόσεις δεδομένων.
- Να αποκτά πληροφορίες, που θα χάνονταν αν τερματίζονταν η λειτουργία του υπολογιστή στόχου όπως π.χ. τις διεργασίες που εκτελούνται στο παρασκήνιο.
- Να ερευνά, τυχόν, παραβατική δραστηριότητα τη στιγμή ακριβώς που εκδηλώνεται.

Wireless StrongHold Bag

Αποτελεί μια μοναδική πατέντα της εταιρείας Paraben Forensics[121]. Είναι μια σακούλα κατασκευασμένη από ειδικά υλικά (τρεις μεμβράνες από νικέλιο, χαλκό και άργυρο), οι οποίες δεν επιτρέπουν σε ασύρματα δίκτυα να έρθουν σε επαφή με κάποια ηλεκτρονική συσκευή. Χρησιμοποιείται, π.χ. για τον αποκλεισμό πρόσβασης στο ασύρματο ενδοδίκτυο ενός φορητού υπολογιστή, ο οποίος εξετάζεται από τον εξερευνητή στο χώρο του οργανισμού για την εύρεση σημαντικών δεδομένων, που πιθανώς έχουν αποθηκευτεί σε αυτόν.

Εικόνα 7.7: Wireless StrongHold Bag

WinHex Editor και X-Ways Trace

Ο WinHex Editor αποτελεί ένα ισχυρό εργαλείο λογισμικού, με το οποίο μπορούν να διεκπεραιωθούν πολλές εργασίες κατά την έρευνα ενός υπολογιστή για την εύρεση ψηφιακών αποδείξεων. Στην έκδοση forensics, που προορίζεται για τις υπηρεσίες επιβολής του νόμου, περιλαμβάνονται διάφορα χαρακτηριστικά[122], όπως αντιγραφή δίσκων (imaging), ανάκτηση αρχείων, αναζήτηση αρχείων, αυτόματη επεξεργασία των

[121] http://www.paraben-forensics.com/catalog/product_info.php?cPath=26&products_id=173 (Ημερομηνία πρόσβασης: 09/09/09)

[122] Βλ. τα πλήρη χαρακτηριστικά της έκδοσης forensics : http://www.x-ways.net/forensics/index-m.html (Ημερομηνία πρόσβασης: 09/09/09)

αρχείων καταγραφής, αυτόματη αναγνώριση εγγράφων του Office και PDF που έχουν κρυπτογραφηθεί, αυτόματη εξαγωγή εικόνων που περιλαμβάνονται σε έγγραφα του Office κ.ά.

Το X-Ways Trace[123] είναι ένα πολύ απλό και ισχυρό εργαλείο για την άντληση πληροφοριών, σχετικά με την δραστηριότητα ενός υπολογιστή στο Διαδίκτυο. Έχει την δυνατότητα να εξάγει πληροφορίες από τα αρχεία index.dat, που δημιουργούνται από τον φυλλομετρητή Internet Explorer. Ένα αρχείο index.dat αποτελεί μια βάση δεδομένων, στην οποία αποθηκεύονται πληροφορίες για τις τοποθεσίες, που επισκέφτηκε ο χρήστης κατά την πλοήγησή του στο Διαδίκτυο. Το κύριο χαρακτηριστικό των αρχείων αυτών είναι ότι οι πληροφορίες που περιέχουν δεν σβήνονται, όταν διαγραφεί το ιστορικό και τα προσωρινά αρχεία και γενικότερα, η διαγραφή τους είναι εφικτή μόνο από έμπειρους χρήστες και μόνο με τη χρήση κατάλληλων εργαλείων λογισμικού. Επομένως, εάν εξετάσουμε τα αρχεία index.dat ενός συστήματος, θα αντλήσουμε πολύ σημαντικές πληροφορίες για τις διευθύνσεις, που έχει επισκεφτεί ο χρήστης του υπολογιστή.

[123] http://www.x-ways.net/trace/index-m.html (Ημερομηνία πρόσβασης: 09/09/09)

ΕΠΙΛΟΓΟΣ

Η μορφή του εγκλήματος, όπως την γνωρίζουμε ως σήμερα, συνεχώς μεταβάλλεται. Οι νέες τεχνολογίες, αλλάζουν τους τρόπους και τα μέσα τέλεσης συμβατικών εγκλημάτων, ενώ νέες μορφές, αμιγώς ηλεκτρονικών εγκλημάτων, κάνουν την εμφάνιση τους. Ως αποτέλεσμα, το έργο των διωκτικών αρχών, η νομοθεσία και γενικά όλοι οι τομείς που επηρεάζουν την μεθοδολογία διερεύνησης των εγκλημάτων και το σύστημα απονομής δικαιοσύνης σε κάθε χώρα, μεταβάλλονται.

Οι σύγχρονες τεχνολογίες, επέφεραν σημαντικές αλλαγές σε κάθε μορφή εγκληματικής συμπεριφοράς, που ως σήμερα χαρακτηριζόταν συμβατική. Η εισχώρηση της τεχνολογίας στις καθημερινές δραστηριότητες του σύγχρονου ανθρώπου, η διείσδυση και χρήση ηλεκτρονικών συσκευών από το σύνολο του πληθυσμού, οδηγούν σε μια μορφή εγκλημάτων, όπου σε κάθε συμβατικό έγκλημα οι τεχνολογικά εξελιγμένες συσκευές, διαδραματίζουν κυρίαρχο ρόλο, χρησιμοποιούνται βοηθητικά ή αποτελούν φορείς σημαντικών αποδείξεων σε ψηφιακή μορφή.

Οι σύγχρονες εγκληματικές απειλές κινούνται σε δύο διαφορετικές διαστάσεις: αφενός, προβάλλουν τα γνήσια εγκλήματα του κυβερνοχώρου, που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και του Διαδικτύου. Κύρια χαρακτηριστικά αυτών, είναι η χρησιμοποίηση τεχνολογικά εξελιγμένων συσκευών και υψηλής τεχνογνωσίας. Αφετέρου, τα γνωστά συμβατικά εγκλήματα αποκτούν μια περισσότερο υβριδική μορφή, όπου οι νέες τεχνολογίες διαδραματίζουν σημαντικό ρόλο.

Για αντιμετώπιση των απειλών αυτών, κάθε οργανισμός πρέπει να μεριμνήσει για την πρόληψη εκδήλωσης των επιθέσεων, την ανίχνευση των επιθέσεων και τέλος την αντίδραση προς αποκατάσταση της ζημιάς που προκλήθηκε από μια επίθεση. Το τρίπτυχο αυτό της ασφάλειας, υπάγεται στην γενικότερη πολιτική ασφάλειας, που αποτελεί ένα συνδυασμό τεχνολογικών μέτρων αλλά και συνεχούς εκπαίδευσης και επιμόρφωσης του προσωπικού, σε θέματα ασφαλείας.

Στο νέο αυτό περιβάλλον, οι διωκτικές αρχές καλούνται, επίσης, να αντιμετωπίσουν το έγκλημα κινούμενες προς δύο κατευθύνσεις: να εκσυγχρονίσουν και να εκπαιδεύσουν τις υφιστάμενες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος και τα εργαστήρια εξέτασης ψηφιακών τεκμηρίων στις υψηλές τεχνολογίες και να εκπαιδεύσουν το προσωπικό των υπηρεσιών στην μεθοδολογία διερεύνησης εγκλημάτων στα οποία συμμετέχει καθ' οποιονδήποτε τρόπο η ψηφιακή τεχνολογία.

Παράρτημα Α'

Γλωσσάρι ορών πληροφορικής

Antivirus Πρόγραμμα το οποίο σαρώνει την μνήμη του υπολογιστή και τα μέσα μαζικής αποθήκευσης για να εντοπίσει, να απομονώσει και να εξαλείψει τους ιούς, ενώ εξετάζει επίσης τα εισερχόμενα αρχεία για ιούς τη στιγμή που τα παραλαμβάνει ο υπολογιστής.

Backup (Εφεδρικό αντίγραφο, αντίγραφο ασφαλείας). Ακριβές αντίγραφο προγράμματος, δίσκου ή δεδομένων, που δημιουργείται είτε για λόγους αρχειοθέτησης είτε για την αποτροπή της απώλειας πολύτιμων αρχείων σε περίπτωση φθοράς ή καταστροφής του ενεργού αντιγράφου. Ορισμένες εφαρμογές δημιουργούν αυτόματα εφεδρικά αντίγραφα των αρχείων δεδομένων, διατηρώντας στο δίσκο τόσο την τρέχουσα όσο και την προηγούμενη εκδοχή του αρχείου. Ονομάζεται επίσης: backup copy, backup file.

Bandwidth (εύρος ζώνης) Η προστασία των δεδομένων που μπορεί να μεταδοθεί σε συγκεκριμένο χρόνο. Σε ψηφιακές συσκευές το bandwidth μετριέτε σε bits ανά δευτερόλεπτο (bps) ή bytes ανά δευτερόλεπτο. Σε αναλογικές συσκευές το bandwidth μετρίεται σε κύκλους ανά δευτερόλεπτο (Hertz – Hz). Το bandwidth είναι ιδιαίτερα σημαντικό σε συσκευές εισόδου – εξόδου (I/O). Για παράδειγμα, ένας ταχύτατος σκληρός δίσκος μπορεί να εμποδίζεται στη λειτουργία του από ένα bus με μικρό bandwidth. Αυτός είναι και ο βασικός λόγος, για τον οποίο συνεχώς σχεδιάζονται και υλοποιούνται νέα bytes για τους υπολογιστές, όπως το AGB και το USB.

BIOS (Basic Input/ Output System) Ένα σύνολο εντολών ενσωματωμένων μέσα στον υπολογιστή που ελέγχει το πώς οι πληροφορίες και τα δεδομένα ρέουν προς και από τον υπολογιστή.

Bit (Binary Digit. Δυαδικό ψηφίο (0 ή 1). Χρησιμοποιείται για την έκφραση μιας από δυο δυνατές καταστάσεις ή τιμές. Στο δυαδικό 0 δεν υπάρχει ροή ή τάση από ηλεκτρικό ρεύμα, ενώ στο 1 υπάρχει.

Boot Sector (Τομέας Εκκίνησης) Σε έναν υπολογιστή ο όρος Boot αναφέρεται στη διαδικασία εκκίνησης του λειτουργικού συστήματος και μεταφοράς του στην κύρια μνήμη. Το Boot Sector είναι η περιοχή στην επιφάνεια ενός δίσκου, όπου είναι η αποθηκευμένες οι πληροφορίες του λειτουργικού συστήματος που θα χρειαστούν κατά την εκκίνηση.

Byte Ο όρος αφορά τον συνδυασμό δυαδικών ψηφίων που αποτελεί ενιαία και αυτοτελή μονάδα για τον ηλεκτρονικό υπολογιστή. Ο συνδιασμός αυτός μπορεί να έχει την τιμή χαρακτήρα μέσα στις υπόλογιστικές διατάξεις. Μια ψηφιολέξη αποτελείται από 8 bits και μπορεί να εκφράζει είτε ένα χαρακτήρα, είτε δύο ψηφία.

Cache Πρόκειται για τη μνήμη που παρεμβάλλεται μεταξύ κύριας μνήμης και επεξεργαστή, με σκοπό την ταχύτερη τροφοδοσία του τελευταίου με δεδομένα και την ταχύτερη ανάκληση εντολών και λειτουργιών από προηγούμενες επεξεργασίες. Η Cache είναι μνήμη υψηλής ποιότητας και ταχύτητας, άρα και κόστους. Όσο περισσότερη διαθέτει ένα σύστημα, τόσο ανεβαίνει κατακόρυφα η απόδοση του.

Chat Συνδιάλεξη σε πραγματικό χρόνο μέσω υπολογιστή. Όταν κάποιος πληκτρολογήσει μια γραμμή κειμένου και μετά πατήσει το πλήκτρο Enter, οι λέξεις εμφανίζονται στις οθόνες όλων των άλλων που συμμετέχουν, οι οποίοι μπορούν να απαντήσουν ανάλογα. Οι

περισσότερες ηλεκτρονικές υπηρεσίες άμεσης επικοινωνίας υποστηρίζουν συνομιλία στο Διαδίκτυο.

Chat room (δωμάτιο συζητήσεων) Ο ανεπίσημος όρος για το κανάλι επικοινωνίας δεδομένων που συνδέει υπολογιστές επιτρέποντας σε χρήστες να συνομιλούν στέλνοντας μηνύματα κειμένου σε πραγματικό χρόνο.

Client/Server network Τοπικό δίκτυο δομημένο με βάση το διαχωριστικό των κόμβων σε μηχανήματα πελάτες(χρήστες) και υπολογιστές-διακομιστές, οι οποίο κάνουν μέρος της επεξεργασίας (που λέγεται παρασκηνιακή επεξεργασία) για τα μηχανήματα πελάτες, για παράδειγμα την ταξινόμηση των εγγραφών μιας βάσης δεδομένων ώστε να παραδοθούν μόνο οι εγγραφές που ζήτησε ο πελάτης.

Cookies Πληροφορίες που αποστέλλονται από έναν Web server σε κάποιον Web browser. Οι πληροφορίες αυτές αποθηκεύονται με τη μορφή ενός text file. Κάθε φορά που ο browser ζητήσει μια ιστοσελίδα από τον Web server, αυτές οι πληροφορίες αποστέλλονται πίσω σε αυτόν.

Crack (σπάζω) Αποκτώ μη εξουσιοδοτημένη πρόσβαση σε κάποιο δίκτυο παραβιάζοντας τα μέτρα ασφαλείας. Επίσης αποκρυπτογραφώ κρυπτογραφημένες πληροφορίες.

Cryptography (κρυπτογραφία) Η κωδικοποίηση πληροφοριών με τρόπο ώστε να μην είναι κατανοητές από κανέναν άλλο εκτός από τα άτομα που διαθέτουν το κλειδί του κώδικα.

Cyberspace (κυβερνοχώρος) Το σύνολο των ηλεκτρονικών κόσμων, όπως το Διαδίκτυο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση.

Dial up Αναφέρεται ή χαρακτηρίζεται μια σύνδεση η οποία χρησιμοποιεί το δημόσιο τηλεφωνικό δίκτυο.

DNS Ακρωνύμιο του Domain Name System, του ιεραρχικού συστήματος που χρησιμοποιείται για την ονομασία τοποθεσιών στο Internet.

FAT file system Το σύστημα που χρησιμοποιείται από το MS-DOS για την οργάνωση και την διαχείριση αρχείων. Ο FAT είναι μια δομή δεδομένων την οποία δημιουργεί το MS-DOS στον δίσκο όταν ο δίσκος διαμορφώνεται. Όταν το MS-DOS αποθηκεύει ένα αρχείο σε ένα φορμαρισμένο δίσκο, το λειτουργικό σύστημα τοποθετεί πληροφορίες για το αποθηκευμένο αρχείο στον πίνακα FAT, ώστε να μπορεί αργότερα να ανακτήσει το αρχείο όταν του ζητηθεί.

Firewall Το firewall είναι ένα λογισμικό ή μια συσκευή που προστατεύει τους πόρους του δικτύου από τους χρήστες άλλων δικτύων.

Format Η διαδικασία διαμόρφωσης ενός αποθηκευτικού μέσου (δισκέτα, σκληρός δίσκος, μαγνητική ταινία) από το λειτουργικό σύστημα, έτσι ώστε το μέσο αυτό να είναι έτοιμο να δεχτεί δεδομένα προς εγγραφή.

Gateway (πύλη) Συνδυασμός υλικού και λογισμικού, που συνδέει δύο διαφορετικούς τύπους δικτύων. Για παράδειγμα, οι πύλες μεταξύ συστημάτων ηλεκτρονικής αλληλογραφίας επιτρέπουν στους χρήστες που δουλεύουν σε συστήματα ηλεκτρονικής αλληλογραφίας διαφορετικής αρχιτεκτονικής, να ανταλλάσουν μηνύματα μεταξύ τους.

Hardware Τα υλικά μέρη ενός συστήματος υπολογιστή, μεταξύ των οποίων και οι τυχόν περιφερειακές συσκευές.

Host Λέγοντας host εννοούμε έναν υπολογιστή, στον οποίο μπορεί να γίνει πρόσβαση από ένα χρήστη από μια απομακρυσμένη τοποθεσία. Συνήθως αυτό γίνεται με τη βοήθεια κάποιου modem μέσω της τηλεφωνικής γραμμής. Ο υπολογιστής, στον οποίο υπάρχουν τα δεδομένα, ονομάζεται host, ενώ ο υπολογιστής, τον οποίο χρησιμοποιεί ο χρήστης για να συνδεθεί, ονομάζεται terminal.

HTML (HyperText Markup Language) Γλώσσα προσδιορισμού ιδιοτήτων υπερκειμένου με εφαρμογή στα κείμενα που αναρτώνται σε Web sites. Καθορίζει το είδος γραμματοσειράς, θέση, μέγεθος, διάφορα εφέ, animation κ.ά. των απεικονιζόμενων χαρακτήρων και γραφικών.

HTTP (HyperText Transfer Protocol) Είναι το πρωτόκολλο επιπέδου εφαρμογών, το οποίο χρησιμοποιείται από το World Wide Web. Το HTTP καθορίζει μια σειρά από παραμέτρους επικοινωνίας και μετάδοσης. Μεταξύ αυτών, καθορίζει τον τρόπο μορφοποίησης και μετάδοσης των μηνυμάτων (e-mail), καθώς και τις ενέργειες που θα κάνουν οι Web servers και οι browsers σε μια σειρά εντολών που θα λάβουν. Στο HTTP κάθε εντολή εκτελείται ξεχωριστά, χωρίς να λαμβάνονται υπ' όψιν οι εντολές που προηγήθηκαν. Βασικό του πλεονέκτημα είναι η δυνατότητα που έχει για τη μεταφορά πολλαπλών αρχείων μέσω της ίδιας σύνδεσης.

Intranet (ενδοδίκτυο) Ιδιωτικό δίκτυο βασισμένο στις τεχνολογίες του Internet, αλλά περιορισμένο για χρήστη μέσα σε ένα οργανισμό, όπως είναι μια εταιρεία.

IP Είναι το μέσο της αναγνώρισης ενός υπολογιστή σε ένα δίκτυο TCP/IP. Τα δίκτυα που κάνουν χρήση του πρωτοκόλλου TCP/IP, κατευθύνουν τα μηνύματα βασισμένα στη διεύθυνση IP του υπολογιστή. Η μορφή μιας διεύθυνσης IP είναι τέσσερις αριθμοί, οι οποίοι διαχωρίζονται με τελείες (000.111.222.333) και μπορεί να έχουν τιμή από 0 έως 255. Σε ένα τοπικό, αυτόνομο δίκτυο μπορεί να αποδοθούν διευθύνσεις IP σε οποιαδήποτε μορφή. Όταν, όμως, συνδέεται ένα ιδιωτικό δίκτυο στο Internet, απαιτείται να γίνεται χρήση συγκεκριμένων, προκαθορισμένων αριθμών για την αποφυγή διπλοεγγραφών.

ISP (Internet Service Provider). Μια εταιρεία που παρέχει στους συνδρομητές της πρόσβαση στο Internet (παροχέας). Με κάποιο προκαθορισμένο, συνήθως μηνιαίο αντίτιμο, ο παροχέας παραχωρεί στο χρήστη ένα κωδικό όνομα και ένα συνθηματικό (password) πρόσβασης, μέσω των οποίων ο τελευταίος πιστοποιεί την ταυτότητα του και έχει την δυνατότητα να χρησιμοποιήσει τις τηλεπικοινωνιακές γραμμές. Η πρόσβαση του χρήστη μπορεί να γίνει είτε με τηλεφωνική κλήση είτε με μόνιμη σύνδεση με τον παροχέα.

Java Αντικειμενοστρεφής γώσσα προγραμματισμού που αναπτύχθηκε από τη Sun Microsystems, inc. Η Java είναι παρόμοια με την C++, αλλά είναι μικρότερη και πιο εύχρηστη από τη C++, επειδή είναι πιο αυθεκτική και διαχειρίζεται τη μνήμη μόνη της. Επίσης η Java είναι σχεδιασμένη έτσι ώστε να είναι ασφαλής και ανεξάρτητη από το σύστημα (δηλ. μπορεί να εκτελεστεί σε οποιοδήποτε σύστημα υλικού). Αυτό οφείλεται στο γεγονός ότι τα προγράμματα τις Java μεταγλωτίζονται σε κώδικες byte, που δεν είναι τόσο εξειδικευέμοι ώστε να επιδέχονται εντολές ειδικές για κάποιο συγκεκριμένο σύστημα, ενώ εκτελούνται στον υπολογιστή σε ένα ειδικό περιβάλλον λογισμικού που είναι γνωστό ώς εικονική μνήμη. Το χαρακτηριστικό αυτό κάνει τη Java γλώσσα χρήσιμη για προγραμματισμό εφαρμογών του Ιστού αφού η πρόσβαση των χρηστών στον Ιστό γίνεται από μεγάλη ποικιλία υπολογιστών. Η

Java χρησιμοποιείται στον προγραμματισμό μικροεφαρμογών για το Παγκόσμιο Ιστό, καθώς και για τη δημιουργία κατανεμημένων εφαρμογών δικτύου.

Linux Έκδοση του Unix που διατίθεται ελεύθερα και μπορεί να εγκατασταθεί σε διάφορες πλατφόρμες. Ο πυρήνας του λειτουργικού (kernel) αναπτύχθηκε κυρίως από τον Linus Torvald. Εξαιτίας της σταθερότητας που προσφέρει, του γεγονότος ότι είναι δωρεάν και ότι μπορεί να τρέξει σε διάφορες πλατφόρμες από –PC μέχρι MAC- έχει γίνει ένα αρκετά δημοφιλές εναλλακτικό λειτουργικό σύστημα.

Macro Virus Ιός γραμμένος σε γλώσσα μακροεντολών και συνδεδεμένος με μια εφαρμογή. Βρίσκεται μέσα σε ένα αρχείο εγγράφου, χρησιμοποιείται με την εφαρμογή και εκτελείται όταν ανοίξει το έγγραφο.

NTFS (Ακρώνυμο του NT file system- σύστημα αρχείων NT). Προηγμένο σύστημα αρχείων, σχεδιαδμένο για χρήση ειδικά με το λειτουργικό σύστημα Windows NT. Υποστηρίζει μεγάλα ονόματα αρχείων, πλήρως ασφαλή έλεγχο πρόσβασης, αποκατάσταση συστήματος αρχείων, εξαιρετικά μεγάλα μέσα αποθήκευσης και διάφορα άλλα χαρακτηριστικά.

Packet Η μονάδα δεδομένων που δρομολογείται μεταξύ ενός αποστολέα και ενός αποδέκτη συστήματος στο Internet ή οποιουδήποτε άλλου δικτύου μεταφοράς πακέτων. Κάθε αρχείο που αποστέλλεται μέσω του δικτύου τεμαχίζεται σε πακέτα, ώστε να είναι ταχύτερη και πιο ευέλικτη η μεταφορά του. Καθένα από τα πακέτα διατηρεί πληροφορίες διευθύνσεις IP για την πηγή και τον αποδέκτη.

PHP Γλώσσα δημιουργίας δυναμικών σελίδων web.

Port (θύρα) Δίαυλος ή σημείο επαφής μέσω του οποίου διακινούνται πληροφορίες μεταξύ ενός υπολογιστή και κάποιας συνδεδεμένης συσκευής εισόδου- εξόδου.

Proxy Server (Διακομιστής μεσολάβησης) Υπολογιστής, μέσω του οποίου είναι δυνατή η ταυτόχρονη πρόσβαση μιας ομάδας χρηστών στο Internet, χωρίς την ανάγκη ύπαρξης ξεχωριστού λογαριασμού (account) για τον καθένα.

RAID Μέθοδος αποθήκευσης δεδομένων στην οποία τα δεδομένα κατανέμονται σε μια ομάδα μονάδων σκληρού δίσκου, οι οποίες λειτουργούν σαν μια ενιαία μονάδα αποθήκευσης.

RAM (Random Access Memory). Μνήμη ημιαγωγών στην οποία η κεντρική μονάδα επεξεργασίας ή άλλες συσκευές του υλικού μέρους μπορούν να εκτελέσουν ανάγνωση και εγγραφή. Η πρόσβαση στις μονάδες αποθήκευσης μπορεί να γίνει σε οποιαδήποτε σειρά. Τα δεδομένα της μνήμης RAM χάνονται όταν κλείσει ο υπολογιστής.

Script (Σενάριο). Είναι ένα σύνολο εντολών που μπορούν να εκτελέστούν χωρίς την παρέμβαση του χρήστη. Μία γλώσσα σεναρίων (script language) είναι μια απλή γλώσσα προγραμματισμού, στην οποία μπορούν να γραφτούν τα scripts.

Sector (Τομέας). Ο όρος αφορά, κυρίως, τους μαγνητικούς δίσκους. Κάθε επιφάνεια δίσκου έχει ομόκεντρους κύκλους ή αυλάκια, όπου γράφονται τα στοιχεία (δεδομένα) με τη μορφή μαγνητικών στιγμάτων. Κάθε αυλάκι είναι χωρισμένο σε τομείς -sectors-, καθένας από τους οποίους έχει τη δική του διεύθυνση.

Server (Διακομιστής) Αποτελεί το κεντρικό, υψηλής δυναμικότητας σύστημα ενός τοπικού ή απομακρυσμένου δικτύου, το οποίο προσφέρει είτε υπηρεσίες είτε τους πόρους του στους χρήστες του δικτύου.

Spoofing (εξαπάτηση). Ένας τρόπος μεταμφίεσης, όπου μια μετάδοση σε ένα δίκτυο εμφανίζεται να προέρχεται από έναν εξουσιοδοτημένο υπολογιστή.

TCP/IP (Transmission Control Protocol over Internet Protocol). Μια ομάδα πρωτοκόλλων που έχει σχεδιάσει για να κάνει εφικτή την επικοινωνία μέσω διασυνδεμένων και πολλές φορές ανόμοιων δικτύων. Το TCP/IP υποστηρίζεται από όλα σχεδόν τα δίκτυα. Βρίσκεται στην καρδιά επικοινωνιών του Internet

UNIX Λειτουργικό σύστημα πολυδιεργασίας και πολλών χρηστών, το οποίο επειδή είναι γραμμένο στην γλώσσα C, είναι περισσότερο φορητό από πολλά άλλα λειτουργικά συστήματα. Σε ορισμένες παραλλαγές του unix διατίθενται δωρεάν και ο πηγαίος κώδικας κάτι που έχει αναγάγει το unix σε καθοριστικό παράγοντα κινήματος του ανοικτού πηγαίου κώδικα.

Virus (Ιός) Μικρό πρόγραμμα που μπορεί να εξαπλώνεται από ένα υπολογιστικό σύστημα σε ένα άλλο. Οι ιοί μπορούν να γραφτούν σε διάφορες γλώσσες προγραμματισμού ακόμα και σε γλώσσα μηχανής και συνήθως προκαλούν ανεπιθύμητες συνέπειες στα συστήματα που εγκαθίστανται.

Visual Basic Εμπορική ονομασία, που αποτελεί ιδιοκτησία της Microsoft Corporation, μιας υψηλού επιπέδου παραλλαγής της γλώσσας προγραμματισμου Basic κατάλληλης για οπτικό προγραμματισμό. Η Visual Basic σχεδιάστηκε για τη δημιουργία εφαρμογών Windows.

Wireless communication (ασύρματη επικοινωνία). Επικοινωνία μεταξύ ενός υπολογιστή και άλλου υπολογιστή ή άλλης συσκευής χωρίς σύρματα. Η μορφή ασυρματης επικοινωνίας που παράχεται ως τμήμα του λειτουργικού συστήματος Windows χρησιμοποιεό το υπέρυθρο φώς για τη μετάδοση αρχείων. Μια άλλη μορφή ασύρματης επικοινωνίας είναι οι ραδιοσυχνότητες, που χρησιμοποιούνται από τα κινητά και τα ασύρματα τηλέφωνα.

ΠΑΡΑΡΤΗΜΑ Β'

Άρθρα ποινικού δικαίου

Άρθρο 348Α
Πορνογραφία ανηλίκων

1. Όποιος από κερδοσκοπία παρασκευάζει, κατέχει, προμηθεύεται, αγοράζει, μεταφέρει, διακινεί, διαθέτει, πωλεί ή θέτει με οποιονδήποτε τρόπο σε κυκλοφορία πορνογραφικό υλικό τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

2. Πορνογραφικό υλικό κατά την έννοια της προηγούμενης παραγράφου συνιστά κάθε περιγραφή ή πραγματική ή εικονική αποτύπωση, σε οποιονδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στη γενετήσια διέγερση, καθώς και η καταγραφή ή αποτύπωση, σε οποιονδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο.

3. Αν κάποια από τις πράξεις της πρώτης παραγράφου αφορά πορνογραφικό υλικό που συνδέεται με την εκμετάλλευση της ανάγκης, της πνευματικής αδυναμίας, της κουφότητας ή της απειρίας ανηλίκου ή με την άσκηση σωματικής βίας κατ' αυτού, επιβάλλεται κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως 100 χιλιάδων ευρώ και αν η πράξη είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ.

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

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση.

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

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

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

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

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

Άρθρο 370Β
Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχος τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

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

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

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

Άρθρο 370Γ
Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών

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

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

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

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

Άρθρο 386
Απάτη

1. Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημιά που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών.

2. Οι διατάξεις του άρθρου 72 για το κατάστημα εργασίας εφαρμόζονται και εδώ.

3. Επιβάλλεται κάθειρξη μέχρι δέκα ετών: α) αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημιά υπερβαίνουν το ποσό των δεκαπέντε χιλιάδων ευρών « ή β) αν το περιουσιακό όφελος ή η προξενηθείσα ζημιά υπερβαίνει συνολικά το ποσό των εβδομήντα τριών χιλιάδων ευρώ.»

Άρθρο 386Α
Απάτη με υπολογιστή

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

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

Ανδρέας Δ. Αργυρόπουλος (2000). Ηλεκτρονική Εγκληματικότητα

Ζάννη Αναστασία (2005). Το διαδικτυακό έγκλημα. Media και Έγκλημα

Κωνσταντίνος Βλαχόπουλος (2007). Ηλεκτρονικό έγκλημα

Anderson, R. (2001). Security Engineering : A guide to building dependable distributed systems. New York: John Wiley and Sons, Inc.

Steven Levy (2001). Hackers: Heroes of the Computer Revolution, 3rd ed., New York: Penguin Books.

Shinder, D. and Tittel, E. (2002). Scene of Cybercrime: Computer Forensics Handbook. Syngress Puplishing

ΑΡΘΡΑ ΚΑΙ ΔΗΜΟΣΙΕΥΣΕΙΣ

Akdeniz, Y. (2004). An 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 (20/08/09)

Barlow, J.P. (1990). Έγκλημα και αμηχανία. Διαθέσιμο στο: http://hyperion.math.upatras.gr/courses/soctech/thefoit/erg99/sintoris_etal.html (15/07/09)

Casey, E. (2002). Practical Approaches to Recovering Encrypted Digital Evidence International Journal of Digital Evidence. Διαθέσιμο στο: http://www.cs.fsu.edu/~yasinsac/group/slides/busey3.pdf (27/07/09)

Ciardhuain, S. (2004). An Extended Model of Cybercrime Investigations International Journal of Digital Evidence. Διαθέσιμο στο: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf (28/07/09)

Colombell, M. (2002). The legislative response to the evolution of computer viruses. The Richmond journal of law and technology. VII (3). Διαθέσιμο στο: http://www.law.richmond.edu/jolt/v8i3/article18.pdf (25/07/09)

Curtin, M. (2001) Firewalls FAQ. Διαθέσιμο στο: http://www.faqs.org/faqs/firewalls-faq/ (07/09/09)

Denning D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Georgetown University. Διαθέσιμο στο: http://www.nautilus.org/archives/info-policy/workshop/papers/denning.html (15/07/09)

Giannis Stamatellos. (2007). Computer Ethics. A Global Perspective. Διαθέσιμο στο: http://books.google.co.uk/books?id=d9pvV-xbmhYC&printsec=frontcover&source=gbs_navlinks_s#v=onepage&q=&f=false (20/07/09)

Goodman Marc and Brenner S. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. UCLA Journal of Law and Technology. Διαθέσιμο από http://lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php (10/07/09)

Kabay M. (2001). Understanding of studies and surveys of Computer Crime. Διαθέσιμο στο: http://www.mekabay.com/methodology/crime_stats_methods.htm (11/07/09)

Maxwell, A. (2001). Cyberstalking. Department of Psychology Auckland University. Διαθέσιμο στο: http://www.netsafe.org.nz/Doc_Library/cyberstalking.pdf (07/09/09)

Newman, R. (2004). Identify Theft. US Department of Justice. Διαθέσιμο από: http://www.cops.usdoj.gov/files/RIC/Publications/e05042360.pdf (14/07/09)

PGP (2004). An Introduction to Cryptography. Διαθέσιμο στο: http://www.hermitagesolutions.com/download/PGP-Introduction_to_Cryptography.pdf (08/09/09)

Raymmond, Eric S. (2004). How to Become A Hacker. Διαθέσιμο από http://www.catb.org/~esr/faqs/hacker-howto.html (15/07/09)

Sinrod, E. and Reilly, W. (2000). Cyber-crimes: A practical approach to the application of Federal Computer Laws. Santa Clara Computer and high technology law journal. Διαθέσιμο από: www.sinrodlaw.com/cybercrime.doc (25/07/09)

Standler, R., (2002). Examples of malicious computer programs. Διαθέσιμο στο: http://www.rbs2.com/cvirus.htm (20/07/09)

US-CERT. (2005). Computer Forensics. Διαθέσιμο από: www.us-cert.gov/reading_room/forensics.pdf (21/07/09)

ΠΗΓΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

About.com
http://www.about.com/

Computer Crime Research Center
http://www.crime-research.org/articles/

Cybercrime
http://cybercrime.planetindia.net/index.htm

Cybercrime Law
http://www.cybercrimelaw.net/

E-crime Watch Survey(2005) Διαθέσιμο στο: www.cert.org/archive/pdf/ecrimesummary05.pdf (26/07/09)

Ελευθεροτυπία Απογευματινή Διαθέσιμο στο:
http://www.enet.gr/

FBI Computer Crime Survey (2005) Διαθέσιμο στο: www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf (26/07/09)

Google
www.google.com

Guidance Software.
http://www.guidancesoftware.com/

Ηλεκτρονικό Έγκλημα
http://www.go-online.gr/ebusiness/specials/article.html?article_id=341

Λάγγαρη Π.Απάτες στα Α.Τ.Μ. των τραπεζών: Το Μοντέρνο «Οικονομικό-Ηλεκτρονικό Έγκλημα. Διαθέσιμο στο: http://www.elesme.gr/elcsmegr/periodika/t22/t22_05.htm (09/09/09)

Lawnet
http://www.lawnet.gr/

Md5
http://www.md5sa.com/el/index.php

Paraben Forensic Tools
http://www.paraben-forensics.com/p2.html

Privacy- Κρυπτογράφηση Διαθέσιμο στο:
http://www.it.uom.gr/project/MultimediaTechnologyNotes/extra/append10.htm (08/09/09)

Προσέγγιση του Εγκλήματος στον Κυβερνοχώρο από τις Διωκτικές Αρχές
http://www.diaplous.org/library/nomothesia.php (07/09/09)

Rootkit
http://www.rootkit.com/index.php

Security focus
http://www.securityfocus.com/

The Law
http://www.originalintent.org/edu/thelaw.php (06/09/09)

X-Ways Forensics Διαθέσιμο στο: http://www.x-ways.net/ (09/09/09)
Web Browser Forensics Διαθέσιμο στο: http://www.securityfocus.com/infocus/1827 (05/09/09)

Wikipedia
http://www.wikipedia.org/