ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ηλεκτρονική διάσταση της σύγχρονης εγκληματικοτητας

Σπουδαστές :Νικόλαος Σαλπιστής

Άγγελος Παπαθανασίου

Επιβλέπων :Ντεμίρης Κωνσταντινος

ΠΑΤΡΑ,2011

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΕΙΣΑΓΩΓΗ

Η Κοινωνία της πληροφορίας δεν είναι μόνο μία κοινωνία γνώσης και ανάπτυξης. Τα δίκτυα ως ρεπλίκα της κοινωνίας χαρακτηρίζονται και περιέχουν όλες τις πλευρές της.

Οι εγκληματίες έχουν επίσης ανακαλύψει τον κυβερνοχώρο.

Η εγκληματικότητα αυτή έχει διάφορες μορφές:

- επίθεση κατά πληροφορικών συστημάτων,
- διάδοση παιδικής πορνογραφίας,
- απάτη,
- παραβιάσεις πνευματικής ιδιοκτησίας,
- προσβολές της ιδιωτικότητας,
- υποστήριξη της διάπραξης παραδοσιακών εγκλημάτων όπως η διακίνηση ναρκωτικών ή το δουλεμπόριο.

Πρέπει να σημειωθεί ο ιδιαίτερα ευάλωτος χαρακτήρας της σημερινής κοινωνίας της πληροφορίας: η οικονομία, η διοίκηση και η κοινωνία είναι σε πολύ υψηλό βαθμό εξαρτημένες από την αποτελεσματικότητα και την ασφάλεια των πληροφορικών συστημάτων. Είναι μία κοινωνία υψηλών ευκαιριών και ευχερειών αλλά ταυτόχρονα μία κοινωνία κινδύνων.

Η ανωνυμία ως βασικό χαρακτηριστικό του δικτύου έχει σοβαρές συνέπειες για το ποινικό δίκαιο.

Δεν δυσχεραίνει απλώς τη διαλεύκανση των εγκλημάτων αλλά δημιουργεί σοβαρό πρόβλημα και ως προς τις αποδείξεις.

Ένα άλλο σοβαρό κοινωνιολογικό-εγκληματολογικό στοιχείο είναι ότι η ανωνυμία ενθαρρύνει τους χρήστες του Διαδικτύου να επιχειρήσουν εγκληματικές πράξεις τις οποίες δεν θα επιχειρούσαν παρά μόνο στον κυβερνοχώρο καθώς στον χώρο αυτό δεν φαίνεται να έχει διαμορφωθεί μία ηθική τάξη και δομή με σαφείς κανόνες δεοντολογίας, επιταγές και απαγορεύσεις.

Η διάδοση της τεχνολογίας των υπολογιστών σε όλες τις πλευρές της ζωής, η διασύνδεση των υπολογιστών σε διεθνή δίκτυα έχουν καταστήσει

το έγκλημα πιο διαφοροποιημένο, πιο επικίνδυνο και διεθνοποιημένο. Τα νέα συστήματα έχουν ειδικά χαρακτηριστικά που διευκολύνουν τους δράστες αλλά δυσχεραίνουν το έργο των διωκτικών αρχών (πολλαπλά συστήματα λογισμικού και hardware, έλλειψη εμπειρίας πολλών χρηστών, ανωνυμία, κρυπτογράφηση, διεθνής κινητικότητα)

Αποτέλεσμα

- Η παραβατικότητα καθίσταται όλο και συχνότερο, πολυπλοκότερο και επικινδυνότερο φαινόμενο.
- Τα εγκλήματα αυτά μπορούν να πραγματοποιηθούν από τον καθένα και να πλήξουν τον καθένα. Δεν χρειάζεται καν να εγκαταλείψει κανείς τον χώρο του σπιτιού του.
- Το computer crime έχει αποκτήσει κινητικότητα και διεθνή χαρακτήρα.
- Το computer crime και το διαδύκτιο έχουν αποκτήσει μεγάλη ελκυστικότητα στο οργανωμένο έγκλημα.

Οι εξελίξεις αυτά θέτουν σοβαρότατα ζητήματα για το ποινικό δίκαιο καθώς τα μεθοδολογικά του παραδείγματα και οι κατηγορίες του τίθενται σε αμφισβήτηση ως προς τη ρυθμιστική τους ικανότητα.

- **Έννοια και μορφές του ηλεκτρονικού εγκλήματος και του κυβερνοεγκλήματος**

Υπάρχουν διχογνωμίες για τη σημασία των όρων.

Είναι αλήθεια ότι κάθε έγκλημα μπορεί να διευκολυνθεί με τη χρήση των υπολογιστών ή των τεχνολογιών της πληροφορικής. Σε πολλές περιπτώσεις η χρήση των υπολογιστών δεν αλλάζει το θεμελιακό χαρακτήρα ενός αδικήματος - μία δωροδοκία παραμένει δωροδοκία ανεξάρτητα εάν τα χρήματα με ηλεκτρονικό τρόπο - παρά το γεγονός ότι η χρήση του υπολογιστή μπορεί να επηρεάζει το βαθμό του αδικήματος. Το βέβαιο είναι ότι η εισαγωγική των πληροφοριακών και επικοινωνιακών

συστημάτων συνιστά για τους λόγους που εκτέθηκαν παραπάνω μία ποιοτική αλλαγή.

Πρέπει εισαγωγικά να σημειωθεί ότι το «ηλεκτρονικό έγκλημα» προηγείται χρονικά και λογικά της κατηγορίας των κυβερνοεγκλημάτων.

Εγκληματικότητα δια μέσου των υπολογιστών «αποτελεί κάθε εγκληματική συμπεριφορά στην οποία ο υπολογιστής είναι εργαλείο ή σκοπός της πράξης» εγκληματικής πράξης.

Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΠΟΣΑ) η εγκληματικότητα μέσω των υπολογιστών «αφορά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που έχει σχέση με την αυτόματη επεξεργασία και μεταφορά στοιχείων».

2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΟΥΕΓΚΛΗΜΑΤΟΣ

Το έγκλημα στον κυβερνοχώρο είναι γρήγορο διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ συχνά δεν αφήνει ίχνη (όπως στα κοινά εγκλήματα είναι τα δακτυλικά αποτυπώματα).

Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις, αυτή τη στιγμή είναι πιο προηγμένο και από το έγκλημα του λευκού περιλαίμιου .

Μπορεί να διαπραχθεί χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.

Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σ όσους έχουν ροπή ή τάση στην παιδοφιλία ή χρήση παιδικής πορνογραφίας να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδια ομάδες συζητήσεως ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (IRC-Internet Relay Chat).

Οι «εγκληματίες του κυβερνοχώρου» πολλές φορές δεν εμφανίζονται με την πραγματική των ταυτότητα π.χ. αποστέλλουν ηλεκτρονικά μηνύματα ή επιστολές ανωνύμως ή και με ψευδή στοιχεία. Πρωταρχικό χαρακτηριστικό της εγκληματικότητας στο διαδίκτυο που αναδεικνύει τη διαφορετικότητά της σε σχέση με άλλες μορφές εγκληματικότητας είναι η έλλειψη φυσικής επαφής του δράστη με το αντικείμενο του εγκλήματος και η έλλειψη βίας, χωρίς αυτό να σημαίνει ότι οι συνέπειες της δε σχετίζονται σε ορισμένες περιπτώσεις με βίαιες συμπεριφορές.

Ο δράστης του διαδικτύου δεν εισβάλλει στην κατοικία του θύματος, προκειμένου να αποσπάσει από τον ηλεκτρονικό υπολογιστή του τελευταίου αποθηκευμένα αρχεία, αλλά αποκτά πρόσβαση στο ηλεκτρονικό

σύστημα του θύματος «σπάζοντας» τους κωδικούς πρόσβασης. Αντίστοιχα δεν προκαλεί ζημιά σε δεδομένα η στη λειτουργία του υπολογιστή του θύματος με φυσικό τρόπο – π.χ. αφαιρώντας τον σκληρό δίσκο – απλά στέλνει ένα ιό που το ίδιο το θύμα ανυποψίαστο ενεργοποιεί.

Ενώ η έλλειψη βίας παραπέμπει σε μορφές ήπιας εγκληματικής συμπεριφοράς, στην περίπτωση του διαδικτυακού εγκλήματος κάθε άλλο περί τούτου πρόκειται.

Η ιδιαίτερη επικινδυνότητα αυτής της μορφής εγκληματικότητας έγκειται στο γεγονός ότι τα θύματα δεν μπορούν να αμυνθούν στην κατάφωρη προσβολή των εννόμων αγαθών τους, αφού συχνά ούτε την αντιλαμβάνονται και όταν τα αποτελέσματα είναι αντιληπτά, ο εντοπισμός των δραστών συνήθως είναι εξαιρετικά δυσχερής.

Επομένως, ο τρόπος τέλεσης των εγκλημάτων αυτών επιφέρει την ατιμωρησία των δραστών.

Είναι έγκλημα «χωρίς πατρίδα», παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους.

Κατά κανόνα είναι πολύ δύσκολο να προσδιοριστεί ο (πραγματικός) τόπος τελέσεως του. Ακόμα όμως και αν προσδιοριστεί αυτός, είναι ακόμα πιο δύσκολο να εντοπιστεί ο δράστης.

Η εξωτερίκευσή του μπορεί να εντοπίζεται στην Α χώρα πλην όμως τα αποδεικτικά στοιχεία μπορεί να βρίσκονται στο άλλο άκρο της γης ή και να βρίσκονται ταυτόχρονα σε πολλούς τόπους. Για την διερεύνησή του απαιτείται κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (δηλ. του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος, και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία).

Περιπτώσεις που το έγκλημα στον κυβερνοχώρο (cybercrime) περιορίζεται στα όρια ενός μόνον κράτους είναι (θεωρητικώς τουλάχιστον)ελάχιστες και σπάνιες. Οι παραδοσιακές (κοινές) Συμβάσεις για αμοιβαία Δικαστική Συνδρομή δεν επαρκούν, λόγω της φύσεως του αποδεικτικού ολικού, δηλαδή της ηλεκτρονικής απόδειξης (electronic evidence) που πρέπει να εντοπιστεί και να κατασχεθεί σε συνδυασμό με την ταχύτητα ενεργείας των διωκτικών Αρχών.

Δεν υπάρχουν επαρκή στατιστικά στοιχεία, όχι μόνο στον Ελληνικό, αλλά και στον Διεθνή χώρο.

Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου (cyber-crimes) καταγγέλλονται.

Και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων οι οποίοι κατά κανόνα είναι εταιρείες.

Κατά συνέπεια ο «σκοτεινός αριθμός» της εγκληματικότητας στον χώρο του διαδικτύου είναι «ακόμα πιο σκοτεινός», από ότι στον «κοινό» εγκληματικό χώρο. Η Αστυνομική διερεύνησή γενικότερα, αλλά και η ανακριτική του προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Εξειδικευμένες γνώσεις επίσης απαιτούνται και για όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (Εισαγγελείς, Δικαστές, Δικηγόρους).

3 Σκιαγράφηση («προφίλ») εγκληματία του Κυβερνοχώρου

Ο «εγκληματίας του κυβερνοχώρου» διαφέρει ουσιωδώς από τον «κοινό εγκληματία».

Δεν μπορεί ο καθένας να διαπράξει έγκλημα που σχετίζεται με το διαδίκτυο. Ο δράστης πρέπει να διαθέτει ειδικές γνώσεις, τεχνική επιδεξιότητα, τεχνικά μέσα.

Ο εγκληματίας του κυβερνοχώρου, (cyber-crime), δεν μπορεί να υποστηρίξει ότι ενήργησε «από ανάγκη» δηλαδή από οικονομική ανέχεια, αφού η ενέργειά του προϋποθέτει την ύπαρξη μιας αρκετά ικανής οικονομικής υποδομής (αγορά και συντήρηση υπολογιστή, αυξημένος τηλεφωνικός λογαριασμός, συνδρομή σε παροχέα πρόσβασης, εκπαίδευση σε υπολογιστές, αγορά σχετικών βιβλίων, κλπ). Δηλαδή χωρίς την κατοχή αυτή των τεχνικών και μη μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

Τους «εγκληματίες του κυβερνοχώρου» μπορούμε να τους διακρίνουμε σε δύο κατηγορίες : α) σ΄ αυτούς που «επιτίθενται» (εισβάλουν) στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν (εμφανώς τουλάχιστον) κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που από το άλλο άκρο του πλανήτη «εισβάλουν» σε υπολογιστή δια της χρήσεως του διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία, β) σ αυτούς που ενεργούν από οικονομικό όφελος (cracker).

Στην δεύτερη ανήκουν αυτοί που δεν « εισβάλουν» απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζά για την μεταφορά ενός ποσού στον λογαριασμό τους.

Σε ειδική έρευνα που έγινε στη Βρετανία από την «επιτροπή πρόβλεψης και πρόληψης εγκλήματος» για το «ποιόν» του μελλοντικού εγκληματία διαπιστώθηκε ότι:

Το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια την λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης, θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο, ακόμα Δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού.

Ειδικότερα τον ανιχνευτή της ίριδος θα τον «ξεγελούν» με την ανάλογη κατασκευή φακών επαφής .

Σχέση «εγκληματία του κυβερνοχώρου»(cyber - criminal) και του «εγκληματία του λευκού περιλαιμίου» (white - collar criminal).

Μπορεί να υποστηριχθεί ότι το έγκλημα στον κυβερνοχώρο (crime) είναι μια ειδικότερη μορφή του εγκλήματος του λευκού περιλαιμίου. Και αυτό γιατί ο εγκληματίας του κυβερνοχώρου πρέπει να διαθέτει:

α) Εξειδικευμένη επιδεξιότητα:

Ο εγκληματίας του κυβερνοχώρου πρέπει να είναι επιδέξιος, να έχει γνώσεις του όλου συστήματος πληροφορικής, είναι κοινωνικός και να μπορεί να αντιληφθεί, που θα «πετύχει» το θύμα του.

β) Γνώση :

Ο εγκληματίας του κυβερνοχώρου δεν έχει απλώς γνώση του όλου συστήματος πληροφορικής και του διαδικτύου.

Γνωρίζει πολύ καλά το επιμέρους «περιβάλλον», καθώς και τα μυστικά του χώρου που θα παραβιάσει.

Όπως ακριβώς ο «κοινός εγκληματίας» συλλέγει πληροφορίες, κατοπτεύει το χώρο κλπ. που πρόκειται να κλέψει ή να ληστέψει, κατ΄ ανάλογο τρόπο και ο εγκληματίας του κυβερνοχώρου (cybercriminal) κατοπτεύει και παρακολουθεί το ηλεκτρονικό περιβάλλον (site), στο οποίο πρόκειται να ενεργήσει την παράνομη πράξη του.

γ) Απαραίτητα τεχνικά και οικονομικά μέσα:

Ο εγκληματίας του κυβερνοχώρου πρέπει, εκτός από τη γνώση, να κατέχει και τα κατάλληλα τεχνικά μέσα.

Χωρίς την οικονομική δυνατότητα για αγορά του εξοπλισμού (computer-software κλπ.) και χωρίς την κατοχή των τεχνικών μέσων, είναι

αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο. Συμπερασματικώς λοιπόν μπορεί να λεχθεί ότι, το έγκλημα του κυβερνοχώρου, είναι πιο προηγμένο και από το έγκλημα του λευκού περιλαιμίου.

4 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΚΑΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΤΟΠΟΥ

Όπως παρατηρείται δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στη διεθνή νομοθεσία, ούτε στη διεθνή νομολογία. Την Ελληνική δικαστική πρακτική δεν έχει απασχολήσει ακόμα περίπτωση σχετική με το έγκλημα στο διαδίκτυο.

Οι υπάρχουσες μέχρι τώρα (ελάχιστες) ποινικές αποφάσεις αφορούν εγκλήματα με ηλεκτρονικούς υπολογιστές και όχι εγκλήματα του κυβερνοχώρου.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο αποτελεί τον ίδιο τύπο εγκλήματος με το «κοινό» ή «συμβατικό έγκλημα» και η μόνη διαφορά που το διακρίνει απ΄ αυτό είναι ότι διαπράττεται σε διαφορετικό περιβάλλον (δηλ. σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται στην πραγματικότητα .

Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται).

Μία άλλη δε κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικώς σε περιβάλλον του κυβερνοχώρου. Με το παραπάνω λοιπόν κριτήριο προτείνεται η ακόλουθη διάκριση:

Α) Σε εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο , πχ η συκοφαντική δυσφήμηση διαπράττεται και με την χρήση του ηλεκτρονικού ταχυδρομείου.

Η αντιγραφή ενός πνευματικού έργου πχ μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή.

Όταν το έγκλημα αυτό τελεστεί σε «περιβάλλον internet» (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

Β) Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενν. χωρίς την χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370 Γ παράγ. 1 του Π.Κ., π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή cd-Rom σε ηλεκτρονικό υπολογιστή.

Γ) Σε «Γνήσια εγκλήματα κυβερνοχώρου» με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς να έχει σχέση με τον κυβερνοχώρο.

Μια τέτοια αξιόποινη συμπεριφορά θα μπορούσε να είναι πχ η μεταβίβαση κρυπτογραφικών κειμένων χωρίς σχετική άδεια ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου. Τέτοια εγκλήματα δεν υπάρχουν ακόμα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία.

Σύμφωνα με αυτήν την προσέγγιση τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικώς με την χρήση του διαδικτύου. Χαρακτηριστικά ο Site λέει:

«Το cybercrime αναφέρεται σε κάθε έγκλημα που περιλαμβάνει υπολογιστές και υπολογιστικά δίκτυα περιλαμβάνοντας εγκλήματα που δεν στηρίζονται έντονα στους υπολογιστές».

Αυτός ο γενικός όρος απαιτείται για να καλύψει καταστάσεις όπου ένα υπολογιστικό δίκτυο δεν χρησιμοποιείται για να διαπραχθεί ένα έγκλημα αλλά εξακολουθεί να περιλαμβάνει ψηφιακά δεδομένα σχετιζόμενα με το έγκλημα.

Σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

Σε σχέση με τα εγκλήματα, στα οποία «εμπλέκεται» ο υπολογιστής και το δίκτυο προτείνεται και η ακόλουθη ταξινόμηση

1. *Ο υπολογιστής ως στόχος.*

Εδώ κατατάσσονται τα εγκλήματα που αφορούν τη δολιοφθορά των συγκροτημάτων ηλεκτρονικών υπολογιστών ή των δικτύων υπολογιστών,

τη δολιοφθορά των λειτουργικών συστημάτων και των προγραμμάτων, την κλοπή των στοιχείων πληροφοριών, τα εγκλήματα που σχετίζονται με την πνευματική ιδιοκτησία, όπως το λογισμικό υπολογιστών, τεχνο-βανδαλισμός και τεχνο-παραβίαση.

2. *Ο υπολογιστής ως συμβολή του εγκλήματος.*

   Για παράδειγμα η διαδικτυακή άπατη), απάτες πιστωτικών καρτών, απάτες που περιλαμβάνουν τις ηλεκτρονικές μεταφορές χρημάτων, απάτες τηλεπικοινωνιών και απάτες σχετικά με το ηλεκτρονικό εμπόριο και την ηλεκτρονική ανταλλαγή δεδομένων.

3. *Ο υπολογιστής ως «συνεργός/ πλατφόρμα» σε άλλα εγκλήματα.* Για παράδειγμα διάδοση ναρκωτικών, ξέπλυμα χρήματος και παράνομες τραπεζικές συναλλαγές, παιδική πορνογραφία, BBS που υποστηρίζουν την παράνομη δραστηριότητα, τζόγος Διαδικτύου.

4. *Εγκλήματα σχετικά με την εξάπλωση των υπολογιστών* όπως για παράδειγμα, πειρατεία λογισμικού πλαστογράφηση, παραβίαση πνευματικών δικαιωμάτων των προγραμμάτων υπολογιστών, πλαστός εξοπλισμός, μαύρος εξοπλισμός υπολογιστών αγοράς και προγράμματα.

Τέλος μία περαιτέρω τυπολογία είναι η ακόλουθη .

4.1 Είδη εγκληματικότητας

Προσβολές της ιδιωτικότητας :

καθαρές προσβολές της ιδιωτικότητας συναντώνται σε περιοχές που ισχύουν και τα παραδοσιακά επαγγελματικά απόρρητα : ιατρικό, δικηγορικό, τραπεζικό. Επίσης τα cookies συνιστούν παράνομη δραστηριότητα

Αδικήματα κατά της περιουσίας

computer hacking:

Ο όρος αυτός δηλώνει παραδοσιακά την προσβολή πληροφορικών συστημάτων που δεν γίνεται με σκοπό την manipulation , το σαμποτάζ ή

την κατασκοπεία αλλά χάριν της ευχαρίστησης της προσβολής των τεχνικών συστημάτων ασφαλείας.

Ηλεκτρονική κατασκοπεία:

Την παράνομη αυτή δραστηριότητα διευκολύνει ιδιαίτερα η σύγκλιση των τεχνολογιών πληροφορικής και τηλεπικοινωνιών.

Πειρατεία προϊόντων πνευματικής ιδιοκτησίας

Σαμποτάζ και εκβίαση: Πρέπει να διακρίνουμε μεταξύ των φυσικών ζημιών και των ζημιών που χαρακτηρίζονται ως ζημιές στο σύστημα.

Αυτό επιτυγχάνεται με προγράμματα που καταστρέφουν δεδομένα. Σοβαρά προβλήματα δημιουργούνται από τα λεγόμενα virus και worm programs καθώς και από τη διάδοση ελαττωματικού λογισμικού

Ηλεκτρονική απάτη: Οι συνήθεις μορφές ψηφιακής απάτης αφορούν την διαχείριση παραστατικών κλπ. που αφορούν την πληρωμή λογαριασμών, μισθών, την κίνηση λογαριασμών τραπεζών κλπ.

Παράνομο και αθέμιτο/επιβλαβές περιεχόμενο: Το ενδιαφέρον σήμερα εστιάζεται σε περιεχόμενο που αφορά την παιδική πορνογραφία και στη διάδοση μισαλλόδοξου λόγου στα διεθνή δίκτυα.

Η δίωξη των παραβατών είναι εξαιρετικά δυσχερής αφενός γιατί πολλοί παραβάτες δρουν από το εξωτερικό και τίθεται το σοβαρότατο πρόβλημα της έλλειψης αρμοδιότητας και δικαιοδοσίας και αφετέρου γιατί οι παραβάτες καλύπτονται πίσω από την ανωνυμία και την τεχνική κάλυψη που εξασφαλίζουν συστήματα όπως οι anonymous remailers ή η κατάχρηση ελεύθερα προσβάσιμου λογιστικού. (παραδείγματα : Γαλλικό δικαστήριο YAHOO). Ανεξάρτητα από τις διάφορες κατηγοριοποιήσεις και τυπολογίες εγκλήματα είναι εκείνα τα οποία ο νομοθέτης προσδιορίζει ως τέτοια, ορίζοντας μάλιστα την λεγόμενη «αντικειμενική υπόστασή» τους καθώς και τις προβλεπόμενες στο νόμο ποινές

4.2 **Ο τόπος του ηλεκτρονικού εγκλήματος- Προβλήματα προσδιορισμού του τόπου τέλεσης**

Το έγκλημα εκτός από τη λεγόμενη αντικειμενική υπόσταση (δηλ. την περιγραφή των πράξεων που συνιστούν κολάσιμη συμπεριφορά) προσδιορίζεται από α) τον χρόνο τέλεσης, β) τον τόπο τέλεσης και γ) τα εμπλεκόμενα πρόσωπα (θύμα, παραβάτης κλπ.).

Ο προσδιορισμός του τόπου τέλεσης του (διαδικτυακού) εγκλήματος έχει κρίσιμη σημασία καθώς από αυτόν εξαρτάται καταρχήν ο προσδιορισμός του εφαρμοστέου δικαίου και τα αρμόδια δικαστήρια. Εξαρτάται κατά περίπτωση από τον τόπο εκδήλωσης της αξιόποινης συμπεριφοράς και τον τόπο επέλευσης των αποτελεσμάτων της.

Ως τόπος τελέσεως ενός εγκλήματος θεωρείται από τις περισσότερες έννομες τάξεις (στις οποίες συμπεριλαμβάνεται και η ελληνική) τόσο ο τόπος στον οποίο ο υπαίτιος προέβη, ολικά ή εν μέρει, στην αξιόποινη ενέργεια όσο και ο τόπος, στον οποίο επήλθε το λεγόμενο αξιόποινο αποτέλεσμα.

Η χρήση των υπολογιστών και το Διαδίκτυο δημιουργούν εντελώς νέα δεδομένα σχετικά με τον προσδιορισμό του τόπου καθώς είτε δεν είναι ευχερής ο προσδιορισμός του τόπου εκδήλωσης μιας συμπεριφοράς επέλευσης ενός αποτελέσματος είτε συντρέχουν περισσότεροι τόποι όπου τελείται ένα έγκλημα.

Στην περίπτωση εγκλημάτων που τελούνται εκδηλώνονται στο Διαδίκτυο ο τόπος επέλευσης είναι ο κυβερνοχώρος, ο οποίος θα μπορούσε να ερμηνευτεί ως «κάθε χώρος στον οποίο αποκτάται πρόσβαση στα δεδομένα, (δηλ. παντού).

Ως τόπος επελεύσεως του αποτελέσματος στην πραγματικότητα μπορεί να θεωρηθεί το Διαδίκτυο, κάθε χώρος δηλαδή στον οποίο αποκτάται πρόσβαση στα δεδομένα.

Ο τόπος του κυβερνοεγκλήματος είναι διαφορετικός από τον τόπο του εγκλήματος στον «φυσικό» κόσμο δεδομένου ότι ο τόπος του

κυβερνοεγκλήματος είναι δυναμικός, αυξάνεται και μπορεί να μεταμορφωθεί.

Ως ψηφιακός τόπος τελέσεως του εγκλήματος μπορεί να θεωρηθεί το εικονικό περιβάλλον που δημιουργείται από το λογισμικό και το υλικό στα οποία υπάρχουν τα ψηφιακά στοιχεία ενός εγκλήματος και τα οποία παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του θύματός του ή μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του δράστη του.

Λόγω της φύσης του Διαδικτύου είναι πολύ δύσκολο να εντοπιστεί τόσο ο τόπος στον οποίο εκδηλώθηκε η συμπεριφορά του εγκληματία όσο και ο τόπος στον οποίο επήλθε το αξιόποινο αποτέλεσμα.

Ενδέχεται μάλιστα να υπάρχουν περιπτώσεις με περισσότερους τόπους τέλεσης της εγκληματικής πράξης [IRC (Internet Relay Channel), τα newsgroups (ομάδες συζητήσεως), το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol) κλπ.]

Σύμφωνα με τη θεωρία της συμπεριφοράς προτείνεται ως τόπος τέλεσης ο τόπος όπου βρισκόταν ο δράστης όταν εκδήλωνε την συμπεριφορά του.

Σύμφωνα με την θεωρία αυτή σαν τόπος τελέσεως του εγκλήματος «θεωρείται μόνο ο τόπος στον οποίο ο δράστης διέπραξε το έγκλημα του».

Έτσι λοιπόν εδώ δεν υπάρχουν χιλιάδες τόποι τελέσεως του εγκλήματος αλλά μονάχα ένας, εκεί που βρίσκεται ο παραβάτης και έχει αποθηκευμένα τα ψηφιακά στοιχεία Η λύση αυτή θα είχε το πλεονέκτημα ότι θα υπήρχε ένας τόπος τέλεσης.

Η προσέγγιση αυτή όμως είναι ασύμβατη με την εγγενώς παγκόσμια φύση του διαδικτύου και επιπρόσθετα θα είχε τον κίνδυνο εγκλήματα που δεν τιμωρούνται στον τόπο συμπεριφοράς να μένουν ατιμώρητα στον τόπο όπου επιφέρουν τα αποτελέσματά τους.

5 ΠΟΡΝΟΓΡΑΦΙΑ

Το φαινόμενο της παιδικής πορνογραφίας στο Διαδίκτυο αποτελεί μία από τις μορφές του ηλεκτρονικού εγκλήματος, το οποίο τα τελευταία χρόνια βλέπουμε να εξελίσσεται σε μάστιγα, καθώς όλο και περισσότερα κρούσματα και υποθέσεις έρχονται στο φώς της δημοσιότητας.

Η συνήθης έκφραση της παιδικής πορνογραφίας είναι η παρουσίαση ανηλίκων μέσω φωτογραφικού υλικού ως συμμετεχόντων σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες.

Οποιοσδήποτε μπορεί, πολύ εύκολα και σχετικά γρήγορα, να διαβιβάσει μέσω του Διαδικτύου φωτογραφίες παιδικού σεξουαλικού περιεχομένου σε παραλήπτες σε όλο τον κόσμο είτε σκανάροντας μια φωτογραφία και αποθηκεύοντας την σε κάποιο αρχείο και στη συνέχεια αποστέλλοντας την μέσω ηλεκτρονικού ταχυδρομείου ή δημοσιεύοντας την σε κάποια ιστοσελίδα είτε «κατεβάζοντας» την από κάποια ιστοσελίδα και προωθώντας την μέσω ηλεκτρονικού ταχυδρομείου προς κάθε ενδιαφερόμενο.

Ο όρος «πορνογραφία» καθορίστηκε αρχικά το 1857 στο αγγλικό λεξικό της Οξφόρδης και παραπέμφθηκε νωρίτερα στο γαλλικό γράψιμο για να αναφερθεί στην πορνεία, στην αισχρολογία, και στις άσεμνες εικόνες.

Η πορνογραφία που επιδεικνύει τα παιδιά είναι το αποτέλεσμα της σεξουαλικής εκμετάλλευσης ή η σεξουαλική κακοποίηση ενός παιδιού.

Σύμφωνα με το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Ελλάδος, παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς.

Ενώ πορνογραφικό υλικό συνιστά κάθε περιγραφή είτε πραγματική είτε εικονική αποτύπωση, σε οποιονδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στην γενετήσια διέγερση, καθώς και η καταγραφή η

αποτύπωση , σε οποιονδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από η με ανήλικο.

Τέλος, ανήλικος σύμφωνα με τις διατάξεις του άρθρου 121 του Ποινικού Κώδικα, όπως αυτό τροποποιήθηκε με τον Νόμο 3189/2003, νοείται κάθε πρόσωπο ηλικίας από οκτώ (8) έως δεκαοκτώ (18) ετών, ενώ οι μικρότερες ηλικίες, υπάγονται στην έννοια του παιδιού.

Ανήλικος, σύμφωνα με τις διατάξεις του άρθρου 121 Π.Κ, νοείται κάθε πρόσωπο ηλικίας από 8 έως 18 ετών, ενώ οι μικρότερες ηλικίες υπάγονται στην έννοια του παιδιού.

5.1 **Διαδύκτιο και παιδική σεξουαλική επίθεση**

Το Διαδίκτυο, παρέχει ένα νέο τόπο συναντήσεως για την εκμετάλλευση παιδιών, μειώνει τα αντικίνητρα με την παροχή ανωνυμίας και διευκολύνει την ανάπτυξη της φαντασίας δίνοντας στους θύτες ευκολότερη πρόσβαση σε ομάδες ομοϊδεατών περιορίζοντας την αίσθηση της περιθωριοποίησης.

Τρόποι επικοινωνίας μέσω διαδυκτίου & η χρήση τους στη διανομή παιδικού πονογραφικού υλικού

1. Δωμάτιο Συνομιλίας
2. Στιγμιαίο Μήνυμα (IM)
3. Ηλεκτρονικό ταχυδρομείο (e-mail)
4. Ηλεκτρονικές ομάδες (e-groups)
5. Κατάλογοι ηλεκτρονικών διευθύνσεων
6. Ομάδες πληροφόρησης
7. Πίνακας δελτίων (BBS)

Παιδόφιλος είναι εκείνος ο ενήλικας που σεξουαλικά προσελκύεται από παιδιά. Τα διαγνωστικά κριτήρια για ένα παιδόφιλο περιλαμβάνουν :

1. Επαναλαμβανόμενες και έντονες σεξουαλικά φαντασίες, ωθήσεις ή συμπεριφορές που αφορούν σεξουαλικές πράξεις με ένα προεφηβικό παιδί

2. Το άτομο έχει δράσει με τέτοιες σεξουαλικές ωθήσεις ή αυτές οι σεξουαλικές ωθήσεις και φαντασίες είναι τα αίτια μιας διαπροσωπικής δυσκολίας

3. Το άτομο είναι 16 ετών ή μεγαλύτερο και έχει τουλάχιστον 5 χρονών ηλικιακή διαφορά από το παιδί

Οι παιδικοί σεξουαλικοί κακοποιοί μπορούν να υποδιαιρεθούν σε 4 κριτήρια :

1. Η ηλικία του δράστη
2. Το φύλο του παραβάτη
3. Ο σεξουαλικός προσανατολισμός ή η προτίμηση
4. Ο τύπος των θυμάτων

Οι παραβάτες διακρίνονται σε δύο κατηγορίες :

1. Προνομιακό
2. Περιστασιακό

Ενώ με τη σειρά του, ο περιστασιακός παραβάτης, διακρίνεται :

1. στον Παλινδρομικό
2. στον Ηθικά άνευ Διακρίσεως
3. στον Σεξουαλικά άνευ Διακρίσεως και
4. στον Ανεπαρκή

Αυτοί που προτιμούν να κακοποιούν σεξουαλικά παιδιά, εκθέτουν τρία γενικά πρότυπα :

1. Προκλητικό
2. Εσωστρεφείς
3. Σαδιστές

Λογισμικές εφαρμογές που χρησιμοποιούνται για τη διανομή παιδικού πορνογραφικού υλικού

Πολλοί έμποροι παιδικής πορνογραφίας χρησιμοποιούν λογισμικές εφαρμογές για να διανείμουν το παράνομο υλικό. Μία από αυτές, είναι η εφαρμογή Peer-to-Peer (P2P) η οποία αναπτύχθηκε πολύ πρόσφατα. Αν και οι περισσότεροι άνθρωποι που χρησιμοποιούν το Διαδίκτυο εξοικειώνονται κάπως με το ηλεκτρονικό ταχυδρομείο και τον Ιστό, ο μέσος χρήστης Διαδικτύου μπορεί να μην είχε ακούσει για την περίπτωση χρήσης του λογισμικού P2P, το οποίο χρησιμοποιείται για να μοιραστεί τα αρχεία.

Ενώ P2P χρησιμοποιείται συχνά, νόμιμα, για να μοιραστεί μουσική, βίντεο και άλλους τύπους αρχείων και λογισμικών, χρησιμοποιείται όλο και περισσότερο στηνκυκλοφορία παιδικού πορνογραφικού υλικού. Το Napster ήταν μια τέτοια P2P εφαρμογή. Τώρα που το Napster εγκαταλείφθηκε, άλλα προγράμματα και υπηρεσίες έχουν τεθεί για να το αντικαταστήσουν.

Ενώ η αρχή είναι βασικά η ίδια, δεδομένου ότι η υπηρεσία επιτρέπει στους χρήστες την ανταλλαγή αρχείων και την αναζήτηση υλικών, εν τούτοις η τεχνολογία και οι κανόνες που διέπουν τις διάφορες υπηρεσίες διαφέρουν η μια από την άλλη. Μερικές από τις δημοφιλέστερες εφαρμογές P2P είναι το KaZaA, το Morpheus, το Gnutella, το FreeNet, το WinMX και το iMes.

Το KaZaA επιτρέπει στους χρήστες να ψάξουν και να μεταφορτώσουν ήχο, βίντεο,εικόνα και αρχεία κειμένων χρησιμοποιώντας είτε το KaZaA MEDIA DESKTOP P2P είτε το Winamp plugin είτε τον ιστοχώρο KaZaA.com.Το KaZaA μπορεί αυτόματα να μετασχηματίσει ισχυρότερους πελάτες σε «SuperNodes» ικανούς να χειριστούν αιτήματα αναζήτησης από κοντινούς χρήστες. Κατ' αυτό τον τρόπο, το δίκτυο KaZaA οργανώνεται σε συστάδες από κοντινούς χρήστες για να κάνει την έρευνα και τη μεταφόρτωση αποδοτικότερη. Εάν ένα αρχείο δεν μπορεί να βρεθεί σε μια κοντινή μηχανή, το KaZaA επεκτείνει την αναζήτηση πέρα από το δίκτυο.

Το Morpheus είναι ένα δίκτυο διανομής αρχείου βασισμένο σε KaZaA.

Χρησιμοποιεί ένα συγκεντρωτικό σύστημα εγγραφής και σύνδεσης χρηστών και δεν διατηρεί μιακεντρική ικανοποιητική περιεκτικότητα σε δείκτες ή φίλτρα.

Το Gnutella είναι ένα αποκεντρωμένο δίκτυο που επιτρέπει στους χρήστες να ψάξουν για αρχεία. Οι χρήστες μπορούν να επιλέξουν να μοιραστούν αρχεία, καταλόγους ακόμα και ολόκληρους τους σκληρούς δίσκους τους.

Η έρευνα αποκεντρώνεται επειδή τα αρχεία αποθηκεύονται στους σκληρούς δίσκους των χρηστών και όχι σε έναν κεντρικό υπολογιστή και όταν εκτελείται μια αναζήτηση, ψάχνει τους σκληρούς δίσκους των χρηστών. Η παιδική πορνογραφία βρίσκεται εύκολα και μεταφορτώνεται από P2P εφαρμογές.

Σε μια και μόνο αναζήτηση όπου χρησιμοποιήθηκαν 12 λέξεις κλειδιά που είναι γνωστές ότι συνδέονται με τη παιδική πορνογραφία στο διαδίκτυο, το GAO (Γραφείο Γενικής Λογιστικής των Ηνωμένων Πολιτειών Αμερικής) προσδιόρισε 1.286 τίτλους και ονόματα αρχείων, δηλώνοντας ότι 543 (περίπου 42%) ήταν συνδεδεμένα με παιδικές πορνογραφικές εικόνες. Από τα υπόλοιπα, το 34% ταξινομήθηκε ως ενήλικη πορνογραφία ενώ μόλις το 24% ήταν μη-πορνογραφικές. Σε μια άλλη αναζήτηση με 3 λέξεις κλειδιά, ένας αναλυτής τελωνείου μεταφόρτωσε 341 εικόνες, των οποίων οι 149(περίπου το 44%) συμπεριλάμβανε παιδική πορνογραφία.

Αυτά τα αποτελέσματα συνέπουν με τις αυξανόμενες εκθέσεις για την παιδική πορνογραφία που μεταφορτώνεται μέσω P2P εφαρμογών. Από τότε που ξεκίνησε η διανομή παιδικού πορνογραφικού υλικού, περίπου το 2001 το Εθνικό Κέντρο Αμερικής για Χαμένα και Υπό Εκμετάλλευση Παιδιά έχει δει μια τετραπλή αύξηση, από 156 το 2001 σε 757 το 2002.

Αν και οιαριθμοί είναι μέχρι τώρα μικροί σε σύγκριση με εκείνους από άλλες πηγές (26.759 εκθέσεις της παιδικής πορνογραφίας σχετικά με τους ιστοχώρους το 2002), η αύξησηείναι ιδιαίτερα σημαντική.

Επίσης, χρησιμοποιείται ευρέως στην μεταφόρτωση ή στην ανταλλαγή εκατοντάδων χιλιάδων εικόνων παράνομου υλικού το Πρωτόκολλο

Μεταφοράς Αρχείων (FILE TRANSFER PROTOCOL – FTP) καθώς δύναται να μεταφορτώνει μεγάλα αρχεία μέσω Διαδικτύου. Στόχοι του FTP είναι:

1) να προωθηθεί η διανομή των αρχείων (προγράμματα ή και στοιχεία υπολογιστών)

2) να ενθαρρυνθεί η έμμεση ή υπονοούμενη (μέσω των προγραμμάτων) χρήση των μακρινών υπολογιστών

3) να προστατευθεί ο χρήστης από τις παραλλαγές στα συστήματα αποθήκευσης αρχείων μεταξύ των οικοδεσποτών και

4) τα στοιχεία μεταφοράς να είναι σοβαρά και αποτελεσματικά.

Χρυσοί κανόνες για την online έρευνα σχετικά με την παιδική σεξουαλική εκμετάλευση

- Ποτέ μην πείτε ή μην κάνετε κάτι που δεν θα θέλατε να το επαναλάβετε στο δικαστήριο.
- Μην στείλετε ποτέ παιδικό πορνογραφικό υλικό, ενήλικο πορνογραφικό υλικό, φωτογραφίες από εσάς ή το παιδί σας μέσω του Διαδικτύου.
- Κρατήστε τα πάντα. Είναι σημαντικό σε αυτές τις περιπτώσεις να κρατάτε πλήρη, καλά τεκμηριωμένα αρχεία οποιωνδήποτε συναλλαγών που προκύπτουν κατά τη διάρκεια της έρευνας
- Μην εργαστείτε ποτέ από το σπίτι σας ή από τον προσωπικό σας λογαριασμό.
- Δώστε τον κατηγορούμενο
- Μη γίνεστε εσείς αυτός που προκαλεί - αυτή είναι δουλειά του κατηγορουμένου.
- Αν αντιλαμβάνεσαι κάτι τότε πρέπει να το ψάξεις.
- Εξετάστε τα πλεονεκτήματα και τα μειονεκτήματα μιας πρόσωπο με πρόσωπο συνάντησης.

5.2 **Δελεασμός ανηλίκου**

Ο όρος «δελεασμός» αναφέρεται στους τρόπους με τους οποίους ένας σεξουαλικός παραβάτης αποκτά έλεγχο πάνω στα θύματα, εκμεταλλεύεται τις αδυναμίες τους για να κερδίσει την εμπιστοσύνη ή να τους ενσταλάξει το φόβο.

Ο δελεασμός, συνήθως, περιλαμβάνει την εκμετάλλευση των αναγκών ενός θύματος όπως η μοναξιά, ο αυτοσεβασμός, η σεξουαλική περιέργεια ή απειρία, η έλλειψη χρημάτων και μέσα από αυτά να αναπτυχθεί ένας δεσμός ανάμεσα στον θύτη και στο θύμα. Τα στοιχεία δελεασμού δεν αποτελούν στοιχεία και αποδείξεις ενός εγκλήματος, αλλά μπορούν να χρησιμοποιηθούν για να παρουσιαστεί η κύρια πρόθεση του υπόπτου.Οι ενήλικες που αναζητούν παιδική λεία πάντα μελετούν τους στόχους τους. Ξέρουν ποια είναι η προτιμημένη ομάδα ηλικίας των παιδιών και ποια είναι τα είδη των πραγμάτων που τους ενδιαφέρουν.

Η εκμετάλλευση παιδιών υπήρξε πολύ πριν από το Διαδίκτυο, και τα δίκτυα των παραβατών που επικοινωνούσαν, πριν την εφεύρεση του προσωπικού υπολογιστή,ήταν μέρος της καθημερινής ζωής.

Τα δίκτυα παραβατών ήταν οργανώσεις παιδόφιλων που επικοινωνούσαν μεταξύ τους και προσέφεραν διάφορες υπηρεσίες στα μέλη τους, όπως για παράδειγμαενίσχυση για τους παιδόφιλους και μια σταθερή πηγή για νέες φιλίες και για ανεφοδιασμό νέων θυμάτων.

Χαρακτηριστική είναι ηκατάθεση ενός παιδόφιλου που άνηκε σε μία τέτοια οργάνωση, του Joseph Henry:Κατά τη διάρκεια της περιόδου 1975-1976, συμμετείχα ενεργά στην οργάνωση παιδοφιλίας της βάσης του Σαν Ντιέγκο «Παιδικός Αισθησιακός Κύκλος» (Childhood Sensuality Circle - CSC). Ανταποκρίθηκα στην Valida Davila, την προϊσταμένη του CSC, και έκανα και μερικές δακτυλογραφήσεις για αυτήν. Καθώς ήταν του CSC, η Davila με έφερε σε επαφή με άλλους παιδόφιλους.Το Νοέμβριο του 1976, ήμουν στη Νέα Υόρκη όταν δέχτηκα ένα τηλεφώνημα από κάποιον που ονομάζονταν Eric Cross.

Ο Cross ήταν φίλος του John Duncan σημαντικό μέλος του CSC, και είπε οτι κατάλαβε ότι έψαχνα μια γυναίκα με μικρά παιδιά που θα συμφωνούσε να με παντρευτεί ώστε να μπορώ να είμαι πατέρας και να αισθανθώ ως ενήλικος, όχι μόνο να κακοποιήσω σεξουαλικά τα παιδιά.

Εκείνη την περίοδο, δεν είχα καμία ιδέα ποιος ήταν ο Cross αλλά έμαθα αργότερα ότι ήταν παιδικός πορνογράφος, εκδότης του περιοδικού Lolitots και ένας παιδόφιλος με διασυνδέσεις όχι μόνο στις Ηνωμένες Πολιτείες, αλλά και σε διάφορες άλλες χώρες.Πήγα στο Λος Άντζελες το φθινόπωρο του 1977 να συναντηθώ με τον Cross. Για αρκετές νύχτες, συναντιόμασταν για να εξετάσουμε παιδικές πορνογραφικές φωτογραφίες. Ο Cross και εγώ ήμασταν σε ένα μοτέλ εξετάζοντας φωτογραφίες γυμνών παιδιών που θα έστελνε σε μια πηγή στον Καναδά. Όταν αφήσαμε το ξενοδοχείο τη νύχτα, συλληφθήκαμε.

Η αστυνομία με απελευθέρωσε λόγω έλλειψης στοιχείων, και επέστρεψα στη Νέα Υόρκη, αλλά μερικές εβδομάδες αργότερα, συνελλήφθησα από τους πράκτορες Αμερικανικού τελωνείου. Μετά από τη σύλληψή μου, έμαθα ότι πολλά άτομα είχαν πάει στο Λος Άντζελες και στο Σαν Ντιέγκο από το 1974 ως το 1976 για να κακοποιήσουν σεξουαλικά παιδιά που ο John Duncan έφερνε στην διάθεση τους. Τα διάφορα μοτέλ και τα σπίτια των ατόμων-μελών χρησιμοποιήθηκαν ως τοποθεσίες για την κακοποίηση. Τα παιδιά φωτογραφήθηκαν επίσης κατά τη διάρκεια των συνευρέσεων. Αν και δεν συμμετείχα σε αυτό, ένα από τα άτομα, πούλησε τις φωτογραφίες στο ολλανδικό παιδοπορνογραφικό περιοδικό Lolita.

Εκτός από τις οργανώσεις των παιδόφιλων, οι ενήλικοι συνήθιζαν να «κυνηγούν» σε ομάδες μαθητών ή σε ερασιτεχνικούς ραδιοφωνικούς σταθμούς. Η τεχνολογία οδηγήθηκε από μόνη της να χρησιμοποιείται από τη νεολαία. Επέτρεψε την επικοινωνία με πολλούς ανθρώπους συγχρόνως και δεν απαίτησε μια ελάχιστη ηλικία στη χρήση της.

Καθισμένο στο καθιστικό του, ένα παιδί μπορούσε να μιλήσει με άλλα παιδιά και ενήλικους.

Ανάλογα με το εάν οι ομάδες μαθητών ή οι ερασιτεχνικές ραδιοσυχνότητες ήταν απασχολημένες, ένα παιδί μπορούσε να επικοινωνήσει με άτομα που βρίσκονταν σε απομακρυσμένες αποστάσεις.

Το ενδιαφέρον των παιδιών για το ερασιτεχνικό ραδιόφωνο μοιράστηκε ανυπόμονα στους ενήλικες παραβάτες διότι ήταν ένα χρήσιμο μέσο για την ανάπτυξη σχέσεων με τα πιθανά θύματα. Προγενέστερα του ερασιτεχνικού ραδιόφωνου, οι ενήλικες παραβάτες στηρίχθηκαν στην απασχόληση, στον εθελοντισμό, την οικογένεια και τους φίλους για να αποκτήσουν πρόσβαση στα παιδιά με την επιθυμητή ηλικία.

Εάν με κάποιο τρόπο ο ενήλικας παραβάτης δεν είχε τη δυνατότητα να έχει πρόσβαση στα παιδιά ή κατείχε κάποιο φυσικό χαρακτηριστικό που τον απέτρεπε από τη σύνδεση του με τα παιδιά, τα ερασιτεχνικά ραδιόφωνα προσέφεραν αυτή την πρόσβαση και μέσα από αυτά μπορούσε να αναπτυχθεί μια σχέση με ένα πιθανό θύμα για μια χρονική περίοδο. Η δυνατότητα να αναπτυχθεί μια σχέση χωρίς επαφή πρόσωπο με πρόσωπο, παρείχε στον ενήλικο παραβάτη τη δυνατότητα να σφυρηλατεί βαθμιαία το τύπο σχέσης που θα του επέτρεπε να αρχίσει τις σεξουαλικές επαφές με το θύμα αποτρέποντας την κοινοποίηση της.

5.3 **Στατιστικά στοιχεία παιδικής πορνογραφίας**

Πριν από πέντε χρόνια, οι καταγγελίες που δεχόταν η Αστυνομία για το κυβερνοέγκλημα ήταν περίπου μία κάθε μήνα. Σήμερα, όμως ανέρχονται σε 30 την ημέρα. Το 45-50% αυτών των καταγγελιών αφορούν την παιδική πορνογραφία. υπάρχουν περίπου 100.000 ιστοσελίδες διακίνησης παιδικού πορνογραφικού υλικού, ο ετήσιος τζίρος ανέρχεται στο 1.000.000.000 € ενώ τα έσοδα από τη γενικότερη διαδικτυακή πορνογραφία ανέρχονται στα 2,6.000.000.000 € ετησίως.

Τα στατιστικά στοιχεία που διαθέτει η Ε.ΚΑΤ.Ο. από έρευνα της Ευρωπαϊκής Επιτροπής είναι σοκαριστικά:

- Τα μισά από τα παιδιά που χρησιμοποιούν το Διαδίκτυο δεν επιβλέπονται κατά τη διάρκεια της πλοήγησης

• Το 1/3 των γονέων που έχουν στο σπίτι υπολογιστή, έχουν εγκαταστήσει κάποιο φίλτρο προστασίας σε αυτόν.

• Ένας στους πέντε ανηλίκους έχει δεχθεί σεξουαλική προσέγγιση ή υποκίνηση στο Διαδίκτυο.

• Ένας στους 33 ανηλίκους έχει δεχθεί επιθετική σεξουαλική προσέγγιση, δηλαδή του ζητήθηκε από παιδόφιλο να συναντηθούν κάπου, ο παιδόφιλος επικοινώνησε τηλεφωνικά μαζί του ή έστειλε επιστολή, χρήματα ή δώρα για να τον παρακινήσει στη συνάντηση

• Ένας στους τέσσερις ανηλίκους έχει εκτεθεί χωρίς να το επιθυμεί σε φωτογραφικό υλικό γυμνών ανθρώπων ή σεξουαλικών περιπτύξεων

• Μόνο το 17% των νέων και το 11% των γονέων γνωρίζουν έστω και έναν φορέα στον οποίο μπορούν να αναφέρουν ένα τέτοιο περιστατικό.

• Περίπου το 25% των νέων που έχουν δεχθεί σεξουαλική προσέγγιση ή παρενόχληση το είπαν στους γονείς τους.

• Το 40% αυτών που εκτέθηκαν σε ανεπιθύμητου περιεχομένου ιστοσελίδες το ανέφεραν στους γονείς τους.

Οι Διαδικτυακοί τόποι που «φιλοξενούν» παιδικό πορνογραφικό υλικό αυξάνονται ραγδαία από το 2001. Συγκεκριμένα, παρατηρείται αύξηση έως και 345% ενώ σταδιακά, εμφανίζονται 67 με 82 νέα sites μηνιαία και 8 με 21 καθημερινά.

Σύμφωνα με μια έρευνα που πραγματοποιήθηκε από το πανεπιστήμιο του New Hampshire σε παιδιά ηλικίας 10-17 ετών που χρησιμοποιούν το Διαδίκτυο:

• Περίπου το ένα στα πέντε έλαβε κάποια μορφή σεξουαλικής παράκλησης πέρα του Διαδικτύου

• Το ένα στα τριάντα τρία έλαβε μια επιθετική σεξουαλική παράκληση (αίτημα να συναντηθεί, να συζητήσει τηλεφωνικώς, κ.λπ.)

• Το ένα στα τέσσερα εκτέθηκε σε ανεπιθύμητες εικόνες που περιείχαν γυμνό ή σεξουαλική δραστηριότητα

• Το ένα στα δεκαεπτά αισθάνθηκε απειλημένο ή παρενοχλημένο (σχετικά με κάποια σεξουαλικό περιεχόμενο)

• Τα κορίτσια στοχεύτηκαν ως σεξουαλικά θύματα δύο φορές περισσότερο από ότι τα αγόρια

• Το 77% της νεολαίας που στοχεύτηκε ως πιθανά σεξουαλικά θύματα ήταν άνω των 14 ετών.

• Αν και το 22% της νεολαίας που θεωρήθηκε πιθανό θύμα ήταν ηλικίες 10 έως 13, αυτή η ηλικιακή ομάδα ενοχλήθηκε δυσανάλογα από το γεγονός

• Οι ενήλικοι (οι περισσότεροι μεταξύ των ηλικιών 18 και 25) αποτέλεσαν το 24% των σεξουαλικών παρακλήσεων

• Οι νεαροί αποτέλεσαν το 48% των επιθετικών παρακλήσεων

• Η ηλικία ήταν άγνωστη για 27% των προαγωγών

• Ελαφρώς περισσότερο από τα 2/3 των παρακλήσεων και των σε απευθείας σύνδεση προσεγγίσεων προήλθαν από αρσενικό φύλο

• 1/4 των επιθετικών προσεγγίσεων προερχόταν από θηλυκό φύλο

5.4 **Επιχείρηση PURITY**

Σύμφωνα με τον Προϊστάμενο του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος, Αστυνόμο Α’, κ. Εμμανουήλ Σφακιανάκη, στη χώρα μας η διακίνηση παιδικής πορνογραφίας μέσω του Διαδικτύου δεν έχει λάβει ακόμη τα χαρακτηριστικά οργανωμένου εγκλήματος, καθώς οι δράστες λειτουργούν στη συντριπτική τους πλειοψηφία μεμονωμένα.

Η επιχείρηση PURITY, είναι μία από τις μεγαλύτερες επιχειρήσεις που εκτέλεσε το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Ασφάλειας Αττικής καθώς ύστερα από κατάλληλη ψηφιακή επεξεργασία ηλεκτρονικών ιχνών, προέκυψε η εμπλοκή ογδόντα (80) Ελλήνων χρηστών internet σε διεθνές κύκλωμα on-line εμπορίας υλικού παιδικής πορνογραφίας.

Στα μέσα του Φεβρουαρίου το 2005, κλιμάκια Αστυνομικών της Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος, μετέβησαν και διενήργησαν έρευνες στις οικίες και σε λοιπούς χώρους των κατηγορουμένων στην Αθήνα, την Θεσσαλονίκη, τα Χανιά, την Μύκονο, την Λάρισα και την Δράμα.

«Το ότι εξιχνιάζουμε περισσότερες υποθέσεις, σημαίνει ότι αυξάνεται συνεχώς και ο αριθμός των εμπλεκομένων», καταλήγει.

Παράλληλα, εκφράζει την ανησυχία του, διότι μέσω του Διαδικτύου πολλοί παιδόφιλοι καταφέρνουν πλέον να προσεγγίζουν παιδιά, να συνομιλούν μαζί τους, ακόμη και να τα πείθουν να φωτογραφηθούν γυμνά.

5.5 **Ασφάλεια και τρόποι προστασίας ανηλίκων**

Οι κίνδυνοι για τα παιδιά που ελλοχεύουν από τη χρήση του Διαδικτύου μπορούν να είναι :

- να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο
- να έρθουν σε επαφή με αγνώστους που μπορεί να τα βλάψουν
- να υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο Διαδίκτυο
- ή ακόμα και να εθιστούν τόσο πολύ στη χρήση του που να κινδυνέψουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις ή τα παιχνίδια με τους φίλους τους.

Πώς θα αντιληφθούν οι γονείς ότι κάτι περίεργο συμβαίνει :

- το παιδί λαμβάνει ανεξήγητα ή ύποπτα δώρα, από ανθρώπους που δεν γνωρίζουν ή δεν έχουν ακούσει ποτέ,
- το παιδί λαμβάνει τηλεφωνήματα από ενήλικους ή από μεγαλύτερους εφήβους που δεν γνωρίζουν,
- το παιδί ξοδεύει ιδιαίτερα μεγάλο χρονικό διάστημα στο Διαδίκτυο,

• το παιδί γρήγορα αλλάζει το παράθυρο που έχει ανοιχτό στην οθόνη του υπολογιστή του ή τον κλείνει τελείως καθώς μπαίνει ο γονιός στο δωμάτιο του,

• το παιδί λαμβάνει ανεξήγητα και ύποπτα δώρα, ιδιαίτερα ψηφιακά, όπως φωτογραφικές μηχανές, κινητά τηλέφωνα, τηλεφωνικές κάρτες, υπολογιστές ή λεφτά,

• το παιδί γίνεται επιθετικό, τρέχει μακριά από το σπίτι ή ξεκινάει κάποια εγκληματική δραστηριότητα

• οι συνήθειες καλλωπισμού του παιδιού ή οι συνήθειες υγιεινής αλλάζουν.

Αλλαγές στο ντύσιμο έτσι ώστε να κρύβουν το παιδικό του σώμα ή να το κάνουν να εμφανίζεται μη ελκυστικό θα πρέπει να προσεχθούν.

Η παιδική πορνογραφία είναι μια από τις γρηγορότερα αυξανόμενες επιχειρήσεις στο χώρο του διαδικτύου και υπολογίζεται να παράγει γύρω στα 3δις € κέρδη ετησίως.

Η ΜΚΟ Ν.Ε.Ο.Ι. (Νέοι Ευρωπαίοι Οργανωμένοι Ικανοί) στην εκστρατεία ενημέρωσης παιδιών και νέων αναφορικά με την ορθή και ασφαλή χρήση του διαδικτύου, που ξεκίνησε το Σεπτέμβριο του 2007 παραθέτει κάποια χρήσιμα στοιχεία που αφορούν τη μάστιγα της παιδικής πορνογραφίας.

Σήμερα, οι Νέες Τεχνολογίες και ειδικότερα το Διαδίκτυο έχουν γίνει μια από τις επικρατέστερες τεχνικές που χρησιμοποιούνται από τους παιδόφιλους, για να μοιραστούν παράνομο ψηφιακό φωτογραφικό υλικό ανηλίκων και για να δελεάσουν τα παιδιά σε παράνομες σεξουαλικές πράξεις.

Το Διαδίκτυο κάνει πιο εύκολη την προσέγγιση από τους παραβάτες των υποψηφίων θυμάτων τους, ενώ παράλληλα δίνει σε αυτούς απεριόριστη πρόσβαση σε μια κοινότητα ανθρώπων με τις ίδιες σεξουαλικές προτιμήσεις.

Σύμφωνα με κεντρική έρευνα της Αμερικής, 200 νέες εικόνες παιδικής πορνογραφίας ταχυδρομούνται καθημερινά, και 1 στα 7 παιδιά έχει λάβει μια σεξουαλική διαδικτυακή παρενόχληση κατά την πλοήγησή του. Αυτό

όμως που συγκλονίζει είναι ότι ένα 35% των παραβατών είναι γονείς κακοποιημένων παιδιών, ενώ ένα 10% αποτελείται από άλλα συγγενικά πρόσωπα.

Κεντρικές στατιστικές μελέτες αποκαλύπτουν ότι περίπου 107.572 εικόνες σεξουαλικά κακοποιημένων παιδιών ταχυδρομήθηκαν στους ελληνικούς ιστοχώρους κατά τη διάρκεια των προηγούμενων τριών ετών, αλλά οι ελληνικές αρχές έχουν κάνει μόνο 119 σχετικές συλλήψεις.

Αντίστοιχα το FBI σε συνεργασία με Interpol και Europol τα τρία τελευταία έτη έχει παρατηρήσει ραγδαία αύξηση σε αντίστοιχα περιστατικά και έχει καταχωρήσει στη λίστα των 10 most wanted του FBI τέσσερα πολύ σοβαρά κρούσματα.

Από εκείνους που έχουν συλληφθεί παγκοσμίως, ένα 19% είχαν στην κατοχή τους εικόνες νηπίων και μικρών παιδιών κάτω της ηλικίας των 3 ετών, 39% των παιδιών ήταν από 3-5 ετών και 83% είχαν εικόνες των παιδιών 6-12 ετών.

Στη Μεγάλη Βρετανία πέρυσι το IWF ερεύνησε περισσότερες από 24.000 καταγγελίες μέσα από την Ανοιχτή Γραμμή επικοινωνίας που διαθέτει για το κοινό και που αφορούσαν την παιδική πορνογραφία σημειώνοντας μια αύξηση της τάξης του 40% σε σχέση με το προηγούμενο έτος.

Το ίδρυμα έλαβε στη συνέχεια μέτρα που φράζουν από τους Βρετανούς χρήστες του Διαδικτύου την πρόσβαση σε περισσότερες από 6.000 περιοχές όπου είχε ανακαλυφθεί περιεχόμενο υλικό παιδικής πορνογραφίας, έναντι 3.438 περιοχών του προηγούμενου έτους, μια αύξηση 75 %.

Περίπου το 40% παιδικού πορνογραφικού υλικού που παρουσιάζεται στη Μεγάλη Βρετανία προέρχεται από τις ΗΠΑ. Περαιτέρω 28% προέρχεται από τη Ρωσία όπου, αν και η παραγωγή της παιδικής πορνογραφίας αυξάνεται γρήγορα, οι αρχές φαίνονται απρόθυμες να ενεργήσουν.

Αυτές οι εικόνες με το τόσο αποτρεπτικό, ανατριχιαστικό και άσεμνο υλικό, συλλέγονται και κυκλοφορούν στο εμπόριο από τους επιτήδειους με το ίδιο πάθος που κάποιος συλλέγουν κάποιοι γραμματόσημα.

Οι «συλλέκτες» προσπαθούν να πάρουν στην κατοχή τους κάθε εικόνα διαθέσιμη στη σειρά ενός ιδιαίτερου παιδιού και συνήθως αναφέρονται σε αυτό: η σειρά της Amy, οι περιπέτειες της Άννας κλπ.

Για να αποκτήσει κάποιος την ιδιότητα ενός νέου μέλους στους επίλεκτους αυτούς ιστοχώρους όπου γίνονται τέτοιου είδους εμπορικές συναλλαγές παιδικής πορνογραφίας τελεί υπό την προϋπόθεση ότι το μέλος θα συνεισφέρει στις αντίστοιχες σειρές με ένα ελάχιστο αριθμό νέων εικόνων που προσδιορίζεται από τους όρους εγγραφής και που προστίθεται στις δεκάδες χιλιάδες που ήδη υπάρχουν αυξάνοντας έτσι το συνολικό αριθμό. Τα θύματα της παιδικής πορνογραφίας παρατηρούμε ότι είναι άτομα ολοένα και πιο νεαρής ηλικίας. Υπάρχουν πολλοί λόγοι γι αυτό.

Ένας λόγος είναι ότι οι παραβάτες χρειάζονται συχνά τις εικόνες των όλο και περισσότερο μικρών παιδιών προκειμένου να επιτευχθεί η σεξουαλική ικανοποίηση.

Ένας άλλος λόγος είναι ότι συχνά τα πιο μικρά παιδιά κακοποιούνται και εκμεταλλεύονται από κάποιο άτομο που τα ίδια εμπιστεύονται, όπως ένα συγγενικό φίλο ή της οικογένειας, και επομένως δεν λένε σε κανέναν τι τους συμβαίνει.

Είναι πιθανότερο να πιστέψουν τον καταχραστή, ο οποίος τους εξαναγκάζει στην υποβολή. Και, φυσικά, τα μικρά παιδιά που δεν μιλούν ακόμα είναι κυριολεκτικά ανίκανα να πουν σε οποιονδήποτε για την κακοποίησή τους.

Υπάρχει μια κοινή παρερμηνεία ότι η κατοχή της παιδικής πορνογραφίας είναι ένα έγκλημα χωρίς «θύματα». Αυτή η άποψη δεν θα μπορούσε να απέχει πιο πολύ από την αλήθεια.

Κάθε ένας και κάθε φορά που κυκλοφορεί, τυπώνεται ή μεταφορτώνεται στο εμπόριο μια από αυτές τις εικόνες, το παιδί που απεικονίζεται στην εικόνα γίνεται θύμα ξανά και ξανά και ξανά. Όταν μια εικόνα δημοσιευτεί στο Διαδίκτυο, είναι εκεί για πάντα, ένα μόνιμο αρχείο της κατάχρησης και κακοποίησης που επιβάλλεται επάνω σε εκείνο το παιδί.

Είναι εκεί διαθέσιμη σε όποιον θέλει να τη δει, για το υπόλοιπο της ζωής εκείνου του παιδιού. Η φυσική και ψυχολογική ζημιά σε αυτά τα παιδιά

είναι ανυπολόγιστη. Η πράξη της κατοχής αυτών των εικόνων βλάπτει αυτά τα παιδιά τόσο όσο και η πράξη δημιουργίας τους.

Η Πρόεδρος της οργάνωσης «Ν.Ε.Ο.Ι.» κα. Άννα Ευθυμίου, με την ιδιότητα της ως Δικηγόρος και ως Εντεταλμένη Σύμβουλος σε Θέματα Νεολαίας Δήμου Θεσσαλονίκης τονίζει: 'Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας.

Ο κοινός παρανομαστής είναι οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες.

Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή ή και καρτούν.

Είναι ευρέως γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις. Επιπλέον, υπάρχουν σημαντικές διαφορές στην αντιμετώπιση της παιδικής πορνογραφίας από χώρα σε χώρα.

Σε ορισμένες χώρες, όπως και στην Ελλάδα, ακόμη και η εν γνώση κατοχή παιδικής πορνογραφίας είναι έγκλημα. Ωστόσο, οι ελληνικές αρχές με δεμένα τα χέρια προσπαθούν να αντιμετωπίσουν την παιδική πορνογραφία στο διαδίκτυο, λόγω των κενών στη νομοθεσία, που εμποδίζει τη σύλληψη ή, σε πολλές περιπτώσεις, την καταδίκη των δραστών.

Σύμφωνα με το νόμο του 2002, όσοι εντοπίζονται να διακινούν παιδοφιλικό υλικό χωρίς να παίρνουν χρήματα γι' αυτό ή χωρίς η εμπορία να είναι δυνατόν να αποδειχθεί, δεν μπορούν να διωχθούν.

Χαρακτηριστική είναι η περίπτωση του 72χρονου πρώην στελέχους της αμερικανικής βάσης στο Ελληνικό, που συνελήφθη πριν από δύο χρόνια ως μέλος διεθνούς κυκλώματος διακίνησης παιδικής πορνογραφίας στο διαδίκτυο και εγκέφαλος της δραστηριότητας στην Ελλάδα. Το πλήθος των στοιχείων που βρέθηκαν τότε στο σπίτι του στην Κηφισιά, και τα οποία έδειχναν σεξουαλικές πράξεις σε παιδιά από δύο έως επτά ετών, δεν στάθηκαν αρκετά για την καταδίκη του.

Για την καταπολέμηση της παιδικής πορνογραφίας πρόσφατα ψηφίστηκε από τη Βουλή ο νέος νόμος 3625/2007, ο οποίος περιλαμβάνει τρεις μεγάλες θεματικές ενότητες:

- Την κύρωση και εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία, που ενσωματώνεται στο εσωτερικό μας Δίκαιο και προσαρτάται στη Διεθνή Σύμβαση για τα Δικαιώματα του Παιδιού, στο πλαίσιο του Οργανισμού Ηνωμένων Εθνών (άρθρα 17).
- Σειρά νέων διατάξεων, οι οποίες εναρμονίζουν την Ελληνική νομοθεσία προς το περιεχόμενο του παραπάνω πρωτοκόλλου και άλλα διεθνή νομοθετήματα, για την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών και της παιδικής πορνογραφίας, σε ένα σύνολο κατηγοριών (σεξουαλικός τουρισμός, ασέλγεια μεταξύ συγγενών, παιδική πορνογραφία στο διαδίκτυο, διανομή και χρήση υλικού παιδικής πορνογραφίας μέσω συστήματος Η/Υ ή με τη χρήση Διαδικτύου, προστασία της ιδιωτικής ζωής του ανηλίκου κλπ.).
- Νέες ρυθμίσεις για τα προσωπικά δεδομένα, στην περίπτωση εγκλημάτων κατά της κοινωνίας και τη λειτουργία των καμερών κατά τη διάρκεια συγκεντρώσεων, εφόσον επίκειται σοβαρός κίνδυνος για τη δημόσια ασφάλεια και μόνον κατόπιν εντολής εκπροσώπου της εισαγγελικής αρχής.

Η εφαρμογή των παραπάνω διατάξεων άρχισε από τις 24/12/2007, με τη δημοσίευση του νόμου 3625/2007 στην Εφημερίδα της Κυβερνήσεως

Σύμφωνα με το Άρθρο 14 του Προαιρετικού Πρωτοκόλλου, η εφαρμογή του αρχίζει ένα μήνα αργότερα, δηλαδή στις 24/01/2008. Με τις παραπάνω ρυθμίσεις, διαμορφώνεται ένα νέο, αποτελεσματικό και ισχυρό οπλοστάσιο της Ελληνικής κοινωνίας και της νέας γενιάς απέναντι στα απειλητικά φαινόμενα της εκμετάλλευσης της εργασίας και της εμπορίας ανθρωπίνων οργάνων με θύματα παιδιά, της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της πορνογραφίας με πρωταγωνιστές παιδιά - φαινομένων που τείνουν να προσλάβουν διαστάσεις σύγχρονης μάστιγας και εμφανίζουν χαρακτηριστικά οργανωμένου εγκλήματος.

Βασικά σημεία των ρυθμίσεων του σχεδίου νόμου - μεταξύ άλλων αποτελούν:

- Η αναμόρφωση του αδικήματος της παιδικής πορνογραφίας ώστε να κολάζεται ο δράστης και όταν ο σκοπός του δεν είναι η αποκόμιση κέρδους, σκοπός που παραμένει ως ιδιαίτερα επιβαρυντική περίσταση.
- Συγχρόνως προσδιορίζεται ως τιμωρητέο υλικό παιδικής πορνογραφίας η αναπαράσταση, ή πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο φορέα: α) του σώματος ή μέρος του σώματος ανηλίκου με τρόπο που προδήλως προκαλεί γενετήσια διέγερση, β) πραγματικής ή εικονικής ασελγούς πράξης.
- Ο αυτεπάγγελτος διορισμός συνηγόρου σε ανήλικα θύματα.
- Η σύμπραξη κατά την ανάκριση παιδοψυχολόγου ή παιδοψυχιάτρου, που λειτουργεί με εχέγγυα πραγματογνώμονα.
- Η καταχώριση της κατάθεσης ανηλίκου θύματος σε ηλεκτρονικό μέσο.
- Η αποφυγή εμφάνισης του ανηλίκου θύματος σε ακροατήριο.
- Η ψυχοδιαγνωστική εξέταση και θεραπεία ανηλίκου θύματος και του δράστη των συγκεκριμένων εγκλημάτων.
- Η απαγόρευση δημοσίευσης περιστατικών, που μπορεί να οδηγήσουν στην εξακρίβωση της ταυτότητας του ανηλίκου θύματος με την απειλή ανάλογων ποινικών κυρώσεων.
- Η αναστολή της παραγραφής καθ' όλη τη διάρκεια της ανηλικότητας και μετά την ενηλικίωση του θύματος επί τρία έτη για τα κακουργήματα και επί ένα έτος για τα πλημμελήματα.
- Η εφαρμογή των ελληνικών ποινικών νόμων για τα εγκλήματα παιδικής πορνογραφίας και της διενέργειας ταξιδιών για την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου, που διαπράττονται από ημεδαπούς ή αλλοδαπούς -φαινόμενο γνωστό και διαδεδομένο ευρύτατα ως «σεξουαλικός τουρισμός».
- Η καθιέρωση ευθύνης νομικών προσώπων με βαρύτατες διοικητικές κυρώσεις.

- Η σύντομη εκδίκαση υποθέσεων σε όλους τους βαθμούς δικαιοδοσίας για τις συγκεκριμένες πράξεις που δεν μπορεί να υπερβεί τη διετία από την τέλεση ή διαπίστωσή τους.

Σε ότι αφορά τα όρια προστασίας των προσωπικών δεδομένων, ο νέος νόμος επιτρέπει τη δημοσίευσή τους, μετά από άδεια των εισαγγελικών ή δικαστικών αρχών, από τη φάση της προανάκρισης έως εκείνη της δίκης για τις εξής περιπτώσεις, σύμφωνα με το άρθρο όγδοο, του νέου νόμου:

1. Η παράγραφος 2 του άρθρου 3 του ν.2472/1997 (ΦΕΚ 50Α) αντικαθίσταται ως εξής:

2. Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων η οποία πραγματοποιείται:

α) από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών,

β) από τις δικαστικές-εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων.

Αποτελεί αδιαμφισβήτητο γεγονός ότι ανεξέλεγκτες διαστάσεις έχει λάβει διεθνώς τα τελευταία χρόνια το φαινόμενο διακίνησης παιδικής πορνογραφίας μέσω Διαδικτύου. Οι εξηγήσεις που δίνουν οι ειδικοί για τη ραγδαία εξάπλωση του φαινομένου είναι ψυχολογικές και κοινωνικές.

Ωστόσο, η παιδική πορνογραφία έχει και μια διόλου ευκαταφρόνητη οικονομική διάσταση.

Ο τζίρος για τους διεστραμμένους οι οποίοι εμπορεύονται παιδικά σώματα αγγίζει πολλές φορές και τα 3 δισ. ευρώ ανά έτος. Κερδισμένοι είναι όλοι όσοι εμπλέκονται σε αυτή την αρρωστημένη συναλλαγή, εκτός

φυσικά από τα παιδιά, οι ψυχές των οποίων μένουν για πάντα σημαδεμένες από τη βαρβαρότητα των εκμεταλλευτών τους.

Λύση για να γλιτώσουν οι γονείς τα παιδιά τους από τέτοιο θέαμα στο Internet δεν είναι μόνο η διαρκής αστυνόμευση. Οι ειδικοί κρούουν τον κώδωνα του κινδύνου στους γονείς και τους συμβουλεύουν να ελέγχουν οι ίδιοι τις ιστοσελίδες που επισκέπτονται τα παιδιά τους.

Στην Ελλάδα το φαινόμενο της παιδικής πορνογραφίας παρουσιάζει έξαρση και οι αξιωματικοί Δίωξης Ηλεκτρονικού Εγκλήματος ανακαλύπτουν ολοένα και πιο ‘σκληρό’ υλικό στους υπολογιστές των δραστών.

6 ΝΟΜΙΚΗ ΔΙΑΣΤΑΣΗ ΣΕ ΕΛΛΑΔΑ ΚΑΙ ΕΥΡΩΠΗ

Η περίοδος την οποία διανύουμε χαρακτηρίζεται από μία αυξανόμενη διαθεσιμότητα και χρήση των τεχνολογιών της Κοινωνίας της Πληροφορικής.

Η περαιτέρω τεχνολογική ανάπτυξη και η αυξημένη χρήση των ανοικτών δικτύων, όπως το Διαδίκτυο, κατά τα επόμενα έτη θα δημιουργήσουν νέες σημαντικές δυνατότητες και θα θέσουν νέες προκλήσεις.

Οι υποδομές πληροφόρησης και επικοινωνίας έχουν καταστεί ουσιαστικό τμήμα των οικονομιών μας. Δυστυχώς, όμως, αυτές οι υποδομές έχουν τα δικά τους αδύνατα σημεία και προσφέρουν νέες ευκαιρίες για εγκληματικές συμπεριφορές. Αυτές οι εγκληματικές δραστηριότητες μπορούν να λάβουν διάφορες μορφές και να διασχίσουν πολλά σύνορα.

Παρά το γεγονός ότι, για μια σειρά από διάφορους λόγους, δεν υπάρχουν αξιόπιστες στατιστικές, είναι αναμφίβολο ότι αυτά τα αδικήματα αποτελούν απειλή για τις βιομηχανικές επενδύσεις και κεφάλαια και, για την ασφάλεια και εμπιστοσύνη στην κοινωνία της πληροφορίας.

Ορισμένα πρόσφατα παραδείγματα επιθέσεων ιών και άρνησης παροχής υπηρεσίας έχουν προξενήσει σημαντικές οικονομικές ζημιές.Οι χρήστες πρέπει να μπορούν να υπολογίζουν στη διαθεσιμότητα υπηρεσιών πληροφόρησης και να έχουν εμπιστοσύνη στο γεγονός ότι οι επικοινωνίες τους και τα δεδομένα τους θα προστατεύονται κατά οιασδήποτε μη εξουσιοδοτημένης πρόσβασης ή τροποποίησης.

Η ανάπτυξη του ηλεκτρονικού εμπορίου και η πλήρης υλοποίηση της Κοινωνίας της Πληροφορίας εξαρτάται από αυτό. Οι νέες ψηφιακές και ασύρματες τεχνολογίες υπάρχουν ήδη παντού. Μας παρέχουν επίσης τη δυνατότητα συμμετοχής, διδασκαλίας και εκμάθησης, από κοινού εργασίας και παιγνιδίου, συμμετοχής στην πολιτική διαδικασία.

Στο μέτρο εντούτοις που οι κοινωνίες θα εξαρτηθούν περισσότερο από αυτή την τεχνική, θα πρέπει να χρησιμοποιηθούν πρακτικά και νομικά μέσα για να αντιμετωπιστούν οι κίνδυνοι που συνδέονται με αυτή την εξέλιξη.

Η κλασική προσέγγιση όσον αφορά την ασφάλεια απαιτούσε την αυστηρή οργανωτική, γεωγραφική και διαρθρωτική στεγανοποίηση των πληροφοριών, ανάλογα με την ευαισθησία και την κατηγορία τους.

Αυτή η προσέγγιση είναι ξεπερασμένη στον ψηφιακό κόσμο, δεδομένου ότι η επεξεργασία της πληροφορίας είναι κατανεμημένη, οι υπηρεσίες παρέχονται σε χρήστες κινητών επικοινωνιών και η διαλειτουργικότητα των συστημάτων αποτελεί προαπαιτούμενο.

Καινοτόμες λύσεις που βασίζονται στις νεοεμφανιζόμενες τεχνολογίες υποκαθίστανται στις κλασικές προσεγγίσεις που αφορούν τα ζητήματα ασφαλείας.

Περιλαμβάνουν τη χρήση τεχνικών κρυπτογράφησης και ψηφιακών υπογραφών, νέα εργαλεία ελέγχου της πρόσβασης και της γνησιότητας, καθώς επίσης όλα τα είδη φίλτρων λογισμικού.

Οι ασφαλείς και αξιόπιστες υποδομές πληροφόρησης απαιτούν όχι μόνο την ύπαρξη κλίμακας τεχνολογιών αλλά εξίσου τη σωστή και αποτελεσματική χρήση τους.

Ορισμένες από αυτές τις τεχνολογίες υπάρχουν ήδη, αλλά οι χρήστες αγνοούν συχνά την ύπαρξή τους, τον τρόπο χρήσης τους ή τους λόγους για τους οποίους αυτές μπορούν να είναι απαραίτητες.

Το έγκλημα πληροφορικής επηρεάζει όλο τον κυβερνοχώρο και δεν σταματά στα παραδοσιακά σύνορα των κρατών.Αυτές οι παραβάσεις μπορούν κατ' αρχήν να διαπράττονται από οποιοδήποτε σημείο σε βάρος οποιουδήποτε χρήστη υπολογιστή, οπουδήποτε και εάν αυτός ευρίσκεται.

Εχει γενικά αναγνωριστεί ότι χρειάζεται αποτελεσματική και διαρκής δράση για την καταπολέμηση του εγκλήματος πληροφορικής τόσο σε εθνικό όσο και σε διεθνές επίπεδο και το πεδίο δράσης υπάρχει τόσο από την άποψη της πρόληψης των εγκληματικών δραστηριοτήτων με την ενίσχυση της ασφάλειας των υποδομών πληροφόρησης όσο και από την άποψη της εξασφάλισης στις αρχές εφαρμογής του νόμου (law enforcement

agencies) των απαραίτητων μέσων δράσης, ενώ ταυτόχρονα θα πρέπει να τηρούνται πλήρως και να είναι σεβαστά τα θεμελιώδη δικαιώματα του ατόμου.

6.1 **Ευρωπαική Διάσταση**

Η μετατροπή της Ευρώπης σε κοινωνία της πληροφορίας χαρακτηρίζεται από βαθιές εξελίξεις σε όλους τους τομείς της ανθρώπινης ζωής: εργασία, εκπαίδευση και ψυχαγωγία, κυβερνητικό σύστημα, βιομηχανία και εμπόριο.

Οι νέες τεχνολογίες πληροφόρησης και επικοινωνίας έχουν επαναστατική και θεμελιώδη επίπτωση στις οικονομίες μας και τις κοινωνίες μας. Η επιτυχία της κοινωνίας της πληροφορίας είναι σημαντική για την ανάπτυξη, την ανταγωνιστικότητα και τις ευκαιρίες απασχόλησης της Ευρώπης και έχει σημαντικές οικονομικές, κοινωνικές και νομικές επιπτώσεις.

6.2 **Η θέση της Ευρωπαϊκής ΄Ένωσης απέναντι στο διαδίκτυο**

Η Ευρωπαϊκή Ενωση δεν έμεινε αδιάφορη απέναντι στο ηλεκτρονικό έγκλημα γενικότερα και στον κυβερνοχώρο ειδικότερα.΄Ετσι στις 17.2.1997 εκδίδεται το No 97/C 70/01 ψήφισμα του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών μελών, που συνήλθαν στα πλαίσια του Συμβουλίου της Ευρωπαϊκής Ένωσης.

Κύριο χαρακτηριστικό του ψηφίσματος αυτού είναι ότι η Ευρωπαϊκή Ένωση αναγνωρίζει τα θετικά οφέλη που προσφέρει ο κυβερνοχώρος, ιδιαίτερα στον τομέα της εκπαίδευσης, παρέχοντας δυνατότητες στους πολίτες, μειώνοντας τα εμπόδια ως προς τη δημιουργία και τη διανομή περιεχομένου και προσφέροντας ευρεία πρόσβαση σε όλο και πλουσιότερες πηγές ψηφιακών πληροφοριών.

Αναγνωρίζει επίσης το παραπάνω ψήφισμα την ανάγκη καταπολέμησης της παράνομης χρήσης των τεχνικών δυνατοτήτων του κυβερνοχώρου, ιδιαίτερα για αξιόποινες πράξεις κατά των παιδιών.

Πριν από την έκδοση του ψηφίσματος αυτού είχαν γίνει για το θέμα διάφορες επίσημες ή ανεπίσημες για το θέμα συναντήσεις .

Χαρακτηριστικό επίσης του ψηφίσματος αυτού είναι ότι, η Ευρωπαϊκή Ένωση διαχωρίζει το περιεχόμενο (content) του διαδικτύου, δηλαδή τα δεδομένα - στοιχεία (data), που διακινούνται, σε παράνομο και επιβλαβές.

α)Παράνομο περιεχόμενο του Internet.Το σχετικό ψήφισμα (97/C 70/01/17-2-1997) του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών μελών της Ευρωπαϊκής Ένωσης για το παράνομο και επιβλαβές περιεχόμενο του διαδικτύου (Internet), δεν καθορίζει τι είναι παράνομο και τι είναι επιβλαβές περιεχόμενο. Κατά συνέπεια λοιπόν οι έννοιες αυτές θα προσδιοριστούν από το νομοθέτη σε περίπτωση που ψηφιστεί σχετικός νόμος που θα ρυθμίζει την συμπεριφορά, όσων «κινούνται» στον χώρο του διαδικτύου. Και λέγοντας εδώ «νομοθέτη» εννοούμε τον εθνικό νομοθέτη κάθε επιμέρους χώρας.

Στο σημείο όμως αυτό προκύπτει το ερώτημα , εάν οι «εσωτερικές νομοθεσίες» μπορούν αυτοτελώς, να αντιμετωπίσουν αποτελεσματικώς τις παρανομίες στο κυβερνοχώρο, λόγω της φύσεως του εγκλήματος και του ιδιαίτερου τρόπου τελέσεώς των.

Κατά την άποψή μας, οι εσωτερικές νομοθεσίες από μόνες τους δεν επαρκούν. Απαιτούνται πολυμερείς Διεθνείς Συμβάσεις .Προς το παρόν ως παράνομο περιεχόμενο μπορεί να θεωρηθεί κάθετί που, είναι μεν παράνομο (και) εκτός δικτύου, μπορεί δε (τεχνικώς) να κινηθεί και εντός κυβερνοχώρου (π.χ. συκοφαντική δυσφήμηση).β) Επιβλαβές περιεχόμενο του Internet. Το «επιβλαβές περιεχόμενο» αποτελεί ευρύτερη έννοια απ΄ αυτή του «παρανόμου περιεχομένου». Εννοείται ότι, οτιδήποτε είναι επιβλαβές, δεν είναι οπωσδήποτε και παράνομο.

Η έννοια του «επιβλαβούς περιεχομένου» ενέχει σε μεγάλο βαθμό και το υποκειμενικό στοιχείο. Είναι ευνόητο βέβαια ότι, η έννοια του επιβλαβούς

περιεχομένου έχει διαφορετική βαρύτητα, όταν πρόκειται για χρήση του του διαδικτύου από ανηλίκους Παράδειγμα:

Στο Internet υπάρχουν εκατοντάδες θέσεις (sites) που αναφέρονται στο Σατανισμό και στη Λατρεία του Σατανά. Για πολλούς το περιεχόμενο των sites αυτών αποτελεί κλασσική μορφή «επιβλαβούς περιεχομένου».

Για άλλους όμως αποτελεί μια μορφή ελεύθερης έκφρασης της προσωπικότητας ή ακόμα και μια μορφή ανεξιθρησκίας.

Γενικώς ως επιβλαβές περιεχόμενο μπορεί να θεωρηθεί, ότι αναφέρεται σε ρατσιστικές διακρίσεις ή σε παραπλανητική διαφήμιση.

Ως χαρακτηριστικό (κατά την άποψή μου) παράδειγμα επιβλαβούς περιεχομένου υλικό του διαδικτύου, μπορεί να θεωρηθεί και η περίπτωση (κατά τον Οκτώβριο του 1999) πλειοδοσίας κατά την πώληση ωαρίων εμφανίσιμων γυναικών σε ειδική τοποθεσία. Ομοίως η περίπτωση της «ερωτικής συνεύρεσης για πρώτη φορά» (τον Αύγουστο 1998) μεταξύ δύο «παρθένων νέων», που όμως τελικά δεν έγινε.

Είναι ευνόητο βέβαια ότι, πριν από την ματαίωση της «παράστασης» εκατομμύρια χρήστες από όλον τον κόσμο είχαν «επισκεφθεί» την αντίστοιχη τοποθεσία, με τεράστια οικονομικά κέρδη για τους «διοργανωτές». Η περίπτωση αυτή μπορεί να θεωρηθεί και ως απάτη, που διαπράττεται στο διαδίκτυο. Είναι ευνόητο όμως ότι, ουδείς βλαπτόμενος (ιδιώτης) ενδιαφέρθηκε για την υποβολή εγκλήσεως προς άσκηση ποινικής διώξεως, λαμβάνοντας υπόψη την μικρή οικονομική ζημία που υπέστη ως άτομο ή την διαπόμπευσή του για τις διαδικτυακές του προτιμήσεις, σε σχέση και με τα τεράστια δικαστικά έξοδα που απαιτούνται, για την κίνηση ενός τέτοιου δικαστικού αγώνα.

Σημειωτέον ότι, για την αντιμετώπιση του παρανόμου και επιβλαβούς περιεχομένου του κυβερνοχώρου έχει προταθεί -μεταξύ των άλλων- και η δημιουργία «οργάνου αυτορύθμισης» στο πλαίσιο λειτουργίας των παροχέων υπηρεσιών, καθώς και λειτουργία «θερμής γραμμής», όπου θα μπορούν να γίνονται σχετικές (επώνυμες ή και ανώνυμες) καταγγελίες .

Η Ευρωπαϊκή Ενωση έχει ήδη θεσπίσει μια σειρά μέτρων για την καταπολέμηση του παράνομου και επιζήμιου περιεχομένου του Διαδικτύου,

για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας και των δεδομένων προσωπικού χαρακτήρα, για την προώθηση του ηλεκτρονικού εμπορίου και τη χρήση των ηλεκτρονικών υπογραφών και την ενίσχυση της ασφάλειας των συναλλαγών.

6.3 **Μέτρα που έχει θεσπίσει η Ευρωπαϊκή Ενωση**

Τον Απρίλιο του 1998, η Επιτροπή παρουσίασε στο Συμβούλιο τα αποτελέσματα μελέτης για το έγκλημα πληροφορικής και την αντιμετώπισή του.

Τον Οκτώβριο 1999, το Ευρωπαϊκό Συμβούλιο του Τάμπερε όρισε ότι οι προσπάθειες να επιτευχθεί συμφωνία για κοινούς ορισμούς και κυρώσεις πρέπει να αφορούν εξίσου τα εγκλήματα υψηλής τεχνολογίας. Το Ευρωπαϊκό Κοινοβούλιο απηύθυνε επίσης έκκληση για κοινά παραδεκτούς ορισμούς των εγκλημάτων πληροφορικής και για πραγματική προσέγγιση των νομοθεσιών, ιδιαίτερα όσον αφορά το ποινικό δίκαιο.

Το Συμβούλιο της Ευρωπαϊκής Ενωσης εξέδωσε κοινή θέση σχετικά με τις διαπραγματεύσεις που αφορούν το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και έλαβε ορισμένα αρχικά μέτρα στο πλαίσιο της στρατηγικής της. Ενωσης για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.

Ορισμένα κράτη-μέλη της Ευρωπαϊκής Ενωσης διαδραμάτισαν επίσης πρωτεύοντα ρόλο στις σχετικές με το θέμα δραστηριότητες των χωρών της Ομάδας των Οκτώ (G8).

Στην Ευρωπαϊκή Ενωση, μέχρι πρόσφατα, τα θεσπιζόμενα νομοθετικά μέτρα αφορούσαν κυρίως τους τομείς των δικαιωμάτων πνευματικής ιδιοκτησίας, της θεμελιώδους αρχής της προστασίας του ιδιωτικού βίου και της προστασίας των δεδομένων, των υπηρεσιών με υπό όρους πρόσβαση, του ηλεκτρονικού εμπορίου, των ηλεκτρονικών υπογραφών και ιδιαίτερα την απελευθέρωση του εμπορίου των συστημάτων κρυπτογράφησης, που συνδέονται έμμεσα με το έγκλημα πληροφορικής.

Κατά τα τελευταία τρία-τέσσερα έτη, επίσης, έχουν ληφθεί ορισμένα σημαντικά νομοθετικά μέτρα.

Αυτά συμπεριλαμβάνουν το πρόγραμμα δράσης για την καταπολέμηση του παράνομου και επιζήμιου περιεχομένου του Διαδικτύου, το οποίο συγχρηματοδοτεί ενέργειες ευαισθητοποίησης, δοκιμές ταξινόμησης και φιλτραρίσματος του περιεχομένου και των απευθείας συνδέσεων (hot-line) και πρωτοβουλίες σχετικά με την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στην κοινωνία της πληροφορίας, την παιδική πορνογραφία και την παρακολούθηση επικοινωνιών για λόγους εφαρμογής του νόμου.

Α) Συμβούλιο Ευρώπης και έγκλημα στον κυβερνοχώρο.

Το Συμβούλιο της Ευρώπης έχει ασχοληθεί τόσο με το ηλεκτρονικό έγκλημα, όσο και με το έγκλημα στον κυβερνοχώρο.

Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα :

α) Η Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer - related crime).

β) Η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology). Στο Συμβούλιο της Ευρώπης καταρτίζεται από το έτος 1997 Διεθνής Σύμβαση με αντικείμενο την καταπολέμηση του εγκλήματος στο Κυβερνοχώρο.

Στην κατάρτιση της Σύμβαση αυτής συμμετέχει και η Ελλάδα.

Σκοπός της Συμβάσεως είναι η προστασία της Κοινωνίας από το έγκλημα στον κυβερνοχώρο, με την θέσπιση της κατάλληλης νομοθεσίας και την επίτευξη της ανάλογης με το θέμα Δικαστικής Συνεργασίας μεταξύ των κρατών, που θα υπογράψουν την Σύμβαση.

Αρχικώς ως χρονοδιάγραμμα για την περαίωση των εργασιών, είχε τεθεί το τέλος του έτους 1999. Επειδή όμως τα προβλήματα (νομικά και τεχνικά) που προέκυψαν κατά την συζήτηση ήταν τόσα πολλά και τόσο περίπλοκα,

ζητήθηκε (και χορηγήθηκε) παράταση της προθεσμίας περαιώσεως μέχρι το τέλος του 2000. Ήδη η Σύμβαση έχει περαιωθεί και πρόκειται να ανοίξει για υπογραφές σε ειδική τελετή που θα γίνει στις 22 και 23 Νοεμβρίου 2001 στην Βουδαπέστη.

Η συγκεκριμένη σύμβαση καθιερώνει την υποχρέωση εναρμονίσεως των Εθνικών νομοθεσιών σε θέματα εγκλημάτων στον κυβερνοχώρο (internet crimes) τόσο σε θέματα ποινικού, όσο και Αστικού Δικαίου.Κύριο χαρακτηριστικό της Διεθνούς αυτής Συμβάσεως είναι η υποχρέωση που αναλαμβάνουν τα κράτη-μέλη, να ποινικοποιήσουν ορισμένη συμπεριφορά στο διαδίκτυο.

Ενδιαφέρουσες διατάξεις, που έχουν σχέση με την ασφάλεια στο διαδίκτυο, από ουσιαστική ποινική άποψη είναι οι παρακάτω:

α)Η Παράνομη πρόσβαση (illegal Access).

Σύμφωνα με το άρθρο 2 της Συμβάσεως κάθε μέλος θα θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα.

Το μέρος μπορεί να απαιτεί ότι, το αδίκημα θα διαπράττεται ή με παραβίαση των μέτρων ασφαλείας ή με το σκοπό αποκτήσεως ηλεκτρονικών δεδομένων ή για άλλο παράνομο σκοπό ή σε σχέση με ένα σύστημα ηλεκτρονικών υπολογιστών, που συνδέεται με άλλο σύστημα ηλεκτρονικών υπολογιστών.

Το άρθρο αυτό έχει ως σκοπό να ποινικοποιήσει αυτό που στην γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως «hacking». Ο όρος στα Ελληνικά μπορεί να αποδοθεί ως «εισβολή».

Ως εισβολή μπορεί να οριστεί η ενέργεια το εισβολέα («hacker») να εισέλθει (διεισδύσει - αποκτήσει πρόσβαση), με διάφορους τεχνικούς τρόπους, σε ξένα συστήματα υπολογιστών. Προστατευόμενο έννομο αγαθό είναι η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης από μη εξουσιοδοτημένα άτομα στο σύστημα.

Αποτελεί δηλαδή το άρθρο αυτό, το «ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο» της διατάραξης οικιακής ειρήνης (άρθρο 334 Π.Κ.).

Όπως δηλαδή ο δικαιούχος της κατοικίας έχει το δικαίωμα να ορίζει ποιος μπορεί να εισέρχεται και να παραμένει σ΄ αυτήν, έτσι και ο «δικαιούχος» του ηλεκτρονικού υπολογιστή δικαιούται να ορίζει ποιος θα τον χρησιμοποιεί και ποιος θα «εισέρχεται» σ΄ αυτόν.

Ο δικαιολογητικός λόγος της ποινικοποιήσεως της παράνομης πρόσβασης συνίσταται στο γεγονός ότι, ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος, τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσεως του υπολογιστή ή του συστήματος υπολογιστή. Ο όρος «πρόσβαση» περιλαμβάνει την «χωρίς εξουσιοδότηση είσοδο» σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή μέρος αυτού (π.χ. σε επιμέρους φακέλους).

Δεν περιλαμβάνει όμως την χωρίς δικαίωμα αποστολή ηλεκτρονικών μηνυμάτων ή φακέλων. Για την θεμελίωση της υποκειμενικής υποστάσεως απαιτείται πρόθεση , όπως αυτός προσδιορίζεται σύμφωνα με το εσωτερικό δίκαιο κάθε μέλους κράτους. Οι περισσότερες νομοθεσίες των κρατών μελών του Συμβουλίου της Ευρώπης περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή.

β) Η αθέμιτη παγίδευση - υποκλοπή (illegal interception) .

Σύμφωνα με το άρθρο 3 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η παγίδευση -υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σ' ένα σύστημα υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που «μεταφέρει» τέτοια στοιχεία.

Ένα μέλος μπορεί να απαιτήσει ότι το αδίκημα διαπράττεται με παράνομο σκοπό ή σε σχέση με ένα σύστημα υπολογιστών, το οποίο συνδέεται με άλλο σύστημα.

Η διάταξη αυτή μπορεί να εφαρμοστεί σε κάθε μορφή υποκλοπής ηλεκτρονικών δεδομένων, είτε αυτά διακινούνται δια του κυβερνοχώρου με μεταφορά φακέλων (file transfer), είτε με e-mail, είτε με FAX.

Προστατευόμενο έννομο αγαθό είναι «το δικαίωμα στην ιδιωτική ζωή και της ασφάλειας των τηλεπικοινωνιών στον κυβερνοχώρο».Αποτελεί δηλαδή το άρθρο αυτό, το «ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο» της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας (υποκλοπή). Στην Ελληνική έννομη τάξη η συμπεριφορά αυτή προβλέπεται στην στο άρθρο 370 Α §§1 και 2 Π.Κ.

Σύμφωνα με αυτό όποιος αθέμιτα παγιδεύει ή με οποιαδήποτε άλλο τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση.

Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση.

Επίσης, 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.

γ) Επέμβαση σε δεδομένα (Data interference) .

Σύμφωνα με το άρθρο 4 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εθνική του νομοθεσία, όταν διαπράττονται εκ προθέσεως η καταστροφή (damaging), η διαγραφή (deletion), η χειροτέρευση (deterioration), η μεταβολή (alteration), ή η απόκρυψη (suppression) δεδομένων χωρίς δικαίωμα.

Σκοπός του άρθρου αυτού είναι να προστατεύσει τα δεδομένα (data) και τα προγράμματα των ηλεκτρονικών υπολογιστών ως «υλικές υποστάσεις» από οποιαδήποτε επέμβαση (παρεμβολή), που γίνεται με πρόθεση πρόκλησης ζημιάς σ΄ αυτά. Προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

Ως εγγύτερο άρθρο στην Ελληνική έννομη τάξη μπορεί να θεωρηθεί αυτό της φοράς ξένης ιδιοκτησίας (άρθρο 381 Π.Κ.). δ)Επέμβαση σε σύστημα (System Interference).

Σύστημα ηλεκτρονικού υπολογιστή («Computer system») σημαίνει κάθε συσκευή ή ομάδα συσκευών που είναι εσωτερικώς συνδεδεμένες μεταξύ των ή με άλλες σχετικές συσκευές, μια ή περισσότερες από τις οποίες επεξεργάζονται αυτομάτως δεδομένα, σύμφωνα με κάποιο πρόγραμμα. Δεδομένα υπολογιστή είναι κάθε αναπαράσταση γεγονότων , πληροφοριών ή εννοιών σε μορφή κατάλληλη για επεξεργασία σε σύστημα υπολογιστή, συμπεριλαμβανομένου προγράμματος κατάλληλο να προκαλέσει σ΄ ένα σύστημα υπολογιστή την εκτέλεση μιας λειτουργίας.

Σύμφωνα με το άρθρο 5 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα, για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττεται εκ προθέσεως η σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση, μεταφορά, καταστροφή, διαγραφή,χειροτέρευση, μεταβολή, ή απόκρυψη δεδομένων υπολογιστών. Το προστατευόμενο έννομο αγαθό στο άρθρο αυτό είναι το δικαίωμα του χρήστη να έχει μια «κανονική» λειτουργία του υπολογιστή του. Η διάταξη αυτή ποινικοποιεί, αυτό που στην γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως «computer sabotage» (δολιοφθορά ηλεκτρονικού υπολογιστή).

ε)Κακή χρήση συσκευών (misuse of devices).

Σύμφωνα με το άρθρο 6 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα προκειμένου να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττονται εκ προθέσεως και χωρίς δικαίωμα η παραγωγή, πώληση, η προετοιμασία για χρήση εισαγωγή, διανομή ή με οποιοδήποτε άλλο τρόπο διάθεση μιας συσκευής συμπεριλαμβανομένου προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως για τους σκοπούς διάπραξης οποιουδήποτε από τα αδικήματα που θεμελιώνονται στα άρθρα 2-5 της Συμβάσεως.

Στην Ελληνική έννομη τάξη το άρθρο αυτό αντιστοιχεί με το 370 Α §7 Π.Κ. Σύμφωνα με αυτό, όποιος διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει για εγκατάσταση τεχνικά μέσα ειδικά μόνο για την τέλεση των πράξεων των §§ 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση και με χρηματική ποινή.

Έρευνα, ανάλυση και αποτύπωση της υφισταμένης τεχνολογικής υποδομής στην αγορά ΤΠΕ της Ν.Α. Ευρώπης

• Εκπόνηση μελετών για τους ενδιαφερόμενους φορείς σε τοπικό και διακρατικό δίκτυο

• Εντοπισμό των υφισταμένων επενδυτικών ευκαιριών στο κλάδο ΤΠΕ της Ν.Α. Ευρώπης

• Οργάνωση συναντήσεων εργασίας, προγραμμάτων κατάρτισης, επιστημονικών ημερίδων, συνεδρίων με σκοπό την μεταφορά τεχνογνωσίας

• Αξιοποίηση δυνατοτήτων που παρέχει η ΕΕ και λοιποί Διεθνείς Οργανισμοί χρηματοδότησης για την ανάπτυξη των τηλεπικοινωνιών των χωρών της Ν.Α. Ευρώπης

6.4 **Προβλήματα προσέγγισης**

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προυποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών και διαδικτύου.

Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στον πεδίο του εγκλήματος στον κυβερνοχώρο, όπως άλλωστε συμβαίνει και στα εγκλήματα με ηλεκτρονικούς υπολογιστές χωρίς την κατοχή αυτών των τεχνικών γνώσεων .

Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός

πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις.

Ο συνδυασμός των δύο βασικών, αλλά και διαφορετικών τρόπων σκέψεως αποτελεί τον σταυρό του μαρτυρίου για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

Ενα εξίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με την νομική πλευρά του θέματος από ποινική άποψη, είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων.

Είναι ευνόητο ότι, η έλλειψη αυτή οφείλεται στο γεγονός ότι, το έγκλημα στον κυβερνοχώρο αποτελεί νέα μορφή εγκλήματος. Αποτελεί κοινή διαπίστωση ότι, η ανάπτυξη των σχετικών νομικών θεμάτων από αστική και εμπορική άποψη έχει διερευνηθεί σε μεγαλύτερη έκταση, από ότι η αντίστοιχη ποινική πλευρά.

Αυτό οφείλεται στην μεγάλη επιρροή του κυβερνοχώρου, τόσο στο αστικό (σύναψη συμβάσεων εξ αποστάσεως δια του κυβερνοχώρου κλπ), όσο και στον οικονομικό τομέα (ηλεκτρονικό εμπόριο, νέα οικονομία κλπ). Σε κάθε περίπτωση όμως ο μελετητής των σχετικών με τον κυβερνοχώρο θεμάτων θα πρέπει να καταφεύγει στα διάφορα (πολυπληθή) τεχνικά περιοδικά για τους ηλεκτρονικούς υπολογιστές, καθώς και σε δημοσιεύματα του ημερήσιου Τύπου.

Αλλωστε και το ίδιο το διαδίκτυο αποτελεί πηγή αντλήσεως πληροφοριών (ίσως την σημαντικότερη), ανατρέχοντας στις ειδικές τοποθεσίες - θέσεις (Sites

Το γενικότερο πρόβλημα της νομικής ορολογίας

Πρέπει ιδιαιτέρως να τονιστεί ότι, η διαφορετική κατανόηση - αντίληψη των ίδιων εννοιών από τον τεχνικό και νομικό αποτελεί ένα από τα σημαντικότερα προβλήματα του υπό εξέταση θέματος.

Ετσι, π.χ. διαφορετικά αντιλαμβάνεται την έννοια του όρου «κυβερνοχώρος», «ασφάλεια», «χάκερ» κλπ ο τεχνικός και διαφορετικά ο νομικός. Για τη νομική επιστήμη οι έννοιες έχουν το περιεχόμενο που ρητώς τους προσδίδει ο νόμος.

Σε περίπτωση δε, που δεν υπάρχει σχετικός νόμος, ανατρέχει ο νομικός στη νομολογία, δηλαδή, στις υπάρχουσες δικαστικές αποφάσεις. Για την ύπαρξη όμως σχετικής νομολογίας, είναι απαραίτητο να έχει «φθάσει» η υπόθεση ή άλλη παρόμοια στο δικαστήριο.

Σε περίπτωση που, ούτε νομολογία υπάρχει, ο νομικός ανατρέχει στη νομική επιστήμη, προς αναζήτηση θεωρητικής τουλάχιστον λύσης του θέματος.

Αυτό βέβαια δεν σημαίνει ότι, η νομική θεωρία, όπως αυτή έχει αναπτυχθεί ή αναπτύσσεται από τη (νομική) επιστήμη, γίνεται υποχρεωτικώς δεκτή στην νομική πρακτική, δηλαδή στην διερεύνηση ή την εκδίκαση των σχετικών εγκλημάτων.

Στο υπό εξέταση λοιπόν θέμα, είναι απαραίτητο να προσδιοριστεί η νομική έννοια των όρων «ασφάλεια», «κυβερνοχώρος – διαδίκτυο», «χάκερ».

Πριν απ΄ αυτό όμως κρίνεται απαραίτητο να οριοθετηθεί η έννοια του εγκλήματος στον κυβερνοχώρο, να προσδιοριστούν τα χαρακτηριστικά του (εγκλήματος στον κυβερνοχώρο), να καθοριστεί η σχέση μεταξύ εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή και να δοθεί το «προφίλ» του εγκληματία στον κυβερνοχώρο.

Η νομική έννοια του διαδικτύου και του κυβερνοχώρου στην Ελληνική νομοθεσία δεν προσδιορίζεται.

Κατά συνέπεια οι έννοιες αυτές λαμβάνονται από την τεχνολογία. Ετσι λοιπόν, ως διαδίκτυο μπορεί να οριστεί η παγκόσμια συλλογή δικτύων και πυλών, που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ των , ενώ ως κυβερνοχώρος μπορεί να οριστεί το σύνολο των ηλεκτρονικών κόσμων, όπως το internet, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών, όπου δηλαδή η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση .

Στο άρθρο 2 του Ν 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών προσδιορίζονται οι έννοιες «δίκτυο καλωδιακής

τηλεόρασης», «ιδιωτικό δίκτυο», «παροχή ανοικτού δικτύου» και «τηλεπικοινωνιακό δίκτυο».

Δεν προσδιορίζεται όμως η έννοια του διαδικτύου ή του κυβερνοχώρου. Πρέπει να λεχθεί ότι, στη συνείδηση του μέσου νομικού, δεν γίνεται διάκριση μεταξύ διαδικτύου και κυβερνοχώρου και κατά κανόνα οι έννοιες αυτές θεωρούνται ως ταυτόσημες και χρησιμοποιούνται πάντα με το ίδιο περιεχόμενο.

Προσδιορισμός της εννοίας του εγκλήματος στον κυβερνοχώρο

Δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στην διεθνή νομοθεσία, ούτε στην διεθνή νομολογία ή βιβλιογραφία .Ομοίως ούτε στην Ελληνική βιβλιογραφία υπάρχει ορισμός του εγκλήματος στον κυβερνοχώρο.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το κοινό ή συμβατικό έγκλημα και η μόνη διαφορά που το διακρίνει απ΄ αυτό είναι ότι, διαπράττεται σε διαφορετικό περιβάλλον , (δηλ. σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται κατά την άποψή μου πλήρως στην πραγματικότητα.

Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Αλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται).

Μια άλλη κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικώς σε περιβάλλον του κυβερνοχώρου. Με το παραπάνω λοιπόν κριτήριο τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν:

α) Σε εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο π.χ. η συκοφαντική δυσφήμηση διαπράττεται και με την χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail).

Η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το

έγκλημα αυτό τελεστεί σε «περιβάλλον internet» (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

β) Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενν. χωρίς την χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο **370 Γ παράγρ. 1 του Π.Κ**. π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM ή σε ηλεκτρονικό υπολογιστή.

γ) Σε «Γνήσια εγκλήματα κυβερνοχώρου» (Cyber crimes) με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς έχει σχέση με τον κυβερνοχώρο.

Μια τέτοια αξιόποινη συμπεριφορά μπορεί να θεωρηθεί η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου.

Τέτοια εγκλήματα δεν υπάρχουν ακόμα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία. Δηλαδή τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικώς σε περιβάλλον διαδικτύου.

Σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή.

Σχέση εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή

Το έγκλημα στον κυβερνοχώρο (Cyber Crime) είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος (Computer Crime), το οποίο με τη σειρά του είναι μία ειδικότερη μορφή του κοινού εγκλήματος, όπως αυτό προσδιορίζεται στο άρθρο 14 Π.Κ.

6.5 Διαδύκτιο και Ποινική Νομοθεσία

Γενικές παρατηρήσεις

Το ερώτημα που προκύπτει από την σχέση διαδικτύου και ποινικής νομοθεσίας είναι , αν η συμπεριφορά των χρηστών του διαδικτύου μπορεί να ρυθμιστεί με ποινικούς κανόνες δικαίου και εάν στην συνέχεια οι ποινικοί αυτοί κανόνες μπορούν να εφαρμοστούν στην πράξη.

Το πρώτο αποτελεί ερώτημα του ουσιαστικού ποινικού δικαίου και το δεύτερο ερώτημα του ποινικού δικονομικού δικαίου.

Η απάντηση είναι: Πάρα πολύ δύσκολα και σε πολύ περιορισμένο τομέα.Και αυτό γιατί, η τεχνολογία εξελίσσεται τόσο γρήγορα, που η νομοθεσία όσο και αν προσπαθεί αδυνατεί να την προφτάσει.

Επιπλέον για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο απαιτούνται εξειδικευμένες γνώσεις, τόσο σε τεχνικό, όσο και σε νομικό επίπεδο. Η απόκτηση των γνώσεων αυτών από νομικούς, που έχουν σχέση με την έρευνα, δίωξη και εκδίκαση των σχετικών υποθέσεων, αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε πολιτείας.

Στο ποινικό πεδίο οι έννομες τάξεις έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικώς τις καταστάσεις, πιεζόμενες από τα πράγματα. Κλασσικό παράδειγμα στον τομέα της τεχνολογίας αποτελεί η εμφάνιση των εγκλημάτων που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes).

Πριν από δυο δεκαετίες περίπου η «συμβατική νομοθεσία» δεν επαρκούσε για την αντιμετώπισή τους.

Σήμερα όλες οι προηγμένες (τουλάχιστον) χώρες έχουν καταρτίσει σχετική νομοθεσία, που προσπαθούν να αντιμετωπίσουν τα εγκλήματα που διαπράττονται με τη χρήση υπολογιστών.

Στην Ελληνική έννομη τάξη ισχύει ο **Ν. 1805/1988**, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes).

Στο ίδιο σημείο με αυτό της προ δεκαπενταετίας, νομοθετικής ελλείψεως βρίσκονται σήμερα οι έννομες τάξεις, όσον αφορά το θέμα του εγκλήματος στον κυβερνοχώρο. Πολλά από τα εγκλήματα που έχουν παρουσιαστεί στο διαδίκτυο, δεν μπορούν να αντιμετωπιστούν με την συμβατική νομοθεσία, στο χώρο τουλάχιστο του ποινικού δικαίου.

Σημειώνεται ότι ελάχιστα κράτη έχουν θεσπίσει μέχρι σήμερα ειδική νομοθεσία, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο.

Στο σημείο αυτό πρέπει να τονιστεί ότι, η κατάρτιση νομοθεσίας για την καταπολέμιση της εγκληματικότητας στον κυβερνοχώρο δεν αποτελεί «εσωτερική υπόθεση» κάθε κράτους χωριστά.

Λόγω των ιδιαιτέρων χαρακτηριστικών των εγκλημάτων του κυβερνοχώρου απαιτείται κατάρτιση συμβάσεων στα πλαίσια Διεθνών οργανισμών, με ιδιαίτερη έμφαση στη Δικαστική και αστυνομική Συνεργασία.

Από μη νομικούς έχει υποστηριχθεί η άποψη ότι, δεν απαιτείται η κατάρτιση νέας νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο και ότι δεν υπάρχει νομικό κενό στο διαδίκτυο , διότι αναλογικά το «κοινό δίκαιο» μπορεί να εφαρμοστεί και στον χώρο του διαδικτύου. Η άποψη βέβαια αυτή είναι εμφανώς εσφαλμένη, καθότι στον ποινικό τουλάχιστο χώρο, δεν ισχύει η αρχή της αναλογίας.

6.6 **Διαδίκτυο και Γενικό Ποινικό Δίκαιο**

Στην Ελληνική έννομη τάξη δεν υπάρχει γενικός νόμος που να αναφέρεται αποκλειστικώς σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου.

Ο Ν**. 1805/88**, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές,δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα.

Όταν καταρτιζόταν ο νόμος αυτός το διαδίκτυο δεν είχε λάβει τις σημερινές του διαστάσεις και κατά συνέπεια δεν είχε γίνει αισθητή η ανάγκη καταρτίσεως ειδικότερης νομοθεσίας. Η διατύπωση όμως του νόμου αυτού έχει γίνει με τέτοιο τρόπο (συνδυασμός τεχνικών και νομικών εννοιών), που είναι εμφανής η επιθυμία του συντάκτη, να περιλάβει στο μέλλον και κάθε μορφή συμπεριφοράς, που θα δημιουργήσει η εξέλιξη της τεχνολογίας.

Ανεξάρτητα όμως από το εάν ο παραπάνω Ν. 1805/1988 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής ,το βέβαιον είναι ότι, δεν επαρκεί να «καλύψει» τα εγκλήματα που έχουν παρουσιαστεί από την χρήση του διαδικτύου.

Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

Προσπάθεια νομικής αντιμετώπισης του θέματος στον Ευρωπαϊκό νομικό χώρο. Η πρωτοπορία και στη νομική αντιμετώπιση το εγκλήματος στον κυβερνοχώρο ανήκει, όπως και η τεχνική, στις Η.Π.Α.

Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων Διεθνών Οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων .

Στον Ευρωπαϊκό χώρο γίνεται προσπάθεια να ρυθμιστεί το θέμα, η δε προσπάθεια αυτή βρίσκεται σε ακόμα σε εξέλιξη. Σχετικές προσπάθειες πάντως έχουν γίνει τόσο στα πλαίσια του Συμβουλίου της Ευρώπης, όσο και στα πλαίσια της Ευρωπαϊκής Ένωσης.

Το άρθρο 386Α Π.Κ και η συμβατότητά του σε σχέση με τη Σύμβαση του Συμβουλίου για το έγκλημα στον κυβερνοχώρο και της απόφασης - πλαίσιο του Συμβουλίου της Ε.Ε για τις επιθέσεις εναντίον των πληροφορικών συστημάτων

Στις 23.11.2001 ψηφίστηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Convention on Cybercrime).

Η Σύμβαση έχει τεθεί σε ισχύ, ήδη από τα τέλη 84 Φεβρουαρίου 2002, σύμφωνα με το άρθρο 36 παρ.2 αυτής, καθώς έχει υπογραφεί από τα περισσότερα μέλη του Συμβουλίου της Ευρώπης, αλλά και από τις ΗΠΑ, τον Καναδά, την Ιαπωνία και τη Νότιο Αφρική.

Στην Ελλάδα η υποστηριζόμενη ερμηνευτική θεώρηση της διάταξης του **άρθρου 386Α Π.Κ** συμβαδίζει με τα οριζόμενα στο **άρθρο 8210** της ανωτέρω Σύμβασης του Συμβουλίου της Ευρώπης.

Σύμφωνα με το άρθρο αυτό, τα Κράτη Μέρη υποχρεούνται να υιοθετήσουν μέτρα ποινικής τιμώρησης: Της πράξης της χωρίς δικαίωμα και με πρόθεση, πρόκλησης απώλειας περιουσίας σε κάποιον, η οποία συντελείται: α) με οποιαδήποτε εισαγωγή, διαγραφή ή απόκρυψη δεδομένων Η/Υ και β) με οποιαδήποτε επέμβαση στη λειτουργία ενός συστήματος Η/Υ, εφόσον συνοδεύεται από σκοπό εξαπάτησης ή αθέμιτο σκοπό πρόκλησης οικονομικού οφέλους στο δράστη ή τρίτο.

Θα πρέπει να σημειωθεί πάντως, ότι, σύμφωνα με το αρχικό σχέδιο της Σύμβασης, ήταν προαιρετική για τα Κράτη Μέρη η απαίτηση να υπάρχει σκοπός εξαπάτησης ή αθέμιτος σκοπός ως προϋπόθεση του αξιοποίνου. Το τελικό κείμενο της Σύμβασης διέπεται από την αντίληψη που διακρίνει αφενός μεταξύ εγκλημάτων .

Οι δύο αυτές κατηγορίες προσβολών διακρίνονται από εκείνες που αφορούν εγκλήματα σχετικά με το περιεχόμενο παραδοσιακών εννόμων αγαθών που απλά διευκολύνονται με τη χρήση Η/Υ (computer related offences), όπως για παράδειγμα μια εξύβριση μέσω του διαδικτύου. που τελούνται εναντίον της ακεραιότητας των συστημάτων και δεδομένων Η/Υ (computer system, compiuter data), χωρίς να απαιτείται ο σκοπός πρόκλησης οικονομικού οφέλους ή ζημίας και αφετέρου εκείνων που σχετίζονται με Η/Υ (computer related crimes).Η παραπάνω ρύθμιση της Σύμβασης δεν απαιτεί καμία ενέργεια αντίστοιχη με την παραπλάνηση της κλασικής απάτης. Θεωρεί ως κυρίαρχη ενέργεια τη, χωρίς δικαίωμα, επίδραση στο πρόγραμμα Η/Υ και την απώλεια περιουσίας, ως το αποτέλεσμα αυτής.

Μόνο το γεγονός ότι τίθεται ως προϋπόθεση ο σκοπός εξαπάτησης δεν πρέπει να μας οδηγήσει στο συμπέρασμα ότι η προτεινόμενη νέα διάταξη θα δομείται παράλληλα με την κλασική απάτη. Μάλλον το αντίθετο ακριβώς συμβαίνει. Ο σκοπός εξαπάτησης πρέπει να συνοδεύει τις ενέργειες της εισαγωγής, αλλοίωσης, διαγραφής ή απόκρυψης στοιχείων ή της οποιασδήποτε επέμβασης στη λειτουργία Η/Υ (βλ. αντίστοιχα στην ελληνική διάταξη 386Α Π.Κ « ή με οποιοδήποτε άλλο τρόπο»), ώστε να αποκλειστεί η περίπτωση της απλής δολιοφθοράς συστημάτων Η/Υ από το πεδίο του αξιοποίνου. Δεν εξυπηρετεί αντίθετα την άποψη που θέλει να εντάσσει στην απάτη με Η/Υ μόνο τις περιπτώσεις που παραλληλίζονται απόλυτα με τα παραδείγματα της κλασικής απάτης.

Σύμφωνα με το επεξηγηματικό κείμενο που συνοδεύει τη Σύμβαση γίνεται δεκτό ότι οι μεν ανωτέρω ρυθμίσεις του άρθρου 7 αφορούν σε παραδοσιακά εγκλήματα προσβολής της περιουσίας, αλλά η νέα ρύθμιση τίθεται με σκοπό να συμπεριλάβει οποιαδήποτε, χωρίς δικαίωμα, επέμβαση σε σύστημα Η/Υ, συνοδευόμενη από σκοπό πρόκλησης παράνομου περιουσιακού οφέλους. Τονίζεται μάλιστα, ότι η Σύμβαση έχει κατά νου ιδίως τις περιπτώσεις του «ηλεκτρονικού χρήματος», συμπεριλαμβάνοντας σε αυτές και τις πράξεις απάτης με πιστωτικές κάρτες.

Σύμφωνα με τους ορισμούς της Σύμβασης στο άρθρο 1 περ. β’, στην έννοια «δεδομένα υπολογιστή» εντάσσονται γεγονότα, πληροφορίες ή έννοιες, τα οποία περιέχονται σε ένα πρόγραμμα υπολογιστή που προκαλεί τη λειτουργία του υπολογιστή.

Εξάλλου, σύμφωνα με το άρθρο 1 περ. α’, ως «σύστημα υπολογιστή» θεωρείται κάθε συσκευή ή κάθε σύνολο συνδεόμενων συσκευών, τα οποία διενεργούν επεξεργασία δεδομένων μέσω ενός προγράμματος υπολογιστή.

Θα μπορούσε λοιπόν να υποστηρίξει κανείς ότι η δική μας 386ΑΠ.Κ αποτελεί τον «πρόγονο της διάταξης της Σύμβασης του Συμβουλίου της Ευρώπης.

Αν κανείς ερμηνεύσει την ισχύουσα διάταξη ανεξάρτητα από την απάτη του άρθρου 386Π.Κ, θα μπορούσε να θεωρήσει ότι το άρθρο 386ΑΠ.Κ καλύπτει τις υποχρεώσεις της Ελλάδας να συμμορφωθεί προς την ανωτέρω

Σύμβαση.218 Ακόμη πιο προωθημένες απόψεις, σχετικά με την τιμώρηση των ανωτέρω συμπεριφορών εξέφρασε η πρόταση της απόφασης –πλαίσιο του Συμβουλίου της Ευρώπης της 27.8.2002 όπως τροποποιήθηκε από τοΕυρωπαϊκό κοινοβούλιο την 4.11.2002.

6.7 **Η θέση της ελληνικής νομολογίας**

Στην ελληνική νομολογία, τόσο των δικαστηρίων της ουσίας όσο και του Άρειου Πάγου, επιχειρήθηκε σχετικά πρόσφατα ο καθορισμός των ορίων μεταξύ απάτης και απάτης με Η/Υ.

Το Εφετείο Αθηνών το 1998, δέχτηκε την ταύτιση του περιεχομένου των δύο διατάξεων, εκτός του τρόπου βλάβης της ξένης περιουσίας, η οποία στην απάτη με υπολογιστή δεν προκαλείται από εξαπάτηση φυσικού προσώπου αλλά από την «επέμβαση σε Η/Υ».

Κατά τα ανωτέρω, το Δικαστήριο θεώρησε την απάτη με Η/Υ ειδική μορφή απάτης και δέχτηκε την πραγμάτωση των όρων αυτής, ακόμη και όταν «οι αθέμιτες επεμβάσεις στον Η/Υ είναι το αναγκαίο μέσο για την πραγματοποίηση του σκοπού αυτού». Η περίπτωση που κρίθηκε από το Δικαστήριο ως απάτη με Η/Υ αφορούσε την πράξη κάποιου ο οποίος, αφού ενέγραψε στη μνήμη του Η/Υ ανύπαρκτες καταθέσεις σε υπαρκτό λογαριασμό τρίτου, εμφάνισε προς πληρωμή στον ταμία της τράπεζας επιταγή με χρέωση του ανωτέρω λογαριασμού και σε συνεννόηση με τον κάτοχο του λογαριασμού.

Ο Άρειος Πάγος το 1995 έκρινε ως απάτη με Η/Υ την περίπτωση εκείνων που καταχωρούσαν στη μνήμη Η/Υ ανύπαρκτες μισθολογικές αποδοχές από την υπηρεσία τους και στη συνέχεια εισέπρατταν τα ποσά αυτά.

Στην περίπτωση αυτή το Δικαστήριο δεν διατύπωσε κάποια ιδιαίτερη αιτιολογία για την υπαγωγή των κρινόμενων περιστατικών στην απάτη με Η/Υ ούτε και κατέστησε σαφές εάν η είσπραξη του μη δικαιούμενου ποσού έγινε με ή χωρίς την παρεμβολή ανθρώπινου παράγοντα.

Το 1998 ο Άρειος Πάγος δέχθηκε ότι η απάτη με Η/Υ είναι «διαφορετικό έγκλημα» από την απάτη που αποτελεί «ειδικό έγκλημα».

Το Δικαστήριο διαχώρισε την απάτη με Η/Υ με τη βασική σκέψη ότι «το άρθρο 386 Π.Κ περιορίζει την απάτη μόνο στις περιπτώσεις που η ξένη περιουσία βλάπτεται με την παραπλάνηση φυσικού προσώπου, ενώ στο άρθρο 386Α Π.Κ η ξένη περιουσία βλάπτεται, ασχέτως παραπλανήσεως, με την αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του υπολογιστή».

Έτσι λοιπόν, σύμφωνα με την ανωτέρω απόφαση, όποτε συνυπάρχουν στα πραγματικά περιστατικά τόσο η πράξη επέμβασης «στη μνήμη ηλεκτρονικού υπολογιστή» όσο και η παράσταση ψευδών περιστατικών σε τρίτους, τότε θα πρέπει να γίνει σαφής διάκριση εάν καταφάσκεται η απάτη με Η/Υ ή η απάτη του άρθρου 386 Π.Κ.

Κατά τα ανωτέρω, το Δικαστήριο αναίρεσε την προσβαλλόμενη απόφαση της ουσίας για το λόγο ότι δεν περιείχε σαφείς αιτιολογίες περί τη μορφή της απάτης που τέλεσε ο δράστης (άρθρο 510 στοιχ δ΄ Κ.Π.Δ) ο οποίος συνέδεσε στη μνήμη Η/Υ τον αριθμό πλαστογραφημένων επιταγών με υπαρκτό λογαριασμό όψεως και στη συνέχεια εισέπραξε χωρίς να δικαιούται χρηματικά ποσά από τον ανωτέρω λογαριασμό, εμφανίζοντας στον ταμία της τράπεζας τις σχετικές επιταγές.

Το 1999 Ο Άρειος Πάγος έκανε και πάλι αποδεκτή τη θεώρηση της απάτης με υπολογιστή ως εγκλήματος διαφορετικού από την απάτη του άρθρου 386 Π.Κ.

Τόνισε όμως ότι το έγκλημα του άρθρου 386Α Π.Κ τελείται «αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του υπολογιστή, δηλαδή με την επέμβαση του δράστη κατά τον προγραμματισμό του συστήματος και την επεξεργασία δεδομένων σε οποιαδήποτε φάση της λειτουργίας του υπολογιστή» και όχι «με την παραπλάνηση ενός φυσικού προσώπου που είναι αρμόδιο να λαμβάνει αποφάσεις ή να διενεργεί έλεγχο ή να εγκρίνει ή να χορηγεί κλπ»

«Όταν όμως, χωρίς να γίνεται επέμβαση στη διαμόρφωση του προγράμματος ή στην εφαρμογή του, χρησιμοποιείται ο υπολογιστής ως

μέσο ή όργανο με την πληκτρολόγηση αναληθών ποσών και παραπλανάται με τον τρόπο αυτό τρίτος που προβαίνει σε πράξη, παράλειψη ή ανοχή η οποία επιφέρει την περιουσιακή βλάβη, τότε στοιχειοθετείται κοινή απάτη του άρθρου 386Α Π.Κ».

Με βάση τις ανωτέρω σκέψεις ο Άρειος Πάγος αναίρεσε την απόφαση του Εφετείου Αθηνών του 1998 (ΠεντΕφΑθ 751/1998), η οποία προαναφέρθηκε, για έλλειψη αιτιολογίας (**άρθρο 510 στοιχ δ Κ.Π.Δ)** αφού δέχθηκε ότι η συνδρομή τόσο της επέμβασης στα στοιχεία υπολογιστή όσο και η παραπλάνηση φυσικού προσώπου που προβαίνει σε περιουσιακή διάθεση επιβάλλουν τον σαφή διαχωρισμό μεταξύ απάτης και απάτης με υπολογιστή.

Ενδιαφέρουσα επίσης παρουσιάζεται η εισαγγελική πρόταση προς το συμβούλιο πλημμελειοδικών Αθηνών **4742/2004168**, η οποία καίτοι δεν κατέληξε σε παραπεμπτικό βούλευμα αναφέρεται με βάση τα πραγματικά της περιστατικά στην παγίδευση μηχανήματος αυτόματης τραπεζικής ανάληψης (ΑΤΜ) τράπεζας με μηχάνημα που διάβαζε τον μυστικό αριθμό των καρτών και μηχάνημα αντιγραφής μαγνητικού πεδίου κάρτας με αποτέλεσμα να μπορεί να προβαίνει σε αναλήψεις ποσών από τους λογαριασμούς των χρηστών του συγκεκριμένου μηχανήματος.

Με βάση το σκεπτικό της παραπεμπτικής διάταξης λοιπόν ο δράστης που χρησιμοποιεί ξένη κάρτα αυτόματης συναλλαγής στα ΑΤΜ παριστά ψευδώς ότι είναι αφενός νόμιμος κάτοχος της κάρτας και αφετέρου δικαιούχος του συνδεδεμένου με αυτή λογαριασμού.

Με την ενέργεια αυτή ο δράστης επιδιώκει να παραπλανήσει την τράπεζα αφενός ως προς το εξωτερικό γεγονός της νομιμοποίησής του για πραγματοποίηση συναλλαγών με τη χρήση της κάρτας και αφετέρου ως προς το εσωτερικό γεγονός της ετοιμότητάς του να ισοφαρίσει την υλοποιούμενη ανάληψη χρημάτων με μια αντίστοιχη μείωση των απαιτήσεών του (ως δήθεν δικαιούχος του συνδεδεμένου λογαριασμού) έναντι της τράπεζας.

Η συμπεριφορά αυτή του δράστη περιέχει «πράξη εξαπάτησης», η οποία πραγματοποιείται με μια συναγόμενη παράσταση με βάση την οποία η τράπεζα θα πρέπει να δεχθεί ένα γεγονός.

Αντίστοιχη σκέψη μπορεί να γίνει και σε περίπτωση όπου επιδιώκεται η άνευ δικαιώματος πραγματοποίηση συναλλαγής σε ΑΤΜ με πλαστή κάρτα που επιχειρεί να παραπλανήσει την τράπεζα, τόσο ως προς τη γνησιότητα της κάρτας, όσο και ως προς τη νομιμοποίησή του για την πραγματοποίηση της συναλλαγής.

Αυτές οι παραστάσεις (σιωπηρώς-συμπερασματικώς συναγόμενες-ανακοινώσεις του χρήστη ΑΤΜ) Θα μπορούσαν να αντιμετωπισθούν ως πράξεις εξαπάτησης τότε μόνο, εφόσον δια της επιδράσεως τους στη συνείδηση κάποιου άλλου ανθρώπου θα μπορούσε να προκληθεί πλάνη. Η πρόκληση πλάνης όμως στο ΑΤΜ είναι αδιανόητη, το ίδιο και η διατήρησή της.

Και αυτό διότι η συσκευή δεν έχει συνείδηση δεν σχηματίζει παράσταση επί της οποίας θα μπορούσε κανείς να επενεργήσει ή να διατηρήσει καθώς τα μηχανήματα ΑΤΜ απλώς μεταθέτουν και προωθούν δεδομένα κατά τρόπο αυτοματοποιημένο σε μια επόμενη φάση της διαδικασίας επεξεργασίας αυτών, βάσει προκαθορισμένων και ενσωματωμένων στο μηχάνημα εντολών.

Οι εντολές αυτές έχουν βεβαίως δοθεί από φυσικά πρόσωπα, τα οποία όμως δεν είναι σωματικώς παρόντα κατά το χρόνο επεξεργασίας των εισαγόμενων στο μηχάνημα δεδομένων.

Για το πρόβλημα αυτό υποστηρίχθηκε μεμονωμένα στην γερμανική θεωρία ότι στο μέτρο που η τράπεζα προβαίνει σε ένα γνήσιο επιμερισμό εργασίας με τον υπολογιστή, στο μέτρο δηλαδή που «εξουσιοδοτεί» τον υπολογιστή να διεκπεραιώνει αλλεπάλληλες εργασίες κάθε φορά που πληρούνται οι εκάστοτε προαπαιτούμενες προϋποθέσεις, οποιαδήποτε εξαπάτηση του υπολογιστή συνεφέλκεται μια αναγκαία πρόκληση πλάνης στο φυσικό πρόσωπο του εξουσιοδοτούμενου με τον έλεγχο των εγγράφων υπαλλήλου.

Η άποψη όμως αυτή δεν μπορεί να γίνει δεκτή καθώς η αποδοχή του μορφώματος προκλήσεως πλάνης σε άνθρωπο διαμέσου του υπολογιστή θα είχε νόημα τότε μόνο εάν η πρόοδος της διαδικασίας ανάληψης ή από την πλευρά της τράπεζας απόδοσης των χρημάτων είχε ως αιτία την προκληθείσα διαμέσου του υπολογιστή πλάνη.

Για να γίνει όμως κάτι τέτοιο θα έπρεπε κάθε φορά που ο πελάτης ζητά την υλοποίηση μιας συναλλαγής να μεσολαβεί ένα νεκρό διάστημα έως ότου τα στοιχεία της συναλλαγής διαβιβαστούν στον αρμόδιο υπάλληλο της τράπεζας που έχει την ικανότητα σχηματισμού παράστασης ως προς αυτά (και κατά τούτο είναι πρόσφορο αντικείμενο παραπλάνησης) και ο οποίος, εγκρίνοντας την αθέμιτη συναλλαγή, προβαίνει σε μια περιουσιακή διάθεση σε βάρος της τράπεζας, ώστε να πληρούται και το τελευταίο στοιχείο της αντικειμενικής υπόστασης της απάτης.

Όμως η πλάνη του υπαλλήλου της τράπεζας που ώρες ή μέρες μετά τη διενέργεια της συναλλαγής ελέγχει το πρωτόκολλο των συναλλαγών που πραγματοποιήθηκαν μέσω του ΑΤΜ είναι σύμφωνα πάντα με την εισαγγελική διάταξη, κάθε άλλο παρά αιτιώδης της γενόμενης ήδη περιουσιακής διάθεσης και ως εκ τούτου δεν πληρούται το στοιχείο προκλήσεως της πλάνης, διότι ο υπάλληλος δεν αποκτά γνώση των αποτελεσμάτων στα οποία κατέληξε ο ηλεκτρονικός υπολογιστής, ούτως ώστε η περιουσιακή διάθεση να συνιστά προϊόν ανθρώπινης βούλησης.

Αντίθετα η συμπεριφορά του δράστη κάλλιστα μπορεί να υπαχθεί στην έννοια της απάτης με υπολογιστή.

6.8 **Διαδύκτιο και ειδικό ποινικό δίκαιο**

1. Γενικές παρατηρήσεις

Είναι γνωστό ότι για να «μπει» κάποιος στον κυβερνοχώρο (απαραίτητη πρϋπόθεση αποτελεί η χρήση του τομέα τηλεπικοινωνιών (σταθερού ή κινητού τηλεφώνου). Η χρήση αυτή επιτυγχάνεται με την σύνδεση του χρήστη με μια εταιρεία παροχής υπηρεσιών διαδικτύου σε ιδιώτες. Απαραίτητο βέβαια είναι να διαθέτει ο χρήστης τον κατάλληλο τεχνολογικό

εξοπλισμό. Κατά συνέπεια οι σχετικοί με τις τηλεπικοινωνίες νόμοι έχουν άμεση ή έμμεση σχέση με την χρήση του διαδικτύου. Με άλλα λόγια το διαδίκτυο δεν είναι τίποτα άλλο παρά μια μορφή επικοινωνίας που γίνεται με την βοήθεια ή δια μέσου των τηλεπικοινωνιών. Σύμφωνα λοιπόν με τα παραπάνω σχετικοί με το διαδίκτυο Νόμοι είναι :

α) **ο 2867/19-12-2000** για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις.

Ο πρόσφατος αυτός νόμος αντικατέστησε τον ισχύοντα Ν. 2246/20.10.1994 για την «Οργάνωση και Λειτουργία του Τομέα Τηλεπικοινωνιών», πλην των διατάξεών του που αφορούν την παροχή ταχυδρομικών υπηρεσιών (άρθρο 13 §12 Ν. 2867/2000) και των διατάξεων εκείνων που αναφέρονται στην σύσταση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (άρθρ. 3§1Ν. 2867/2000).

β) Ο **Ν.2774/22.12.99** για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με το Ν.2472 /10.4.97 «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

γ) Ο **Ν. 2225/20.7.94** για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας.

δ) ο 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις.

Ο νόμος αυτός ρυθμίζει κάθε είδους τηλεπικοινωνιακής δραστηριότητος, που αναπτύσσεται εντός της Ελληνικής Επικρατείας. Είναι γνωστός και ως νόμος «για την απελευθέρωση των τηλεπικοινωνιών», καθότι επιτρέπει την ελεύθερη εγκατάσταση, λειτουργία, διαχείριση και εκμετάλλευση των τηλεπικοινωνιακών δικτύων. Όπως και ο προηγούμενος Ν. 2246/1994, έτσι και αυτός προσδιορίζει όχι μόνον τεχνικούς, αλλά και νομικούς όρους. Έτσι ως «παροχος τηλεπικοινωνιακών υπηρεσιών» ορίζεται η τηλεπικοινωνιακή επιχείρηση που παρέχει τηλεπικοινωνιακές υπηρεσίες διαθέσιμες στο κοινό, ενώ ως «χρήστης» θεωρείται κάθε φυσικό ή νομικό πρόσωπο, που χρησιμοποιεί ή ζητά να χρησιμοποιήσει δημόσιες τηλεπικοινωνιακές υπηρεσίες.

Ο Ν. 2774/22.12.1999, ο οποίος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, αποτελεί ειδικότερη μορφή του Ν. 2472/97, και αποτελεί υλοποίηση της οδηγίας 97/66/Ε.Κ. Δηλαδή οι προηγμένες ψηφιακές τεχνολογίες στα δημόσια τηλεπικοινωνιακά δίκτυα, δημιουργούν ειδικές απαιτήσεις στη προστασία δεδομένων προσωπικού χαρακτήρα (Βλ. Εισηγ. Έκθεση Νόμου 2774/99).

Σκοπός του νόμου αυτού είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Ο ν. 2472/1997 (ΦΕΚ 50 Α/10.4.1997) προστατεύει το άτομο από την αυτοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ο νόμιμος κάτοχος των δεδομένων (ακόμα και των προσωπικών) προστατεύεται από το άρθρο 370 Β Π.Κ., όπως αυτό προστέθηκε με το άρθρο 3 ν. 1805/88. Ο Ν. 2472/1997 προστατεύει το ίδιο το άτομο από την επεξεργασία των στοιχείων αυτών .

Χαρακτηριστικό παράδειγμα εφαρμογής του Ν. 2472/97 στο διαδίκτυο αποτελεί η διασύνδεση αρχείων .

Ν. 2225/94 Για την προστασία της ελευθερίας της ανταπόκρισης

Ο νόμος αυτός έχει άμεση σχέση με τον κυβερνοχώρο αφού όπως ήδη ελέχθη το Internet δεν είναι τίποτα άλλο, παρά μια μορφή επικοινωνίας που γίνεται δια μέσου των τηλεπικοινωνιών.

Με το άρθρο 1 του Νόμου αυτού (2225/94) ιδρύεται η Εθνική Επιτροπή Προστασίας Απορρήτου των Επικοινωνιών, της οποίας αποστολή είναι (μεταξύ των άλλων) και η προστασία του απορρήτου της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης.

Ετσι με τις προϋποθέσεις 4 του Νόμου αυτού μπορεί να γίνει η παρακολούθηση (ανταλλαγής) e-mail π.χ. Ο Α εκβιάζει (άρθρ. 385 Π.Κ.) τον Β, στέλνοντας e-mail. Ο Β καταγγέλλει στην Αστυνομία. Η Αστυνομία ζητά από τον Παροχέα (ISP) να παρακολουθεί την ανταλλαγή e-mail. Ο παροχέας στην περίπτωση αυτή δεν μπορεί να επικαλεσθεί το απόρρητο των επικοινωνιών.

2.Ειδικές ποινικές διατάξεις στον χώρο του διαδικτύου.

Τιμωρείται ποινικώς,εάν διαπράττεται στον χώρο του διαδικτύου η παρακάτω συμπεριφορά:

α)Σύμφωνα με το άρθρο 11 του Ν. 2867/2000 η κατά παράβαση των άρθρων 5 (αναφέρεται στην χορήγηση γενικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) και 6 (αναφέρεται στην χορήγηση ειδικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) άσκηση τηλεπικοινωνιακών δραστηριοτήτων τιμωρείται με φυλάκιση τουλάχιστον δώδεκα (12) μηνών και με χρηματική ποινή ύψους από πέντε εκατομμύρια (5.000.000) έως πεντακόσια εκατομμύρια (500.000.000) δραχμές. Επίσης όποιος παραβαίνει με οποιονδήποτε τρόπο τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής και τήρησης του απορρήτου των κάθε είδους δεδομένων που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο (2) ετών και χρηματική ποινή πέντε εκατομμυρίων (5.000.000) έως είκοσι εκατομμυρίων (20.000.000) δραχμών. εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις.

Σε περίπτωση που ο παραβάτης της παρούσας διάταξης ανήκει στο προσωπικό τηλεπικοινωνιακής επιχείρησης, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον τριών (3) ετών και η χρηματική ποινή τουλάχιστον δέκα εκατομμύρια (10.000.000) δραχμές.

Ο τεχνικός εξοπλισμός και τα μέσα που χρησιμοποιήθηκαν για την τέλεση των παραπάνω αξιόποινων πράξεων δημεύονται.

Σε περιπτώσεις πολλαπλών ή καθ' υποτροπή παραβάσεων προβλεπόμενων στον παρόντα νόμο, όπως εκάστοτε ισχύει, ή στον Ποινικό Κώδικα, σε σχέση με τα ανωτέρω αδικήματα, επιβάλλονται αθροιστικά οι βαρύτερες ποινές.

β)Σύμφωνα επίσης με το άρθρο 13 Ν.2774/22.12.99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα,όποιος κατά παράβαση του νόμου αυτού χρησιμοποιεί, επεξεργάζεται, μεταδίδει, ανακοινώνει, δημοσιοποιεi δεδομένα προσωπικού

χαρακτήρα συνδρομητών ή χρηστών, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο τιμωρείται με φυλάκιση και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή του τουλάχιστον ενός εκατομμυρίου (1.000.000) έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις πράξεις της Αρχής που επιβάλλουν τις διοικητικές κυρώσεις των περιπτώσεων γ' (προσωρινή ανάκληση αδείας), δ' (οριστική ανάκληση αδείας) και ε' (καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων) της παρ. 1 του άρθρου 21 του ν. 2472/1997 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

Οι διατάξεις των παραγράφων 6 έως και 14 του άρθρου 22 του Ν. 2472/1977 εφαρμόζονται και επί των πράξεων των προηγουμένων παραγράφων.

γ) Σύμφωνα με το άρθρο **22 Ν 2472/1977** τιμωρείται:

1. Όποιος παραλείπει να γνωστοποιήσει στην Αρχή, κατά το άρθρο 6 τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορηγήσεως της άδειας, που προβλέπεται από την παρ. 3 του άρθρου 7 του παρόντος νόμου, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000. 000) δραχμών.

2. Όποιος κατά παράβαση του άρθρου 7 του παρόντος νόμου διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της άδειας της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

3. Οποιος κατά παράβαση του άρθρου 8 του παρόντος νόμου προβαίνει σε διασύνδεση αρχείων χωρίς να την γνωστοποιήσει στην Αρχή, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της άδειας που του έχει χορηγηΘεf, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρfου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

4.Όποιος χωρίς δικαίωμα επεμβαίνει με , οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και εάν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

5. Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις αποφάσεις της Αρχής, που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με την παρ. 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με την παρ. 2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ', δ' και ε' της παρ. 1 του άρθρου 21 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρlου (1.000.000) δραχμών έως πέντε εκατομμυρfων (5.000. 000) δραχμών.

Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9, καθώς και εκείνος που δεν συμμορφώνεται προς τη δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

6. Αν ο υπαίτιος των πράξεων των παρ.1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, ή να βλάψει τρίτον, επιβάλλεται κάθειρξη έως δέκα 10 ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

7. Αν από τις πράξεις των παρ.1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε εκατομμυρίων (5.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

3. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ).

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ) αποτελεί σημαντική Αρχή στον χώρο του διαδικτύου . Σύμφωνα με το άρθρο 3 Ν. 2867/2000 αποτελεί την Εθνική ρυθμιστική Αρχή σε θέματα τηλεπικοινωνιών. Είναι ανεξάρτητη διοικητική Αρχή με έδρα την Αθήνα και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας.

Τα μέλη της Ε.Ε.Τ.Τ. κατά την άσκηση των καθηκόντων τους απολαύουν πλήρους προσωπικής και λειτουργικής ανεξαρτησίας. Ο Πρόεδρος, οι Αντιπρόεδροι και τα υπόλοιπα μέλη της διορίζονται με απόφαση του υπουργού Μεταφορών και Επικοινωνιών μετά από προηγούμενη επιλογή τους από τη Διάσκεψη των Προέδρων της Βουλής με την αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της:

Ως μέλη της Ε.Ε:Τ.Τ. επιλέγονται πρόσωπα εγνωσμένου κύρους, που απολαύουν ευρείας κοινωνικής αποδοχής και διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στον τεχνικό, οικονομικό ή νομικό τομέα. Κατά την εκτέλεση των καθηκόντων τους, τα μέλη της Ε.Ε.Τ.Τ. δεσμεύονται από το νόμο, έχουν δε υποχρέωση τηρήσεως, των αρχών της αντικειμενικότητας και αμεροληψίας.

Ο Πρόεδρος οι Αντιπρόεδροι και τα μέλη της Ε.Ε.Τ.Τ. υποχρεούνται στην τήρηση εμπιστευτικότητας εμπορικών πληροφοριών για τέσσερα (4) έτη μετά την εκούσια ή ακούσια αποχώρηση τους από την Ε.Ε.Τ.Τ..

4. Η νομική φύση του παροχέα υπηρεσιών (ISP - Internet Service provider)

Ιδιαίτερη σημασία για την ασφάλεια και την μυστικότητα του διαδικτύου έχει η συμμετοχή του παροχέα (τηλεπικοινωνιακών) υπηρεσιών. Αποτελεί μάλιστα «κομβικό σημείο» για τον εντοπισμό των παρανομιών και την συλλογή των αποδεικτικών στοιχείων, δεδομένου ότι, όλα τα στοιχεία (data) «περνούν» από τις εγκαταστάσεις του.

Σύμφωνα με το άρθρο 1 παρ. 2 περίπτ. Δ του Ν.2246/20.10.1994 φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες από καθεστώς ελεύθερου ανταγωνισμού με βάση την άδεια ή δήλωση ή έγκριση.

Αποτελούν δηλαδή τηλεπικοινωνιακή επιχείρηση, για την λειτουργία της οποίας απαιτείται άδεια παροχής τηλεπικοινωνιακής υπηρεσίας.΄Αδεια παροχής τηλεπικοινωνιακής υπηρεσίας είναι η ατομική διοικητική πράξη, βάσει της οποίας επιτρέπεται σε ορισμένη τηλεπικοινωνιακή επιχείρηση να παρέχει ελευθέρως και σε εμπορική βάση, καθορισμένες τηλεπικοινωνιακές υπηρεσίες, καθώς και να αναλαμβάνει κάθε αναγκαία δραστηριότητα για την ίδρυση ανάπτυξη ή επέκταση, εγκατάσταση και λειτουργία των απαιτουμένων για την εν λόγω παροχή διευκολύνσεων.

Ορισμένοι παροχής υπηρεσιών είναι πολυεθνικές επιχειρήσεις, που παρέχουν πρόσβαση σε πολλές τοποθεσίες - θέσεις.

Ο παροχέας τηλεπικοινωνιακών υπηρεσιών καλείται και φορέας παροχής υπηρεσιών (service provider) ή απλώς «φορέας πρόσβασης» (access provider).

Σύμφωνα με την με αριθμό ΥΑ 74.631/18.7.1995 Υπουργική απόφαση του Υπουργού Μεταφορών, που εκδόθηκε προς υλοποίησή του Ν 2249/94 (ρυθμίζει τις προϋποθέσεις και την διαδικασία υποβολής δηλώσεως για λήψη αδείας για την άσκηση επιχειρηματικής δραστηριότητος στον τομέα των τηλεπικοινωνιών) για την λήψη της σχετικής αδείας, ο ενδιαφερόμενος

οφείλει να υπογράψει και σχετική δήλωση του Ν. 1599/86 με την οποία να βεβαιώνει ότι, έχει λάβει γνώση του Κανονισμού, του Κώδικα Δεοντολογίας και των λοιπών διατάξεων, που διέπουν την άσκηση των τηλεπικοινωνιακών δραστηριοτήτων.

Επίσης δεσμεύεται ότι, θα τηρεί τις απαιτήσεις που υπαγορεύονται από την Εθνική Αμυνα και την δημόσια ασφάλεια, ότι θα τηρεί τις διατάξεις τις σχετικές με την διασφάλιση του απορρήτου των επικοινωνιών και ότι θα αποφεύγει κάθε ενέργεια αθέμιτου ανταγωνισμού.

Ερώτημα γεννάται, για το κατά πόσο ο ίδιος ο παροχέας μπορεί να υπέχει ποινική ευθύνη, από αμέλεια ή και από (ενδεχόμενο) δόλο, για τις παρανομίες που «περνούν» από τις εγκαταστάσεις του, υποπίπτουν στην αντίληψή του και ουδέν πράττει για να σταματήσει την διάπραξή των.

Ένα δεύτερο, εξ όσου σημαντικό ερώτημα είναι, το κατά πόσο μπορεί (νομοθετικώς) να υποχρεωθεί ο παροχέας να φυλλάτει τα δεδομένα που διέρχονται από τις εγκαταστάσεις του, για ένα ορισμένο χρονικό διάστημα (π.χ. 48 ώρες), προκειμένου να τα παραδώσει στις Αρχές, σε περίπτωση που του ζητηθούν.

Κάτι τέτοιο βέβαια θα επιβαρύνει οικονομικώς τον παροχέα, δεδομένου ότι θα πρέπει, τουλάχιστον να διπλασιάσει τον τεχνικό εξοπλισμό του.

Το δίκαιο της Πνευματικής ιδιοκτησίας σε σχέση με την κοινωνία των πληροφοριών και το Internet

Την κύρια πηγή του δικαίου της πνευματικής ιδιοκτησίας στην Ελλάδα αποτελεί ο **Νόμος 2121/1993** με τίτλο Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα" όπως τροποποιήθηκε από τον Νόμο 3057/2002.

Με την έναρξη της ισχύος αυτού του νόμου όλοι σχεδόν οι προγενέστεροι νόμοι που αφορούσαν την πνευματική ιδιοκτησία καταργήθηκαν.

Στον νόμο αυτόν περιέχονται μεταξύ άλλων και διατάξεις σχετικές με τα προγράμματα ηλεκτρονικών υπολογιστών και τις βάσεις δεδομένων και φωτογραφιών. Ανάλογες διατάξεις περιλαμβάνονται και στη συνθήκη του

Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για την πνευματική ιδιοκτησία που κυρώθηκε με τον Νόμο 3184/2003.

Επίσης ισχύει και η Συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για τις εκτελέσεις και τα φωνογραφήματα, που κυρώθηκε με τον Νόμο 3183/2003. Σημαντική αρωγή στην προστασία των πνευματικών δικαιωμάτων προσφέρουν η Επιτροπή Ανταγωνισμού, που με σχετικές αποφάσεις της (π.χ. 245/ΙΙΙ.2003 σχετικά με την καταγγελία μουσικοσυνθετών κατά της ΑΕΠΙ) βοηθά στην διασφάλιση των δικαιωμάτων πνευματικής ιδιοκτησίας και οργανισμοί που ως σκοπό λειτουργίας τους έχουν τη διαχείριση πνευματικών δικαιωμάτων (ΥΑ 2170/2003).

Η Ελληνική Νομολογία ενισχύει και αυτή με τη σειρά της την μάχη κατά της παραβίασης δικαιωμάτων πνευματικής ιδιοκτησίας, αν και κυρίως εστιάζεται σε θέματα συλλογικής διαχείρισης πνευματικών δικαιωμάτων (π.χ. 687/2003 Απόφαση Μονομελούς Πρωτοδικείου Τρικάλων) και ραδιοτηλεοπτικής φύσεως διενέξεων (π.χ. 1404/2002 Απόφαση του Συμβουλίου της Επικρατείας).

Στην Ευρώπη ισχύει η Οδηγία 93/98 περί εναρμονίσεως της διάρκειας προστασίας του δικαιώματος πνευματικής ιδιοκτησίας και ορισμένων συγγενών δικαιωμάτων καθώς και η Οδηγία 2001/29 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας.

Σχετικά με την πνευματική ιδιοκτησία στην κοινωνία των πληροφοριών υπάρχουν πληθώρα αποφάσεων νομολογίας που αναφέρονται τόσο σε προϊόντα λογισμικού δηλαδή προγράμματα ηλεκτρονικών υπολογιστών όσο και σε παράνομη αναπαραγωγή και ανταλλαγή δεδομένων και αρχείων μέσω του Internet που καταπατούν δικαιώματα πνευματικής ιδιοκτησίας των δημιουργών τους.

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.

Τα δικαιώματα πνευματικής ιδιοκτησίας λοιπόν καθώς και η κατοχύρωση και προστασία τους αποτελούν απαραίτητη προϋπόθεση ανάπτυξης του πολιτισμού γενικότερα αλλά και κάθε επιχείρησης μεμονωμένα.

6.9 **Νομοθεσία για πορνογραφία**

Η Πρόεδρος της οργάνωσης Ν.Ε.Ο.Ι. κα. Ευθυμίου, με την ιδιότητα της ως Δικηγόρος και ως Εντεταλμένη Σύμβουλος σε Θέματα Νεολαίας Δήμου Θεσσαλονίκης τονίζει:

Η παιδική **πορνογραφία** ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Ο κοινός παρανομαστής είναι οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες.

Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή ή και καρτούν.

Είναι ευρέως γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις. Επιπλέον, υπάρχουν σημαντικές διαφορές στην αντιμετώπιση της παιδικής πορνογραφίας από χώρα σε χώρα.

Σε ορισμένες χώρες, όπως και στην Ελλάδα, ακόμη και η εν γνώση κατοχή παιδικής πορνογραφίας είναι έγκλημα. Ωστόσο, οι ελληνικές αρχές με δεμένα τα χέρια προσπαθούν να αντιμετωπίσουν την παιδική πορνογραφία στο διαδίκτυο, λόγω των κενών στη νομοθεσία, που εμποδίζει τη σύλληψη ή, σε πολλές περιπτώσεις, την καταδίκη των δραστών.

Σύμφωνα με το νόμο του 2002, όσοι εντοπίζονται να διακινούν παιδοφιλικό υλικό χωρίς να παίρνουν χρήματα γι' αυτό ή χωρίς η εμπορία να είναι δυνατόν να αποδειχθεί, δεν μπορούν να διωχθούν.

Χαρακτηριστική είναι η περίπτωση του 72χρονου πρώην στελέχους της αμερικανικής βάσης στο Ελληνικό, που συνελήφθη πριν από δύο χρόνια ως

μέλος διεθνούς κυκλώματος διακίνησης παιδικής πορνογραφίας στο διαδίκτυο και εγκέφαλος της δραστηριότητας στην Ελλάδα.

Το πλήθος των στοιχείων που βρέθηκαν τότε στο σπίτι του στην Κηφισιά, και τα οποία έδειχναν σεξουαλικές πράξεις σε παιδιά από δύο έως επτά ετών, δεν στάθηκαν αρκετά για την καταδίκη του.

Για την καταπολέμηση της παιδικής πορνογραφίας πρόσφατα ψηφίστηκε από τη **Βουλή** ο νέος νόμος **3625/2007**, ο οποίος περιλαμβάνει τρεις μεγάλες θεματικές ενότητες:

Την κύρωση και εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία, που ενσωματώνεται στο εσωτερικό μας Δίκαιο και προσαρτάται στη Διεθνή Σύμβαση για τα Δικαιώματα του Παιδιού, στο πλαίσιο του Οργανισμού Ηνωμένων Εθνών (άρθρα 17).

Σειρά νέων διατάξεων, οι οποίες εναρμονίζουν την Ελληνική νομοθεσία προς το περιεχόμενο του παραπάνω πρωτοκόλλου και άλλα διεθνή νομοθετήματα, για την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών και της παιδικής πορνογραφίας, σε ένα σύνολο κατηγοριών (σεξουαλικός τουρισμός, ασέλγεια μεταξύ συγγενών, παιδική πορνογραφία στο διαδίκτυο, διανομή και χρήση υλικού παιδικής πορνογραφίας μέσω συστήματος Η/Υ ή με τη χρήση Διαδικτύου, προστασία της ιδιωτικής ζωής του ανηλίκου κλπ.).

Νέες ρυθμίσεις για τα προσωπικά δεδομένα, στην περίπτωση εγκλημάτων κατά της κοινωνίας και τη λειτουργία των καμερών κατά τη διάρκεια συγκεντρώσεων, εφόσον επίκειται σοβαρός κίνδυνος για τη δημόσια ασφάλεια και μόνον κατόπιν εντολής εκπροσώπου της εισαγγελικής αρχής.

Η εφαρμογή των παραπάνω διατάξεων άρχισε από τις 24/12/2007, με τη δημοσίευση του νόμου 3625/2007 στην Εφημερίδα της Κυβερνήσεως (Τεύχος Ά, Αρ. φύλλου 290, 24/12/07). Σύμφωνα με το Άρθρο 14 του Προαιρετικού Πρωτοκόλλου, η εφαρμογή του αρχίζει ένα μήνα αργότερα, δηλαδή στις 24/01/2008.

Με τις παραπάνω ρυθμίσεις, διαμορφώνεται ένα νέο, αποτελεσματικό και ισχυρό οπλοστάσιο της Ελληνικής κοινωνίας και της νέας γενιάς απέναντι στα απειλητικά φαινόμενα της εκμετάλλευσης της εργασίας και της εμπορίας ανθρωπίνων οργάνων με θύματα παιδιά, της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της πορνογραφίας με πρωταγωνιστές παιδιά -φαινομένων που τείνουν να προσλάβουν διαστάσεις σύγχρονης μάστιγας και εμφανίζουν χαρακτηριστικά οργανωμένου εγκλήματος.

Βασικά σημεία των ρυθμίσεων του σχεδίου νόμου - μεταξύ άλλων αποτελούν:Η αναμόρφωση του αδικήματος της παιδικής πορνογραφίας ώστε να κολάζεται ο δράστης και όταν ο σκοπός του δεν είναι η αποκόμιση κέρδους, σκοπός που παραμένει ως ιδιαίτερα επιβαρυντική περίσταση. Συγχρόνως προσδιορίζεται ως τιμωρητέο υλικό παιδικής πορνογραφίας η αναπαράσταση, ή πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο φορέα: α) του σώματος ή μέρος του σώματος ανηλίκου με τρόπο που προδήλως προκαλεί γενετήσια διέγερση, β) πραγματικής ή εικονικής ασελγούς πράξης.

- Ο αυτεπάγγελτος διορισμός συνηγόρου σε ανήλικα θύματα.
- Η σύμπραξη κατά την ανάκριση παιδοψυχολόγου ή παιδοψυχιάτρου, που λειτουργεί με εχέγγυα πραγματογνώμονα.
- Η καταχώριση της κατάθεσης ανηλίκου θύματος σε ηλεκτρονικό μέσο.
- Η αποφυγή εμφάνισης του ανηλίκου θύματος σε ακροατήριο.
- Η ψυχοδιαγνωστική εξέταση και θεραπεία ανηλίκου θύματος και του δράστη των συγκεκριμένων εγκλημάτων.
- Η απαγόρευση δημοσίευσης περιστατικών, που μπορεί να οδηγήσουν στην εξακρίβωση της ταυτότητας του ανηλίκου θύματος με την απειλή ανάλογων ποινικών κυρώσεων.
- Η αναστολή της παραγραφής καθ’ όλη τη διάρκεια της ανηλικότητας και μετά την ενηλικίωση του θύματος επί τρία έτη για τα κακουργήματα και επί ένα έτος για τα πλημμελήματα.

- Η εφαρμογή των ελληνικών ποινικών νόμων για τα εγκλήματα παιδικής πορνογραφίας και της διενέργειας ταξιδιών για την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου, που διαπράττονται από ημεδαπούς ή αλλοδαπούς -φαινόμενο γνωστό και διαδεδομένο ευρύτατα ως ‘σεξουαλικός τουρισμός’.
- Η καθιέρωση ευθύνης νομικών προσώπων με βαρύτατες διοικητικές κυρώσεις.
- Η σύντομη εκδίκαση υποθέσεων σε όλους τους βαθμούς δικαιοδοσίας για τις συγκεκριμένες πράξεις που δεν μπορεί να υπερβεί τη διετία από την τέλεση ή διαπίστωσή τους.

Σε ότι αφορά τα όρια προστασίας των προσωπικών δεδομένων, ο νέος νόμος επιτρέπει τη δημοσίευσή τους, μετά από άδεια των εισαγγελικών ή δικαστικών αρχών, από τη φάση της προανάκρισης έως εκείνη της δίκης για τις εξής περιπτώσεις, σύμφωνα με το άρθρο όγδοο, του νέου νόμου:

1. Η παράγραφος 2 του άρθρου 3 του ν.2472/1997 (ΦΕΚ 50Α) αντικαθίσταται ως εξής:

2. Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων η οποία πραγματοποιείται:

α) από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών,

β) από τις δικαστικές-εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων.

Αποτελεί αδιαμφισβήτητο γεγονός ότι ανεξέλεγκτες διαστάσεις έχει λάβει διεθνώς τα τελευταία χρόνια το φαινόμενο διακίνησης παιδικής

πορνογραφίας μέσω Διαδικτύου. Οι εξηγήσεις που δίνουν οι ειδικοί για τη ραγδαία εξάπλωση του φαινομένου είναι ψυχολογικές και κοινωνικές.

Ωστόσο, η παιδική πορνογραφία έχει και μια διόλου ευκαταφρόνητη οικονομική διάσταση.

Ο τζίρος για τους διεστραμμένους οι οποίοι εμπορεύονται παιδικά σώματα αγγίζει πολλές φορές και τα 3 δισ. ευρώ ανά έτος. Κερδισμένοι είναι όλοι όσοι εμπλέκονται σε αυτή την αρρωστημένη συναλλαγή, εκτός φυσικά από τα παιδιά, οι ψυχές των οποίων μένουν για πάντα σημαδεμένες από τη βαρβαρότητα των εκμεταλλευτών τους. Λύση για να γλιτώσουν οι γονείς τα παιδιά τους από τέτοιο θέαμα στο Internet δεν είναι μόνο η διαρκής αστυνόμευση. Οι ειδικοί κρούουν τον κώδωνα του κινδύνου στους γονείς και τους συμβουλεύουν να ελέγχουν οι ίδιοι τις ιστοσελίδες που επισκέπτονται τα παιδιά τους.

Στην Ελλάδα το φαινόμενο της παιδικής πορνογραφίας παρουσιάζει έξαρση και οι αξιωματικοί Δίωξης Ηλεκτρονικού Εγκλήματος ανακαλύπτουν ολοένα και πιο σκληρό υλικό στους υπολογιστές των δραστών.

6.10 Η πρόοδος των Βαλκανίων σε νομοθετικό επίπεδο

Συνοπτική παρουσίαση της προόδου των Βαλκανικών χωρών σε σχέση με τις υποχρεώσεις που έχουν αναλάβει για την υλοποίηση της eSEE Agenda (Stability Pact) έως τον Φεβρουάριο του 2006:

Νομοθεσία για την Προστασία των Προσωπικών

Δεδομένων

Εκπλήρωση υποχρεώσεων

χωρών NAE (eSEE Agenda)

Νομοθεσία για την Προστασία των Προσωπικών Δεδομένων

Αλβανία

Μερική ρύθμιση μέσω του Τηλεπικοινωνιακού Νόμου κ.α. Δεν υπάρχει ξεχωριστή νομοθεσία.

Βοσνία και Ερζεγοβίνη

Υιοθετήθηκε το 2001. Νέος Νόμος κατατέθηκε προς έγκριση. Αρχή Προστασίας Π.Δ. ιδρύθηκε και λειτουργεί.

Κροατία

Υιοθετήθηκε τον Ιούνιο του 2003. Αρχή Προστασίας Π.Δ. ιδρύθηκε το 2004 και λειτουργεί πλήρως. Προετοιμασία Κεντρικού συστήματος καταγραφής Προσωπικών Δεδομένων.

ΠΓΔΜ

Αρχικός Νόμος από το 1984 και τροποποίηση αυτού τον Ιανουάριο του 2002. Η συνθήκη του Συμβουλίου επικυρώθηκε στις 24 Ιανουαρίου 2005. Νέος Νόμος εν ισχύ από τις 26 Ιανουαρίου 2005.

Μολδαβία

Σχέδιο Νόμου για την Προστασία των Π.Δ. έχει κατατεθεί στη Βουλή.

Μαυροβούνιο

Νομοθεσία σε ομοσπονδιακό επίπεδο. Το αρμόδιο Υπουργείο του Μαυροβουνίου έχει προτείνει σχέδια Νόμου για το Μαυροβούνιο και σχετικές τροποποιήσεις του Ποινικού Κώδικα.

Νόμος για την προστασία της πνευματικής Ιδιοκτησίας υιοθετήθηκε τον Ιούλιο του 2005.

Σερβία

Ομοσπονδιακός Νόμος από το 1998. Δεν εφαρμόζεται σε επίπεδο Σερβικής Ομοσπονδιακής Δημοκρατίας. Τον Φεβρουάριο του 2005 ξεκίνησε η προετοιμασία του νέου νόμου.

Κόσοβο

Υιοθετήθηκε τον Ιούλιο του 2005.

Χώρες

Η νομική αντιμετώπιση σε Ελλάδα και Ευρωπαϊκή Ένωση

Όπως προείπαμε έχουν γίνει πολλές και ποικίλης αποτελεσματικότητας προσπάθειες από τα περισσότερα κράτη, ώστε να ρυθμισθεί το ζήτημα αυτό.

Στην Ελλάδα τα ποινικά ζητήματα όσον αφορά στη χρήση υπολογιστών και διαδικτύου αντιμετωπίστηκαν κυρίως από το νόμο 1805/1988, ο οποίος βασισμένος σε γερμανικά πρότυπα θέσπισε σημαντικές διατάξεις όπως το άρθρο 370Β και 370Γ ΠΚ που αφορούν τη παράνομη αντιγραφή και παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών καθώς και το 386Α που έχει ως αντικείμενο την απάτη με υπολογιστή αλλά και δευτερευόντως από το άρθρο 4 του νόμου 2246/1994.

Αναλυτικότερα: Ο νόμος 1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes), δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα.

Μολονότι ο νόμος είναι σχεδόν 20 ετών, γεγονός, που ειδικά όσον αφορά στο συγκεκριμένο τομέα φαινεται ανησυχητικά παλαιός, αναλογιζόμενοι τους ραγδαίους ρυθμούς με τους οποίους εξελίσσεται το διαδίκτυο και οι σχετικές δραστηριότητες, είναι γραμμένος με μία μελλοντική προοπτική, ώστε να εμφανίσει μία προσαρμοστικότητα και στα νέα δεδομένα που τυχόν θα παρουσιάζονταν.

Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον διαδικτύου, τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

Το άρθρο 370Β προστατεύει όπως αναφέρθηκε την προστασία του απορρήτου από τις εισβολές και των hackers.Όπως αναφέρεται στο άρθρο αυτό: Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών.

Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Το άρθρο 370Γ§2 Π.Κ προβλέπει ότι: Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29) ΕΥΡΩ [10.000 δρχ.].Το άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και προστέθηκε με το άρθρο 4 Ν. 1805/1988.

Αυτό σημαίνει ότι, η θέσπιση του συγκεκριμένου άρθρου δεν αποβλέπει στην προστασία της ασφάλειας στον κυβερνοχώρο, αλλά στην προστασία του απορρήτου.

Δεν είναι λοιπόν υπερβολικό να λεχθεί ότι, η ύπαρξη της εννοίας του hacker στην ελληνική νομοθεσία αποτελεί ένα τυχαίο γεγονός, που οφείλεται στην ευρεία διατύπωση του άρθρου 370 Γ §2 Π.Κ. Η Ελληνική νομοθεσία επίσης δεν προσδιορίζει τις έννοιες των διαφόρων κατηγοριών hackers όπως είναι οι cracker, whacker κλπ.

Ανεξάρτητα του θεωρητικού ορισμού περί hacker που δώσαμε προηγουμένως θα πρέπει να σημειωθει οτι ο νομικός ορισμός βασει του άρθρου 370 Γ Π.Κ. διαφέρει, καθώς ως hacker μπορεί να οριστεί το άτομο εκείνο, το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

Το άρθρο αυτό εφαρμόζεται μόνο στις περιπτώσεις που έχουμε απλά εισβολή του hacker σε ένα σύστημα υπολογιστών χωρίς εξουσιοδότηση χώρις να έπεται κάποια άλλη ενέργεια ή βλάβη.Εάν έχουμε και προσβολή άλλων εννόμων αγαθών εφαρμόζονται και οι αντίστοιχες σχετικές διατάξεις.

Οι προυποθέσεις για την εφαρμογή του άρθρου 370 Γ §2 Π.Κ. είναι:

α) πρόσβαση σε στοιχεία.

Ως πρόσβαση θεωρείται κάθε διείσδυση του δράστη, που αποβέπει να λάβει γνώση των στοιχείων. Αντικείμενο της πρόσβασης είναι στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

β) η πρόσβαση αυτή να πραγματοποιείται χωρίς εξουσιοδότηση ή χωρίς κάποιο δικαίωμα.

Σε περίπτωση που υφίσταται συγκατάθεση δεν πληρούται η αντικειμενική υπόσταση του άρθρου 370 Γ §2 Π.Κ. και συνεπώς δεν εφαρμόζεται. Σε περίπτωση που ο δράστης είναι στην υπηρεσία του νομίμου κατόχου των στοιχείων, τότε τεκμαίρεται οτι αυτός έχει το δικαίωμα νόμιμης πρόσβασης στα στοιχεία. Αυτό συνάγεται από την §3 του ίδιου άρθρου 370 Γ Π.Κ., σύμφωνα με την οποία η πράξη της §2 τιμωρείται, μόνον αν απαγορεύεται ρητά από εσωτερικό κανονισμού ή από εγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

Η έλλειψη δικαιώματος πρόσβασης τεκμαίρεται ιδίως όταν γίνεται με παραβίαση οποιασδήποτε παραμέτρου ασφαλείας που να υποδεικνύει οτι ο νόμιμος χρήστης δεν επιθυμεί την παρέμβαση από ξενους πράγοντες στο σύστημά του.Μέθοδοι εξασφάλισης τέτοιας μορφής είναι τα συνθηματικά και οι κωδικοί αριθμοί χρήστη ή τα τείχη προστασίας(firewall) για παράδειγμα.

Η διατύπωση του άρθρου 370 Γ§2 Π.Κ. είναι «αρκούντως ευρεία», ώστε να περιλαμβάνει κάθε πρόσβαση σε δεδομένα και αρχεία. Στην ευρεία αυτή διατύπωση του, οφείλεται και το γεγονός ότι, μπορεί να υπαχθούν στο άρθρο αυτό οι hackers και τα σχετικά περιστατικά hacking. Αλλωστε, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα.

Το έγκλημα του άρθρου 370 Γ§2 Π.Κ. είναι έγκλημα διακινδύνευσης και όχι έγκλημα βλάβης. Όσον αφορά στο νόμο 2246/1994 άρθρο 4 αυτός

αναφέρεται συμπληρωματικά σε παραβάσεις σχετικές με την άσκηση τηλεπικοινωνιακών δραστηριοτήτων.Όπως αναφέρει και το ίδιο το άρθρο:

Στη διάταξη αυτή υπάγονται όλες οι περιπτώσεις παράνομης λειτουργίας ραδιοηλεκτρικών συστημάτων μετάδοσης μηνυμάτων και δεδομένων.

Οποιος με οποιονδήποτε τρόπο παραβαίνει τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής, τήρησης του απορρήτου και διαφύλαξης της πνευματικής ιδιοκτησίας του περιεχομένου των μηνυμάτων και δεδομένων, που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων, που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματικές ποινές.

Υφίστανται και άλλες παράμετροι όπως δήμευση του χρησιμοποιηθέντος εξοπλισμού καθώς και διατάξεις που κυρίως αφορούν στην παροχή υπηρεσιών χωρίς τις νόμιμες προυποθέσεις που αφορούν κυρίως θέματα παροχέα διαδικτυακών υπηρεσιών.

Επίσης το ζήτημα έχει εξεταστεί και από την Ευρωπαϊκή Ένωση.Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα:

α)Η Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer related crime

β)Η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology).

Η σπουδαιότητα της σύστασης αυτής είναι πολύ μεγάλη, διότι καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο, οι γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων.

Στη συνέχεια καταρτίσθηκε Διεθνής Σύμβαση (N. 185, Βουδαπέστη, 23.11.2001)για την αντιμετώπιση του διαδικτυακού εγκλήματος. Στην κατάρτιση της Σύμβαση αυτής έλαβε μέρος και η Ελλάδα.

Σκοπός της Σύμβασης είναι η αποτελεσματική προστασία της κοινωνίας από το έγκλημα στον κυβερνοχώρο θεσπίζοντας νομοθεσία, η οποία να

ανταποκρίνεται στις ιδιαιτερότητες και αυξημένες απαιτήσεις του συγκεκριμένου κλάδου αλλά παράλληλα,όπως κατέδειξε και η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology), με μία διάθεση για ενιαίο και εναρμονισμένο ρυθμιστικό πλαίσιο, τουλάχιστον στις περισσότερες χώρες.

Η συζήτηση της Σύμβασης άρχισε τον Απρίλιο του 1997 με αρχικό χρονοδιάγραμμα περάτωσης το τέλος του έτους 1999. Λόγω όμως των ιδιαιτέρων προβλημάτων (η εξέλιξη της τεχνολογίας και η παρουσία νέων μορφών συμπεριφορών που θα μπορούσαν να θεωρηθούν ως αξιόποινες έτρεχαν ταχύτερα από τις εργασίες της Σύμβασης), η προθεσμία περάτωσης παρατάθηκε μέχρι το τέλος του έτους 2000.

Η Σύμβαση περατώθηκε και έχει ήδη υπογραφεί από αρκετά κράτη. Η ανάλυση των επιμέρους παραμέτρων της σύμβασης αυτής απαιτεί ιδιαίτερη μνεία, η οποία θα υπερέβαινε τα όρια της συγκεκριμένης εργασίας.

Παρόλο όμως που υπάρχει ένα νομικό πλαίσιο το οποίο δείχνει να συντονίζει σιγά αλλά σταθερά τις προσπάθειες δίωξης των hackers είναι γεγονός οτι η εφαρμογή των νόμων και η καταστολή των hacking περιστατικών συναντά αρκετά προβλήματα για λόγους που θα αναλύσουμε στο ακόλουθο κεφάλαιο.

7 ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΑΠΟ ΤΙΣ ΔΙΩΚΤΙΚΕΣ ΑΡΧΕΣ

Ο «παραδοσιακός» τρόπος προσεγγίσεως του εγκλήματος , δηλ. της περιγραφής του δράστη με την κατάθεση του θύματος , της συλλογής πληροφοριών από πληροφοριοδότες της διεξαγωγής έρευνας, κατάσχεσης κλπ. δεν ισχύει στον κυβερνοχώρο.

Ο «ηλεκτρονικός δράστης» ή «ηλεκτρονικός εγκληματίας» δεν θα πάρει το όπλο, ούτε θα φορέσει τα γάντια και θα εισέλθει στη Τράπεζα για να τη ληστέψει ή σ΄ ένα σπίτι για να κλέψει.

Αντίθετα με τους κατάλληλους κωδικούς αριθμούς, που κατά κανόνα παράνομα έχει αποκτήσει (πάλι διαπράττοντας ένα ηλεκτρονικό έγκλημα) θα δώσει εντολή για μεταφορά ενός χρηματικού ποσού από τον λογαριασμό του «ηλεκτρονικού θύματος» σ΄ ένα άλλο στο εξωτερικό .

Και όταν το θύμα πάρει είδηση την εναντίον του ενέργεια ο δράστης ή θα έχει μεταφέρει τα χρήματα σε διάφορους άλλους λογαριασμούς για να χαθούν τα ίχνη του , ή θα τα έχει «σηκώσει» και θα έχει εξαφανισθεί .

Στο μέλλον οι κλέφτες δεν θα κυκλοφορούν με την κουκούλα και το περίστροφο στο χέρι, ούτε θα τους περιμένει ο συνεργός τους με την μηχανή αναμμένη για να διαφύγουν. Οι μελλοντικοί κλέφτες θα είναι σκυμμένοι πάνω σ΄ ένα πληκτρολόγιο, μέσω του οποίου θα δίνουν εντολές σε μικρούς , αλλά πανίσχυρους ηλεκτρονικούς υπολογιστές και οι κλοπές τους θα απαιτούν από τους Αστυνομικούς, όλο και πιο εξειδικευμένες γνώσεις .

Αλλά και στην περίπτωση εκείνη που ο παθών αντιλαμβάνεται εγκαίρως ότι έπεσε θύμα ηλεκτρονικού εγκλήματος, ερωτάται:

Σε ποια Αρχή θα καταγγείλει το έγκλημα αυτό; Έχει η Αρχή αυτή τις απαιτούμενες γνώσεις να ερευνήσει την αξιόποινη πράξη που της καταγγέλθηκε;

7.1 Αρμόδιες υπηρεσίες για την έρευνα του εγκλήματος στον κυβερνοχώρο

Στα λεγόμενα τεχνολογικώς αναπτυγμένα κράτη, όπου το έγκλημα στον κυβερνοχώρο «ανθεί», έχουν συσταθεί ειδικές υπηρεσίες για την έρευνα και καταπολέμηση του νέου αυτού εγκλήματος. Ενδεικτικώς αναφέρεται ότι στις Η.Π.Α. το F.B.I. έχει συστήσει το **National Infrastructure Protection Center (NIPC)**, με παραρτήματα σε διάφορες πολιτείες για την έρευνα των σχετικών εγκλημάτων.

Στα πλαίσια μάλιστα της «Ηλεκτρονικής Αστυνομίας» έχει συσταθεί ειδική μονάδα, που έχει ως αντικείμενο το «σπάσιμο» των κωδικών των ηλεκτρονικών επιστολών (e-mails), που χρησιμοποιούν οι έμποροι ναρκωτικών και τα δίκτυα παιδεραστίας.

Ομοίως έχει συσταθεί ειδικό σώμα Εισαγγελέων, οι οποίοι ύστερα από κατάλληλη εκπαίδευση, ασχολούνται με το έγκλημα στον κυβερνοχώρο . Παρόμοια εκπαίδευση έχει γίνει και στους Δικαστές.

Στην Scotland Yard έχει συσταθεί το Computer Fraud Squad.

Στον Καναδά έχει συσταθεί το the Royal Canadian Mounted Police Computer Crime Unit.

Δεκάδες συναντήσεις, συνέδρια κλπ γίνονται κάθε χρόνο από τις παραπάνω υπηρεσίες για θέματα σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Επίσης έχουν εκδοθεί δεκάδες γραπτές οδηγίες (guide lines) και Κώδικες Πρακτικής (Code of Practice), που απευθύνονται στους δημόσιους εκείνους λειτουργούς, οι οποίοι είναι επιφορτισμένοι με την έρευνα και την καταπολέμηση των σχετικών εγκλημάτων.

Ενδεικτικώς αναφέρεται ο Κώδικας Πρακτικής του Τμήματος Εμπορίου και Βιομηχανίας (DTI) της Βρετανίας (The British Code of Practice - Department of Industry).

7.2 **Γενικά για τις έρευνες που έχουν σχέση με το έγκλημα στον κυβερνοχώρο**

Οι δικαστικές-Αστυνομικές έρευνες που γίνονται προς διακρίβωση εγκλημάτων του κυβερνοχώρου, ουδεμία σχέση έχει με τις έρευνες , που μέχρι τώρα γνωρίζουμε. Στις μέχρι τώρα «παραδοσιακές» έρευνες ο ερευνών έψαχνε σε συγκεκριμένο χώρο π.χ. δωμάτια, συρτάρια κλπ. για να εντοπίσει το αναζητούμενο αντικείμενο. Σήμερα έχει να ψάξει files , note pads , botes, dada, κρυπτογραφημένα στοιχεία κλπ. Μπορεί το προς έρευνα αντικείμενο να βρίσκεται μπροστά στα μάτια του ερευνητή και να μην μπορεί να το εντοπίσει , εάν δεν έχει τις απαραίτητες τεχνικές γνώσεις.

Ερωτάται λοιπόν, πως θα διεξαχθεί σε μια τέτοια περίπτωση η αστυνομική έρευνα ; Ο «παραδοσιακός Εισαγγελέας» και η «παραδοσιακή αστυνομία» δεν επαρκούν πλέον για την εξιχνίαση των σχετικών εγκλημάτων.

Ενα άλλο πρόβλημα είναι ότι στην κοινή έρευνα το αντικείμενο βρίσκεται σ΄ ένα σημείο .

Αντίθετα στο έγκλημα του κυβερνοχώρου το αντικείμενο μπορεί να βρίσκεται σε πολλούς υπολογιστές οι οποίοι μάλιστα μπορεί να βρίσκονται σε διάφορες χώρες. Το πρόβλημα του τόπου τελέσεως είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζεται κατά την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, δεδομένου ότι, η ίδια αξιόποινη πράξη μπορεί να διαπράττεται ταυτόχρονα σε εκατοντάδες ή και χιλιάδες τόπους τελέσεως.

Γενικώς ο αριθμός των τόπων τελέσεως εξαρτάται από την συγκεκριμένη λειτουργία του διαδικτύου (αποστολή e-mails, new groups, internet relay chat, κλπ). Ακόμα και σε δορυφόρους (Satellite-technology) είναι δυνατό να βρίσκονται τα αποδεικτικά στοιχεία , δεδομένου ότι , οι επικοινωνίες (κινητά τηλέφωνα κλπ.) γίνονται πλέον δορυφορικώς.

Σε κάθε περίπτωση όμως δημιουργείται πρόβλημα όχι μόνο σε θέματα Δικαστικής και Αστυνομικής συνεργασίας, αλλά και σε θέματα κατά τόπον αρμοδιότητος ως προς την εκδίκαση της πράξεως. Η έννοια επίσης των γεωγραφικών συνόρων είναι άγνωστη στα εγκλήματα του κυβερνοχώρου.

Ειδικότερα, όταν οι υπολογιστές (computers) είναι συνδεδεμένοι μεταξύ των ολόκληρος ο πλανήτης αποτελεί «μία χώρα».

Κατά συνέπεια οι μέχρι τώρα Διεθνείς Συμβάσεις περί αμοιβαίας Δικαστικής Συνδρομής και Συνεργασίας, είναι «παραχωρημένες» στο πεδίο του εγκλήματος στον κυβερνοχώρο. Η Δικαστική συνεργασία στα συγκεκριμένα θέματα του κυβερνοχώρου, για να είναι αποτελεσματική, πρέπει να είναι ταχύτατη.

7.3 **Η Ελληνική Αστυνομική Πραγματικότητα**

Στην Ελληνική Αστυνομία δεν υπάρχει ακόμα ειδικό Τμήμα, που να ερευνά αποκλειστικώς το έγκλημα στον κυβερνοχώρο. Το ερευνούμενο έγκλημα εξετάζεται από το αντίστοιχο «συμβατικό» τμήμα της Αστυνομίας. Έτσι η παιδική πορνογραφία ερευνάται από το τμήμα Ανηλίκων, ενώ μια ανθρωποκτονία θα ερευνηθεί από το Τμήμα ανθρωποκτονιών.

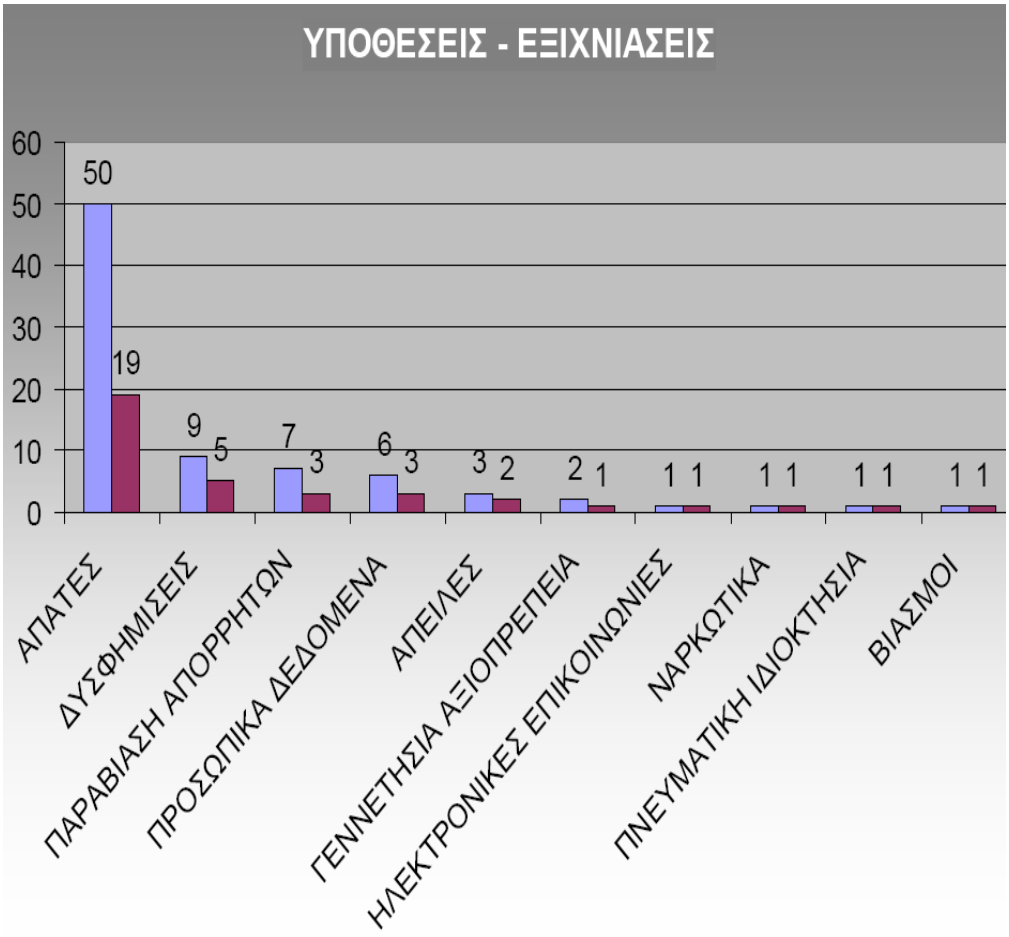
Επειδή κατά κανόνα τα περισσότερα εγκλήματα του κυβερνοχώρου έχουν οικονομικό αντικείμενο,το Τμήμα Οικονομικού Εγκλήματος, θεωρείται πιο εξειδικευμένο στο σχετικό αντικείμενο. Εχει μάλιστα συσταθεί ειδική ομάδα αντιμετωπίσεως του Ηλεκτρονικού Οικονομικού Εγκλήματος, το οποίο στελεχώνεται από εκπαιδευμένους στο ηλεκτρονικό έγκλημα α στυνομικούς.

Σε κάθε περίπτωση όμως την σχετική έρευνα συνδράμει με τις ειδικές της γνώσεις η Διεύθυνση Εγκληματολογικών Ερευνών (Δ.Ε.Ε.) και ειδικότερα το εργαστήριο γραφολογίας, στο οποίο υπάγεται και λειτουργεί ο Τομέας Ανάλυσης Ψηφιακών δεδομένων.

Ο Τομέας αυτός δημιουργήθηκε το 1992, στελεχώνεται δε από ειδικά εκπαιδευμένους αστυνομικούς, με τεχνογνωσία στην εξέταση λογισμικού κατασχεθέντων ηλεκτρονικών υπολογιστών, στο σπάσιμο κωδίκων κλπ Επίσης στο Υπουργείο Δημοσίας Τάξεως λειτουργεί η Διεύθυνση

Πληροφορικής, η οποία όμως δεν έχει σχέση με την έρευνα των εγκλημάτων του κυβερνοχώρου.

Η Διεύθυνση αυτή υπάγεται στον κλάδο Διοικητικής Υποστήριξης του Υ.Δ.Τ. και έχει ως αρμοδιότητα την ανάπτυξη και την τεχνική υποστήριξη στον τομέα της πληροφορικής, για όλες τις υπηρεσίες της Αστυνομίας .



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%

7.4 **Συλλογή και διατήρηση των αποδεικτικών στοιχείων**

Η ανακριτική τεχνική, όπως είναι η συλλογή των αποδεικτικών στοιχείων, η λήψη των μαρτυρικών καταθέσεων, η διενέργεια των ερευνών κλπ, απαιτεί διαφορετική τεχνική από εκείνη των «κοινών» εγκλημάτων . Κύριο χαρακτηριστικό της συλλογής και εκτίμησης των αποδεικτικών στοιχείων είναι ότι, οι νομικές γνώσεις του (προ) ανακριτικού υπαλλήλου δεν επαρκούν για την έρευνα της υποθέσεως.

Οι κατάλληλες και επαρκείς ειδικές τεχνικές γνώσεις είναι εξ ίσου σημαντικές -αν όχι και σημαντικότερες- από τις νομικές.

Π.χ. η εσφαλμένη αποσύνδεση των καλωδίων του ηλεκτρονικού υπολογιστή, στον οποίο είναι «αποθηκευμένα» τα αποδεικτικά στοιχεία. μπορεί να οδηγήσει στην εξαφάνισή («χάσιμο») των .

Η παρατηρητικότητα επίσης του (προ)ανακριτικού υπαλλήλου είναι σημαντική, π.χ. ο συνδυασμός αριθμών, που μπορεί μεν να εμφανίζονται

(εξωτερικώς) ως αριθμοί τηλεφώνων, ενδεχομένως να αποτελούν τα «κλειδιά» (passwords) πρόσβασης στο σύστημα ή ακόμα και τους κωδικούς αποκρυπτογράφησης, σε περίπτωση που τα στοιχεία (data) τηρούνται κρυπτογραφημένα.

Μετά την συλλογή των αποδεικτικών στοιχείων σημαντική είναι η γνώση του προανακριτικού υπαλλήλου για την διατήρησή των. Η έκθεσή των π.χ. σε ήλιο, υγρασία, σκόνη κλπ, ενδεχομένως να οδηγήσει στην καταστροφή των.

7.5 **Ηλεκτρονική απόδειξη**

Η λεγομένη ηλεκτρονική απόδειξη δεν ταυτίζεται με τα «παραδοσιακά» αποδεικτικά μέσα. Τα τελευταία αυτά είναι «χειροπιαστά», έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα τα ηλεκτρονικά αποδεικτικά μέσα είναι κατά κανόνα «μη χειροπιαστά» μπορεί να τα κατευθύνει ή και να τα διαχειρίζεται κάποιος από μακριά, να αλλάζει την μορφή και το περιεχόμενό των ή ακόμα και να τα εξαφανίζει με το πάτημα ενός πλήκτρου.

Παράδειγμα: ο εγκληματίας Α αποστέλλει με το ηλεκτρονικό ταχυδρομείο (e-mail) κρυπτογραφημένη επιστολή από την χώρα Χ, στον επίσης εγκληματία Β, ο οποίος διαμένει στην χώρα Ψ, αναφέροντάς του λεπτομέρειες σχετικά με την ελεγχομένη παράδοση (άρθρο 9 Ν. 1990/91) μεγάλης ποσότητος ναρκωτικών ουσιών .

Η Αστυνομική Αρχή της χώρας που παρακολουθεί την περίπτωση διαπιστώνει ότι ο Β, δεν παραλαμβάνει αμέσως το γράμμα (e-mail), γιατί κατά την ώρα αποστολής - λήψεως έχει κλειστό τον ηλεκτρονικό υπολογιστή του.

Ερωτάται:

Σε ποιες νόμιμες ενέργειες μπορεί να προβεί η Αστυνομία προκειμένου να αποκτήσει και στη συνέχεια να χρησιμοποιήσει το «κλειδί» του κρυπτογραφημένου μηνύματος;

Θεωρείται το «e-mail» επιστολή τηλεγράφημα ή τηλεομοιοτυπικό έγγραφο (fax) ; Σε περίπτωση που αυτό (e-mail) θεωρείται ως επιστολή, πρέπει να εφαρμοστούν οι σχετικές διατάξεις περί ανοικτών επιστολών (Συνταγματική προστασία κλπ.) ή περί κλειστών επιστολών (ευκολότερη κατάσχεση κλπ.) Δικαιούται η Αστυνομία να κατάσχει το «γράμμα» (e-mail) στις εγκαταστάσεις του παροχέα; Σε θετική περίπτωση δικαιούται να ανοίξει το e-mail και να το διαβάσει; Οταν το e-mail βρίσκεται στις εγκαταστάσεις του παροχέα; αποτελεί κλειστή ή ανοικτή επιστολή;

Μπορεί η Αστυνομική Αρχή να υποχρεώσει τον παροχέα να της παραδώσει όλη την ηλεκτρονική αλληλογραφία μεταξύ Α και Β;

Μπορεί να υποχρεωθεί ο παροχέας να φυλάττει για ορισμένο χρονικό διάστημα (και για πόσο) τα «στοιχεία – δεδομένα» που «περνούν» από τις εγκαταστάσεις του; Και μόνο το παραπάνω απλό (για το διαδίκτυο) παράδειγμα αρκεί για να δώσει το μέγεθος των σημαντικών προβλημάτων που αντιμετωπίζει, αυτός που ασχολείται με την έρευνα του εγκλήματος στο διαδίκτυο.

7.6 **Συνεργασίες στον ελληνικό και διεθνή χώρο**

International Cybercrime Convention – Διεθνής

Συνθήκη για το Ηλεκτρονικό Έγκλημα

• Η Διεθνής Συνθήκη για το Ηλεκτρονικό έγκλημα προβλέπει την ποινικοποίηση πράξεων όπως hacking, η παραγωγή, πώληση και διανομή προγραμμάτων hacking, παιδικής πορνογραφίας, και θέματα πνευματικών δικαιωμάτων

• Προβλέπει επίσης την παραχώρηση σχετικών εξουσιών για την έρευνα και σύλληψη στις κατασταλτικές αρχές

• Προβλέπει διαδικασία συνεργασίας μεταξύ των αρχών των χωρών στην προσπάθεια καταστολής μετά από την υποβολή σχετικού αιτήματος στο μέγιστο δυνατό βαθμό.

Συμπεράσματα

• Η ηλεκτρονική ασφάλεια και η καταπολέμηση του ηλεκτρονικού εγκλήματος είναι κοινή ευθύνη της πολιτείας, του ιδιωτικού τομέα και των χρηστών

• Απουσία ασφαλών δικτύων και πληροφοριακών συστημάτων κινδυνεύουμε να χάσουμε τα οφέλη της χρήσης των ΤΠΕ

• Οι εθνικές στρατηγικές για την ηλεκτρονική ασφάλεια πρέπει να καλύπτουν όλους τους τομείς και όλες τις δραστηριότητες

• Η ηλεκτρονική ασφάλεια δεν περιορίζεται από εθνικά σύνορα και απαιτεί διασυνοριακή συνεργασία

Προτάσεις - Βήματα για το μέλλον

• Υιοθέτηση και υλοποίηση των Ευρωπαϊκών και Διεθνών Συνθηκών

για τα πνευματικά δικαιώματα και την ηλεκτρονική ασφάλεια

• Ενίσχυση της εφαρμογή της νομοθεσίας με εξειδικευμένο ανθρώπινο δυναμικό και εξοπλισμό (ειδικές ομάδες για την

Προστασία τη; πνευματικής ιδιοκτησίας, εκπαίδευση οργάνων τηςτάξης)

• Αύξηση της ενημέρωσης και αφύπνιση των πολιτών – αλλαγή της κουλτούρας των πολιτών

• Υποστήριξη ΜΜΕ και χρηστών

• Διασυνοριακή συνεργασία με γνώμονα την καταπολέμηση του ηλεκτρονικού εγκλήματος.

Η πρωτοβουλία eSEE του Συμφώνου Σταθερότητας παρέχει το πλαίσιο για κοινές ενέργειες στον τομέα ΤΠΕ για τις χώρες τις Ν.Α. Ευρώπης.

Η τάση αυτή εγκληματοποίησης των hackers οδήγησε αναπόφευκτα στη διαμόρφωση ενός ποινικού πλαισίου νομικής αντιμετώπισης το οποίο όμως από πλευράς εγκληματολογικής θεωρίας και αποτελεσματικότητας δε φαίνεται να είναι πλήρες και να ικανοποιεί ιδιαίτερα.

Case Study 1: ΠΓΔΜ - Έλλειμμα νομοθεσίας για την λειτουργία των Internet Café

Στην ΠΓΔΜ λόγω έλλειψης σχετικής νομοθεσίας πρόσφατα αναδείχτηκαν προβλήματα σχετικά με την λειτουργία των internet cafes. Ανήλικοι έχουν πρόσβαση σε ακατάλληλο υλικό όταν σερφάρουν στο διαδίκτυο σε internet café. Τα internet Café λειτουργούν βάση του Νόμου Περί Τυχερών Παιχνιδιών.

Για την αντιμετώπιση του ζητήματος κάποια Internet Café έχουν προβλέψει ξεχωριστούς χώρους για ενήλικους και ανήλικους όπως και τη χρήση ειδικού λογισμικού που σβήνει το ιστορικό των ιστοσελίδων που επισκέφτηκε ο προηγούμενος χρήστης, ώστε να εξασφαλίζεται το απόρρητο, αλλά και να προστατεύονται από μη κατάλληλο υλικό οι ανήλικοι.

Σε κάποια άλλα Internet Café οι υπάλληλοι παρακολουθούν τις ιστοσελίδες που επισκέπτονται οι ανήλικοι.

Εκπρόσωπος της τοπικής ΜΚΟ Metamorphosis ζήτησε να παρθούν άμεσα μέτρα είτε νομοθετικά, είτε με την συμπλήρωση σχετικών προβλέψεων στην ψηφιακή στρατηγική της χώρας

Case Study 2: Βουλγαρία – Η/Υ κυβερνητικών οργανισμών χρησιμοποιούνται για την διακίνηση παράνομου λογισμικού

Σύμφωνα με το διαχειριστή ιστοσελίδας που παρέχει αποθηκευτικό χώρο στο διαδίκτυο, Βουλγαρικά Υπουργεία και δημόσιοι οργανισμοί δημιουργούν σχεδόν τη μισή κίνηση για την αποθήκευση σε free servers παράνομου λογισμικού και πειρατικού περιεχομένου (multimedia)

Σε μια μόνο εβδομάδα το ποσοστό έφθανε το 47% της κίνησης.

Πρώτο στη λίστα των κυβερνητικών οργανισμών ήταν το Εθνικό Ινστιτούτο για την Κοινωνική Ασφάλιση (873 terabytes of downloaded

content) ακολουθούμενο από το Υπουργείο Εσωτερικών (544 terabytes) και το Υπουργείο Οικονομικών (411 terabytes)

Οι πιο ενεργοί Uploaders χρησιμοποιούν τη διεθνή διασύνδεση των κυβερνητικών δικτυακών τόπων που υποστηρίζει ο Βουλγαρικός Οργανισμός Τηλεπικοινωνιών (BTC). Σύμφωνα με αυτά τα στοιχεία μόνο οι υπάλληλοι του Υπουργείου Οικονομικών είναι εμπλεκόμενοι στην διανομή μεσω του διαδικτύου 30,000 DVX files

Case Study 3: http://www.efrauda.ro/**www.eFrauda.ro**

Ρουμανικό Κέντρο για την Καταπολέμηση του

Ψηφιακού Εγκλήματος στο Διαδίκτυο

Το eFrauda δημιουργήθηκε τον Ιανουάριο του 2004 από το Ρουμανικό Υπουργείο Επικοινωνιών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και λειτουργεί αμφίδρομα ως κόμβος πληροφόρησης, ενημέρωσης αλλά και μείωσης της γραφειοκρατίας.

Για τα θύματα απάτης μέσω διαδικτύου παρέχει ένα φιλικό στο χρήστη μηχανισμό καταγγελίας ηλεκτρονικής απάτης και άμεσης ειδοποίησης των Αρχών ενώ για όλους τους εμπλεκόμενους κυβερνητικούς φορείς αποτελεί ένα κεντρικό μηχανισμό καταγραφής περιστατικών ηλεκτρονικής παραβατικότητας.

Βασική αποστολή του eFrauda είναι η προστασία των καταναλωτών – χρηστών, και των προμηθευτών υπηρεσιών,η μείωση της γραφειοκρατίας και η αύξηση της διαφάνειας και η δημιουργία του απορρέει από τις προβλέψεις της Συνθήκης για το Ηλεκτρονικό Έγκλημα που η Ρουμανία επικύρωσε το 2004.

Τα πρώτα αποτελέσματα στη Ρουμανία

Η ηλεκτρονική διακίνηση πληροφοριών μπορεί να διεξάγεται πλέον με ασφάλεια, εφόσον είναι εγγυημένη η ασφάλεια των πληροφοριακών συστημάτων των δημόσιων οργανισμών και των ιδιωτικών εταιριών ακόμα και όταν τα κρούσματα ηλεκτρονικής απάτης αυξάνονται διεθνώς

Το 2005 οι εξειδικευμένες υπηρεσίες στη Ρουμανία εξέτασαν 579 παραβάσεις:

• 237 σχετίζονταν με δικτυακή απάτη

• 114 με πληροφοριακές παραβάσεις

• 103 με παραβάσεις πιστωτικών καρτών

• 30 με βρεφική πορνογραφία

• 95 λοιπές ηλεκτρονικές απάτες

Ο αριθμός των ατόμων που κατηγορήθηκαν για τις παραπάνω παραβάσεις είναι 345, ενώ 46 από αυτούς καταδικάστηκαν.

Παρόλο που ο αριθμός των χρηστών του Internet έχει αυξηθεί κατά 28% κατά το 2005, η Ρουμανία συνεχίζει να κατέρχεται στη λίστα που αφορά την ηλεκτρονική εγκληματικότητα

Πόσο σημαντικός είναι ο ρόλος του Internet στη Ν.Α. Ευρώπη;

Ποσοστά διείσδυσης του Internet

Χώρα	**Ποσοστό**
Αλβανία	22.7%
Βοσνία-Εργεζοβίνη	9.2%
Βουλγαρία	15.5%
Κροατία	15.3%
Ρουμανία	8.5%
Μαυροβούνιο	19.2%
Σερβία	33.6%
Κόσοβο	18.5%
ΠΓΔΜ	20.8%
Τουρκία	1.3%

Διείσδυση ανά 100 άτομα πληθυσμού

8 HACKERS

«Αυτός είναι ο κόσμος μας τώρα...Ο κόσμος των ηλεκτρονίων και των διακοπτών .Κάνουμε χρήση μίας υπηρεσίας που ήδη υπάρχει χωρίς να πληρώνουμε και η οποία θα ήταν πάμφθηνη εάν δε διοικείτο από αχόρταγους κερδοσκόπους και μας αποκαλείτε εγκληματίες. Εξερευνούμε και μας αποκαλείτε εγκληματίες, αναζητούμε τη γνώση και μας αποκαλείτε εγκληματίες.»

«Υπάρχουμε χωρίς φυλή, χωρίς εθνικότητα, χωρίς θρησκευτικές επιρροές και μας αποκαλείτε εγκληματίες. Εσείς, που φτιάχνετε ατομικές βόμβες, διεξάγετε πολέμους, δολοφονείτε, μας εμπαίζετε και μας παραπλανείτε οτι είναι γιά το δικό μας καλό κι όμως εμείς είμαστε οι εγκληματίες.Ναι, είμαι εγκληματίας και έγκλημά μου είναι η περιέργεια,το οτι κρίνω τους ανθρώπους από το τί λένε και τις πράξεις τους και όχι από την εμφάνιση τους.Το έγκλημά μου είναι οτι αποδείχτηκα εξυπνότερος από εσάς, κάτι που ποτέ δε θα μου συγχωρήσετε»

Hackers: Ευφυείς νεαροί επαναστάτες και σύγχρονοι ταχυδακτυλουργοί ενός καινούριου εικονικού σύμπαντος ή απλά ανεύθυνοι και επικίνδυνοι εγκληματίες με εξειδίκευση στις μοντέρνες υψηλές τεχνολογίες;

Εάν κάποιος ήθελε να είναι δίκαιος θα έπρεπε να συμφωνήσει και με τις δύο απόψεις.Από τον δεκατετράχρονο που εισβάλει σε ένα site με υλικό για ενηλίκους για να κλέψει μία ματιά στο απαγορευμένο, ως ένα τρομοκράτη που διεισδύει σε βάσεις δεδομένων του στρατού για να προκαλέσει την κατάρρευση συστημάτων άμυνας, έχουμε την ίδια διαδικασία. Το μόνο που διαφοροποιείται είνα το κίνητρο και το εύρος της δεξιότητας.

Το νόημα του hacking εκτείνεται σε τέτοιο βαθμό, ώστε να περιλαμβάνει ριζικά αντίθετες αλληλοαναιρούμενες και αλληλοαποκλειόμενες αντιλήψεις, οι οποίες αναφέρονται σε ριζικά διαφορετικές πραγματικότητες.

Ίσως το κυριότερο πρόβλημα προς μία ορθή εκτίμηση της hacker κοινότητας και των πράξεών της είναι η τέλεσή τους σε ένα κόσμο ακόμη

άγνωστο σε μία πλειονότητα πολιτών αλλά και κοινωνικοπολιτικών Αρχών, αυτόν του διαδικτύου.

Στη σύγχρονη κοινωνία της πληροφορίας το πλήθος των hackers είναι πολύ μεγάλο και η δράση τους ξεπερνά τα όρια αντίληψης του μέσου ανθρώπου για τις λειτουργίες και τα προγράμματα που διέπουν το χώρο του Internet.

Όπως εξελίχθηκαν οι δυνατότητες και οι υπηρεσίες που προσφέρει ο παγκόσμιος ιστός, έτσι και οι τρόποι και τα κίνητρα δράσης των ατόμων αυτών υπερδιπλασιάστηκαν. Αυτό βεβαίως συνέβη όπως θα δούμε κυρίως την τελευταία δεκαπενταετία,καθώς παλαιότερα οι hackers είχαν πιό περιορισμένο πεδίο δράσης.

8.1 **Hackers: ορισμοί και είδη**

Όπως αναφέρθηκε, οι hackers βρίσκονται σε μεγάλη ποικιλία σήμερα και δραστηριοποιούνται σε πολλούς τομείς, έχοντας πληθώρα τρόπων δράσεως και κυρίως πληθώρα κινήτρων.

Για το λόγο αυτό και είναι απαραίτητη μία διευκρίνιση των διαφόρων τύπων hacker, ώστε να διευκολυνθεί και η ανάλυση αλλά και η κατανόηση των διαφόρων παραμέτρων περί hacking που θα εκθέσουμε εν συνεχεία.

PHREAKS:

Καθώς το τηλεφωνικό δίκτυο προυπήρξε του δικτύου υπολογιστών, έτσι και των σύγχρονων hacker προηγήθηκαν οι phone phreaks.

Αυτοί ήταν άνθρωποι που χρησιμοποιούσαν το τηλεφωνικό σύστημα κυρίως για επικοινωνία με οποιοδήποτε μέρος του κόσμου με τρόπο φθηνό,γρήγορο και φυσικά μη αντιληπτό,εκμεταλλευόμενοι κλεμμένους τηλεφωνικούς κωδικούς και κάνοντας τροποποιήσεις σε τηλεφωνικά κέντρα.

Στα μέσα της δεκαετίας του ’80, η δημοσιοποίηση των κωδικών αυτών γιά κοινή χρήση αποτελούσε μία βασική προϋπόθεση για να θεμελιωθεί μία bona fides μεταξύ του επίδοξου phreak και της phreaking κοινότητας

HACKERS:

Hacker είναι όποιος ενδιαφέρεται για τις μυστικές και κρυφές διεργασίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή. Έχουν εκτενή γνώση λειτουργικών συστημάτων και γλωσσών προγραμματισμού.Προσπαθούν να ανακαλύψουν τα κενά και ρήγματα στα συστήματα υπολογιστών καθώς και τους λόγους ύπαρξης αυτών.

Αναζητούν σταθερά πρόσθετη γνώση,τη μοιράζονται ελεύθερα και δεν καταστρέφουν ποτέ και τίποτα σκοπίμως.

CRACKERS:

Cracker χαρακτηρίζεται αυτός που διεισδύει ή παραβιάζει την ακεραιότητα συστημάτων (σπάει κωδικούς ασφαλείας κλπ.)με πρόθεση τη διάπραξη κακόβουλων πράξεων, όπως καταστροφή δεδομένων, στρέβλωση συστημάτων και παρεμπόδιση λειτουργιών.

8.2 **Hackers: Οι 4 γενιές**

Ο Γρ. Λάζος βασισμένος στην εργασία του Levy (Hackers,1984), κάνει μία πλήρη αναφορά στις γενιές των hacker από την απαρχή ως τις μέρες μας. Η πρώτη γενιά των hackers αποτελείται από μέλη πανεπιστημιακών ομάδων των μεγάλων τεχνολογικών πανεπιστημίων MIT και Stanford.

Αυτοί οι επιστήμονες,σχεδόν αποκομμένοι απο την υπόλοιπη κοινωνία, ζούσαν εργαζόμενοι στα εργαστήριά τους και ανέπτυξαν τις πρώτες μεθόδους προγραμματισμού κατά το 1950 και 1960 στις υπηρεσίες κυρίως, βέβαια, της Αμερικανικής κυβέρνησης.

Η δεύτερη γενιά αποτελείται από εμπορικά προσανατολισμένους επιστήμονες που ως σκοπό είχαν την ευρεία διάδοση της πληροφορικής τεχνολογίας στις μάζες.

Ηταν αυτοί που δημιούργησαν τους πρώτους προσωπικούς υπολογιστές. Επιπρόσθετος στόχος της νέας γενιάς αυτής ήταν η μελέτη και ο

πειραματισμός για τη βελτίωση της αλληλεπίδρασης ανθρώπου με υπολογιστή,παραδειγματικό επίτευγμα της οποίας ήταν το γνωστό και απαραίτητο σήμερα «ποντίκι».

Η τρίτη γενιά αποτελείται από τους προγραμματιστές, οι οποίοι δημιούργησαν τις βασικές δομές στις οποίες στηρίχθηκε μετέπειτα η δημιουργία των ηλεκτρονικών παιχνιδιών.

Η γενιά αυτή δείχνει πλέον να αντιλαμβάνεται πλήρως την οικονομική δυναμική του συγκεκριμένου τομέα και εργάζεται δραστικά για να ανταποκριθεί στη ζήτηση που δημιουργεί η ευρεία εξάπλωση της χρήσης προσωπικού ηλεκτρονικού υπολογιστή αλλά και για να διαμορφώσει νέες προοπτικές αγοράς και νέες ανάγκες.

Η τέταρτη όμως γενιά είναι αυτή που συγκρότησε την hacker κοινότητα όπως την ξέρουμε σήμερα. Ενώ με τις προηγούμενες γενιές υπήρχε μια προσήλωση στην επίτευξη μίας εκλαίκευσης του νέου μέσου και κυρίως μία χρήση αυτού βασισμένη σε ανάγκες και δεδομένα της καθημερινότητας, η νέα αυτή γενιά εμφάνισε για πρώτη φορά μία αντεστραμμένη ψυχολογική συμπεριφορά, μία αναρχική τάση όχι σύνθεσης νέων δεδομένων και προγραμμάτων, αλλά αντίθετα μία αποδομητική και μία ενδοσκοπική εξερευνητική ενέργεια, που εξελίχθηκε στη μοντέρνα μορφή hacking, η οποία προσεγγίζει την εικόνα που έχουμε στο μυαλό μας γιά τον hacker, εικόνα που άπτεται και εγκληματικών συμπεριφορών.

Η γενιά αυτή αποδέχεται γενικά τις ηθικές αρχές που εξέθεσε ο Levy και τις οποίες θα δούμε αναλυτικά παρακάτω, αλλά παράλληλα αποτελεί ένα πολυπληθές σύνολο που έχει γεννηθεί και κοινωνικοποιηθεί σε ένα ήδη υπάρχον πληροφορικό περιβάλλον, το οποίο αποτελείται από άτομα που ζούν σε διαφορετικά μήκη και πλάτη του κόσμου και έχουν αναπόφευκτα ποικίλες ιδιοσυγκρασίες και ήθη.

Όπως αναφέρει και ο Kenneth Rosenblatt, εισαγγελέας στη Santa Clara, California, «η κοινωνία μας πρόκειται να βιώσει τον αντίκτυπο που θα έχει η πρώτη γενιά παιδιών γαλουχημένων στη χρήση προσωπικών υπολογιστών.

Η αυξημένη εντρύφηση και η εξειδίκευση των hackers θα οδηγήσει σε αύξηση της εγκληματικότητας, καθώς μέλη της νέας γενιάς θα μπούν στον πειρασμό διάπραξης εγκληματικών πραξεων».

Η εκρηκτική εξέλιξη του διαδικτύου δημιούργησε ένα νέο κοινωνικό μόρφωμα, όπου αναπόφευκτα διάφορες συμπεριφορές αποκτούν μία νέα σημασία, όταν πραγματώνονται εκτός εργαστηρίων και επηρεάζουν την ανθρώπινη καθημερινότητα πλέον.

Έτσι, η πρόσβαση σε έναν υπολογιστή δε θεωρείται πλέον ελεύθερη, αλλά απαιτείται μία εξουσιοδότηση. Χωρίς την εξασφάλιση αυτής, εισερχόμαστε πλέον στη νομικά ενδιαφέρουσα περίπτωση της παραβίασης, η οποία θα μπορούσε να αξιολογηθεί ως ανήθικη και εγκληματική.

8.3 **Η θετική πλευρά του hacking**

Λευκοί Hackers

Οι «λευκοί» hackers είναι οι απόγονοι των επιστημονικών-ηθικών στοιχείων που αποτέλεσαν τις τρείς πρώτες γενιές. Είναι τα άτομα, τα οποία έχουν το hacking ως παιχνίδι αλλά και ως μία ευκαιρία επικοινωνίας και επανάστασης στις κατεστημένες εμπορικές και πολιτικές δυνάμεις του χώρου.

Ούτως ή άλλως, η κίνηση αυτή έχει τις ρίζες της στην χίππι-αναρχική κίνηση των Yippies στα 1970, που μεταξύ άλλων σκοπό είχαν την αντίδραση ενάντια στις ιμπεριαλιστικές και διψασμένες για ισχύ πολιτικές δυνάμεις της εποχής.

Είναι μία ρομαντική ομάδα που συντηρεί τα υψηλά ιδανικά που κληρονόμησαν και χρησιμοποιούν τις δεξιότητες τους για πολλές δραστηριότητες πάντοτε όμως χωρίς κακόβουλο σκοπό.

Για να αντιληφθούμε όμως την ουσία αυτής της κοινότητας θα πρέπει να δούμε αναλυτικά το ψυχολογικό της προφίλ αλλά και τα κινητρά της.

Μόνο μέσα από μία τέτοια θεώρηση είναι εφικτή η ορθή εκτίμηση του φαινομένου του hacking και θα γίνει πιό γλαφυρός και ο διαχωρισμός των

υποκατηγοριών της hacker κοινότητας. Για τους hackers υπάρχουν κάποιες θεμελιώδεις αρχές ηθικής

Οι βασικές είναι οτι η πρόσβαση σε καθετί που διδάσκει κάτι για τη λειτουργία του κόσμου (και τους υπολογιστές) ,θα πρέπει να είναι συνολική και απεριόριστη και οτι κάθε πληροφορία πρέπει να είναι ελεύθερη.

Όχι ως προς την τιμή της αλλά την ελευθερία αντιγραφής και προσωπικής χρήσης της. Λέγοντας χρήσιμη δεν εννοώ εμπιστευτικές πληροφορίες για άτομα ή αριθμούς πιστωτικών καρτών για παράδειγμα.»

Οι αρχές αυτές αναλύονται σε μερικότερες αρχές:

Α)Οι πληροφορίες πρέπει να είναι ελεύθερες στον καθένα

Β)Έλλειψη εμπιστοσύνης στην εξουσία-προώθηση αποκέντρωσης

Γ)Οι hackers πρέπει να κρίνονται με βάσει την ικανότητά τους και όχι με κριτήρια όπως πτυχία, ηλικία, φυλή κλπ.

Δ)Μπορεί να δημιουργηθεί τέχνη και ομορφία στον υπολογιστή

Ε)Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο.

Οι hackers έχοντας αυτά τα ιδανικά αποτελούν ένα σύγχρονο avant-garde πυρήνα ατόμων, τα οποία εναντιώνονται στις σύγχρονες τάσεις που θέλουν τη διαχείρηση των πληροφοριών αποκλειστικά απο το σύστημα και την επιβολή περιορισμών στην κυκλοφορία τους από τους απλούς πολίτες.

Όλοι οι hackers είναι εμποτισμένοι με ένα ηρωικό αντιγραφειοκρατικό συναίσθημα. Επιδιώκουν την αναγνώριση σαν ένα αξιέπαινο πολιτισμικό αρχέτυπο,το μεταμοντέρνο ηλεκτρονικό αντίστοιχο του cowboy.

Τα κίνητρα των hackers κατά τη Denning εμπεριέχουν την έμφυτη ανάγκη των ατόμων αυτών για γνώση.Επιδιώκουν πρόσβαση σε δεδομένα και δίκτυα για να μάθουν.Και ο Levy και ο Landreth διαπιστώνουν αυτή την τάση των ατόμων αυτών, τα οποία μάλιστα δραστηριοποιούνται και στον τομέα της πληροφορικής επαγγελματικά με μεγάλη συχνότητα.

Στόχος τους επίσης, όπως λένε, είναι η ανακάλυψη των ρηγμάτων σε δίκτυα και υπολογιστικά προγράμματα, έτσι ώστε να εξασφαλισθεί μία αυξημένη ασφάλεια στο διαδίκτυο με την βελτίωση των προγραμμάτων

άμυνας των υπολογιστών και τη διόρθωση λαθών σε λειτουργικά συστήματα.

Αυτό φαίνεται ξεκάθαρα στη διακύρηξη του Nomad Mobile Research Centre, ένα δίκτυο hacker που εργάζεται για την ασφάλεια των υπολογιστών, δηλαδή την αντιστροφή της εφαρμοσμένης μηχανικής: *«Στόχος μας είναι να υποχρεώσουμε τις εμπορικές εταιρίες λογισμικού να διορθώνουν τα προϊόντα τους και να προσφέρουμε εναλλακτικές επιλογές.*

Όλα τα hacks /cracks γίνονται με σκοπό να προβληθεί η ιδέα οτι δεν μπορείς να εξασφαλίσεις ένα σύστημα για πολύ χρόνο.» .

Οι hackers έχουν στήσει ένα ιδιωτικό σύστημα εκπαίδευσης που τους δεσμεύει, τους διδάσκει και τους επιτρέπει να χρησιμοποιούν τη γνώση τους σε σκόπιμες, αν όχι πάντα νόμιμες δραστηριότητες.

Στα πλαίσια της αθρόας διασποράς της γνώσης και των αποκτηθέντων δεδομένων, οι hackers αποτελούν μία κολλεκτίβα που λειτουργεί σαν μία μυστική κοινωνία.

Υπάρχουν δάσκαλοι και μαθητές, μέντορες και μαθητευόμενοι,οι οποίοι αλληλοσυνδέονται σε ένα ηλεκτρονικό πάρε-δώσε, όπου επικρατεί ο σεβασμός, η εμπιστοσύνη και η αλληλεγγύη. Η μόνη διαφορά είναι οτι ως προυπόθεση εισόδου απαιτούν την ικανότητα και όχι κάποια αριστοκρατική καταγωγή ή οικονομική επιφάνεια. Και φυσικά δεν υπάρχει όρκος σιωπής στους hackers. Μπορεί να είναι ντροπαλοί ή και αντικοινωνικοί, αλλά όταν μιλάνε, αρέσκονται στην αυτοπροβολή.

Είναι ο μόνος τρόπος, ώστε να αναγνωρισθεί κάποιος από την κοινότητα και να αποκτήσει κύρος, φήμη, να θεωρηθεί άξιο μέλος και να απολαύσει και τη συνεργασία των συναδέλφων hacker.

Το κοινωνικό και ψυχολογικό υπόβαθρο της κοινότητας αυτής παρουσιάζει ιδιαίτερο ενδιαφέρον. Όπως αναφέρθηκε η ηλικία της πλειονότητας των παιδιών αυτών ξεκινά από την εφηβεία και σπάνια ξεπερνά τα 20-25 χρόνια.

Αυτοί προέρχονται συνήθως από μεσοαστικές οικογένειες και είναι αντιυλιστές ως επί το πλείστον (εκτός σε ό,τι μπορεί να αφορά τον

υπολογιστή τους). Όποιος δείχνει ενδιαφέρον για χρήματα απορρίπτεται αμέσως ως διεφθαρμένος και άξιος περιφρόνησης.

Γι’ αυτούς το hacking εκτός από μία πρόκληση συχνά αποτελεί και το αγαπημένο τους παιχνίδι.Όπως δηλώνει και ο Κέβιν Μίτνικ, ένας από τους θρυλικότερους hackers: «Βρίσκοντας διάφορους τρόπους να παραβιάζω τα συστήματα ασφαλείας απλώς περνούσα καλά, είχε πλάκα.».

Το εικονικό περιβάλλον προσφέρει μία αίσθηση ασφαλείας, καθώς ο νεαρός κατορθώνει από την ασφάλεια του δωματίου του σαν super ήρωας να υπερπηδήσει τα εμπόδια αρκετά πιό μορφωμένων και μεγαλυτέρων σε ηλικία προγραμματιστών και να τους εμπαίξει.

Η πιό κοινή αντίληψη για τους hackers από το 60’ ως σήμερα είναι οτι αποτελούν μία ελίτ. Όταν είσαι ο ίδιος hacker, τότε είναι η ίδια σου η εσωτερική πεποίθηση για το ανώτερο status σου που σου επιτρέπει να υπερπηδήσεις τους κανόνες.

Λόγω αυτής τους της φύσης, ενός elite underground συνόλου με αναρχικές-αντικαπιταλιστικές τάσεις, πρέπει διαρκώς να διατηρούν μία μεμβράνη διαφοροποίησης.

Αστεία και ξεχωριστά ρούχα και μαλλιά, ειδική διάλεκτο με διαφορετικές ορθογραφίες γραμμάτων π.χ. 0 αντί για ο, ειδικές περιοχές γκέτο στις πόλεις, διαφορετικά ωράρια ζωής.

Συχνά χρησιμοποιούν παραποιήσεις ονομάτων από μεγάλες επιχειρήσεις και περιπαικτικά λογοπαίγνια ως ψευδώνυμα (Phortune 500),κυβέρνηση και αστυνομία(NASA elite) και πολλά άλλα.

Η κοινωνία των hacker είναι κυριαρχούμενη από έφηβα αγόρια και γι’ αυτό έχει μία ανδροκρατούμενη κουλτούρα. Μολονότι οι γυναίκες είναι σήμερα μία ανερχόμενη δύναμη στο χώρο, αντιμετωπίζουν ακόμη προκατάληψη και λοιδορία.

Πολλοί άνδρες hackers, όπως οι Toxic Shock Group παραδέχονται οτι το hacking το κάνουν και για να ικανοποιήσουν μία υποσυνείδητη σεξουαλική επιθυμία κι ερωτική φόρτιση.

Hacktivism

Στη σύγχρονη εποχή ένας εναλλακτικός τρόπος δράσης με αμφιλεγόμενα αποτελέσματα έχει δώσει τροφή για συζητήσεις στον πολιτικό κόσμο.

Η δράση αυτή είναι ο ακτιβισμός, δηλαδή η αντίδραση σε μία κατεστημένη αρνητική κατάσταση με ενέργειες όπως πορείες,καθιστικές διαμαρτυρίες,καταλήψεις, μέχρι και επιθέσεις με τούρτες και αυγά κατά οικονομικών και πολιτικών παραγόντων.

Ο χακτιβισμός είναι ένα τέτοιο είδος πολιτικού ακτιβισμού, ένα συστεμικό σύνολο προτάσεων για αντίσταση και κριτικό διάλογο.

Συνεπώς, ο χακτιβισμός αποτελεί μία μεταφορά του ακτιβισμού της πραγματικής ζωής σε ένα εικονικό επίπεδο έκφρασης, το διαδίκτυο, και υποδεικνύει πώς ο άνθρωπος μαθαίνει να χειρίζεται ψηφιακά πλέον τις δυνατότητες που του προσφέρονται και πώς μαθαίνει να σκέφτεται και να λειτουργεί στα πλαίσια της περιρρέουσας ηλεκτρονικής κουλτούρας.

Υπάρχουν 2 είδη χακτιβισμού:

Το πρώτο επιχειρεί να γιατρέψει το Internet από κάθε κακό κώδικα και ελαττωματικό πρόγραμμα.

Το δεύτερο και πιό ενδιαφέρον είδος είναι η χρησιμοποίηση του δικτύου ως όργανο για κοινωνική δικαιοσύνη, διαμέσου διαφόρων δραστηριοτήτων διαμαρτυρίας ή ως μέσο για δημοσιότητα.

Χαρακτηριστικό παράδειγμα χακτιβιστών είναι οι Electronic Disturbance Theatre, υποστηρικτές hackers των Ζαπατίστας με έδρα τη Νέα Υόρκη αλλά και οι Electrohippies. Και τα δύο αυτά γκρούπ ειδικεύονται σε virtual καθιστικές διαμαρτυρίες.

Οι πρώτοι είχαν καταφέρει να κλείσουν την ιστοσελίδα του προέδρου του Μεξικό με την οργάνωση αποστολής 16000 e-mails διαμαρτυρίας για την πολιτική του, υπερφορτώνοντας το σύστημα και υποχρεώνοντάς το να καταρρεύσει.

Οι δεύτεροι είναι ιδιαίτερα γνωστοί για την οργάνωση διαμαρτυρίας κατά του Παγκοσμίου Οργανισμού Εμπορίου και την πίεση που άσκησαν

με e-mail σε πολλούς πολιτικούς σχετικά με τα γενετικώς τροποποιημένα προϊόντα.

Ο χακτιβισμός όμως είναι κάτι παραπάνω από μία τυπική αντίδραση, καθώς έχει περάσει και μέσα στην τέχνη ή καλύτερα έχει μετατραπεί σε μία μορφή καλλιτεχνικής έκφρασης με πολιτικά και κοινωνικά μηνύματα.

Όπως δηλώνει και η Τζ. Μαρκέτου, πολλοί καλλιτέχνες πιστεύουν οτι δημιουργικότητα δεν είναι να δημιουργείς κάτι καινούριο μόνο, αλλά να χρησιμοποιείς ό,τι ήδη υπάρχει. Ο χακτιβιστής διαδικτυακός καλλιτέχνης αντί να παράγει φυσικά αντικείμενα,οργανώνει και αποδομεί το σύστημα με σκοπό την αφύπνιση του χρήστη. Στα πλαίσια της ελευθερίας δεδομένων στο NET, η τέχνη δε νοείται να είναι διαθέσιμη επί πληρωμή.

Γι’ αυτό και μία ομάδα χακτιβιστών καλλιτεχνών από τη Μπολόνια, η 0100101110101101.ORG εισέβαλε στην ιστοσελίδα του πιό δημοφιλούς μουσείου τέχνης στο διαδίκτυο, το hell.com και δημιούργησε ένα αντίγραφο του μουσείου με σπασμένους τους κωδικούς ασφαλείας, ώστε να είναι ελεύθερη η πρόσβαση.

Αυτοί οι καλλιτέχνες του παγκοσμίου ιστού προσπαθούν να διαπιστώσουν αν η τέχνη στο Internet μπορεί να γίνει αληθινά συμμετοχική,συνδετική και ανοιχτού κώδικα.

Απ’ τη μία εξερευνούν ελεύθερα τις τακτικές του χακτιβισμού και απ’ την άλλη επιτίθενται στο μηχανισμό και το μύθο του καλλιτεχνικού συστήματος, όχι μόνο αμφισβητώντας την πρωτοτυπία ή τη δημιουργία ως συλλογική διαδικασία αλλά και διαμορφώνοντας τα μοντέλα τους μέσα από τη διαδικασία αυτή.

Και με την παράμετρο αυτή κλείνουμε την αναφορά μας στην υγιή πλευρά του hacking για να ασχοληθούμε με το μέρος που άπτεται της σκοτεινής πλευράς του φαινομένου, αυτή που εκδηλώνεται αντικοινωνικά, ανήθικα και φυσικά εγκληματικά.

8.4 **Η σκοτεινή πλευρά του hacking**

Το διαδίκτυο αποτελεί σήμερα μία νέα κοινωνική πραγματικότητα, η οποία είναι όντας ανθρώπινο δημιούργημα, δομημένη με τα προτερήματα και τα ελαττώματα που συναντά κανείς και στην πραγματική κοινωνική ζωή.

Όπως δραστηριοποιούνται άνθρωποι ηθικοί και σκεπτόμενοι, που εργάζονται για την κοινωνική ευημερία λοιπόν, έτσι υπάρχουν και άνθρωποι ανήθικοι, οι οποίοι βλέπουν το νέο αυτό δημιούργημα ως μία νέα δίοδο για να ασκήσουν τις παράνομες δραστηριότητες τους με λιγότερες ενοχλήσεις και να επιδιώξουν την ικανοποίηση των φιλοδοξιών και των απωθημένων τους με τα πλεονεκτήματα της ανωνυμίας και του δύσκολου εντοπισμού από τις Αρχές.

Αυτοί οι hackers είναι το διεφθαρμένο κομμάτι τους και δυστυχώς αυτοί που απολαμβάνουν τη μεγαλύτερη δημοσιότητα και προσοχή και συνεπώς αυτοί που σκιαγραφούν τη δημόσια εικόνα όλου του κινήματος.

Το προφίλ του απροσάρμοστου αθώου εφήβου μπορεί να ίσχυε για τους hackers της δεκαετίας του 1980 αλλά όχι στις μέρες μας. Πολλοί hackers σήμερα είναι κακοήθεις και άπληστοι.Ταλαντούχοι και ικανοί hackers συχνά βρίσκουν δουλειά στη Μαφία, τα κολομβιανά καρτέλ ναρκωτικών,τα τρομοκρατικά δίκτυα και γενικά το οργανωμένο έγκλημα.

Τα κίνητρα των crackers αυτών είναι ευτελή, εκτεινόμενα από το πάθος για χρήμα και δύναμη μέχρι το βανδαλισμό και την καταστροφή συστημάτων για απλή αυτοπροβολή και για την αίσθηση εξουσιασμού των λιγότερο καταρτισμένων και των αδαών.

Είναι άτομα τα οποία διαθέτουν χαλαρούς ηθικούς φραγμούς λόγω ελλιπούς μόρφωσης ως προς τους ηλεκτρονικούς υπολογιστές, καθώς, όπως υποστηρίζει και ο Larry Martin, οι γονείς, ο τύπος και οι καθηγητές δεν αντιλαμβάνονται την υποχρέωσή τους να συμβάλουν στην ανάπτυξη ηθικών αρχών σχετικά με τους υπολογιστές.

Είναι τεχνολογικά αναλφάβητοι και συνεπώς οι πολιτισμικές νόρμες υστερούν ως προς τις εξελίξεις της τεχνολογίας και τις εξαρτήσεις της κοινωνικής ζωής από αυτές.

Ατυχώς, τόσο για την κοινωνία όσο και γι'αυτούς που χρειάζονται καθοδήγηση δεν υπάρχει κάποιο δεδομένο καθεστώς στην κοινότητα των ηλεκτρονικών υπολογιστών που να ορίζει πότε ακριβώς το παιχνίδι έχει βγεί εκτός ελέγχου.

Σημαντικό ρόλο στην ηθική ανεπάρκεια που εμφανίζουν οι νέοι hackers, είναι το νεαρό της ηλικίας τους που δεν τους επιτρέπει μία ανεπτυγμένη αίσθηση ηθικής, ώστε να έχουν πλήρη αντίληψη για το πότε οι ενέργειές τους είναι βλαπτικές για τους συνανθρώπους τους.

Αλλά και μέσα από τα μάτια ενός hacker, του Chris Goggans, μέλος μίας ομάδας που στιγμάτισε τη δεκαετία του 90' με τη δράση της, τους Legion Of Doom, βλέπουμε οτι η νέα γενιά δεν του εμπνέει εμπιστοσύνη.

Αναφέρει οτι με τον καιρό τα άτομα έγιναν πιό αντικοινωνικά και καθώς πέρναγαν τα χρόνια χάθηκε αυτο το αίσθημα συναδελφικότητας που επικρατούσε στους κύκλους των hackers.

Οι άνθρωποι άρχισαν να μαζεύουν μανιωδώς πληροφορίες για τον εαυτό τους και να καταδίδουν για εκδίκηση.

Το hacking έπαψε να είναι πιά διασκεδαστικό. Έγινε μια διαδικασία πρωτόγονη και διψασμένη για δύναμη σε ατομικό επιπεδο.

Αυτό έχει τις ρίζες του και στην αθρόα αύξηση των επίδοξων hacker που αλλοίωσαν το αίσθημα κοινότητας μεταξύ των παλαιών και λόγω πλήθους έχασε σε νόημα και η διανομή δεδομένων και πληροφοριών αλλά και η εκπαίδευση νέων από τους παλαιοτέρους.

Πρόβλημα επίσης αποτελεί κατά τον Spafford η αντίληψη του υπολογιστή ως μηχάνημα με λειτουργία αδιάφορη με την κοινωνική και καθημερινή λειτουργία των ανθρώπων και τις αξίες τους.

Τα τελευταία δεδομένα συντελούν στη διαμόρφωση μίας εικόνας για το ηθικό υπόβαθρο ή μάλλον την ανυπαρξία ενός τέτοιου όσον αφορά στου crackers, ώστε να δικαιολογηθεί η πορεία που καταλήγουν να ακολουθούν.

8.5 Οι hackers ως εγκληματικά στοιχεία

Τα αίτια και το παρασκήνιο της εγκληματοποίησης

Είναι αναμφισβήτητο οτι πολλοί hackers επιδίδονται σε εγκληματικές συμπεριφορές.

Από την εισβολή σε συστήματα τραπεζών και καταστημάτων ηλεκτρονικού εμπορίου (e-shops) για κλοπή κωδικών πιστωτικών καρτών μέχρι την εισβολή σε κρατικούς υπολογιστές για κλοπή ευαίσθητων δεδομένων και απορρήτων αρχείων ή την απελευθέρωση ιών για καταστροφή προγραμμάτων και συστημάτων, οι hackers παραβιάζουν το νόμο για να αποκομίσουν κάποιο ώφελος, είτε είναι χρηματικό είτε όχι.

Σήμερα όμως ακόμη και η απλή εισβολή σε ένα δίκτυο υπολογιστών χωρίς την παραμικρή επίπτωση στον χειριστή ή το ίδιο το σύστημα έχει αποκτήσει ποινικό ενδιαφέρον, προξενώντας έντονες συζητήσεις σε νομικούς και όχι μόνο κύκλους για το κατά πόσο κάθε πράξη hacking πρέπει να έχει ποινικό αντίκτυπο αλλά και για τους λόγους που έχει δημιουργηθεί ένα τέτοιο κλίμα συνολικής ποινικοποίησης αυτής της δραστηριότητας.

Και είναι όπως θα δούμε γεγονός οτι βρίσκονται ισχυρές κοινωνικοπολιτικές δυνάμεις και τάσεις που τροφοδοτούν αυτή την κατάσταση δαιμονοποίησης των hackers, οι οποίοι χωρίς να είναι φυσικά άμοιροι ευθυνών δεν είναι αυτονόητα και πάντοτε ένοχοι.

Η δημιουργία ενός κοινωνικού ορίου μεταξύ δύο διαφοροποιημένων ομάδων-τάξεων συντελείται με μία έντονη διαδικασία, όπου κάποια ομάδα διαφοροποιείται, περιθωριοποιώντας άλλες ομάδες και θεμελιώνοντας έτσι την ταυτότητά της.

Ένα τέτοιο κυνήγι μαγισσών έχουμε σε περιόδους κοινωνικής ανακατάταξης και όπως φαίνεται η κοινωνία μας βρίσκεται σε μία τέτοια περίοδο αλλαγής.

Οι κύκλοι της οικονομίας επιχειρούν να επιβάλουν σχέσεις ιδιοκτησίας επί των πληροφοριών αλλά η μεταβαλλόμενη φύση της πληροφορίας υπονομεύει τις ιδιοτητές της ως αγαθό.

Μία κοινότητα, αποκτά αίσθηση του κοινωνικού της status προσδιορίζοντας τί δεν είναι. Η αποστασιοποίηση από τους έξωθεν βοηθά τα μέλη μίας ομάδας να έχουν μία αίσθηση συνοχής.. Επίσης μία κουλτούρα τείνει να περιθωριοποιεί δράσεις που πλήττουν τις αξίες της.

Στην περίπτωση των hackers αυτό συνέβη, διότι με τις αντιλήψεις τους περί ελευθερίας της πληροφορίας απείλησαν ένα από τα βασικά δεκανίκια του καπιταλισμού, τα δικαιώματα ιδιοκτησίας.

Βασικός επίσης παράγοντας περιθωριοποίησης και εγκληματοποίησης των hackers είναι το γεγονός οτι δημιουργείται ένας νεός τομέας επαγγελμάτων αντίθετος με τη hacking κουλτούρα και ηθική: η βιομηχανία ασφαλείας υπολογιστών.

Μία βιομηχανία, πολύ ισχυρή σύμμαχος των καθεστώτων που θέλουν να έχουν τον απόλυτο έλεγχο των νέων τεχνολογιών για την εξυπηρέτηση των δικών τους σκοπών. Δεν ανέχονται τους ενοχλητικούς hackers, οι οποίοι αποκαλύπτουν κρατικές και εταιρικές παρασπονδίες και φυσικά εξαναγκάζουν τις εταιρίες προστασίας υπολογιστών να ξοδεύουν υπέρογκα ποσά, ώστε να αναπτύσσουν ικανά αμυντικά συστήματα σε τακτά χρονικά διαστήματα για να μπορούν να διατηρήσουν μία τυπική αμυντική γραμμή έναντι των εισβολών.

Έτσι η ηθική καταδίκη αποτελεί τρόπο για αποποίηση των ευθυνών, για τα ρήγματα και ελαττώματα των συστημάτων από πλευράς υπευθύνων ασφαλείας.

Όπως εύγλωττα δηλώνουν στις εκκλήσεις των hackers για συνεργασία στην ανακάλυψη των συστεμικών προβλημάτων ,εάν οι hackers δεν υπήρχαν, τότε δε θα υπήρχε και η ανάκη για τόσα αμυντικά προγράμματα που κοστίζουν σε έσοδα και δημιουργικό χρόνο.

Και πράγματι εδώ ο προβληματισμός δίκαιως ευσταθεί, καθώς είναι αμφίβολο εάν δικαιολογεί την υπαρξή της μία απειλή (οι hackers), ως προστάτης της κοινωνικής και ηλεκτρονικής ασφάλειας και ευημερίας,

όταν η ύπαρξη της ιδίας της απειλής, εξωθεί στην ανάγκη για δημιουργία και διαρκή εξέλιξη αμυντικών μηχανισμών.

Η αντίληψη για τους hackers τροφοδοτείται και από τη τάση να υποθέτουμε το χειρότερο δυνατό κινητρο για τον κάθε εισβολέα, γεγονός που ενισχύεται ακόμα περισσότερο από την ανωνυμότητα αλλά και τη λαϊκη άγνοια ως προς τη διαδικασία του hacking.

Η προκατάληψη βασίζεται πάνω στη δυνητική ζημία που είναι σε θέση να επιφέρει ένας hacker.Ακόμη και χωρίς καμία κακόβουλη πρόθεση από τον hacker, η υποψία και η αμφιβολία υπάρχουν.

Αυτό διογκώνεται από τη δυσνόητη φύση της δράσης των ατόμων αυτών αλλά και τις δεδομένες δυσκολίες παρακολούθησης τους καθώς και από ένα αυτονόητο χάσμα γενεών που υπάρχει μεταξύ των διαχειριστών της οικονομικής και πολιτικής ζωής και των συστεμικά απορροφημένων ενηλίκων- μαζοποιημένων μελών της καπιταλιστικής κοινωνίας έναντι των επαναστατικών νέων που αποτελούν την πλειοψηφία των hackers σήμερα.

Είναι αδιαμφισβήτητο οτι σταδιακά στις μέρες μας αξίες όπως συναδελφικότητα και αλληλεγγύη έχουν αρχίσει να ατονούν με αποτέλεσμα να ασθενεί αυτό το αίσθημα κοινότητας και συντροφικότητας που επικρατούσε σε παλαιότερες εποχες και να δίνει τη θέση του στην επιδίωξη της προσωπικής ανέλιξης και τον εγωκεντρισμό.

Το δημόσιο ήθος βιώνει μία παρακμή και για το λόγο αυτό επιζητά έναν αποδιοπομπαίο τράγο ώστε να δημιουργήσει ένα κλίμα αποπροσανατολισμού και να δικαιολογήσει τα ανησυχητικά δεδομένα. Έτσι οι hackers αναλαμβάνουν αυτό το ρόλο.

Μέσα σε ένα τέτοιο αρνητικά προδιατεθειμένο περιβάλλον, έρχεται να προστεθεί η καταλυτική επιρροή των ΜΜΕ, τα οποία φυσικά είναι αυτά που δίνουν μορφή σε όσα αναφέραμε ως τώρα.

Ο τύπος έχει υπάρξει ιδιαίτερα ενεργός στη διαδικασία της δημιουργίας στερεοτύπων και τη διόγκωση περιστατικών hacking, μία διαδικασία που οδήγησε στην ανάπτυξη ενός περιθωριακού status για τους hackers.

Τα ΜΜΕ έχουν δώσει τέτοια έκταση και σημασία στο φαινόμενο hackers γιατί προσφέρονται για ηρωοποίηση ή δαιμονοποίηση. Ειδικά στις

τεχνολογικά ανεπτυγμένες χώρες, ο λόγος για το hacking είναι πλέον μέρος της λαικής συνείδησης.

Μολονότι τα ΜΜΕ δεν υποστήριξαν την εφαρμογή του ποινικού δικαίου στον κόσμο της πληροφορικής, δημιούργησαν ένα κλίμα σοβαρού και πιθανοτάτου κινδύνου στην κοινή γνώμη, με την προβολή πραγματικών ή και φανταστικών ιστοριών με hackers και συχνά προβεβλημένες υπό ένα πρίσμα υπερβολής.

Γλαφυρότατη είναι η δήλωση του δημόσιου σχολιαστή Gene Spafford περί του τί είναι hacking και τί προεκτάσεις έχει: «το να δίνεις δουλειά σε ένα hacker είναι σαν να κάνεις αρχηγό της πυροσβεστικής έναν εμπρηστή, καθηγητή σχολείου έναν παιδεραστή...»

Έτσι οι πράξεις των hackers τοποθετούνται εκτός διαδικτύου και επανασυστήνονται στον κανονικό κόσμο με όρους καθημερινούς και αντιληπτούς σαν αληθινές απειλητικές καταστάσεις. Εάν αυτό επιτευχθεί, τότε ο κίνδυνος και η ζημία που μπορεί να έχουν τέτοιες πράξεις γίνονται ευκολότερα κατανοητά και τρομακτικά και οι hackers παρουσιάζονται ως ηθικοί παρίες.

Το πρόβλημα, έγκειται στη ρεαλιστική έκθεση και περιγραφή των περιστατικών hacking, καθώς παρουσιάζουν σύνθετη τεχνική ορολογία, η οποία πρέπει να γίνει αντιληπτή από τον τηλεθεατή αλλά παράλληλα με τρόπο ευχάριστο και διασκεδαστικό.

Έτσι συνήθως η ακρίβεια και η λεπτομέρια θυσιάζονται στο βωμό της τηλεθέασης και τα γεγονότα περιγράφονται με τρόπο διογκωμένο και τα κίνητρα των hacker παρουσιάζονται αρκετά πιο σκιώδη.

΄Ολη αυτή η σύνθετη διαδικασία εγκληματοποίησης έχει φυσικά αντίκτυπο στην ίδια την κοινωνία και το λαϊκό αίσθημα απέναντι στους hackers αλλά και στους ίδιους όπως θα δούμε στη συνέχεια της παρουσίασης μας.

8.6 **Συνέπειες εγκληματοποίησης σε κοινωνία και hacker κοινότητα**

Αναμφισβήτητα αυτός ο πανικός που έχει δημιουργηθεί γύρω από την επικινδυνότητα του hacking έχει οδηγήσει την κοινωνία σε μία οπισθοδρομική πορεία όσον αφορά στην εμπιστοσύνη και την ενασχόληση του μέσου πολίτη με το διαδίκτυο και τις ποικίλες υπηρεσίες που προσφέρει.

Η μεγαλυτερη ζημία των hackers είναι η παράνοια που δημιουργείται, η οποία οδηγεί στη δικαιολόγηση αυστηρότερου ελέγχου από τις Αρχές, γεγονός που φυσικά περιορίζει τις δυνατότητες των πολιτών και μειώνει την ποιότητα ζωής που θα μπορούσαν να εξασφαλίσουν οι χρήστες.

Με αυτό συμφωνεί και η D.Denning, η οποία δηλωνει οτι η προβολή μίας τέτοιας εγκληματικής εικόνας των ατόμων αυτών οδηγεί σε μία τάση για κοινωνικό έλεγχο σε μία περίοδο που θα έλεγε κανείς οτι ήδη βρισκόμαστε υπό υπερβολικό έλεγχο.

Κι όμως, όπως φαίνεται από έρευνα του Pew Internet & American Life Project, ενώ η ανησυχία των Αμερικανών ως προς την εγληματικότητα σε υπολογιστές είναι αυξημένη (87% ανησυχούν για κλοπή πιστωτικών καρτών on-line, 82% φοβούνται τη δυνατότητα τρομοκρατών να σπείρουν πανικό μέσω διαδικτύου, 78% πιστεύουν οτι οι hackers δύνανται να έχουν πρόσβαση σε κρατικά δίκτυα και 76% σε εμπορικά δίκτυα και ένα 70% φοβάται για φαρσέρ και εγκληματίες που στέλνουν ιούς και τροποποιούν ή σβήνουν αρχεία), τα ποσοστά των ατόμων που εμπιστεύονται τις Αρχές για έλεγχο και προστασία είναι αρκετά χαμηλότερα (54% των Αμερικανών συμφωνεί με παρακολούθηση του ηλεκτρονικού ταχυδρομίου υπόπτων από το FBI, από την αστυνομία το ποσοστό υποχωρεί κι άλλο, ενώ μόνο ένα 31% δείχνει να εμιστεύεται τη σωστή κρίση της κυβέρνησης.

Κι αυτό σε μία χώρα όπου το Internet είναι πλέον θεμελιώδες εργαλείο της κοινωνίας, αποτελεί πατρίδα των hackers και διαθέτει μία από τις αυστηρότερες πολιτικές κατά τέτοιου είδους προσβολών.

Η δαιμονοποίηση όμως αυτή δημιουργεί μία κοινωνική ανισορροπία και καταλήγει να πλήττει και μία νέα κοινωνική ομάδα, η οποία ενώ αποτελεί σημαντική κινητήρια δύναμη της σύγχρονης οικονομικοκοινωνικής πορείας, απειλείται με στιγματισμό.

Υπάρχουν σήμερα πολίτες, οι οποίοι εργάζονται στον τομέα της ηλεκτρονικής, λειτουργώντας στα πλαίσια του νόμου σε πολύ υψηλο επίπεδο ειδίκευσης και ικανότητας. Όταν συγκεντρώνονται σε κυβερνητικές θέσεις πανεπιστήμια και πολυεθνικές και αναγκάζονται να ακολουθούν συγκεκριμένους κανόνες, τότε τίθενται κάποιοι συμβατικοί περιορισμοί στην ελευθερία δράσης τους

Όταν όμως βρεθούν ανεξάρτητοι και ελεύθεροι να δημιουργήσουν, αυτή η επίλεκτη κατηγορία ταλαντούχων ενηλίκων είναι πολύ πιό επικίνδυνη από οποιαδήποτε ομάδα από cyberpunks.

Αυτοί οι hackers διαθέτουν δύναμη, ικανότητα και επιθυμία να επιδράσουν επί της κοινωνικής διαστρωμάτωσης. Αποτελούν μία elite που αν απομακρυνθεί και δράσει αποκομμένη από τις κοινωνικές αρχές και στερεότυπα, εάν αποκλεισθεί απ' αυτά, μπορεί να καταστεί επικίνδυνη. Αυτοί οι άνθρωποι γνωρίζουν ενστικτωδώς οτι μία πολιτική επίθεση στους hackers θα τους αγγίξει αναπόφευκτα.

Οτι η δαιμονοποίηση του όρου hacker μοιραία θα τους επηρεάσει, θα θίξει την ισχύ και την ελευθερία που απολαμβάνουν και θα τους αφανίσει. Και φυσικό είναι να θέλουν με κάθε τρόπο να αποφευχθεί κάτι τέτοιο.

Όσον αφορά τώρα στους ίδιους τους hackers, η εγκληματοποίηση της δράσης τους αλλά και η προπαγάνδα που συντελείται όπως είδαμε με την ευχή της καθεστηκυίας τάξης δημιουργώντας ένα στερεότυπο εικόνας για τα άτομα αυτά επιδρά τόσο στην ατομική ιδιοσυγκρασία και επιλογές τους όσο και στον τρόπο που αλληλεπιδρούν με την κοινωνία και διαμορφώνουν την κοινότητά τους.

Μετέτρεψε τους hackers σε μία πιό οργανωμένη για την επιβίωσή της ομάδα, ενώ η συντονισμένη επίθεση από τις διωκτικές Αρχές, τα ΜΜΕ και τους σύγχρονους ιδεολογικούς μηχανισμούς, τροφοδότησε τις αντιλήψεις τους με μία ενισχυμένη επαναστατικότητα και αντιδραστικότητα στους

κατεστημένους μηχανισμούς κοινωνικού αποπροσανατολισμού και υποβολής.

Σε άλλες περιπτώσεις πάλι, οι hackers παρασύρθηκαν από τη λαίλαπα μυθοποίησης του hacker-προτύπου και έτσι ακολούθησαν ένα ρόλο γραφικού εγκληματία-μορφής του υποκόσμου που ήταν, όπως πίστευαν, ό,τι περίμενε η κοινωνία να δεί από αυτούς.

Όπως λέει και η Τζ. Μαρκέτου στη συνέντευξή της, η αρνητική δημοσιότητα του hacking μέσω των ελεγχόντων την ροή και μορφή των πληροφοριών, υποβίβασε τη σημασία του hacking και του χακτιβισμού σε απλή δραστηριότητα μέσω υπολογιστή, αφαιρώντας έτσι το κοινωνικοπολιτικό περίβλημα που διαθέτει. Μετατρέποντας τους hackers σε δημοσιότητες κατάφερε να τους αποδυναμώσει και μέσω του καταναλωτισμού να απορροφήσει το δημιουργικό – ανατρεπτικό τους πνεύμα.

8.7 **Προβλήματα δίωξης και καταστολής των hackers**

Παρά τη ραγδαία αύξηση του ηλεκτρονικού εγκλήματος ένα 72% των αστυνομικών τμημάτων δεν διαθέτουν εξειδικευμένο προσωπικό για τη δίωξή του. Αξίζει να σημειωθεί οτι σε έρευνα του FBI σε ιστοσελίδες κυβερνητικών οργανισμών σε 428 χώρες διαπιστώθηκε οτι το 40% είχε παραβιαστεί, ενώ σύμφωνα με έκθεση που δημοσιεύει ο αμερικανικός όμιλος Science Applications International Corp. κάθε χρόνο 40 μεγάλες εταιρίες αναφέρουν ζημίες απο hackers γύρω στα 800 εκατ. δολλάρια. Όμοια στην Αγγλία το κόστος των επιθέσεων ανέρχεται στα 200 εκατ. λίρες.

Η αστυνομία έχει ως στόχο την καταπολέμηση του εγκλήματος και τη διατήρηση της κοινωνικής ειρήνης. Εφόσον λοιπόν το έγκλημα του δρόμου παραμένει μία κύρια και προπάντων μία εμφανής απειλή με αντίκτυπο στην κοινή γνώμη φυσικό και λογικό είναι οι πόροι αλλά και το ενδιαφέρον της πλειονότητας των αστυνομικών οργάνων και των πολιτών να απευθύνονται σε πιό «απτές» μορφές εγκληματικότητας.

Ειδικότερα,σημαντικότατο πρόβλημα είναι φυσικά και η έλλειψη κατάρτισης των ενασχολουμένων με τέτοιου τύπου εγκλήματα,καθώς ελάχιστοι σήμερα διαθέτουν την απαραίτητη γνώση σχετικά με την πληροφορική τεχνολογία και με τα τεχνικά χαρακτηριστικά και ιδιαιτερότητες του πληροφορικού εγκλήματος.

Η έλλειψη κατάρτισης δεν πλήττει μόνο τις αστυνομικές αλλά και τις δικαστικές Αρχές και τους συνηγόρους των θυμάτων και θυτών.

Οι γοργοί ρυθμοί της πληροφορικής τεχνολογίας είναι φυσικό να δυσκολεύουν ιδιαίτερα τους εφαρμοστές του δικαίου, καθώς μάλιστα αυτή τη στιγμή στην πλειοψηφία τους είναι άτομα, τα οποία έχουν μεγαλώσει χωρίς επαφή με ηλεκτρονικούς υπολογιστές.

Έτσι παρουσιάζουν δυσκολίες στον προσδιορισμό, στην περιγραφή και τον τρόπο δίωξης των hacking περιστατικών. Επίσης σε συνδυασμό με την όχι σπάνια ανεπάρκεια στη νομοθεσία ή και σε ιδιαίτερες περιπτώσεις, όπως στις ΗΠΑ, επικαλυπτόμενη πολιτειακή και ομοσπονδιακή νομοθέτηση, η πλειονότητα των δικαστικών λειτουργών τείνει εκ φύσεως να ερμηνεύει τις σχετικές διατάξεις με βαση παραδοσιακά δεδομένα που συχνά όπως είναι εύκολα αντιληπτό,δεν ανταποκρίνονται και δεν αντιστοιχούν στα δεδομένα του πληροφορικού εγκλήματος.

Και όπως οι νέες μορφές εγκληματικότητας δημιουργούν νέες τεχνικές και λειτουρικές ανάγκες και απαιτήσεις, έτσι «επαναδομούν» και τους ποινικούς νόμους και όρους αλλά και τις παραδοσιακές αντιλήψεις περί σήμανσης και πειστηρίων.

Η μεταπήδηση από ένα περιβάλλον αστυνομικής έρευνας με υλικά, απτά στοιχεία σε ένα σύμπαν με αόρατα ηλεκτρονικά στοιχεία θα μπορούσε να δημιουργήσει ιδιαίτερα προβλήματα σε άτομα συνηθισμένα να εργαζονται με στοιχεία γραμμένα σε χαρτί, όπως υποστηρίζει ο Dan Duncan, εκπαιδευτής στο Federal Law Enforcement Training Centre.

Ο χαρακτήρας του διαδικτύου. που παρουσιάζει μία παγκοσμιότητα αλλά παράλληλα αποτελεί ένα νοητό επίπεδο της κοινωνίας, δημιουργεί πολλά προβλήματα και νομικά ζητήματα κατά την προσπάθεια αντιμετώπισης των hackers.

Κι αυτό διότι τα άτομα αυτά χρησιμοποιώντας διάφορες μεθόδους (weaving,looping), είναι σε θέση να κρύβουν τα ίχνη τους αλλά και να διατρέχουν το διαδίκτυο μέσα από πολλά διαφορετικά συστήματα, τα οποία μπορεί να ελέγχουν παροδικά, ώστε να δημιουργούν εκτός από μία αυτονόητη δυσκολία εντοπισμού της πραγματικής τους τοποθεσίας, πολυ σημαντικά ζητήματα δικαιοδοσίας και έκδοσης, καθώς η νομοθεσία ποικίλει από χώρα σε χώρα.

Είναι πραγματικά άξιο προβληματισμού το ζήτημα επιλογής νομικού πλαισίου αντιμετώπισης ενός hacker που μπορεί να βρίσκεται σε μία χώρα, να επικοινωνεί με έναν παροχέα σε δεύτερη χώρα και να επιτίθεται κατά ενός θύματος του σε μία τρίτη χώρα..

Μεγάλο ποσοστό της δραστηριότητας των hackers δε γνωστοποιείται ποτέ και αυτό φυσικά έχει να κάνει με λόγους κύρους ευθιξίας και επαγγελματικής φήμης μεγάλων οργανισμών αλλά και με το πολύ απλό ζήτημα οτι δε γίνονται πάντοτε αντιληπτές οι επιθέσεις.

Συνεπώς το πληροφορικό έγκλημα γίνεται ακόμη πιό δύσκολα αντιμετωπίσιμο καθώς τα θύματα δεν το αναφέρουν στην πλειοψηφία των περιπτώσεων.

Ειδικά για τις μεγάλες εταιρίες, συχνά η ζημία του hacker είναι πολύ μικρότερη από τις απώλειες που θα υποστεί από την αρνητική δημοσιότητα και τη δυνητική απώλεια πελατών εξ αυτού του λόγου. Δεν έχουν εμπιστοσύνη στη αστυνομία για την ορθή αντιμετώπιση του προβλήματος και συχνά θεωρούν τη συμβολή τους αναποτελεσματική.

Ένα 65% του δείγματος έρευνας που διεξήχθη από το Computer Security Institute σε εταιρίες, ανέφερε οτι ο φόβος αρνητικής δημοσιότητας αποθάρρυνε από το να αναφέρει την εισβολή, ενώ ένα εντυπωσιακό 83% ανέφεραν οτι δεν απευθύνθηκαν καν στην αστυνομία, όταν έπεσαν θύματα πληροφορικού εγκλήματος.

Με τόσο ελλιπή ενημέρωση λοιπόν, είναι φυσικό να μην είναι δυνατή η αποτελεσματική αντιμετώπιση του φαινομένου, ενώ πολλές φορές οι πολυεθνικές φτάνουν αφού αποκρύψουν την εισβολή να επικοινωνούν με τον hacker και να τον στρατολογούν στις τάξεις τους, ώστε να έχουν το

προβάδισμα στον ανταγωνισμό και την εμπορική κατασκοπεία. Επιλογικά θα μπορούσαμε να κάνουμε μία αναφορά και σε επιμέρους στοιχεία που ενισχύουν τη δυσκολία ανακάλυψης και καταπολέμησης των hackers, όπως για παράδειγμα η ευκολία με την οποία είναι εφικτή η καταστροφή και εξαφάνιση κάθε στοιχείου του εγκλήματος ή η πραγματοποίηση του εγκλήματος μετά από ικανό χρονικό διάστημα ώστε να χαθούν τα όποια ίχνη και φυσικά για τις νέες μεθόδους κρυπτογράφησης και κωδικοποίησης όπου η ψηφιακή πληροφορία μετατρέπεται σε άλλη μορφή μέσω ψηφιακού αλγορίθμου, ο οποίος δεν είναι αποκωδικοποιήσιμος χωρίς το συνθηματικό.

Συμπληρώνοντας και αυτό το κεφάλαιο ουσιαστικά κλείνουμε και με τα θεωρητικά ζητήματα που θα αποτελέσουν αντικείμενο αυτής της εργασίας.

Κρίνεται σκόπιμο όμως να εξεταστούν τόσο τα μέσα και οι τρόποι που χρησιμοποιούνται από τους hackers για την επιτέλεση των σκοπών τους, όσο και μερικά περιστατικά στην πορεία του hacking που αποτέλεσαν σημαντικά γεγονότα και στιγμάτησαν τη δράση τους.

8.8 **Είδη, μεθοδολογία και περιπτώσεις επιθέσεων**

Είδη επιθέσεων

1)Απόκτηση πρόσβασης σε ένα σύστημα υπολογιστή/ών με το «σπάσιμο» του κωδικού χρήσης

2)Καταστροφή - διαγραφή στοιχείων και κλοπή εμπιστευτικών αρχείων και πληροφοριών

3)Απόκτηση ελέγχου συστήματος και μεταβολή δεδομένων πρόσβασης με σκοπό τον αποκλεισμό χρηστών

4)Χρησιμοποίηση – διαχείρηση ενός συστήματος υπολογιστή/ών για αποστολή δεδομένων σε τρίτο σύστημα

5) Παρεμπόδιση ομαλής λειτουργίας συστήματος με την επιβολή πρόσθετων εργασιών ή με την υπερφόρτωση με υπερβολικές ποσότητες δεδομένων.

.

Εργαλεία του επαγγέλματος

Denial of service (DoS attack): οι hackers τρέχουν πολλαπλά προγράμματα με αυτοματοποιημένη αποστολή μηνυμάτων και εντολών τα οποία βομβαρδίζουν το δίκτυο με δεδομένα και έτσι το υπερφορτώνουν ώστε να αδυνατεί να ανταποκριθεί.

- **Distributed denial of service (DDoS attack):**

Οι hackers με τη χρήση δουρείων ίππων αποκτούν τον έλεγχο πολλών υπολογιστών ανυποψίαστων χρηστών.Σε μία δεδομένη στιγμή συντονίζουν όλους τους υπολογιστές να απαιτήσουν δεδομένα και υπηρεσίες από ένα συγκεκριμένο σύστημα, το οποίο και φυσικά μετά από την υπερβολική ζήτηση που αντιμετωπίζει, καταρρέει.

- **DNS Spoofing:**

Στην περίπτωση αυτή ο hacker τροποποιεί το Domain Name Code το οποίο είναι η αριθμιτική, δυαδικά ψηφιοποιημένη διεύθυνση του site, έτσι ώστε να την αντιλαμβάνεται και ο υπολογιστής και να ανταποκρίνεται στην εντολή.

Οπότε οι χρήστες ζητώντας μία ιστοσελίδα με αλλοιωμένη την αριθμιτική της διεύθυνση (numerical address), θα βρεθούν σε άλλη ιστοσελίδα αυτόματα.

Αυτό μπορεί να σημαίνει απώλεια εσόδων για την ιστοσελίδα που δεν κατόρθωσε να επισκευθεί ο χρήστης τελικά αλλά και με τη δημιουργία ενός ακριβούς αντιγράφου κάποιας ιστοσελίδας (mirror site) να εκμαιεύσει ο hacker ευαίσθητα προσωπικά δεδομένα που ο χρήστης πιστύει οτι δίνει στην αληθινή ιστοσελίδα που ζήτησε

- **Packet Sniffers:**

Στην ουσία είναι προγράμματα που επιτρέπουν στο χρήστη να προσλαμβάνει και να ερμηνεύει πακέτα πληροφοριών που διακινούνται στο διαδίκτυο.

Κάθε πληροφορία που κοινοποιείται σε ένα δίκτυο υπολογιστών (όνομα χρήστη, κωδικός εισόδου, e-mail κλπ.) μεταφράζεται σε πακέτα, τα οποία στέλλονται στο δίκτυο.Το Internet λειτουργεί κυρίως με το Ethernet πρωτόκολλο μετάδοσης.

Όταν λοιπόν κάποιος στείλει ένα πακέτο στο Ethernet, κάθε μηχάνημα στο δίκτυο βλέπει το πακέτο. Κάθε πακέτο που αποστέλλεται μέσω διαδικτύου έχει μία Ethernet κεφαλή-μία αριθμητική διεύθυνση, ώστε να είναι βέβαιο οτι η σωστή μηχανή παίρνει τη σωστή πληροφορία. Κάθε μηχάνημα υποτίθεται οτι εντοπίζει τα πακέτα δεδομένων με τη δική της διεύθυνση.

Όμως το Ethernet packet sniffer είναι λογισμικό που επιτρέπει στο hacker ή το διαχειριστή του δικτύου κανονικά να υποκλέπτει πληροφορίες, οι οποίες δεν προορίζονται για τη διεύθυνσή του.

Δούρειοι Ίπποι:

Τα προγράμματα αυτά είναι κερκόπορτες σε ένα σύστημα υπολογιστή. Ο hacker μεταμφιέζει τον ίππο σε ένα άλλο πρόγραμμα, όπως για παράδειγμα παιχνίδι, ώστε να ξεγελαστεί ο χρήστης και να κατεβάσει και να εγκαταστήσει το πρόγραμμα. Μόλις ο ίππος εγκατασταθεί στον υπολογιστή του θύματος, ο hacker αποκτά πρόσβαση στο σκληρό δίσκο ή στο e-mail του χρήστη.

Κρύβοντας προγράμματα ώστε να τρέξουν αργότερα ο hacker μπορεί να αποκτήσει πρόσβαση και σε άλλα συστήματα ή και να πραγματοποιήσει DDoS επιθέσεις.

Ο απλούστερος ίππος αντικαθιστά τα μηνύματα που εμφανίζονται όταν ζητείται ένα συνθηματικό από τον χρήστη. Οι χρήστες παρέχουν τα ονόματα χρήστη και κωδικούς πρόσβασης θεωρώντας οτι συνδέονται στο σύστημα, ενώ στην ουσία αυτά καταγράφονται από τον ίππο προς χρήση του hacker.

Ο διασημότερος ίππος είναι ο Black Orifice που δημιουργήθηκε από το hacker group: Cult of the Dead Cow και που προσφέρει πρόσβαση και έλεγχο σε καθε προσωπικό υπολογιστή που λειτουργεί με το λειτουργικό

σύστημα Windows 95/98 και επόμενα, εκμεταλλευόμενο ένα ελάττωμα σε ένα πρόγραμμα για αποστολή e-mail.

Ιοί και σκουλήκια:

Τα σκουλήκια και οι ιοί είναι αυτοαναπαραγόμενα προγράμματα, τα οποία μπορούν να εξαπλώνονται σε ευρεία κλίμακα σε όλο το διαδίκτυο.Συνήθως οδηγούν στην καταστροφή και δυσλειτουργία συστημάτων και αρχείων.

Τα σκουλήκια αντιγράφονται από υπολογιστή σε υπολογιστή χωρίς να απαιτούν τη συμβολή κανενός άλλου προγράμματος ή αρχείου.

Το διασημότερο σκουλήκι ILOVEYOU υπολογίζεται οτι επηρέασε περίπου 45 εκατ. υπολογιστές.

8.9 **Τα πιό σημαντικά περιστατικά hacking**

Οι περιπτώσεις εδώ έχουν κάτι κοινό. Καθεμία από αυτές σηματοδοτεί και μία σημαντική εξέλιξη στην πορεία του hacking.

Το 1988, ένας 23χρονος απόφοιτος του Κορνέλ, δημιούργησε το πρώτο «σκουλήκι». Έγραψε 99 γραμμές κώδικα και το ελευθέρωσε στο δίκτυο πειραματικά. Πολλοί υπολογιστές κατέρρευσαν. Για να περιοριστεί η διάδοση της επιδημίας, πολλά δίκτυα αναγκάστηκαν να αποσυνδεθούν από το διαδίκτυο.

Το 1990, Ο Μόρρις καταδικάστηκε σε 400 ώρες κοινωνικής υπηρεσίας και 10,000 δολλάρια πρόστιμο. Μολονότι ο Morris επέμεινε οτι δεν είχε πρόθεση να προξενήσει ζημίες σε δίκτυα, παραδέχτηκε οτι επεδίωκε να αποκτήσει πρόσβαση στα «μολυσμένα συστήματα» και έτσι βρέθηκε ένοχος υπό το νόμο Computer Fraud & Abuse Act του 1986, για μη εγκεκριμένη πρόσβαση σε υπολογιστή κυβερνητικού ενδιαφέροντος, δηλαδή υπολογιστές που χειρίζεται αποκλειστικά η ομοσπονδιακή κυβέρνηση ή οικονομικά ιδρύματα.

Ένα διεθνές δίκτυο,οι «Phonemasters», εισέβαλαν στα δίκτυα των εταιριών MCI WorldCom, Sprint, AT&T,και Equifax..

Το FBI εκτιμά οτι η συμμορία προξένησε απώλειες του ποσού του 1.85 εκατ. δολλαρίων.

Οι Phonemasters αναφέρεται οτι προώθησαν μία γραμμή του FBI σε μία sex-chat γραμμή, δημιουργώντας λογαριασμούς γύρω στα 200,000 δολλάρια. Εισέβαλαν σε αρχεία του FBI για να ανακαλύψουν ποίων τα τηλέφωνα παρακολουθούνταν από τη Δίωξη Ναρκωτικών. Εισέβαλαν στα συστήματα διαφόρων εταιριών και «κατέβασαν» νούμερα από τηλεκάρτες και προσωπικά δεδομένα πελατών και δημιούργησαν τηλεφωνικούς αριθμούς για δική τους χρήση.

Το Σεπτέμβρη του 1999 μέλη του δικτύου αυτού καταδικάστηκαν για κλοπή, κατοχή συσκευών γιά μη εξουσιοδοτημένη είσοδο σε δίκτυα και σε κυβερνητικούς υπολογιστές. Ο υποτιθέμενος εγκέφαλος Lindsly καταδικάστηκε σε 41 μήνες φυλάκιση, μία από τις πιό αυστηρές ποινές για hacker στην Αμερική.

Η υπόθεση των Phonemasters είναι η πρώτη όπου ο τίτλος III της Omnibus Crime Control and Safe Streets Act του 1968, αρχικά προορισμένος να επιτρέπει στις Αρχές να παρακολουθούν καλωδιακές και προφορικές επικοινωνίες, ερμηνεύθηκε έτσι, ώστε να επιτρέπει την τοποθέτηση «κοριού δεδομένων» σε ένα δίκτυο υπολογιστών.

Η υπόθεση Citibank στιγμάτησε την κοινότητα των hackers. Το 1994, ο Ρώσος hacker Vladimir Levin οργάνωσε μία κλοπή, κάνοντας τους υπολογιστές της εταιρίας να διανείμουν περίπου 10 εκατ. δολλάρια στον ίδιο και τους συνεργούς του σε 7 διαφορετικές χώρες.

Όταν ο Levin δήλωσε ένοχος το Γενάρη του 1998, παραδέχτηκε οτι χρησιμοποίησε κλεμμένους κωδικούς από πελάτες της Citibank για να μεταφέρει χρήματα στους λογαριασμούς του.

Ενώ οι εκπρόσωποι της Citibank υπόστήριξαν οτι ο Levin απέκτησε πρόσβαση στο σύστημα διαχείρισης ρευστού της εταιρίας μέσω έγκυρων λογαριασμών που δεν ήταν κωδικοποιημένοι, υπάρχει η φήμη οτι κάποιος μέσα από την εταιρία ήταν συνεργός του. Η Citibank όμως το αρνείται.

Η Citibank κατάφερε να ανακτήσει τα περισσότερα χρήματα. Ο Levin δήλωσε ένοχος σε κατηγορίες συνομωσίας για τραπεζική απάτη και απάτη

με υπολογιστές. Το Φεβρουάριο του 1998 ο Levin καταδικάστηκε σε 3 έτη φυλάκιση και υποχρέωση αποζημίωσης της Citibank 240,000 δολλαρίων.

Το Μάιο του 2000,ο Timothy Lloyd κατάδικαστηκε οτι έγραψε 6 γραμμές κωδικού,στην ουσία μία βόμβα κωδικό, η οποία αφάνισε τα προγράμματα σχεδιασμού και παραγωγής της Omega Engineering Corporation. Η βόμβα ήταν προορισμένη να πυροδοτηθεί στις 31 Ιουλίου του 1996.

Με την είσοδό του στο σύστημα, ο υπάλληλος αυτός απελευθέρωσε τον κωδικό που έδωσε εντολή να σβηστούν τα προγράμματα παραγωγής της Omega. Η μυστική υπηρεσία δήλωσε οτι ο Lloyd είχε διαπράξει τη μεγαλύτερη πράξη computer sabotage,προξενώντας στην Omega σχεδόν 10 εκατ. δολλάρια σε απώλειες πωλήσεων.

Μετά το «σκουλήκι» Morris το σημαντικότερο αντίστοιχο φαινόμενο των επομένων ετών υπήρξε ο Melissa. Οι ζημίες υπολογίζονται περί τα 400 εκατ. δολλάρια. Αποτέλεσε επίσης σημαντικό γεγονός και διότι ο Melissa ήταν το πρώτο περιστατικό τετοίου τύπου που έπληξε το εμπορικό Internet.

Τα πρώτα στοιχεία του Melissa βρέθηκαν σε μία δημοσίευση στο alt.sex newsgroup από ένα AOL e-mail.Ένας AOL server υπήρξε αγωγός γιά τον ιό, ο οποίος εμπεριέχετο σε ένα αρχείο ονόματι «list.zip.» Τα θύματα που περίμεναν το list.zip να περιέχει μία λίστα από ιστοσελίδες σεξουαλικού περιεχομένου μαζί με τα ονόματα χρήστη και τους κωδικούς, κατέβαζαν και έτρεχαν το πρόγραμμα.

Με τον τρόπο αυτό γίνονταν και οι ίδιοι κοινωνοί του ιού. Το Δεκέμβρη του 1999, ο δημιουργός δήλωσε ένοχος γιά δημιουργία και κυκλοφορία καταστροφικού και ζημιογόνου ιού και συμφώνησε οτι προκάλεσε περίπου 80 εκατ. δολλάρια ζημίες.Εξέτισε και 5 χρονια φυλάκισης.

Το Φεβρουάριο του 2000, μερικά από τα πιό αξιόπιστα sites έγιναν σχεδόν μη προσβάσιμα από μία συντονισμένη επίθεση άρνησης εξυπηρέτησης [distributed denial-of-service (DDoS) attacks].Το Yahoo δέχθηκε το πρώτο χτύπημα το Φεβρουάριο του 2000. Μερικές ημέρες αργότερα τοι ιστοσελίδες , Buy.com, eBay, CNN, Amazon.com, ZDNet.com, E*Trade, και Excite κατέρρευσαν από DDoS επιθέσεις.

Οι εκτιμήσεις ζημιών ποικίλουν με το FBI να υπολογίζει οτι οι εταιρίες είχαν απώλειες της τάξης των 1.7 δις. Δολλαρίων.

Στις 18 Απριλίου του 2000 ένας νεαρός από τον Καναδά, γνωστός στο διαδίκτυο με το ψευδώνυμο "mafiaboy," συνελήφθη ως σχετιζόμενος με τις εν λόγω επιθέσεις. Οι Αρχές ισχυρίστηκαν οτι εισέβαλε σε πολλούς υπολογιστές, κυρίως αμερικανικών πανεπιστημίων και χρησιμοποίησε τα δίκτυα αυτά για να εξαπολύσει τις επιθέσεις του στα sites αυτά.

Σύμφωνα με την αστυνομία ο mafiaboy υπερηφανευόταν για την επίτευξη των επιθέσεων σε διάφορα Chat rooms και έτσι εντοπίστηκε. Τον Ιανουάριο του 2001 ο 16χρονος hacker ομολόγησε ένοχος σε 56 κατηγορίες,όπως απάτη και παράνομη χρήση δικτύου υπολογιστών.

Συμπερασματικά μπορούμε να αναφέρουμε ότι δεν είναι εφικτό να γίνει ένας διαχωρισμός εύκολα ως προς το κατά πόσο οι hackers είναι πληγή του κοινωνικού γίγνεσθαι, μία καταστροφική, ασυνείδητη κολλεκτίβα ή μία νέα ανερχόμενη δύναμη, ένας επαναστατικός άνεμος που μέσα από ένα νεόσυσταθέν σχετικά επικοινωνιακό μέσο και εργαλείο κοινωνικής αλληλεπίδρασης προσπαθεί να σταθεί εμπόδιο στις σύγχρονες αυταρχικές τάσεις που ζώνουν την ανθρώπινη καθημερινότητα.

Η ουσία είναι οτι το hacking είναι σαν το μαχαίρι: μπορεί να μας βοηθήσει να τραφούμε, να επιβιώσουμε και να εξελιχθούμε ή να σκοτώσουμε και να σκοτωθούμε. Τη διαφορά θα την κάνει η επιλογή μας και όχι το εργαλείο.

Αυτό υπάρχει και δεν είναι δυνατό να πάψει να υφίσταται.

Και ας μην ξεχνάμε οτι η επανάσταση είναι μία οριακή κατάσταση και πολλές φορές τα όρια, είτε λόγω ζήλου, είτε από σκοπιμότητα καταπατούνται μέσα στην πραγματοποίησή της.

Σκοπός δεν πρέπει να είναι η καταδίκη της επανάστασης, λόγω των φανατικών μελών της και των πράξεών τους, αλλά η συλλογική εκατέρωθεν προσπάθεια για αποπομπή των εγκληματικών και ανήθικων στοιχείων και η συνειδητοποίηση, διατύπωση και θεμελίωση των αποκτημάτων αυτής της αντίδρασης.

9 ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

Η επέλευση της ψηφιακής εποχής συνοδεύτηκε από την έντονη αμφισβήτηση του θεσμού της πνευματικής ιδιοκτησίας.

Ωστόσο, η πρόοδος και η εξέλιξη του πολιτισμού είναι συνυφασμένη με την πνευματική δημιουργία. Η πνευματική ιδιοκτησία αποτελεί το πιο παραδεκτό σύστημα χρηματοδότησης της πνευματικής δημιουργίας, γιατί παρέχει στο δημιουργό τις βασικές προϋποθέσεις κάλυψης των βιοτικών του αναγκών, εξασφαλίζοντάς του τη δυνατότητα παραγωγής έργων μακριά από εξωτερικούς αναγκασμούς και παρεμβάσεις.

Ο σεβασμός των δικαιωμάτων των δικαιούχων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων επιβάλλεται αν θέλουμε η πολιτιστική παραγωγή της χώρας μας να συνεχίσει να αναπτύσσεται.

Στο δίκαιο υφίστανται οι ασφαλιστικές δικλείδες προστασίας των χρηστών απέναντι σε ενδεχόμενη κατάχρηση των δικαιωμάτων πνευματικής ιδιοκτησίας.

Ίσως δεν είναι υπερβολή να πούμε ότι η Ελλάδα αυτή τη στιγμή παρουσιάζει την εικόνα ενός βασίλειου της πειρατείας, όπου παραβιάζονται συστηματικά και κατ' εξακολούθηση κάθε είδους πνευματικά δικαιώματα με προεξάρχοντα αυτά που αφορούν τα προγράμματα ηλεκτρονικών υπολογιστών, τα μουσικά έργα, τα τηλεοπτικά προγράμματα και τα εκπαιδευτικά βιβλία ξένων γλωσσών.

Κι αυτό συμβαίνει παρά το γεγονός ότι η χώρα μας έχει υπογράψει τις περισσότερες από τις διεθνείς συνθήκες για την προστασία της πνευματικής ιδιοκτησίας και μολονότι η εθνική της νομοθεσία περιλαμβάνει έναν σχετικά σύγχρονο νόμο πλαίσιο περί πνευματικής ιδιοκτησίας.

Ορισμός πνευματικού δικαιώματος

Πνευματικό Δικαίωμα ή Πνευματική Ιδιοκτησία αποκτά ο πνευματικός δημιουργός πάνω στο πρωτότυπο έργο του, που περιλαμβάνει:πνευματικότω δημιούργημα λόγου,τέχνης η επιστήμης,που εκφράζεται με οποιαδήποτε μορφή, ιδίως τα γραπτά η προφορικά κείμενα, οι μουσικές συνθέσεις, τα θεατρικά έργα, οι χορογραφίες και οι παντομίμες,τα οπτικοακουστικά έργα,τα έργα των εικαστικών τεχνών, στα οποία πειλαμβάνοται τα σχέδεια, τα έργα ζωγραφικής και γλυπτικής, τα χαρακτικά έργα και οι λιθογραφίες, τα αρχιτεκτονικά έργα, οι φωτογραφίες, τα έργα των εφαρμοσμένων τεχνών, οι εικονογραφήσεις, οι χάρτες, τα τρισδιάστατα έργα που αναφέρονται στη γεωγραφία, την τοπογραφία, την αρχιτεκτονική ή την επιστήμη.

Η πνευματική ιδιοκτησία που αποκτά ο δημιουργός πάνω στο έργο του περιλαμβάνει δύο απόλυτα και αποκλειστικά δικαιώματα:

-Το δικαιώμα της εκμετάλλευσης του έργου(περιουσιακό δικαίωμα)

Η δυνατότητα του πνευματικού δημιουργού από το νόμο να εκχωρήσει/μεταβιβάσει και να αναθέσει τη διαχείρηση του περιουσιακού δικαιώματος του σε τρίτους,φυσικά ή νομικά πρόσωπα.

Ποιες εξουσίες περιλαμβάνει το περιουσιακό δικαίωμα.

- Το δικαίωμα της εγραφής του έργου
- Την αναπαραγωγή του έργου
- Τη μετάφραση του
- Τη διασκευή, την προσαρμογή ή άλλη μετατροπή του
- Την εξουσία διανομής του πρωτότυπου έργου
- Την εισαγωγή αντιτύπων του, που παρήχθησαν στο εξωτερικό
- Την εκμίσθωση και το δημόσιο δανεισμό του

- Τη δημόσια εκτέλεσή του
- Τη ραδιοτηλεοπτική μετάδοσή του
- Την παρουσίασή του στο κοινό ενσυρμάτως, ασυρμάτως ή με οποιονδήποτε άλλο τρόπο (μετάδωση του έργου μέσω διαδικτίου)

-Το δικαίωμα προστασίας του προσωπικού δεσμού με το έργο(ηθικό δικαίωμα)

Το ηθικό δικαίωμα περιλαμβάνει την ηθική εξουσία δημοσίευσης, την εξουσία να αποφασίζει δηλ. αν,πώς,πότε, το έργο θα γίνει προσιτό στο κοινό, την εξουσία αναγνώρισης της πατρότητας πάνω στο έργο και ειδικότερα την εξουσία να μνημονεύεται το όνομά του στα αντίτυπα του έργου του και σε κάθε δημόσια χρήση του ή ακόμα και το δικαίωμα χρήση του ή ακόμα και το δικαίωμα του να κρατάει την ανωνυμία του ή να χρησιμοποιεί ψευδώνυμο.

Η εξουσία του δίνει τη δυνατότητα να απαγορεύει δηλαδή την κάθε παραμόρφωση, περικοπή ή άλλη τροποποίση του έργου.

Το ηθικό δικαίωμα είναι προσωποπαγές και αμεταβίβαστο,παραμένει δε στο δημιουργό ακόμα και μετά τη μεταβίβαση του περιουσιακού δικαιώματος.

9.1 **Πειρατεία**

Μεσώ της τεχνολογίας κάθε μέσος άνθρωπος μπορεί να είναι εκδότης πνευματικού έργου ή να παράγει τέλεια αντίτυπα από πνευματικά έργα καταβάλλοντας μόνο ένα μικρό κόστος.

Πρόκειται για μία επανάσταση ανάλογη της τυπογραφίας. Όταν ανακαλύφθηκε η τυπογραφία έγινε δυνατό οι εκδότες να τυπώσουν και να διαθέσουν βιβλία.

Σήμερα είναι δυνατόν να γίνουμε όλοι εκδότες της δουλειάς μας ή να αναπαράγουμε αντίτυπα πνευματικής εργασίας. Κάθε υπολογιστής δίνει απεριόριστες δυνατότητες στη διαχείριση πνευματικού έργου, όχι μόνο όταν αυτό αφορά κείμενο, αλλά και στην περίπτωση εικόνας, ήχου, κινηματογράφου.

Για έναν μουσικό για παράδειγμα, ο υπολογιστής μπορεί να γίνει ολοκληρωμένο στούντιο ηχογραφήσεων. Για τον ακροατή μουσικής μπορεί να γίνει το μέσο με το οποίο θα αντιγράφει μουσική χωρίς να πληρώνει δικαιώματα.

Οι μουσικοί πλέον δεν εξαρτώνται από πανάκριβα στούντιο Α και τις εταιρίες που αυτά ανήκουν για να εκδώσουν τη δουλειά τους, και ο ακροατής δεν εξαρτάται από αυτές τις εταιρίες για να αποκτήσει μία ηχογράφηση. Μπορεί έτσι να συμμετέχει ο καθένας σε αυτή τη μικρή επανάσταση που τελικά θα γίνει μεγάλη επιφέροντας την κατάργηση των πνευματικών δικαιωμάτων.

Οι τεράστιες δυνατότητες επικοινωνίας των υπολογιστών μέσω δικτύου είναι ίσως η δυνατότητα κλειδί στην επανάσταση αυτή. Οι αποστάσεις εκμηδενίζονται στην ελεύθερη ανταλλαγή και διάδοση πνευματικού έργου ακόμα και μεταξύ αγνώστων μεταξύ τους ανθρώπων (με λογισμικό τύπου napster).

Σε αυτόν τον τρόπο διάδοσης είναι αδύνατο να ευνοηθούν κάποιοι «αστέρες» της τέχνης, γιατί κανένας επιχειρηματίας δεν αποκτά κάποιο όφελος από μια ευνοϊκή τους μεταχείριση.

Έργα πολιτισμού, ιδέες, γνώσεις εξαπλώνονται ταχύτατα. Όσο και αν φαίνεται περίεργο εταιρίες λογισμικού είναι οι πρώτες ωφελούμενες από την πειρατεία, μιας και δυσκολεύει τη δημιουργία μονοπωλίων, τα οποία θα έπνιγαν τη πλειοψηφία των προγραμματιστών.

Η ισχύς του νόμου για τα πνευματικά δικαιώματα πρέπει να συνεχίσει να υπάρχει μόνο σε περίπτωση εκμετάλλευσης πνευματικού έργου με σκοπό απόκτηση κέρδους ή προβολής. Εκεί δεν μπορεί και δεν πρέπει ίσως να καταργηθεί.

Απλώς πρέπει όπως είπαμε να μειωθεί δραστικά το διάστημα που απαιτείται για να γίνει κτήμα της κοινωνίας ένα έργο. Κάθε ένας όμως που δεν αποκομίζει πλούτο και δόξα από χρήση πνευματικού έργου δεν θα οφείλει αντίτιμο για τη χρήση του, διότι όπως είπαμε, οι ιδέες και το πνεύμα είναι δωρεάν, άρα λοιπόν δεν είναι δυνατή η κοστολόγησή τους στην περίπτωση που δεν αποφέρουν κέρδος.

Προτάσεις

Πρέπει να αντιγράφουμε ελεύθερα ότι υλικό έχουμε για φίλους, για γνωστούς ακόμα και για αγνώστους. Αν όμως κάποιος είναι ιδιοκτήτης disco, θα πρέπει να αγοράζει cd από το εμπόριο. Δεν είναι σωστό να παίζει μουσική με αντεγραμένα μέσα. Μπορεί βέβαια να αντιγράφει τα ήδη αγορασμένα και να τα διαδίδει σε όσους θέλει.

Ένας ιδιοκτήτης εργοστασίου πρέπει να πληρώσει για κάθε πρόγραμμα που τρέχει σε υπολογιστές της επιχείρησής του, όπως πρέπει να είναι πληρωμένο το λογισμικό που χρησιμοποιούν τα net-cafe και οι διαφημιστές.

Είναι δε ιδιαίτερα χαλαροί οι έλεγχοι για τέτοιες περιπτώσεις, κι αυτό είναι κάτι που πρέπει να διορθωθεί. Ένας μαθητής ή φοιτητής όμως που μαθαίνει ή διασκεδάζει από προσωπική χρήση της τεχνολογίας, δεν πρέπει να χρεώνεται. Προσοχή όμως: ούτε εκείνος όμως πρέπει να χρεώνει τους άλλους όταν τους προσφέρει έργα σε ψηφιακή μορφή.

Τότε γινόμαστε πολύ χειρότεροι από τις μεγάλες εταιρίες και τα μονοπώλια γιατί χρεώνουμε εργασία άλλων, που αντιγράψαμε με τεχνολογία άλλων!

Η μόνη δικαιολογία για κάποια μικρή χρέωση σε αυτή την περίπτωση είναι το ρίσκο της σύλληψης από την αστυνομία. Πέρα από την δημιουργία κόμβων ελεύθερης διάδοσης πολιτισμού, μπορούμε να συμμετέχουμε στην αθόρυβη επανάσταση και με άλλους τρόπους.

Στην ψηφιοποίηση έργων που δεν έχουν ακόμη ψηφιοποιηθεί Έχει ήδη ξεκινήσει στο διαδύκτιο μία προσπάθεια καταγραφής λογοτεχνικών και φιλοσοφικών έργων σε ψηφιακή μορφή με σκοπό την ελεύθερη διάδοσή τους ως προϊόντα της παγκόσμιας πολιτιστικής κληρονομιάς.

Το καταπληκτικό αυτό project πολύ σοφά ονομάστηκε «Guttenberg».

Θα μπορούσαν να εξαιρεθούν από το έργο της πειρατείας έργα που γράφτηκαν σε χρόνο μικρότερο από 4 χρόνια πριν. Βέβαια σε εξαιρετικά πλούσιους δημιουργούς (βλέπε Madonna, Bill Gates, κλπ) είναι ανούσιο να περιμένουμε αυτά τα 4 χρόνια.

Γενικώς κάθε ένας που αντιγράφει χωρίς να πληρώνει πνευματικά δικαιώματα πρέπει να λειτουργεί κατά συνείδηση. Ο νόμος μπορεί να θέτει κάποια όρια για περιπτώσεις που ήδη αναφέραμε.

Έτσι σιγά θα διαμορφωθεί παγκοσμίως μία νέα νοοτροπία στην οποία θα προσαρμοστεί και ο νόμος. Η αδικία θα εκλείψει από εμάς τους ίδιους αρχικά και στο τέλος θα επισημοποιηθεί η προσπάθειά μας και από το επίσημο κράτος.

Ειδική αναφορά θα πρέπει να γίνει εδώ και στους μικρούς ήρωες αυτής της επανάστασης, που δεν είναι άλλοι από τους hackers. Μέσα σε αυτούς υπάρχουν κάποιοι οι οποίοι διαδίδουν ιούς, καταστρέφουν συστήματα, κλέβουν περιουσίες, παρακολουθούν αδιάκριτα ανυποψίαστους χρήστες υπολογιστών.

Αυτές είναι σίγουρα κατακριτέες πράξεις. Δε μιλούμε εδώ όμως γι αυτούς. Εννοούμε αυτούς που απομακρύνουν κάθε μορφής προστασία από τα μέσα αποθήκευσης, έτσι ώστε να αντιγράφονται εύκολα. Αυτούς που δημιουργούν δικτυακούς τόπους που βοηθούν στην αντιγραφή, βοηθούν στην κατάργηση στην πράξη των πνευματικών δικαιωμάτων.

Κυρίως αυτοί οι επιστήμονες που εργαζόμενοι συνήθως αθόρυβα σπάνε και τις πιο δύσκολες προστασίες ψηφιακών έργων.

Από τα τελευταία παραδείγματα είναι η περίπτωση του Ρώσου προγραμματιστή που έσπασε το πρότυπο προστασίας ηλεκτρονικού βιβλίου που είχε εφεύρει η adobe και γι αυτό κατέληξε στη φυλακή, το σπάσιμο του υδατόσημου σε μουσικά αρχεία, το θρυλικό πλέον πρόγραμμα DECCS που καταργεί τη προστασία του dvd – υπόθεση για την οποία έπεσαν οι μηνύσεις βροχή.

Είναι πάντως κρίμα το γεγονός ότι η προσπάθεια για την κατάργηση της πειρατείας έχει συνδυαστεί τόσο πολύ με τις κακές πλευρές του hacking που αναφέρθηκαν παραπάνω, με το πορνό και γενικότερα με μια υποκοσμική νοοτροπία.

Είναι πολύ δύσκολο σήμερα να βρει κάποιος ένα site με τρόπους παράκαμψης των πνευματικών δικαιωμάτων το οποίο να μην έχει και πορνοδιαφημίσεις.

Είναι κρίμα ένα σωρό νέα παιδιά να πράττουν πράξεις πειρατείας και να μην ξέρουν ότι κάνουν κάτι καλό και ηθικό. Έτσι νιώθοντας ότι είναι ήδη στο βούρκο, δεν έχουν πρόβλημα να προχωρήσουν σε κάθε μορφής κακή χρήση των γνώσεων που διαθέτουν. Αν όμως από την αρχή ήξεραν ότι η πειρατεία είναι μία πράξη δημοκρατίας και προόδου, πολύ δύσκολα θα τη συνδύαζαν με άλλες δικτυακές «σκανταλιές». Αυτός είναι και ένας από τους στόχους αυτών των σημειώσεων: Να απενοχοποιήσουν μέσα μας την πειρατεία.

9.2 **Τα δίκτυα Peer To Peer (P2P)**

Peer-to-Peer Network	**ΠΕΛΑΤΕΣ**
APH	APH
Blubster	Blubster
Filespree	Filespree
Filetopia	Filetopia
Gnutella	Aqualime,Bearshare,FileNavigator,Freewire,Gnucleus,Limewire,Phex,Shareaza,Xolox ultra
DirectConect	Direct Connect, dc++,MLDonkey,Shakespeer
Edonkey2000	eDonkey2000, emule
Fasttrack	Morpheus, Kazaa, kazza Litem ,Grokster,iMesh
Open Nap	Napster,Shuban,AudioGnone, AudioSwap,CQ EX,File Navigator,Rapigator,Spotlight, StaticNap,SunshineUN,Swaptor,WinMX
Overnet	Overnet,eDonkey2000,MLdonkey
KAD	Emule,MLDonkey,AMule
Piolet	Piolet
Freenetp	Feenet,Entropia,Frost,Freenet

Ένα δίκτυο peer to peer είναι δίκτυο που στηρίζεται περισσότερο στους ίδιους τους συμμετέχοντες σε αυτό, παρά σε ένα κεντρικό εξυπηρετητή (server). Έτσι προκύπτει και η ονομασία του (ίσος προς ίσο). Κάθε χρήστης έχει έναν κόμβο που η τάση είναι να είναι ισότιμοι (δηλαδή να εκτελούν τις ίδιες διαδικασίες και να έχουν πρόσβαση στα ίδια δεδομένα όλοι).

Μια αρχική χρήση των P2P δικτύων είναι συνδέσεις ad hoc – δηλαδή για μια περιορισμένη εφαρμογή. Για παράδειγμα η ανταλλαγή αρχείων όπως ήχου, βίντεο, δεδομένων ή οποιονδήποτε άλλων αρχείων βρίσκονται σε ψηφιακή μορφή. Η βασική αρχή των P2P δικτύων είναι η ισότητα μεταξύ των κόμβων του. Η πληροφορία διαδίδεται μέσα σε αυτό το δίκτυο. Που ακριβώς βρίσκεται αυτή η πληροφορία και πως μπορεί να τη βρει ο χρήστης, είναι που διαφοροποιεί τα p2p δίκτυα μεταξύ τους.

9.2.1 Το napster

Το napster όχι μόνο ήταν το πρώτο p2p που απέκτησε μαζικότητα, αλλά ήταν και η πρώτη μάχη που κέρδισαν οι πολυεθνικές της μουσικής βιομηχανίας ενάντια στα p2p.

Από την αρχή της εμφάνισής του το Napster άρχισε να συλλέγει μηνύσεις (από τη Recording Industry Association of America (RIAA) στις 11/9/1999 και από την A & M Records, Inc στις 2/10/2000). Τελικά μέσα από δίκαστικούς αγώνες που έλαβαν χώρα το 2001 το Napster αναγκάστηκε να κλείσει τον κεντρικό του server, με αποτέλεσμα να διαλυθεί και ολόκληρο το p2p δίκτυο. Ωστόσο όμως «το κακό είχε γίνει».

Η διάδοση του p2p ήταν μια πραγματικότητα για εκατομμύρια χρήστες παγκόσμια, και νέες μορφές p2p επρόκειτω να προκύψουν.

9.2.2 Το Freenet

Το Freenet είναι ένα διαδίκτυο μέσα στο διαδίκτυο. Ξεκίνησε από τη διπλωματική ενός φοιτητή, του πανεπιστημίου του Εδιμβούργου, ονόματι Ian Clark, και ολοκληρώθηκε τον Ιούλη του 1999.

Βασίζεται στην τεχνολογία peer to peer (ίσος προς ίσο, θα μπορούσε να μεταφραστεί).

Στο Freenet επιπλέον, καθένας συνεισφέρει ένα τμήμα της μνήμης του υπολογιστή του όπου αποθηκεύεται μέρος των πληροφοριών του συνολικού δικτύου. Δεν μπορεί όμως να έχει κανέναν έλεγχο στο τι πληροφορίες περιέχει το μέρος της μνήμης που έχει παραχωρήσει στο δίκτυο, ούτε στο τι πληροφορίες δέχεται ή αποστέλλει.

Αυτό εξασφαλίζει και την ανευθυνότητα του κάθε χρήστη του Freenet για τα αρχεία που ανταλλάσσονται μέσω του υπολογιστή του, καθώς και την ανωνυμία του.

Το Freenet είναι ακόμα υπό ανάπτυξη (δεν υπάρχει έκδοση 1.0). Ωστόσο έχει καταφέρει να προκαλέσει αρκετή συζήτηση γύρω από τον εαυτό του ήδη. Σύμφωνα με το SiteSeer (μηχανή αναζήτησης επιστημονικών συγγραμμάτων) η μελέτη για το Freenet εκείνη με τις περισσότερες αναφορές σε επιστημονικές μελέτες για το έτος 2000

Συνοπτική περιγραφή της λειτουργίας του Freenet.

Ο χρήστης μπορεί να εγκαταστήσει το απαιτούμενο λογισμικό που μπορείς να προμηθευτεί δωρεάν από το www.freenetproject.org. Έτσι ο υπολογιστής του χρήστη αποτελεί ένα κόμβο στο Freenet. Κατά τη διαδικασία εγκατάστασης, παραχωρεί στο δίκτυο ένα χώρο από το σκληρό δίσκο του. Όσο μεγάλο ή όσο μικρό επιθυμεί. Όσο πιο πολλή μνήμη παραχωρήσει τόσο πιο γρήγορα θα μπορεί να βρίσκει κάθε φορά τα δεδομένα που θέλει (οι ταχύτητες είναι πολύ πιο αργές από το www- World Wide Web).

Η διαδικασία ανταλλαγής αρχείων μέσω του Freenet έχει ως εξής: Αρχικά ο χρήστης προσθέτει ένα αρχείο δίνοντάς του ένα μοναδικό όνομα-κλειδί. Αντίγραφα του αρχείου διασκορπίζονται στο δίκτυο. Όσο πιο πολλοί ζητάνε αυτό το αρχείο (με το όνομα-κλειδί που του δόθηκε) τόσο πιο πολλά αντίγραφα θα υπάρχουν στο δίκτυο και για τόσο περισσότερο χρόνο. Αντίστοιχα αρχεία που υπάρχουν σε έναν κόμβο θα διαγράφονται αν μένουν για πολύ καιρό στα αζήτητα.

Έτσι τα αρχεία προοδευτικά μαζεύονται σε «γειτονιές» χρηστών όπου είναι πιο χρήσιμα, δηλ. έχουν μεγαλύτερη ζήτηση, και διαγράφονται από περιοχές που δεν ζητούνται. Αυτό διευκολύνει τόσο στην αναζήτησή τους όσο και στο να μην γεμίζουν οι κόμβοι με αρχεία που δε χρησιμοποιούν.

Η αναζήτηση ενός αρχείου γίνεται όπως αναφέραμε με βάση μια λέξη κλειδί. Όταν ένας χρήστης-κόμβος ζητήσει ή απαντήσει στο αίτημα για την απόκτηση ενός αρχείου, μπορεί να επικοινωνήσει άμεσα μόνο με τους γειτονικούς του χρήστες- κόμβους. Οι γειτονικοί με τους γειτονικούς τους κ.ο.κ μέχρι η αναζήτηση να φτάσει στον κόμβο που θα έχει την επιθυμητή πληροφορία και να επιστρέψει μέσα από την αντίστροφη διαδικασία.

Επίσης είναι διαθέσιμοι κατάλογοι που έχουν λίστες διευθύνσεων που πιθανώς να έχουν ακόμα κάποια συγκεκριμένα αρχεία. Σε αυτούς τους καταλόγους εμφανίζεται η περίοδος που έχει περάσει από την τελευταία φορά στην οποία βρέθηκε το αρχείο που παρουσιάζεται ότι περιέχεται σε αυτή τη διεύθυνση.

Όσο πιο πολύ χρησιμοποιείς το Freenet τόσο ο κόμβος σου γίνεται πιο έμπειρος. Αποκτά μια πιο σαφή εικόνα των κοντινών του κόμβων και της πιθανής τοποθεσίας διαφόρων αρχείων. Αυτή η εικόνα καταγράφεται σε ένα πίνακα με πιθανές διευθύνσεις. Έτσι η αναζήτηση αρχείων γίνεται όλο και πιο γρήγορη.

Για παράδειγμα μπορεί κάποιος να ζητήσει αρχικά μια πληροφορία για το πως ταΐζει κανένας ένα χάμστερ. Αν την βρει, αποθηκεύει ποιος κόμβος τον βοήθησε να την βρει. Στην επόμενη αναζήτηση της ίδιας πληροφορίας θα την βρει πιο εύκολα.

Επίσης αν του ζητηθεί ένας οδηγός για να εκπαιδεύσεις ένα χάμστερ θα ψάξει πάλι εκεί, όπου είναι και περισσότερο πιθανό με βάση τα προηγούμενα να υπάρχει τέτοια πληροφορία. Όπως είπαμε ο χρήστης δεν μπορεί να ξέρει τι ψάχνει ή τι έχει ο κόμβος του. Μπορεί ο κόμβος ενός χρήστη να έχει αποθηκευμένο δηλαδή έναν οδηγό εκπαίδευσης χάμστερ, χωρίς να το γνωρίζει ο χρήστης! Επίσης η «γειτονιά» του να μπορεί να είναι μια «γειτονιά» που πολλοί ασχολούνται με χάμστερ, οπότε οι χρήστες

σε αυτή τη γειτονιά θα μπορούν γρήγορα και εύκολα να πάρουν πληροφορίες για τα χάμστερ.

Freenet, μουσική και ταινίες.

Προφανώς μια από τις χρήσεις του Freenet είναι η ανταλλαγή ταινιών και τραγουδιών. Στη «Φιλοσοφία του Freenet» αναφέρεται ότι η επιβολή του copyright, απαιτεί έλεγχο των τηλεπικοινωνιών, πράγμα που αποτελεί ντε φάκτο κατάργηση της ελευθερίας του λόγου.

Απέναντι λοιπόν στην πνευματική ιδιοκτησία της μουσικής ο χλευασμός είναι η απάντηση που δίνουν οι δημιουργοί του Freenet, παραπέμποντας σε τρόπους καλλιτεχνικής δημιουργίας ανεξάρτητους από τις εταιρίες.

Παραπέρα... Freenet 0.7

Το Freenet αποδείχθηκε ένα πολύτιμο εργαλείο επικοινωνίας σε χώρες με έντονη λογοκρισία, όπως η Κίνα. Η αστυνομία του διαδικτύου εκεί δεν μπόρεσε να βρει τον τρόπο να λογοκρίνει τους χρήστες του, οπότε απαγόρεψε την ίδια τη χρήση του.

Αυτό οδήγησε τους εμπνευστές του να κατασκευάσουν ένα p2p δίκτυο όπου να υπάρχει ανωνυμία σε σχέση με τους ίδιους τους συμμετέχοντες σε αυτό. Έτσι ετοιμάζεται μια νέα έκδοση του Freenet, η έκδοση 0.7[8]. Θα είναι ένα darknet.

Αυτό σημαίνει ότι οι χρήστες θα χρησιμοποιούν το ίντερνετ για να συνδέονται σε άλλους χρήστες που γνωρίζουν από πριν και οι οποίοι είναι έμπιστοι (λέγεται αλλιώς και friend to friend). Έτσι κανένας άλλος δε θα ξέρει ότι χρησιμοποιούν το Freenet.

Αυτό θα μπορέσει να βοηθήσει την ανταλλαγή πληροφοριών σε χώρες που απαγορεύεται το Freenet, όπως η Κίνα. Η πρώτη διανομή της έκδοσης 0.7 (η 0.7a) λειτουργεί αυτή τη στιγμή σε πειραματικό στάδιο, αριθμώντας 300-400 κόμβους.

Η σκέψη στην οποία βασίζεται το 0.7 είναι λοιπόν η σχέση μεταξύ έμπιστων κόμβων. Το δίκτυο θα μπορεί να εξαπλώνεται μέσα από την ανταλλαγή ενός cd ή ενός DVD μεταξύ γνωστών. Ωστόσο πάλι, θα μπορέσει να εξαπλωθεί αυτό;

9.2.3 Η σταυροφορία της RIAA ενάντια στους χρήστες του p2p.

Η Recording Industry Association of America (RIAA) βιώνει μια περίοδο έξαλλης συμπεριφοράς. Εξαπολύει νομικές επιθέσεις ενάντια σε ανυποψίαστους Αμερικανούς πολίτες σε ολόκληρη την επικράτεια των ΗΠΑ. Παρά το γεγονός ότι πάνω από 18.000 (που συνεχώς αυξάνονται) μηνύσεις ενάντια σε χρήστες p2p, η ανταλλαγή αρχείων συνεχίζει να αυξάνεται ραγδαία. Εν τω μεταξύ, λάτρεις της μουσικής, όπως η 12χρονη Brianna LaHara, μαθήτρια στο κολέγιο του Cassi Hunt αναγκάζεται να πληρώσει χιλιάδες δολάρια που δεν έχει, για να ικανοποιήσει ένα διακανονισμό με τις μηνύσεις των μελών του RIAA.

Αυτή η παράλογη σταυροφορία δεν αποφέρει ούτε μια δεκάρα στους καλλιτέχνες που η RIAA ισχυρίζεται ότι προστατεύει. Οι καλλιτέχνες των ΗΠΑ σταδιακά αρχίζουν να στρέφονται ενάντια στις μηνύσεις.

9.2.4 Το EFF για τη διαμάχη εταιρειών – p2p

Η επιστολή του Electronic Frontiers Foundation (EFF) στην Ομοσπονδιακή Επιτροπή Εμπορίου είναι μάλλον αποστομωτική για τα επιχειρήματα των πολυεθνικών μουσικής και κινηματογράφου. Απέναντι σε κραυγές που κινδυνολογούν, λέγοντας ότι η διάδοση των δικτύων p2p μπορεί να βλάψει θανάσιμα τις βιομηχανίες του θεάματος παραθέτει μια σειρά από στοιχεία που δείχνουν ότι δεν βασίζονται πουθενά αυτοί οι ισχυρισμοί.

Από τη μια δεν είναι η πρώτη φορά που αυτές οι βιομηχανίες στρέφονται ενάντια στην εξέλιξη της τεχνολογίας. Το ίδιο είχε γίνει και με την επινόηση του VCR (video cassete recorder). Στην αρχή της δεκαετίας του '80 αντιμετωπίστηκε σαν το τέλος της βιομηχανίας του κινηματογράφου. Όπως είναι πλέον γνωστό σε όλους το Hollywood κατάφερε να κάνει τεράστια κέρδη από τα home videos.

Την ίδια στιγμή, η διάδοση του p2p σε μια σειρά από χώρες δείχνει ότι οι πωλήσεις των ιδιοκτητών των copyright όχι μόνο μειώνονται, αλλά αυξάνονται!

Σύμφωνα δε με σχετική έρευνα του Economist η συνολική πτώση των πωλήσεων των CD από τις αρχές του '90δεν έχει να κάνει με την «πειρατεία», αλλά με λόγους όπως η υψηλή τιμή των CD, το γεγονός ότι τα ραδιόφωνα παίζουν συνέχεια τα ίδια και τα ίδια τραγούδια, η είσοδος νέων ανταγωνιστών για τα χρήματα και το χρόνο των καταναλωτών (όπως video games, DVD, Internet), κ.ά.

Παράλληλα τα κέρδη της βιομηχανίας των ταινιών φτάνουν σε ιστορικά μεγάλα ύψη, από έσοδα τόσο σε προβολές, όσο και σε πωλήσεις DVD, χωρίς να αποδεικνύεται πουθενά ότι τα p2p δίκτυα περιορίζουν τη διαδικασία πλουτισμού αυτών των εταιριών.

9.3 Προστασία Ψηφιακών Πνευματικών Δικαιωμάτων

Μιλώντας για Προστασία Ψηφιακών Πνευματικών Δικαιωμάτων, εννοούμε την ανάγκη που έχουν οι εκδότες ηλεκτρονικών περιοδικών και βιβλίων, οι παραγωγοί Διαδικτυακής τηλεόρασης και ραδιοφώνου, εταιρίες μουσικής, δημιουργοί λογισμικού, ηλεκτρονικών πολυμέσων και παιχνιδιών καθώς και business-to-business επιχειρήσεις που δραστηριοποιούνται στο Διαδίκτυο, να ελέγχουν τους τελικούς χρήστες ως προς την χρήση και την πρόσβαση στα πνευματικά τους έργα και να επωφελούνται οικονομικά από αυτές, αλλά και την προστασία των δικαιωμάτων των τελικών χρηστών στην πρόσβαση και χρήση αυτών των πληροφοριών για παραγωγή γνώσης.

Ειδικότερα, η «Διαχείριση Ψηφιακών Πνευματικών Δικαιωμάτων» (Digital Rights Management – DRM) επιχειρεί να ελέγξει την χρήση των Ψηφιακών μέσων με το να απαγορεύει την πρόσβαση, αντιγραφή ή μετατροπή τους από τους τελικούς χρήστες..

Γιατί υπάρχει τέτοιος όρος; Από που προέκυψε η ανάγκη προστασίας;

Το Διαδίκτυο απλοποίησε τη διάθεση ψηφιακού περιεχομένου σε παγκόσμιο επίπεδο.Υποσχέθηκε μείωση του κόστους της υποβιβάζοντας τον ρόλο των μεσαζόντων που παράγουν, διανέμουν και πουλούν φυσικά αντίγραφα.

Η ψηφιακή εποχή όμως δημιούργησε μια «παγίδα» για τους παραγωγούς: Κατέστησε δυνατή την πρόσβαση στο πνευματικό τους έργο από τελικούς καταναλωτές οι οποίοι το χρησιμοποιούν χωρίς να πληρώνουν για αυτό. (Ham, Atkinson, 2003).

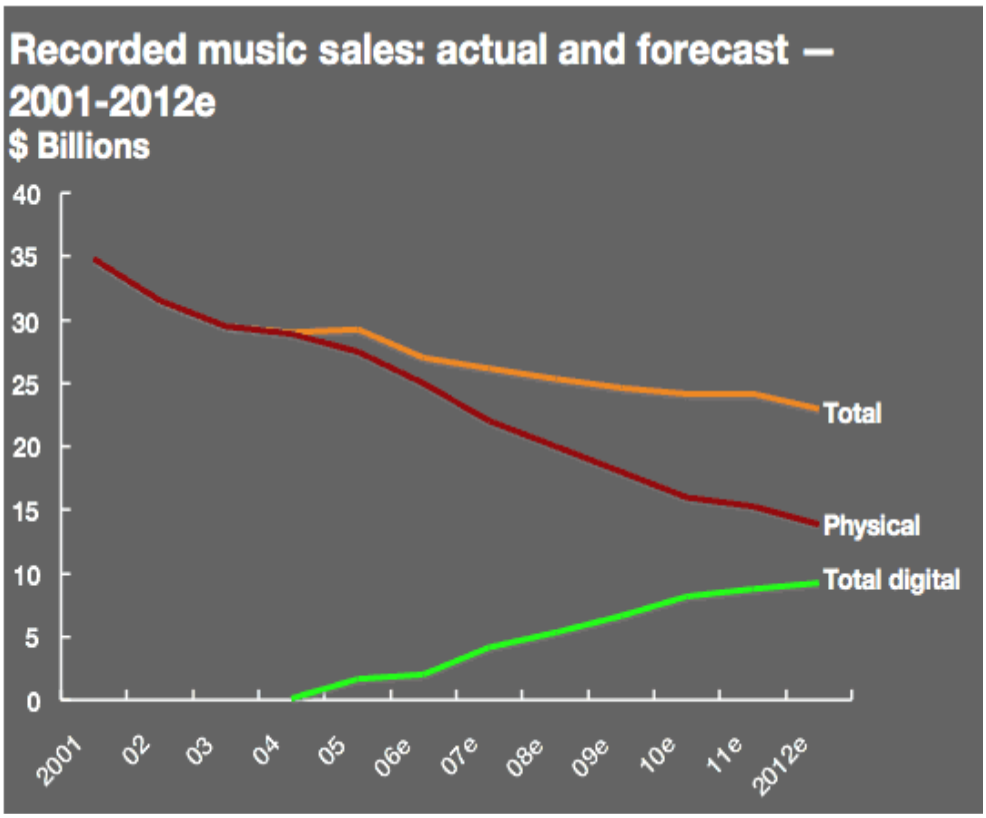
Για να κατανοήσουμε καλύτερα τους λόγους ύπαρξης της Προστασίας Ψηφιακών Πνευματικών Δικαιωμάτων αλλά και την ανάγκη για προστασία, αρκεί να συζητήσουμε για... μουσική! Η κωδικοποίηση αρχείων μουσικής με το πρότυπο mp3 βοήθησε την ταχεία διανομή μουσικών κομματιών μέσω του Διαδικτύου λόγω του μικρού τους μεγέθους.

Μέσα σε μικρό χρονικό διάστημα αναπτύχθηκαν μέθοδοι και τεχνολογίες κωδικοποίησης, αναπαραγωγής και ανταλλαγής μουσικών κομματιών mp3 με ραγδαίους ρυθμούς, τόσο που η εδραίωση των mp3 επηρέασε την οικονομική κατάσταση των δισκογραφικών εταιριών και γενικά του τζίρου της μουσικής βιομηχανίας.

Ο τρόπος που αποκτούμε, ακούμε και ανταλλάζουμε μουσικά κομμάτια άλλαξε ριζικά. Το ποιος επωφελείται και το ποιος ζημιώνει επίσης ανατράπηκε. Ο Όρος «πειρατεία της Μουσικής» εμφανίστηκε για να δώσει την μορφή παρανομίας, ακόμα και εγκληματικότητας στην διαδικασία δωρεάν αναπαραγωγής και διανομής μουσικών κομματιών.

Σε μια έρευνα που πραγματοποίησε η Βρετανική εταιρία δημοσκοπήσεων «Enders Analysis» σχετικά με τις πωλήσεις μουσικής από το 2001 μέχρι της προβλεπόμενες (σημειωμένες με «e» στο διάγραμμα) πωλήσεις μέχρι το 2012, προκύπτει το εξής διάγραμμα:

Διάγραμμα



Τι πρέπει να προστατεύεται, από ποιους και γιατί;

Για να προωθείται και να αναβαθμίζεται η γνώση, πρέπει κανείς να μπορεί να αξιοποιεί την υπάρχουσα, για να κτίζει πάνω της τη νέα, έχοντας τόσο τα οικονομικά μέσα που απαιτούνται όσο και την κατάλληλη υποδομή για να την βρίσκει αλλά και για να την προωθεί.

Άρα, πρέπει με κάποιο τρόπο να βρεθεί κάποιος ή κάτι που να βρίσκεται ανάμεσα στα δύο στρατόπεδα με σημαίες από την μια το κέρδος και από την άλλη την διάδοση της δωρεάν γνώσης και χρήσης, που να προστατεύει αν είναι δυνατόν και τους δύο.

Αυτός ο κάποιος πρέπει να γνωρίζει τις ισχύουσες πρακτικές, τη νομοθεσία, να έχει την απαραίτητη τεχνογνωσία και τα κίνητρα να προωθεί την προστασία των ψηφιακών πνευματικών δικαιωμάτων όπως αυτή περιγράφεται στο παρόν κομμάτι. «Τα προϊόντα εκμετάλλευσης των

πνευματικών δικαιωμάτων, όλοι οι διεθνείς οργανισμοί που ασχολούνται μαζί τους, οι ισχύουσες νομοθεσίες που τους δίνουν ισχύ, οι πολιτικοί και κοινωνικοί μηχανισμοί που τα νομιμοποιούν, πρέπει να οργανωθούν σε ένα χαλαρά οργανωμένο αλλά ισχυρά συνεκτικό υβριδικό δίκτυο για να αντιμετωπίσουν την κατάσταση»

Οι πατέντες λογισμικού

Οι πατέντες λογισμικού συγχέονται αρκετές φορές με το copyright λογισμικού. Κάτω από διεθνείς συνθήκες, όπως του Παγκόσμιου Οργανισμού Εμπορίου, οποιοδήποτε λογισμικό είναι γραμμένο, αυτομάτως καλύπτεται από το copyright. Αυτό επιτρέπει στους ιδιοκτήτες copyright να εμποδίσουν κάποιον άλλον από τον να αντιγράψει τον πηγαίο κώδικα. Δεν είναι ανάγκη να καταχωρήσεις κώδικα για να έχεις προστασία από το copyright.

Αν ωστόσο ένας συγγραφέας πάει να καταχωρήσει πηγαίο κώδικα και ο κώδικας είναι αντιγραμμένος χωρίς άδεια, τότε μπορεί να συλλέξει ποινικές κυρώσεις. Το copyright ισχύει μέχρι 90 χρόνια.

Οι πατέντες λογισμικού είναι ευρέως διαδεδομένες στις ΗΠΑ. Μέχρι το 2004 περίπου 145.000 πατέντες (διπλώματα ευρεσιτεχνίας) είχαν εκδοθεί σε 22 κατηγορίες πατεντών, που καλύπτουν εφαρμογές υπολογιστών. Περίπου 17.000 πατέντες εκδίδονται κάθε χρόνο.

Ένα μεγάλο μέρος αυτών των πατεντών ανατίθεται σε μεγάλες επιχειρήσεις. Η Microsoft για παράδειγμα είχε περίπου 5.000 πατέντες μέχρι τον Απρίλη του 2006. Η IBM αποκτά κάθε χρόνο περίπου 3.000 πατέντες, αν και ένα σημαντικό μέρος αυτών δεν αφορά το λογισμικό.

Τι ακριβώς πατεντάρουν στο λογισμικό;

Οι πατέντες στο λογισμικό καλύπτουν αλγόριθμους και τεχνικές που εφαρμόζονται σε ένα πρόγραμμα. Τα προγράμματα των υπολογιστών αποτελούνται συχνά από χιλιάδες εντολές. Οι αλγόριθμοι και οι τεχνικές είναι διαδικασίες που υλοποιούνται μέσω των εντολών. Είναι ουσιαστικά σκέψεις, λογικές και μαθηματικές. Αυτές οι σκέψεις είναι που πατεντάρονται.

Πρακτικά, όταν το Γραφείο Πατεντών χορηγεί μια πατέντα για έναν αλγόριθμο ή μια τεχνική, λέει στους προγραμματιστές ότι δεν μπορούν να χρησιμοποιήσουν αυτή τη μέθοδο χωρίς την άδεια του ιδιοκτήτη της ιδέας. Είναι σαν κάποιος να πατεντάρει το αυγολέμονο και να μην μπορείς να κάνεις κοτόσουπα χωρίς την άδεια του.

Θεωρητικά μια ιδέα για να πατενταριστεί πρέπει να είναι «μη προφανής». Πρακτικά όχι. Σήμερα μια σειρά από συνήθειες στο διαδίκτυο είναι πατενταρισμένες στις ΗΠΑ.

Για παράδειγμα η αγορά ενός λογισμικού μέσω διαδικτύου (Patent No 4,949,257), το ίδιο το ηλεκτρονικό εμπόριο (Patent No. 5,715,314). Πατενταρισμένη είναι και η «ιδέα» η αυτόματη διόρθωση σε ένα κείμενο να ξεκινάει όταν πατήσεις το space, όταν θα έχεις τελειώσει την πληκτρολόγηση της λέξης – από την XyQuest. Οι πατέντες λογισμικού διαρκούν 20 χρόνια.

9.3.1 Τεχνικές μέθοδοι και μέτρα προστασίας

Στη διεθνή βιβλιογραφία συναντάται ο όρος «Technical Protection Measures» (TPM), δηλαδή «Τεχνικά Μέτρα Προστασίας». Αυτός ο όρος αναφέρεται στις τεχνολογίες που ελέγχουν ή/και περιορίζουν τη χρήση και την πρόσβαση σε ψηφιακό περιεχόμενο σε συσκευές που έχουν εγκατεστημένες αυτές τις τεχνολογίες.

Επιπρόσθετα, το DRM (Digital Rights Management), η Διαχείριση Ψηφιακών Δικαιωμάτων βασίζεται στο TPM για να υλοποιήσει αυτούς τους ελέγχους και τους περιορισμούς. (Fact Sheet, 2006).

Τα TPM συχνά κατηγοριοποιούνται βάσει των λειτουργιών τους. Μια συχνά χρησιμοποιούμενη διάκριση συχνά γίνεται μεταξύ των TPM που ελέγχουν την πρόσβαση σε ψηφιακά πνευματικά έργα και αυτών που ελέγχουν τη χρήση των έργων.

Τεχνικά μέτρα προστασίας ελέγχου πρόσβασης

Η πρώτη κατηγορία χρησιμοποιείται για να αποτρέψει μη εξουσιοδοτημένα άτομα από το να έχουν πρόσβαση σε ψηφιακά πνευματικά έργα λειτουργώντας ως νοητή-ψηφιακή κλειδαριά (Fact Sheet, 2006). Για να «κλειδώνεται» και να «ξεκλειδώνεται» ένα ψηφιακόπνευματικό έργο, συχνά χρησιμοποιούνται κωδικοί πρόσβασης και κρυπτογραφία.

Κρυπτογραφία

Η κρυπτογραφία είναι η επιστήμη της κρυπτογράφησης και της αποκρυπτογράφησης. Η κρυπτογράφηση είναι η κωδικοποίηση απλού κειμένου σε μια μη αναγνώσιμη και μη επεξεργάσιμη μορφή από όσους δεν κατέχουν τον κώδικα που χρησιμοποιήθηκε κατά την κωδικοποίηση. Ο κώδικας αυτός ονομάζεται «κλειδί κωδικοποίησης».

Η αποκρυπτογράφηση είναι η διαδικασία μετατροπής το κρυπτογραφημένου μηνύματος σε κανονικό αναγνώσιμο και επεξεργάσιμο κείμενο. Όσο η κρυπτογράφηση τόσο και η αποκρυπτογράφηση, γίνονται με ειδικό λογισμικό που είναι κάποιες φορές ενσωματωμένο στο λειτουργικό σύστημα ή και σε ειδικές αποσπώμενες συσκευές που λειτουργούν ως φυσικό αντίστοιχο του μεταλλικού κλειδιού που ξεκλειδώνει μια κλειδαριά, έχοντας αποθηκευμένο μέσα τους τον κώδικα αποκρυπτογράφησης.

Η κρυπτογραφία επιτρέπει την ανταλλαγή πληροφοριών σε «μεταμφιεσμένη» μορφή κρατώντας έτσι το περιεχόμενο κρυμμένο από άγνωστους ή μη εξουσιοδοτημένους παραλήπτες. (Fact Sheet, 2006).

Σύμφωνα με τον Rich Mogull, αναλυτή συστημάτων (2005), είναι «νόμος» να κρυπτογραφείται οποιαδήποτε πληροφορία βρίσκεται εν κινήσει, είτε σε φορητούς υπολογιστές, είτε σε φορητά αποθηκευτικά μέσα και πολύ περισσότερο όταν διαδίδεται μέσα από οποιασδήποτε κλίμακας δίκτυα είτε με τη μορφή αρχείων, είτε επισυναπτόμενης αλληλογραφίας. (T. Olzak, 2006).

Ένας ακόμα νόμος του ίδιου αναλυτή είναι ότι πρέπει να κρυπτογραφείται οποιαδήποτε πληροφορία δεν εμπίπτει στην εργασία κάποιου εξουσιοδοτημένου προσώπου.

Για παράδειγμα, ένας τεχνικός που δουλεύει σε ένα τηλεοπτικό πλατό δεν πρέπει να έχει πρόσβαση σε μη κρυπτογραφημένο ψηφιακό υλικό από το αρχείο ταινιών του καναλιού. Εφαρμόζοντας τους δύο αυτούς νόμους, το πνευματικό έργο μπορεί (θεωρητικά) να ελέγχεται ως προς την πρόσβαση, μεταποίηση και διακίνηση του μόνο από εξουσιοδοτημένα άτομα που κατέχουν το κλειδί της κρυπτογράφησης του έργου.

Απαραίτητη προϋπόθεση είναι η κρυπτογράφηση να εφαρμόζεται με τους ενδεικνυόμενους τρόπους και από καταρτισμένο προσωπικό με τέτοιο τρόπο που να είναι «άτρωτο» οτιδήποτε κρυπτογραφείται, χωρίς αυτό να το καθιστά δύσχρηστο ως προς τον τελικό εξουσιοδοτημένο χρήστη.

Μια παρόμοια με αυτή της κρυπτογράφησης μέθοδος χρησιμοποιείται για τη δημιουργία «ψηφιακών υπογραφών» που μπορούν να χρησιμοποιούνται για την πιστοποίηση της ταυτότητας ενός προσώπου για να μπορεί να διαπιστωθεί αν δικαιούται να έχει πρόσβαση σε ένα ψηφιακό έργο.

Μια απλή ψηφιακή υπογραφή αποτελείται από τον κώδικα του κρυπτογραφημένου μηνύματος. Όταν ένα άτομο υπογράψει το μήνυμά του και το στείλει σε ένα άλλο μαζί με ψηφιακή υπογραφή, το άλλο άτομο μπορεί να αποκρυπτογραφήσει την υπογραφή χρησιμοποιώντας το κλειδί αποκρυπτογράφησης και να συγκρίνει το αποτέλεσμα με το κείμενο που έλαβε. Εάν είναι ταυτόσημα, μπορεί να υποθέσει ότι το μήνυμα έφτασε πράγματι από τον αποστολέα του και όχι από κάποιον άλλο.

Ψηφιακά πιστοποιητικά

Μια τρίτη μέθοδος πιστοποίησης που είναι όμοια με τις ψηφιακές υπογραφές είναι τα «ψηφιακά πιστοποιητικά». Τα πιστοποιητικά αυτά ταυτοποιούν τους χρήστες στον ψηφιακό κόσμο και διανέμονται έναντι τρίτου από εταιρίες γνωστές ως «Αρχές Πιστοποίησης».

Ένα πιστοποιητικό περιέχει τον αριθμό έκδοσής του, τον σειριακό αριθμό χρήστη, τον αλγόριθμο που χρησιμοποιήθηκε για τη δημιουργία της υπογραφής του, το όνομα της Αρχής Πιστοποίησης που το εκδίδει, την ημερομηνία λήξης του πιστοποιητικού, το όνομα χρήστη, το δημόσιο κλειδί κρυπτογράφησης και την ψηφιακή υπογραφή του χρήστη.

Τα πιστοποιητικά αυτά παίζουν σημαντικό λόγο στην ασφάλεια,αφού οι διαχειριστές συστημάτων μπορούν να ρυθμίζουν τους servers να δέχονται μόνο πιστοποιητικά υπογεγραμμένα από συγκεκριμένες Αρχές Πιστοποίησης. (Fact Sheet, 2006). Μια πασίγνωστη εταιρία που δρα ως «Αρχή πιστοποίησης» είναι η VeriSign.

Για να αυξηθεί περισσότερο η ασφάλεια στο Διαδίκτυο και να αξιοποιηθούν οι προαναφερθείσες μέθοδοι, έχουν αναπτυχθεί ειδικά πρωτόκολλα ασφαλούς επικοινωνίας που μπορούν να χειρίζονται μόνο την κρυπτογράφηση και την αποκρυπτογράφηση της πληροφορίας.

Ένα παράδειγμα είναι το προτόκολλο στρώματος ασφαλούς σωλήνωσης (Secure Socket Layer Protocol – SSL). Το πρωτόκολλο αυτό λειτουργεί ως εργαλείο πιστοποίησης και για άλλα πρωτόκολλα Διαδικτυακών εφαρμογών όπως το HTTP, SMTP, TELNET, FTP κλπ.

Συσκευές και Προγράμματα αναπαραγωγής που εφαρμόζουν TPM

Από τη στιγμή που εφαρμόστηκε η κρυπτογραφία ως μοντέλο, έχουν αναπτυχθεί πολλές μέθοδοι που συνδέουν τα κρυπτογραφημένα αρχεία ψηφιακού πνευματικού έργου με τις συσκευές ή τα προγράμματα αναπαραγωγής τους με τέτοιο τρόπο ώστε τα τελευταία να συμπεριλαμβάνουν υλικό ή λογισμικό που θα επιτρέπει την αναπαραγωγή του κρυπτογραφημένου υλικού μόνο από αυτά. (Fact Sheet, 2006). Μερικές από αυτές τις μεθόδους παρουσιάζονται πιο κάτω:

Σφραγισμένο περιεχόμενο (Sealed Content): Σε αυτή την μέθοδο το ψηφιακό περιεχόμενο κρυπτογραφείται και μπορεί μόνο να ανοιχθεί όταν υπάρχει ένα μοναδικό και αυθεντικό «κουπόνι» (token) εγκατεστημένο στη συσκευή. Το κουπόνι αυτό δεν μπορεί να αντιγραφεί, με αποτέλεσμα το περιεχόμενο να μην μπορεί να αναπαραχθεί σε άλλη συσκευή.

Δέσμευση συσκευής (Device Binding): Η μέθοδος αυτή χρησιμοποιεί τη μοναδική ταυτότητα των ηλεκτρονικών μερών μιας συσκευής (σκληρός δίσκος, επεξεργαστής κλπ) για να φτιάξει το κλειδί αποκρυπτογράφησης του περιεχομένου.

Έμπιστο πρόγραμμα αναπαραγωγής (Trusted Player): Μερικές συσκευές ανάγνωσης ηλεκτρονικών βιβλίων βρίσκουν το κλειδί αποκρυπτογράφησης μέσα στο ίδιο το περιεχόμενο του βιβλίου. Ο συγγραφέας του ηλεκτρονικού βιβλίου με αυτό τον τρόπο επιτρέπει την ανάγνωση του βιβλίου του μόνο μέσα από συγκεκριμένες συσκευές.

Σε κάποιες άλλες περιπτώσεις η συσκευή μπορεί να διαβάζει και απροστάτευτο κείμενο, αλλά με την προσθήκη επιπρόσθετου λογισμικού.

Έμπιστη συσκευή αναπαραγωγής (Trusted Device): Με την προσθήκη μικρής βυσματούμενης συσκευής πάνω στη συσκευή αναπαραγωγής, αυτή μπορεί να λειτουργεί όπως ένας Trusted Player.

Κάποιες συσκευές μπορούν να διαβάζουν προστατευμένο κείμενο αλλά δεν μπορεί να εγκατασταθεί πάνω τους επιπρόσθετο λογισμικό ή απαιτείται επιπρόσθετος κωδικός για την αναπαραγωγή πολυμεσικού υλικού.

Σε αυτό το σημείο είναι χρήσιμο να διευκρινιστεί ότι παρουσιάζοντας τις πιο πάνω μεθόδους, αναφερθήκαμε μόνο στους τρόπους με τους οποίους ελέγχουν την πρόσβαση στο πνευματικό υλικό για ανάγνωσή του, χωρίς να εξετάσουμε καθόλου πως αντιμετωπίζουν την περαιτέρω χρήση του (αντιγραφή, αποθήκευση, εκτύπωση κλπ).

Σύστημα κωδικοποιημένου περιεχομένου

Content Scramble System (CSS). Το σύστημα αυτό δημιουργήθηκε για να προστατεύει τις ταινίες που κυκλοφορούν γραμμένες σε DVDs, και διέπεται από τα ακόλουθαμχαρακτηριστικά:

Τα περιεχόμενα των DVD είναι κρυπτογραφημένα

Τα κλειδιά που επιτρέπουν την αναπαραγωγή των DVD είναι επίσης κρυπτογραφημένα

Μόνο οι συσκευές που είναι κατασκευασμένες με άδεια από το CSS μπορούν να αναπαράγουν τις ταινίες στα DVD.

Οι συσκευές απαγορεύουν την αντιγραφή περιεχομένου από τα DVD εκτός εξαιρετικών περιπτώσεων

Από τη στιγμή που μια συσκευή αναπαραγωγής υλικού εξασφαλίσει άδεια από το CSS,εξυπονοείται ότι «αποδέχεται» και λειτουργεί σύμφωνα με τους ακόλουθους κανόνες: Το περιεχόμενο που αποκρυπτογραφείται από τη συσκευή πρέπει να προστατεύεται από μη εξουσιοδοτημένη χρήση από «μέσα» από τη συσκευή. Με λίγα λόγια από αποσυναρμολόγηση και μετατροπή της συσκευής.

Τα περιεχόμενα των DVD μπορούν να αναπαράγονται σε συγκεκριμένες συσκευές εξόδου όπως αναλογικές εξόδους με τεχνολογία που εμποδίζει την αντιγραφή (με τρόπους που θα δούμε αργότερα) όπως αναλογικά VCR, και ασφαλείς ψηφιακές εξόδους όπως είναι το DTCP που θα δούμε επίσης αργότερα.

Συσκευές που πωλούνται σε διαφορετικές γεωγραφικές ζώνες μπορούν να αναπαράγουν DVDs που φτιάχτηκαν ειδικά για αναπαραγωγή στις ίδιες ζώνες. Οταν οι κατασκευαστές των συσκευών που έχουν άδεια από το CSS παραβιάζουν τους κανόνες διώκονται δικαστικά.

Τα στούντιο παραγωγής ταινιών δικαιούνται να κωδικοποιούν τα ίδια τις ταινίες τους και να απαγορεύουν την αντιγραφή των DVDs τους. (Fact Sheet, 2006).

Ψηφιακά Εισιτήρια

Πρόκειται για πλαστικές κάρτες οι οποίες πιστοποιούν τον χρήστη και που καταμετρούν τις φορές που ένα κομμάτι ψηφιακού πνευματικού έργου χρησιμοποιείται. Αυτές οι κάρτες μπορούν να πιστοποιούν χρήστες και να καταμετρούν χρήσεις ακόμα και όταν το περιεχόμενο σταλεί μέσω email ή όταν αντιγραφεί. (Fact Sheet, 2006).

TPMs για έλεγχο χρήσης

Αυτή η δεύτερη κατηγορία από TPMs επιτρέπει στους κατόχους δικαιωμάτων πάνω στα ψηφιακά πνευματικά έργα να ελέγχουν όλες τις χρήσεις που μπορεί να κάνει κανείς στα έργα (έλεγχος μη

εξουσιοδοτημένης αντιγραφής, ελεγχόμενη αντιγραφή κλπ), ακόμα και όταν επιτευχθεί νόμιμη και πιστοποιημένη πρόσβαση σε αυτά. (Fact Sheet, 2006).Παρακάτω παρουσιάζονται κάποια από τα πιο δημοφιλή TPMs για αυτό το σκοπό:

Macrovision

Ο όρος αυτός δεν φαίνεται να έχει ακριβή ελληνική μετάφραση.

Πάντως, αναφέρεται σε μια μέθοδο προστασίας από αντιγραφή στους αναλογικούς καταγραφείς βιντεοκασετών (VCRs) που χρησιμοποιείται για να αποτρέπει και όχι να απαγορεύει- την αντιγραφή προ-καταγεγραμμένων βιντεοταινιών. Αν μια προστατευμένη ταινία αντιγραφεί, οι εικόνες από το αντίγραφο θα παίζονται σκοτεινές και ασταθείς πάνω σε μια συσκευή VCR με προστασία Macrovision.

Το Macrovision χρησιμοποιείται για προστασία των εταιριών που προσφέρουν συνδρομητική και «pay-per-view» τηλεόραση, καθώς και εταιριών ενοικίασης και πώλησης βιντεοταινιών. (Fact Sheet, 2006)

Σύστημα διαχείρισης σειριακής αντιγραφής

Serial Copy Management System (SCMS).

Αυτό το σύστημα αποτρέπει την παράνομη παραγωγή πολλών γενεών ψηφιακών αντιγράφων (αντίγραφα των αντιγράφων) από ένα αυθεντικό έργο προστατευμένο από νόμους πνευματικής ιδιοκτησίας. Αυτό γίνεται με την βοήθεια υδατογραφημάτων (watermarks). Ένα υδατογράφημα είναι πληροφορία ψηφιακά κωδικοποιημένη και ενσωματωμένη με φανερό η κρυμμένο τρόπο μέσα στο ίδιο το ψηφιακό έργο.

Η πληροφορία από ένα υδατογράφημα μπορεί να χρησιμοποιηθεί για να ταυτοποιήσει το έργο ή τον δημιουργό του, να εντοπίσει τα αντίγραφά του, και στην περίπτωση του φανερού υδατογραφήματος, να το καταστήσει ακατάλληλο για αναπαραγωγή ή εκθεσή του.(Φανταστείτε μια γκαλερί τέχνης που να φιλοξενεί μια έκθεση φωτογραφίας, όπου οι φωτογραφίες να φέρουν ορατά υδατογραφήματα όμοια με την εικόνα 1 που ακολουθεί). Τα υδατογραφήματα επίσης χρησιμοποιούνται σε έργα που χρησιμοποιούνται μόνο για λόγους διαφήμισης και προώθησης, ή ως δείγματα

Εικόνα 1: Ορατό υδατογράφημα σε εικόνα για χρήση σε έκθεση

Εικόνα 2:Ορατό υδατογράφημα σε εικόνα
για χρήση ως δείγμα

Τα υδατογραφήματα ενσωματώνονται στο έργο (είτε εικόνας, είτε κειμένου, είτε βίντεο, είτε ήχου) με τη χρήση ειδικού λογισμικού. Το ίδιο λογισμικό μπορεί να ανιχνεύσει την ύπαρξη αόρατου υδατογραφήματος σε ένα έργο να εξάξει όλες τις πληροφορίες που φέρει , και μπορεί να το αφαιρέσει μόνο εφόσον είναι το ίδιο που το ενσωμάτωσε).

Ένα αόρατο υδατογράφημα πρέπει να μην αλλοιώνει την αρχική εικόνα του έργου αλλά να είναι ανιχνεύσιμο, ενώ ένα ορατό υδατογράφημα πρέπει να μην μπορεί να αφαιρεθεί εύκολα από μη εξουσιοδοτημένους χρήστες. (Εργαστήριο Ψηφιακών Συστημάτων & Επεξεργασίας Ψηφιακών Μέσων Ελληνικού Ανοικτού Πανεπιστημίου, 2000- 2006).

Στο ίδιο κλίμα, οι καλές τεχνικές ψηφιοποίησης περιεχομένου της Ευρωπαϊκής Ένωσης προτείνουν όλες οι εικόνες αλλά και τα βίντεο ή ηχητικά αποσπάσματα να είναι διαθέσιμα στο διαδίκτυο σε πολύ χαμηλή ανάλυση ή ευκρίνεια, είτε να προστίθεται σε αυτά θόρυβος, ή να υπόκεινται σε γεωμετρικούς μετασχηματισμούς, φιλτράρισμα, οριζόντια και κάθετη μετατόπιση frames κλπ, ούτως ώστε όποιος θέλει να μπορεί να τα βλέπει, αλλά να μην του είναι χρήσιμα για αντιγραφή και άλλη χρήση.

Προστασία Περιεχομένου από ψηφιακή μετάδοση

Digital Transmission Content Protection (DTCP).

Ο σκοπός αυτής της τεχνολογίας είναι να αποτρέπει μη εξουσιοδοτημένη διανομή οπτικοακουστικού υλικού που υπάρχει στο σπίτι σε ψηφιακή μορφή σε αποκρυπτογραφημένη μορφή.

Αυτή η τεχνολογία ελέγχει την μετάδοση χρησιμοποιώντας μια συσκευή «πηγή» με DTCP (καλωδιακή ή δορυφορική τηλεόραση, DVD Player, PlayStation) η οποία αναπαράγει το οπτικοακουστικό υλικό και μια πηγή «νεροχύτη» η οποία το προβάλλει (Απλή οικιακή τηλεόραση, ηλεκτρονικός υπολογιστής, VCR).

Η συσκευή «νεροχύτης» (sink device) προγραμματίζεται με τρόπο που να μην μπορεί να διανέμει το περιεχόμενο που προβάλλει στο διαδίκτυο. Η τεχνολογία εκδίδει και αυτή με τη σειρά της ειδικές άδειες, όπως κάνει και η CSS που είδαμε πιο πριν. (Fact Sheet, 2006).

Πρωτοβουλία Ασφαλούς Ψηφιακής Μουσικής

Secure Digital Music Initiative (SDMI).

Από τη στιγμή που η κρυπτογράφηση δεν εφαρμόστηκε στα απλά CD μουσικής, η μουσική μπορεί εύκολα να αντιγραφεί και μάλιστα να συμπιεστεί με το πρότυπο mp3 και να αναπαραχθεί ή να διανεμηθεί πανεύκολα στο διαδίκτυο, σε φορητές συσκευές, σκληρούς δίσκους, κάρτες μνήμης, κινητά τηλέφωνα κλπ.

Για να αντιμετωπιστούν τα προβλήματα στην προστασία των ψηφιακών πνευματικών δικαιωμάτων που προέκυψαν από αυτό, ανέλαβε πρωτοβουλία μια τεράστια ομάδα από 200 εταιρίες και οργανισμούς που εκπροσώπευαν τον χώρο της πληροφορικής, των ηλεκτρονικών συσκευών, τις τεχνολογίες της ασφάλειας, την παγκόσμια δισκογραφία και τους παροχείς υπηρεσιών διαδικτύου, να καταγράψει οδηγίες και προδιαγραφές που σκόπευαν στην υλοποίηση τεχνολογιών προστασίας των εμπορικών μουσικών κομματιών.

Οι οδηγίες αυτές διακήρυτταν ένα «άτρωτο» και αδιάβλητο σύστημα κρυπτογράφησης και υδατογραφημάτων το οποίο θα προστάτευε τα

μουσικά κομμάτια από μη εξουσιοδοτημένη αναπαραγωγή και χρήση (αντιγραφή και διαμοιρασμό).

Τα αποτελέσματα αυτού του κολοσσιαίου και πολλά υποσχόμενου εγχειρήματος εξετάζονται στο επόμενο κεφάλαιο, μαζί με τα αποτελέσματα όλων των άλλων, καθώς το επόμενο κεφάλαιο εξετάζει τους παράγοντες αποτυχίας όλων αυτών των μέτρων.

Διαχείριση Ψηφιακών Δικαιωμάτων

Digital Rights Management (DRM). *'*Όπως έχουμε προαναφέρει, με τον όρο DRM εννοούμε αφ' ενός τις τεχνολογίες που περιγράφονται πιο πάνω (TPM), και αφετέρου τις διαδικασίες σε διαχειριστικό επίπεδο που απαιτούνται για να ελέγξουν (με σκοπό τελικά να περιορίσουν ή να απαγορεύσουν) την πρόσβαση σε ψηφιακό πνευματικό έργο και την χρήση του.

Σε αυτό το σημείο εξετάζουμε τις διαδικασίες σε διαχειριστικό επίπεδο που ακολουθούνται (ή που προτείνεται να ακολουθούνται), έτσι όπως παρουσιάζονται από το Επιχειρησιακό πρόγραμμα «Κοινωνία της Πληροφορίας» που έλαβε χώρα από το 2000 μέχρι το 2006 στην Ελλάδα με την στήριξη του Γ' Κοινοτικού Πλαισίου Στήριξης.

Σύστημα διαχείρισης και αξιοποίησης των πνευματικών δικαιωμάτων του ψηφιακού περιεχομένου

Το σύστημα αυτό χρησιμοποιεί μια από τις σύγχρονες γλώσσες διαχείρισης πνευματικών δικαιωμάτων και βασίζεται σε διεθνή πρότυπα μεταδεδομένων για τη διαχείριση δικαιωμάτων πολυμεσικού υλικού. Για παράδειγμα μπορεί να χρησιμοποιεί μια «Γλώσσα Έκφρασης Δικαιωμάτων» (Rights Expression Language – REL).

Με αυτές τις γλώσσες μπορεί κανείς να δημιουργεί αξιόπιστες άδειες και εξουσιοδοτήσεις οι οποίες να περιγράφουν τους περιορισμούς στη χρήση ενός ψηφιακού αντικειμένου σύμφωνα με τα πνευματικά του δικαιώματα.

Οι ειδικοί έφτιαξαν την MPEG-21 REL καθοδηγούμενοι από 48 απαιτήσεις που συνετάχθησαν από ιδιοκτήτες περιεχομένου, κατασκευαστές συσκευών και μεσάζοντες» (Rights.com, 2003).

Σύστημα μοναδικής αναγνώρισης

Βασίζεται στην ανάθεση ενός μοναδικού αναγνωριστικού σε κάθε ψηφιακό αντικείμενο και παρέχει ένα σύνολο από λειτουργίες και πολιτικές διαχείρισης που σχετίζονται με τον κύκλο ζωής του αντικειμένου στο Διαδίκτυο.

Μέσω εγγραφής ένας οργανισμός εφοδιάζεται με ένα μονοσήμαντο αναγνωριστικό που το συνδέει με ένα ψηφιακό αντικείμενο και την μονοσήμαντη διασύνδεσή του με το σύνολο των μεταδεδομένων του και των περιορισμών που απορρέουν από αυτά.

Τα μεταδεδομένα για την προστασία και διαχείριση των πνευματικών δικαιωμάτων ψηφιακών έργων είναι:

1. Ονόματα: ομάδες ανθρώπων με διαφορετικές ιδιότητες, όπως είναι ο δημιουργός, ο ψηφιοποιητής, ο παραγωγός και γενικά όποιος μπορεί να αποκτήσει αξιώσεις επί των δικαιωμάτων.

2. Περιορισμοί χρήσης: δικαιώματα για εμπορική εκμετάλλευση, για εκπαιδευτική χρήση κλπ.

3. Υποχρεώσεις: συνθήκες που πρέπει να ικανοποιούνται για να είναι νόμιμη η χρήση.

4. Στοιχεία επικοινωνίας του κατόχου ή του διαχειριστή των δικαιωμάτων του έργο

10 ΚΥΒΕΡΝΟΣΦΕΤΕΡΙΣΜΟΣ

Το ζήτημα της προστασίας διακριτικών γνωρισμάτων στο διαδίκτυο έχει ανακύψει πρόσφατα στην ελληνική νομολογία. Μέχρι στιγμής έχουν εκδοθεί επτά αποφάσεις ασφαλιστικών μέτρων σχετικές με την προστασία διακριτικών γνωρισμάτων.

Με τις αποφάσεις αυτές επιβεβαιώνεται η δυνατότητα προστασίας του διακριτικού τίτλου, της επωνυμίας και της ηλεκτρονικής διεύθυνσης των συναλλασσομένων με βάση τις διατάξεις για τον αθέμιτο ανταγωνισμό και τις διατάξεις για την προστασία της προσωπικότητας, το πιθανότερο δε είναι ότι θα προστατεύονται και πιθανές προσβολές δικαιωμάτων σε εμπορικό σήμα ή σήμα φήμης βάσει της οικείας νομοθεσίας.

Η ελληνική νομική επιστήμη έχει ασχοληθεί με το ζήτημα σε εύλογα μικρό αριθμό δημοσιεύσεων, αλλά εμπεριστατωμένα και περιεκτικά.

10.1 Ονόματα διαδικτύου

Η προστασία των διακριτικών γνωρισμάτων στο διαδίκτυο αφορά πρώτιστα την πιθανή προσβολή δικαιωμάτων σε διακριτικά γνωρίσματα από την καταχώρηση domain name. Ο όρος domain name στην ελληνική γλώσσα αποδίδεται με διάφορες εκφράσεις, Όπως ηλεκτρονική διεύθυνση, όνομα πεδίου ή περιοχής, χώρος ονομάτων διαδικτύου (ονομασία την οποία φαίνεται να προτιμούν οι ειδικοί του χώρου), καμία από τις οποίες δεν είναι απόλυτα ικανοποιητική.

Για τις ανάγκες του σημειώματος αυτού χρησιμοποιείται ο όρος όνομα διαδικτύου. Η λειτουργία της καταχώρησης ονομάτων διαδικτύου καλείται διευθυνσιοδότηση ή ονοματοδοσία.

Το διαδίκτυο αφορά επικοινωνία μεταξύ ηλεκτρονικών υπολογιστών. Κάθε συνδεδεμένος υπολογιστής διαθέτει ένα πολυψήφιο αριθμό με τον οποίο αναγνωρίζεται στο διαδίκτυο και με τον οποίο συνδέεται σε αυτό μέσω του modem του υπολογιστή.

Ο πολυψήφιος αυτός αριθμός, ο κωδικός του υπολογιστή στο διαδίκτυο (το πρωτόκολλο διαδικτύου), εκφράζεται μέσω του συστήματος διευθυνσιοδότησης με συνδυασμό γραμμάτων, σημείων στίξης ή και αριθμών.

Το όνομα διαδικτύου είναι, δηλαδή, από τεχνικής πλευράς, ένας πολυψήφιος αριθμός, ο οποίος μετατρέπεται σε ένα συνδυασμό γραμμάτων του (λατινικού) αλφάβητου, σημείων στίξης και αριθμών.

Το όνομα διαδικτύου αποτελείται από περισσότερα επίπεδα, τα οποία χωρίζονται μεταξύ τους με τελείες.

Το δεύτερο επίπεδο αποτελεί το επιλεγμένο όνομα διαδικτύου και, τελικά, το μεταβαλλόμενο τμήμα του ονόματος ένας συνδυασμός γραμμάτων, σημείων στίξης και αριθμών.

Με βάση το {κορυφαίο} επίπεδο (top level domain name), που φαίνεται στο ακραίο δεξιά τμήμα του ονόματος, διαχωρίζονται τα ονόματα σε εθνικά και διεθνή, όπου τα εθνικά αποτυπώνονται με συνδυασμό δύο ψηφίων, gr για την Ελλάδα και τα διεθνή με ένα από τα edu, int, net, org, com, τα οποία αντιστοιχούν σε συγκεκριμένες δραστηριότητες.

Στα εθνικά ονόματα μπορεί να παρεισφρύσει τρίτο επίπεδο ανάμεσα στο πρώτο και το δεύτερο. Το τρίτο επίπεδο του ονόματος διαδικτύου αποτελείται από συντμήσεις αντίστοιχες των διεθνών ονομάτων πρώτου επιπέδου και αφορά ειδικότερο προσδιορισμό του κατόχου, για παράδειγμα .com, οπότε το όνομα διαμορφώνεταισε com.gr

10.2 **Καταχώρηση ονομάτων διαδικτύου**

Αρμόδια για την καταχώρηση ελληνικών ονομάτων στο διαδίκτυο αρχή είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).

Εχει τις ακόλουθες αρμοδιότητες:

Καταρτίζει και τροποποιεί το Εθνικό Σχέδιο Αριθμοδότησης (Ε.Σ.Α.) και εκχωρεί αριθμούς ή ομάδες αριθμών στους Τηλεπικοινωνιακούς Οργανισμούς και στους Παρόχους Τηλεπικοινωνιακών Υπηρεσιών και καθορίζει τα τέλη εκχώρησης και χρήσης των αριθμών.

Κανονίζει τα σχετικά με τη Φορητότητα των Αριθμών Κλήσης και την Προεπιλογή Φορέα. Επίσης ρυθμίζει τα θέματα του διαδικτύου και εκχωρεί ονόματα χώρου (domain name) με κατάληξη gr.

Έως τη θέση σε ισχύ του ν.2867/2000 με τον οποίο για πρώτη φορά ανατίθεται και τυπικά η σχετική αρμοδιότητα στην ΕΕΤΤ, η ΕΕΤΤ είχε εν τοις πράγμασι αναλάβει την εποπτεία τουλάχιστον της διαχείρισης της διευθυνσιοδότησης, θεωρώντας τη δραστηριότητα αυτή ως μέρος της αρμοδιότητας της εκχώρησης αριθμών σε τηλεπικοινωνιακές επιχειρήσεις και της εποπτείας της λειτουργίας της αριθμοδότησης στον τομέα των τηλεπικοινωνιών (ν.2246/1994, ΦΕΚ Α, 172).

Είναι σύνηθες, σε ευρωπαϊκό τουλάχιστον επίπεδο, ο αρμόδιος για την εποπτεία των τηλεπικοινωνιών φορέας να αναλαμβάνει τη διαχείριση ή/ και την εποπτεία της διευθυνσιοδότησης στο διαδίκτυο. Και στο ν.2867/2000, εξάλλου, η διευθυνσιοδότηση εμφανίζεται ως τμήμα της κατάρτισης του Εθνικού Σχεδίου Αριθμοδότησης από την ΕΕΤΤ. Η ΕΕΤΤ είχε αναθέσει από το Δεκέμβριο του 1999.

Με την από 1.12.1999 απόφασή της, που μπορεί να βρεθεί στην ιστοσελίδα της ΕΕΤΤ, http://www.eett.gr τη διαχείριση της καταχώρησης στο Ίδρυμα Τεχνολογίας και Ερευνας - Ινστιτούτο Πληροφορικής (ΙΤΕ , ΙΠ), το οποίο ως την ανάθεση αυτή ήταν ο φορέας διαχείρισης των **ονομάτων διαδικτύου** με κατάληξη gr με εξουσιοδότηση του έως το 1998 φορέα διαχείρισης σε παγκόσμιο επίπεδο, Internet Assigned Numbers Authority (IANA). Έως το 1998 οι ΗΠΑ διαχειρίζονταν τα ονόματα διαδικτύου μέσω της IANA και της NSI (Network Solutions Inc).

Μπορεί να αναφερθεί ενδεικτικά ότι θα μπορούσε να αμφισβητηθεί η νομιμότητα της άσκησης εποπτείας έως την 1/1/2001 και της διατύπωσης κατευθυντηρίων αξόνων από την ΕΕΤΤ σε ζητήματα διευθυνσιοδότησης, ελλείψει νομοθετικής εξουσιοδότησης, όπως θα μπορούσε να αμφισβητηθεί η νομιμότητα της ανάθεσης μιας διοικητικής αρμοδιότητας στο ΙΤΕ-ΙΠ, ένα ίδρυμα ιδιωτικού δικαίου (ερευνητικό ινστιτούτο μη κερδοσκοπικού χαρακτήρα), εποπτευόμενο από το Υπουργείο Ανάπτυξης.

Θα πρέπει να ειπωθεί, όμως, ότι η έως τώρα αντιμετώπιση στην Ελλάδα, δεν διαφοροποιείται σημαντικά από εκείνη των περισσοτέρων ευρωπαϊκών χωρών.

Το όνομα διαδικτύου αποτελεί {πολύτιμο εισιτήριο εισόδου στο διαδίκτυο, ενός χώρου συναλλαγών και επικοινωνίας με εκρηκτική ανάπτυξη. Η σημασία του χώρου ονομάτων είναι προφανής όχι μόνο για την ανάπτυξη εμπορικής δραστηριότητας, αλλά και γενικότερα για την εκμετάλλευση των δυνατοτήτων που παρέχει το διαδίκτυο σε ομάδες χρηστών, ενώσεις επαγγελματιών, επιστημόνων κλπ.

Η σημασία των ονομάτων διαδικτύου οδήγησε σε ανταγωνισμό για την απόκτηση των πλέον εμπορικά εκμεταλλεύσιμων ονομάτων και σε αθέμιτες πρακτικές, όπως η καταχώρηση ονομάτων που αποτελούσαν την επωνυμία ή το εμπορικό σήμα άλλων δικαιούχων, με σκοπό την πώληση αυτών στους δικαιούχους.

Στην Ελλάδα η μεταβίβαση ονομάτων διαδικτύου απαγορεύεται, σύμφωνα με την από 1.12.1999 απόφαση της ΕΕΤΤ.

Στην πράξη παραιτείται ο δικαιούχος του ονόματος διαδικτύου από το δικαίωμά του, ώστε να μείνει ελεύθερο το όνομα διαδικτύου και να το κατοχυρώσει ο δικαιούχος του διακριτικού γνωρίσματος.

Υπάρχει ήδη σημαντική νομολογία πάνω σε ζητήματα παράνομης οικειοποίησης διακριτικών γνωρισμάτων στο χώρο του διαδικτύου, κυρίως στις Η.Π.Α., αλλά και σε μεγάλες ευρωπαϊκές χώρες.

Προσπάθεια αντιμετώπισης της παράνομης οικειοποίησης ονομάτων στο διαδίκτυο γίνεται και από τα διεθνή όργανα διαχείρισης ονομάτων διαδικτύου, ιδίως την Internet Corporation for Domain Names and Numbers (ICANN), στα πλαίσια της, κατά βάση, συμβατικής φύσης και οργάνωσης του διαδικτύου.

Προς το παρόν σχεδιάζεται ένας κώδικας δεοντολογίας. COM (2000) 202,7.4.2000.

10.3 **Το όνομα διαδικτύου ως διακριτικό γνώρισμα**

Έχοντας υπόψη τα δεδομένα σχετικά με τη λειτουργία του ονόματος και της επωνυμίας (αλλά και άλλων διακριτικών γνωρισμάτων) στο αστικό και εμπορικό δίκαιο, ένας βασικός προβληματισμός σχετικά με τη φύση του ονόματος διαδικτύου πηγάζει από το γεγονός ότι το όνομα διαδικτύου διακρίνει ένα συγκεκριμένο ηλεκτρονικό υπολογιστή και όχι ένα συγκεκριμένο πρόσωπο ή επιχείρηση .

Η ιδιαιτερότητα αυτή συνδέεται με την τεχνική παράμετρο που αναφέρθηκε προηγουμένως, ότι δηλαδή από τεχνικής απόψεως τα ονόματα διαδικτύου αποτελούνται από μία σειρά αριθμών. Βέβαια, η τεχνική απεικόνιση και το μέσο μετάδοσης του μηνύματος (ονόματος) δεν θα έπρεπε να αποτελούν το κύριο πρόκριμα για τη δικαιική αντιμετώπιση και το νομικό χαρακτηρισμό του.

Ο νομικός χαρακτηρισμός βασίζεται σε κριτήρια κοινωνικά, δηλαδή σε κριτήρια συναλλαγών. Η επικοινωνιακή λειτουργία του ονόματος διαδικτύου είναι, κατά τις αντιλήψεις των συναλλαγών, η βασική λειτουργία του.

Με βάση αυτή τη λειτουργία το όνομα διαδικτύου φαίνεται κατ' αρχήν να διακρίνει φυσικά πρόσωπα και επιχειρήσεις στα πλαίσια των συναλλαγών και ως μέσο που διακρίνει και εξατομικεύει γίνεται αντιληπτό.

Χαρακτηριστικά έχει αναφερθεί ότι στο όνομα διαδικτύου ενδιαφέρει ο λεκτικός συνδυασμός που επιτρέπει τη σύνδεση ενός υπολογιστή με ένα πρόσωπο και τη διαφοροποίηση ενός κατόχου ιστοσελίδας από τους υπόλοιπους.

Η εξατομικευτική αυτή λειτουργία του ονόματος διαδικτύου δεν αρκεί ίσως για την εξομοίωσή του με την επωνυμία του νομικού προσώπου ή το όνομα του φυσικού προσώπου για παράδειγμα, αλλά αντικατοπτρίζει σε μεγάλο βαθμό την αντίληψη στις συναλλαγές.

Θα μπορούσε, χάριν παραδείγματος της εξατομικευτικής λειτουργίας των ονομάτων διαδικτύου να αναφερθεί το γεγονός ότι οι έμπειροι χρήστες

διαδικτύου κατά κανόνα μαντεύουν τα ονόματα διαδικτύου τα οποία ανήκουν σε φορείς, επιχειρήσεις κλπ, τις οποίες αναζητούν.

Σχετικά με τη λειτουργία του ονόματος διαδικτύου έχουν διατυπωθεί δύο κατά βάση απόψεις, καμία από τις οποίες δεν αναιρεί την από νομικής απόψεως θεμελίωση της διακριτικής δυναμικής του ονόματος διαδικτύου. Με βάση την παλαιότερη αντίληψη, δινόταν έμφαση στο χαρακτηρισμό του ονόματος διαδικτύου ως μέσου πρόσβασης, ως διόδου προς το διαδίκτυο, ως ηλεκτρονικής διεύθυνσης αντίστοιχης με την ταχυδρομική, σύμφωνα και με το χαρακτήρα του ονόματος διαδικτύου ως σειράς αριθμών, και απορριπτόταν ο διακριτικός ρόλος του ονόματος διαδικτύου.

Κατά την κρατούσα, νεότερη γνώμη, τα ονόματα διαδικτύου, εφόσον διακρίνουν τον κάτοχό τους, αποτελούν, εκτός των άλλων και διακριτικά γνωρίσματα.

Είναι δε η ιδιότητά τους αυτή δύσκολο να αμφισβητηθεί με βάση τα δεδομένα για τη σημασία του διαδικτύου στην ανάπτυξη των συναλλαγών (πολλές επιχειρήσεις θεωρούν πλέον σημαντικό να προσεγγίσουν άλλους συναλλασσόμενους μέσω του διαδικτύου, ενώ άλλες δραστηριοποιούνται αποκλειστικά στο διαδίκτυο).

Σε κάθε περίπτωση, και αν ακόμα το όνομα διαδικτύου αποτελεί απλά μέσο πρόσβασης ή διεύθυνση και έτσι προσδιορίζει τον ιδιαίτερο χώρο. Ο ν.2867/2000 (άρθρο 314 α) μιλά για ονόματα χώρου του κατόχου σε συγκεκριμένο πεδίο επικοινωνίας και συναλλαγών, επιτελεί εξατομικευτική λειτουργία, ανάλογη με εκείνη της κατοικίας του φυσικού προσώπου ή της έδρας του νομικού προσώπου, ως στοιχείων που διακρίνουν το πρόσωπο κατά τρόπο ανάλογο με τις διατάξεις των γενικών αρχών του αστικού δικαίου.

Θα μπορούσε επίσης να θεωρηθεί ότι, αφού το όνομα διαδικτύου στην πράξη λειτουργεί και ως δίοδος προς τις ιστοσελίδες του κατόχου ή εκείνες που συνδέονται με αυτές, η ταυτότητα του κατόχου και η πλήρης περιγραφή του εμπεριέχονται στις ιστοσελίδες και όχι στη δίοδο πρόσβασης.

Ο συλλογισμός αυτός δεν αναιρεί τη λειτουργία του ονόματος διαδικτύου ως μέσου εξατομίκευσης του κατόχου, αλλά μπορεί να αποτελέσει τη βάση για τη διαμόρφωση της προστασίας των συναλλασσομένων στο διαδίκτυο με έμφαση στο περιεχόμενο των ιστοσελίδων, με την επιβολή για παράδειγμα υποχρέωσης προσθήκης στην ιστοσελίδα διευκρινήσεων, που αίρουν το ενδεχόμενο σύγχυσης σχετικά με τους κατόχους των ονομάτων

10.4 Ζητήματα προστασίας διακριτικών γνωρισμάτων στο διαδίκτυο

Τα σοβαρότερα προβλήματα σχετικά με την ονοματοδοσία στο διαδίκτυο προκύπτουν, όχι από τα τεχνικά χαρακτηριστικά του ίδιου του ονόματος ως σειράς αριθμών, αλλά από τη φύση του διαδικτύου. Το όνομα διαδικτύου, το μεταβλητό τμήμα του ονόματος συγκεκριμένα, είναι μοναδικό.

Τα σήματα κατατάσσονται σε διαφορετικές κατηγορίες (κλάσεις) και το ίδιο σήμα είτε λεκτικό είτε απεικόνισημπορεί να χαρακτηρίζει διαφορετικά προϊόντα.

Διαφορετικές επιχειρήσεις μπορεί να έχουν την ίδια επωνυμία ή διακριτικό τίτλο αντίστοιχα. Κάτι τέτοιο δεν είναι δυνατόν για τα ονόματα διαδικτύου.

Σε αντιστάθμισμα της μοναδικότητας των ονομάτων διαδικτύου, προβάλλεται συχνά ο ισχυρισμός ότι στις συναλλαγές στο διαδίκτυο, με βάση τη σχετική εμπειρία των χρηστών, ακόμα και μια μικρή διαφοροποίηση στο όνομα διαδικτύου, ένα μόνο σημείο στίξης, αρκεί για να διαφοροποιηθεί επαρκώς ένα όνομα διαδικτύου από ένα άλλο όνομα διαδικτύου.

Η παρατήρηση αυτή δεν απαντά στο ζήτημα της διαφοροποίησης ενός ονόματος διαδικτύου από ένα εκτός διαδικτύου διακριτικό γνώρισμα. Με αφορμή όμως την παρατήρηση αυτή τίθεται το ζήτημα εάν η διαπίστωση της προσβολής διακριτικών γνωρισμάτων από καταχωρήσεις ονομάτων

διαδικτύου θα πρέπει να περιοριστεί στο χώρο του διαδικτύου ή θα πρέπει να αφορά το σύνολο της συναλλακτικής δραστηριότητας.

Στην έως τώρα νομολογία έχει κριθεί ότι ως χώρος των συναλλαγών θεωρείται το σύνολο της συναλλακτικής δραστηριότητας, τη δε στάση αυτή συνάγουμε και από την υπ' αριθμόν 637/1999 απόφαση του Μονομελούς Πρωτοδικείου Σύρου (υπόθεση amazon), η οποία αφορούσε διαφορά μεταξύ δύο επιχειρήσεων {ηλεκτρονικών βιβλιοπωλείων}.

Παρόμοια είναι κατά τα φαινόμενα η τάση και στη νομολογία των περισσοτέρων κρατών την ιστοσελίδα http://www.eon.law.Harvard.ed /h2o/property/domain /main.html, και τις αναφορές στη νομολογία στην ιστοσελίδα http//www.mama-tech.com/foreign.html.

Εξάλλου, κατά τεκμήριο το διαδίκτυο έρχεται να προσθέσει ένα χώρο συναλλαγών στη συναλλακτική ζωή και όχι να περιχαρακώσει το χώρο του Internet.

Η πρόθεση των συναλλασσομένων στη συντριπτική τους πλειοψηφία είναι να μην περιορίσουν τη δραστηριότητά τους στο διαδίκτυο. Οι έως τώρα δικαστικές αποφάσεις εξέτασαν τις συναλλαγές συνολικά για να διαπιστώσουν την προσβολή διακριτικών γνωρισμάτων.

Με βάση την οπτική αυτή (και εφαρμόζοντας τις γενικότερες αρχές του δικαίου των διακριτικών γνωρισμάτων), οι δικαστικές αποφάσεις θεώρησαν τις μικρές διαφοροποιήσεις στην εμφάνιση των ονομάτων διαδικτύου σε σχέση με εκείνη των διακριτικών γνωρισμάτων ως ήσσονος σημασίας, και πάντως όχι αποφασιστικές όσον αφορά την αποδοχή της προσβολής.

Συνακόλουθο της θεώρησης του διαδικτύου ως ενός χώρου συναλλαγών, μέρους του συνόλου της συναλλακτικής δραστηριότητας, αποτελεί το γεγονός ότι μέτρο για τη διαπίστωση της προσβολής διακριτικού γνωρίσματος, κατά την εφαρμογή του κριτηρίου της σύγχυσης στις συναλλαγές, αποτελεί ο μέσος συναλλασσόμενος και/ ή ο μέσος καταναλωτής, όχι ο μέσος χρήστης του διαδικτύου, πόσο μάλλον ο πεπειραμένος χρήστης.

Ας σημειωθεί, εξάλλου, ότι η διευθυνσιοδότηση βασίζεται στην αρχή της χρονικής προτεραιότητας, που αποτελεί αρχή του δικαίου των

διακριτικών γνωρισμάτων, αλλά στην πράξη η χρονική προτεραιότητα στην καταχώρηση αφορά μόνο τα ονόματα διαδικτύου.

Εφόσον, όμως, τα ονόματα διαδικτύου είναι και διακριτικά γνωρίσματα, η αρχή της χρονικής προτεραιότητας και η ανάγκη προστασίας του δικαιώματος ελεύθερης ανάπτυξης της προσωπικότητας - υπό το πρίσμα της άποψης ότι το διαδίκτυο αποτελεί μέρος του συνόλου των συναλλαγών - επιβάλλουν την εναρμόνιση της λειτουργίας της αρχής της χρονικής προτεραιότητας όσον αφορά την καταχώρηση ονομάτων με τα οποία θίγονται άλλα, χρονικά προηγούμενα δικαιώματα σε εκτός διαδικτύου διακριτικά γνωρίσματα. Άλλο είναι το ζήτημα που δημιουργείται εάν το εκτός διαδικτύου διακριτικό γνώρισμα έπεται χρονικά του ονόματος διαδικτύου.

Εδώ θα ανέκυπτε το πρόβλημα της επιλογής του ισχυρότερου ανάμεσα στα δύο κάτι που όμως φαίνεται να οδηγεί σε διακριτική αντιμετώπιση σε βάρος του διακριτικού γνωρίσματος στο διαδίκτυο.

Ίσως η απόκρουση αιτήματος προστασίας στη δεύτερη περίπτωση να μπορεί να χαρακτηριστεί ως καταχρηστική.

Από τη στιγμή που δεν υφίσταται κίνδυνος σύγχυσης, θα ήταν αντίθετο στις βασικές αρχές της Βιομηχανικής Ιδιοκτησίας, αλλά και στην αρχή της οικονομικής ελευθερίας να επιβληθεί στο δικαιούχο του νεώτερου σήματος (εκτός του χώρου του διαδικτύου) να παραιτηθεί από τη χρήση του ως domain name προς όφελος του δικαιούχου χρονικά προγενέστερου σήματος

10.5 **Φύση δικαιώματος στο όνομα διαδικτύου**

Η νομική επιστήμη και η νομολογία δεν φαίνεται να έχουν αντιμετωπίσει εκτενώς το πρόβλημα του νομικού χαρακτηρισμού της σχέσης κατόχου προς καταχωρημένο όνομα διαδικτύου, ίσως διότι δεν παρουσιάζει ιδιαίτερα προβλήματα από τη σκοπιά του ιδιωτικού δικαίου ή διότι η κατοχύρωση θα πρέπει πλέον να θεωρηθεί αποτέλεσμα διοικητικής απονομής.

Είναι σαφές ότι η κρατούσα τάση είναι αντίθετη στο να αναγνωριστεί υπέρ του κατόχου (η του αιτούμενου) ονόματος διαδικτύου, δικαίωμα ανάλογο με αυτό επί του σήματος ή δικαίωμα αντίστοιχο με εκείνα που προβλέπονται στο δίκαιο πνευματικής ιδιοκτησίας.

Ενόψει του εν πολλοίς αρρύθμιστου περιβάλλοντος του διαδικτύου και της ρευστότητας ως προς τη λειτουργία των διακριτικών γνωρισμάτων στο διαδίκτυο, η στάση αυτή είναι δικαιολογημένη.

Από νομικής απόψεως θα πρέπει να γίνει δεκτό ότι παρέχεται στον κάτοχο τουλάχιστον δικαίωμα χρήσης κατ' αναλογία με την εκχώρηση αριθμών τηλεφώνου. Το δικαίωμα αυτό είναι, θα πρέπει να γίνει δεκτό, ισχυρότερο εκείνου επί του αριθμού τηλεφώνου λόγω της ισχυρότερης εξατομικευτικής λειτουργίας του ονόματος διαδικτύου και της σύνδεσης με αυτό της επιχειρηματικής ή επικοινωνιακής δραστηριότητας του προσώπου ή της επιχείρησης.

Με την αναγνώριση δικαιώματος χρήσης τονίζεται επίσης ο χαρακτήρας της διευθυνσιοδότησης ως λειτουργίας της διοίκησης, αφού αποτελεί τμήμα της αριθμοδότησης και αφορά έτσι τη διαχείριση σπάνιων πόρων, η οποία επιφυλάσσεται στην οργανωμένη πολιτεία.

Επί των πόρων αυτών δεν νοείται να υπάρχει αποκλειστικό ή/ και απόλυτο δικαίωμα.

Με το χαρακτηρισμό του δικαιώματος του κατόχου ονόματος διαδικτύου ως δικαιώματος χρήσης γίνεται σαφές ότι πρόκειται για δικαίωμα το οποίο θα πρέπει να μπορεί να λήγει σχετικά εύκολα και για λόγους διαχείρισης του διαδικτύου και αποτελεσματικής λειτουργίας του ή έστω να τελεί υπό την αίρεση μιας περιοδικής ανανέωσης κατά τρόπο ανάλογο με εκείνον του δικαιώματος στο σήμα.

Το δικαίωμα χρήσης, θα πρέπει να γίνει δεκτό, ότι δεν μπορεί καταρχήν να υπερισχύσει δικαιώματος στο σήμα ή στην επωνυμία. Δικαίωμα σε κατοχύρωση ονόματος διαδικτύου είναι φυσικό να μπορεί να αποκτήσει κάθε συναλλασσόμενος, θα ενισχύονταν δε η σημασία του στην, απίθανη με τα σημερινά δεδομένα, περίπτωση που η παροχή πρόσβασης στο διαδίκτυο θα χαρακτηριζόταν ως υποχρέωση που εντάσσεται στην

καθολική υπηρεσία των τηλεπικοινωνιακών οργανισμών ως ελάχιστο απαιτούμενο παροχής.

10.6 **Προστασία διακριτικών γνωρισμάτων**

Ζητήματα προστασίας διακριτικών γνωρισμάτων στο διαδίκτυο ανακύπτουν όταν καταχωρημένο όνομα διαδικτύου είναι όμοιο ή παρουσιάζει σημαντική ομοιότητα με άλλο διακριτικό γνώρισμα (σήμα, επωνυμία, σήμα φήμης, άλλο όνομα διαδικτύου), οπότε το καταχωρημένο όνομα διαδικτύου φέρεται να προσβάλλει (άλλο) διακριτικό γνώρισμα.

Το καταχωρημένο όνομα διαδικτύου θα πρέπει να εκφράζεται με την ίδια ή παρόμοια λεκτική διατύπωση και να δημιουργεί την ίδια ηχητική ή/ και οπτική εντύπωση με το διακριτικό γνώρισμα, το δικαίωμα στο οποίο φέρεται να προσβάλλεται. Η ειδική νομοθεσία για τα διακριτικά γνωρίσματα ή οι γενικές διατάξεις του εμπορικού ή αστικού δικαίου μπορούν να αποτελέσουν τη βάση της προστασίας των διακριτικών γνωρισμάτων από καταχωρήσεις στο διαδίκτυο. Η προστασία έως τώρα παρέχεται σχεδόν αποκλειστικά με βάση το δίκαιο του αθέμιτου ανταγωνισμού.

10.7 **Αθέμιτος ανταγωνισμός**

Όλες ανεξαιρέτως οι αποφάσεις των ελληνικών δικαστηρίων σε ζητήματα προστασίας διακριτικών γνωρισμάτων στο διαδίκτυο βασίστηκαν στο δίκαιο του ανταγωνισμού.

Μέχρι στιγμής δεν υπάρχει απόφαση που να αφορά την προστασία σήματος. Οι έως τώρα αποφάσεις αφορούσαν προσβολή σε δικαίωμα στην επωνυμία ΜονΠρΑθηνών 1250/2000, ΕΕμπΔ 2000, σελ. 386.σε διακριτικό τίτλο Μον Πρ Αθηνών 9689/1999. ή σε άλλο διακριτικό Γνώρισμα Μον Πρ Σύρου 637/1999.

Με την εξαίρεση μίας, όλες οι αποφάσεις βασίστηκαν στα άρθρα 1 και 13 του ν.146/14 αν και κατά περιπτώσεις αναφέρθηκε ως βάση της προστασίας ειδικά για την περίπτωση της επωνυμίας και ο ν.1089/1980 περί εμπορικών και βιομηχανικών επαγγελματικών και βιοτεχνικών επιμελητηρίων.

Ιδίως το άρθρο 8 σχετικά με τα δικαιώματα του κατόχου επωνυμίας και τίτλου. Έμφαση δόθηκε στο άρθρο 13 του ν.146/14 που επιβάλλει να αποδειχθεί ο κίνδυνος σύγχυσης από τη χρήση του ονόματος διαδικτύου στις συναλλαγές.

Ο κίνδυνος σύγχυσης έγινε δεκτός με βάση την ακουστική και ηχητική ομοιότητα ανάμεσα στο διακριτικό γνώρισμα και το όνομα διαδικτύου που είχε καταχωρήσει ο καθ' ου, η οποία κατά τα διδάγματα της κοινής πείρας μπορούσε να προκαλέσει σύγχυση στο καταναλωτικό κοινό.

Τονίστηκε ειδικά για την καταχώρηση ονόματος διαδικτύου ότι έχει απλά δηλωτική σημασία και αποτελεί μαχητό τεκμήριο ότι ο πρώτος καταχωρήσας είναι δικαιούχος του διακριτικού γνωρίσματος

Στις υποθέσεις SMARTNET ΜονΠρΑθηνών 9689/1999. Αφορούσε την κατοχύρωση του ονόματος διαδικτύου που περιείχε τη λέξη SMARTNET,η οποία περιλαμβανόταν στην επωνυμία της αιτούσας και ήταν διακριτικός τίτλος της αιτούσας.

Η αιτούσα ήταν εταιρεία που παρείχε υπηρεσίες εγκατάστασης δικτύων Η/Υ, τηλεπικοινωνιακών, ηλεκτρολογικών και ηλεκτρικών δικτύων και εμπορευόταν το σχετικό εξοπλισμό.

Η καθ' ης διατηρούσε κατάστημα εμπορίας ηλεκτρονικών υπολογιστών και συναφούς υλικού, χρησιμοποιούσε δε τον ανωτέρω διακριτικό τίτλο στις υπηρεσίες τις οποίες προσέφερε για πρόσβαση στο διαδίκτυο και στην εμπορία κατάλληλου ηλεκτρονικού εξοπλισμού.

Το δικαστήριο θεώρησε ότι είναι δίδαγμα της κοινής πείρας ότι η μεγάλη οπτική ομοιότητα δύο παραστάσεων και η ταυτιζόμενη ηχητική των, μπορεί να προκαλέσει σύγχυση στο μέσο συναλλασσόμενο κοινό.

Τόνισε δε ότι πολλοί συναλλασσόμενοι με την αιτούσα νόμιζαν ότι οι δύο εταιρείες συνεργάζονταν.

Το δικαστήριο διέγνωσε ιδιαίτερα τον ανταγωνιστικό σκοπό της καθ' ης., ΕΛΕΞ ΠρΑθηνών 1250/2000, ΕΕμπΔ 2000, σελ. 386.

Η αιτούσα ήταν εταιρεία εισαγωγής και εμπορίας ηλεκτρικών ειδών (τηλεοράσεων, στερεοφωνικών, ασύρματων τηλεφωνικών συσκευών κλπ). Το ΕΛΕΞ ήταν τμήμα της επωνυμίας της.

Η καθ' ης ήταν εταιρεία εισαγωγής και εμπορίας ηλεκτρονικών ειδών κινητής τηλεπικοινωνίας. Κατοχύρωσε το elex ως όνομα διαδικτύου (και χρησιμοποιούσε το ΕΛΕΞ στις συναλλαγές της).

Επήλθε έτσι, όπως θεώρησε το δικαστήριο, σύγχυση μεταξύ των καταναλωτών και των συνεργατών της αιτούσας, αφού η αιτούσα και η καθ' ης σε ορισμένα σημεία έχουν κοινούς εμπορικούς στόχους, η δε αιτούσα αδυνατούσε να δημιουργήσει ανάλογη με της καθ' ης σελίδα στο διαδίκτυο.

Πρόκειται για τη γνωστή υπόθεση όπου η αιτούσα εταιρεία λιανικής πώλησης βιβλίων και κασετών μέσω του διαδικτύου ήταν δικαιούχος του ονόματος διαδικτύου amazon.com, το οποίο αποτελούσε τμήμα της επωνυμίας της και διακριτικό της τίτλο, είχε δε δημιουργήσει το πρώτο ηλεκτρονικό ψηφιακό βιβλιοπωλείο, η δε καθ' ης δραστηριοποιούνταν μέσω των amazon.gr και amazon.com.gr τα οποία είχε κατοχυρώσει ως ηλεκτρονικό βιβλιοπωλείο.

Το δικαστήριο τόνισε ότι το διακριτικό .gr δεν διαφοροποιεί την εντύπωση του χρήστη ότι έχει βρει το ελληνικό παράρτημα της αιτούσας, από δε την οπτική και ηχητική ομοιότητα των ενδείξεων των καθ' ων και εκείνων της αιτούσας προέκυψε πρόθεση των καθ' ων να εκμεταλλευτούν τη σύγχυση που επέρχεται με την αθέμιτη χρησιμοποίηση του διακριτικού γνωρίσματος το αντικείμενο της δραστηριότητας των καθ' ων ήταν τουλάχιστον συναφές με εκείνο των αιτούντων.

Αντιθέτως, στις υποθέσεις Stargate και Data Defender Group. Πρόκειται για αιτήσεις ασφαλιστικών μέτρων της Οργανωτικής Επιτροπής Ολυμπιακών Αγώνων Αθήνα 2004 Α.Ε. κατά των δικαιούχων των ονομάτων διαδικτύου olympicgames2004.gr και athensolympics.gr.

Οι αιτήσεις βασίστηκαν εκτός των άλλων στις διατάξεις του άρθρου 31,7 του ν.2598/1998 (ΦΕΚ Α 66) σύμφωνα με τις οποίες οι όροι, εκτός των άλλων, Ολυμπιακός, Ολυμπιάδα, ο διακριτικός τίτλος της αιτούσας Αθήνα 2004 Ολυμπιακοί Αγώνες Αθήνα 2004, Ολυμπιακοί Αγώνες 2004, Ολυμπιακοί Αγώνες 196 Ελλάδα προστατεύονται υπέρ της αιτούσας με βάση τις διατάξεις του ν.2239/1994, η δε απαγόρευση χρήσης των όρων αυτών από τρίτους επεκτείνεται και στις χρήσεις των όρων αυτών στο Internet (άρθρο 37, ν.2598/1998).

Έγινε επίσης επίκληση ειδικών για την αιτούσα διατάξεων του ν.2819/2000 (ΦΕΚ Α, 84,) για την ίδρυση Ολυμπιακού Χωριού κ.ά. Οι καθ' ων ήταν παροχείς, εκτός των άλλων, υπηρεσιών διαδικτύου, όπως η κατασκευή ιστοσελίδων. Τονίστηκε στην υπόθεση Stargate ότι η μικρή παραλλαγή των προστατευομένων διακριτικών γνωρισμάτων δεν παρεμποδίζει τον κίνδυνο σύγχυσης και ότι από τα κατοχυρωθέντα ονόματα διαδικτύου ήταν δυνατόν να δημιουργηθεί η εντύπωση στους χρήστες ότι υπήρχε σχέση μεταξύ της αιτούσας και των καθ' ων.

Για πρώτη φορά στις εν λόγω αιτήσεις ασφαλιστικών μέτρων, η αιτούσα στρέφεται, εύστοχα, και εναντίον του ΙΤΕ-ΙΠ, ώστε με την απόφαση να διατάσσονται συγκεκριμένες ενέργειες του διαχειριστή της διευθυνσιοδότησης, όπως η διακοπή της καταχώρισης.

Έγιναν σχετικές καταχωρήσεις σε ημερήσιες εφημερίδες (βλ. Κυριακάτικη Ελευθεροτυπία 19-11-2000). καθώς και στην υπόθεση BMG ΜονΠρωτΑθ 1318/8-2-2001. Η αιτούσα, της οποίας, η επωνυμία περιείχε το στοιχείο BMG και το οποίο ήταν και διακριτικός της τίτλος, ήταν εταιρεία παραγωγής μουσικών και γενικά φωνητικών εκτελέσεων.

Η πρώτη των καθ' ων ήταν εταιρεία παροχής υπηρεσιών διαδικτύου και είχε, κατά την απόφαση, κατοχυρώσει το όνομα διαδικτύου bmg.gr. Η εν λόγω εταιρεία ισχυρίστηκε έλλειψη παθητικής νομιμοποίησης, διότι είχε κατοχυρώσει το όνομα διαδικτύου για λογαριασμό πελάτη της. η ομοιότητα του αντικείμενου κάθε άλλο παρά προφανής ήταν.

Στην υπόθεση Stargate, όπου, αν και υπήρχε ειδική νομοθετική πρόβλεψη για την προστασία της επωνυμίας, θα αρκούσε ο ν.146/1914 ως

βάση για την προστασία του γνωρίσματος, τονίστηκε ότι, αν και υπήρχαν μικρές παραλλαγές μεταξύ ονόματος διαδικτύου και προστατευόμενου γνωρίσματος, δεν αποτρεπόταν ο κίνδυνος σύγχυσης, το δε μέτρο για τη διαπίστωση του κινδύνου σύγχυσης απετέλεσε η εντύπωση που μπορεί να δημιουργηθεί στο μέσο καταναλωτή. Ας σημειωθεί εδώ ότι η σύγχυση θα αφορούσε την επωνυμία οργανισμού (Οργανωτική Επιτροπή Ολυμπιακών Αγώνων Αθήνα 2004 Α.Ε.), ο οποίος στο μέσο καταναλωτή είναι αμφίβολο εάν θα γίνει γνωστός.

Στην υπόθεση BMG η μεν αιτούσα είχε ως αντικείμενο δραστηριότητας την παραγωγή φωνητικών και εν γένει μουσικών εκτελέσεων, η δε καθ' ης, τη διαμόρφωση ιστοσελίδων και την καταχώρηση ονομάτων διαδικτύου. Ο κίνδυνος σύγχυσης τεκμαίρεται απλά από την ομοιότητα του ονόματος διαδικτύου προς την επωνυμία της αιτούσας.

Στην υπόθεση ΕΕΤΕΜ Μον Πρωτ Λασ 496/2000. Το αιτούν ήταν αστικό σωματείο (επιστημονική ένωση) και ο καθ' ου, πρώην μέλος του. Η απόφαση επικαλέστηκε την προστασία του ονόματος με βάση τη διάταξη του 58 ΑΚ, σύμφωνα με την οποία προστατεύεται κατ' αναλογία η επωνυμία σωματείου.

Το δικαστήριο πιθανολόγησε τη σύγχυση των καταναλωτών/ χρηστών με βάση την οπτική και ηχητική ομοιότητα του ονόματος διαδικτύου με την επωνυμία του σωματείου, βασίστηκε όμως για την απόφασή του στο άρθρο 1 του ν.146/1914, θεωρώντας αθέμιτη τη χρήση της επωνυμίας του σωματείου από μέλος του και με σαφή πρόθεση εκμετάλλευσης της φήμης του σωματείου, το δικαστήριο αποφάσισε υπέρ του αιτούντος αστικού σωματείου εναντίον ενός πρώην μέλους του, αγνοώντας τους ισχυρισμούς του καθ' ου περί διαφορετικής εμφάνισης του ονόματος διαδικτύου (δεν υπήρχαν τελείες ανάμεσα στα γράμματα).

Όπως αναφέρθηκε, το γεγονός ότι στην ηλεκτρονική διεύθυνση του καθ' ου υπάρχουν τελείες ανάμεσα στα γράμματα του ακρωνυμίου, δεν επιτελεί διακριτική λειτουργία και δεν διαφοροποιεί στο ελάχιστο την εντύπωση του χρήστη, ο οποίος πιστεύει ότι έχει εισαχθεί στην ηλεκτρονική σελίδα του

αιτούντος σωματείου και περί διαφορετικής σημασίας των γραμμάτων του ακρωνυμίου.

Η στάση αυτή του δικαστηρίου έχει ιδιαίτερη σημασία διότι είναι μάλλον συχνό το φαινόμενο της καταχώρησης ακρωνυμίων ως ονομάτων διαδικτύου τα οποία είναι ομόηχα με επωνυμίες, διακριτικούς τίτλους ή ονόματα διαδικτύου με κατάληξη .com, με διαφορετική σημασία των γραμμάτων του ακρωνυμίου, όπως τουλάχιστον ισχυρίζονται οι κάτοχο, με βάση το άρθρο 1 του ν.146/1914, θεωρώντας ότι η χρήση (και προφανώς και μόνη η καταχώρηση) του επίδικου ονόματος διαδικτύου αποτελεί σαφώς πράξη αθέμιτου ανταγωνισμού.

Είναι ορθό το ότι στην έως τώρα νομολογία και ιδίως με τις αποφάσεις στις υποθέσεις Stargate, Data Defender Group και BMG, εκφράζεται η αποφασιστικότητα των δικαστηρίων:να προστατεύσουν έγκαιρα τα διακριτικά γνωρίσματα που προϋπάρχουν των ονομάτων διαδικτύου,να εναρμονίσουν τη ρύθμιση των ονομάτων διαδικτύου με εκείνη των άλλων διακριτικών γνωρισμάτων,να μη θεωρούν ως ιδιαίτερο χώρο συναλλαγών το διαδίκτυο, να μην περιορίζονται από ιδιαιτερότητες των ονομάτων διαδικτύου, όπως η (υποτιθέμενη) ευχέρεια διάκρισης με βάση μικροδιαφορές στην οπτική ή ηχητική εντύπωση,να χρησιμοποιήσουν ως μέτρο κρίσης το μέσο καταναλωτή, και όχι τον ειδικευμένο ούτε μάλιστα το χρήστη διαδικτύου.

Το σύνολο των κατευθύνσεων αυτών κρίνεται θετικά.

Θα ήταν μάλιστα δυνατόν να θεωρηθεί ότι με το να αρκείται η νομολογία στις υποθέσεις Stargate, Data Defender Group και BMG στη φαινομενική σύμπτωση της ταυτότητας του δικαιούχου του διακριτικούγνωρίσματος, η οποία είναι δυνατόν να συναχθεί από την οπτική και ηχητική ομοιότητα, στην πραγματικότητα προσφέρει εκτεταμένη προστασία.

Ορθό είναι επίσης να σημειωθεί ότι στην κρίση των δικαστηρίων υφέρπει σταθερά μια αρνητική αξιολόγηση του καθ' ου τα ασφαλιστικά μέτρα και ότι η αξιολόγηση αυτή βαρύνει τελικά αποφασιστικά στο τελικό αποτέλεσμα.

Ας σημειωθεί ότι η συναγωγή καταχρηστικής συμπεριφοράς είναι ευχερής σε όλες τις έως τώρα περιπτώσεις. Θα μπορούσε βέβαια να θεωρηθεί ότι, αν και στην εξέλιξή της η νομολογία δείχνει μεγαλύτερη εξοικείωση με το διαδίκτυο, η πραγματικότητα είναι ότι δεν είχε έως τώρα την ευκαιρία να εμβαθύνει στις ιδιαιτερότητες του διαδικτύου και της ονοματοδοσίας σε αυτό. Ο αντίλογος εδώ θα ήταν ότι η διαφοροποίηση της ρύθμισης για το διαδίκτυο δεν φαίνεται να δικαιολογείται από τις ανάγκες και τις συνθήκες στις συναλλαγές.

Η ιδιαίτερη μεταχείριση του διαδικτύου αφορά περισσότερο τη διαχείρισή του τον αποτελεσματικό έλεγχο στην καταχώρηση, την άμεση λήξη καταχωρίσεων, αν υπάρχει ανάγκη, την επίλυση των διαφορών παρά την αντιμετώπισή του στις συναλλαγές.

Ας τεθεί ως προβληματισμός ότι στα πλαίσια του γενικά αρρύθμιστου διαδικτύου, τα δικαστήρια δεν εμβαθύνουν στις λεπτομέρειες της διακριτικής λειτουργίας των εκάστοτε διακριτικών γνωρισμάτων, αλλά στέκονται στη γενικότερη εικόνα της αθέμιτης ανταγωνιστικής πρακτικής.

10.8 **Προστασία σημάτων**

Είναι δυνατόν το καταχωρημένο όνομα διαδικτύου να παρουσιάζει σημαντική τουλάχιστον ομοιότητα με κατατεθειμένο σήμα και να δημιουργεί τον κίνδυνο συσχέτισης του ονόματος και του κατόχου αυτού ή, για παράδειγμα, του διαφημιζόμενου στις αντίστοιχες ιστοσελίδες με το δικαιούχο του δικαιώματος σε κατατεθειμένο σήμα ή σε σήμα φήμης .

Με βάση τη σχετική νομοθεσία περί σημάτων, η οποία εδράζεται επί της αρχής της χρονικής προτεραιότητας, θα πρέπει να υφίσταται κίνδυνος σύγχυσης από την καταχώρηση ή/ και χρήση του ονόματος διαδικτύου (άρθρο 261 του ν.2239/1994).

Από την έως τώρα εμπειρία θα πρέπει να συναχθεί ότι η αποδοχή της προϋπόθεσης της σύγχυσης δεν θα πρέπει να παρουσιάζει δυσχέρειες, ιδίως αν υπάρχουν στοιχεία κακοπιστίας ως προς την καταχώρηση.

Εάν βέβαια δεν υφίσταται κίνδυνος σύγχυσης, θα πρέπει να γίνει δεκτό ότι η αρχή της χρονικής προτεραιότητας θα πρέπει να εφαρμόζεται και υπέρ του κατόχου ονόματος διαδικτύου σε βάρος του αμελού ως προς την καταχώρηση στο διαδίκτυο δικαιούχου δικαιώματος σε σήμα .

Ιδίως ως προς τα ονόματα φήμης, η επιπλέον προϋπόθεση της αθέμιτης εκμετάλλευσης (άρθρα 4 και 261 του ν.2239/1994) του διακριτικού χαρακτήρα του σήματος φήμης, ίσως δημιουργήσει ζητήματα, ιδίως όσον αφορά την απόδειξη της αθέμιτης εκμετάλλευσης, και πάλι όμως το πιθανότερο είναι ότι τα δικαστήρια δεν θα δυσκολευτούν να προστατεύσουν τους δικαιούχους των σημάτων.

Σύγκρουση διακριτικών γνωρισμάτων

Δυσκολότερη θα είναι η περίπτωση που δύο διακριτικά γνωρίσματα του υλικού κόσμου συγκρούονται με καταχώρηση ονόματος διαδικτύου. Η διαφορά θα λυνόταν στη βάση της αρχής της χρονικής προτεραιότητας ως προς την καταχώρηση στο διαδίκτυο, εφόσον δεν συνάγεται κακοπιστία στη συμπεριφορά κάποιου μέρους. Προϋπόθεση εφαρμογής της αρχής της χρονικής προτεραιότητας είναι βέβαια η ύπαρξη κινδύνου σύγχυσης.

Αδικοπραξίες

Με βάση τις 914 και 919 ΑΚ θα ήταν δυνατόν να προστατευθεί ο κάτοχος διακριτικού γνωρίσματος, αφού η καταχώρηση του ονόματος διαδικτύου, με το οποίο προσβάλλεται το δικαίωμα άλλου σε διακριτικό γνώρισμα, θα είναι συνήθως παράνομη και άδικη πράξη. Αίτημα της αγωγής θα ήταν η παύση της προσβολής και η παράλειψή της στο μέλλον και πιθανώς η αποζημίωση του δικαιούχου διακριτικού γνωρίσματος.

Αν το δικαίωμα χρήσης του ονόματος διαδικτύου θεωρηθεί ενοχικής φύσης, ίσως τεθεί ζήτημα ως προς το κατά πόσο η προσβολή του είναι παράνομη.

Το παράνομο της προσβολής θα πρέπει να γίνει δεκτό με την έννοια της προσβολής της επιχειρηματικής και επαγγελματικής δραστηριότητας του δικαιούχου του διακριτικού γνωρίσματος

Αδικαιολόγητος πλουτισμός

Αν και ως νομικό πρόβλημα είναι ενδιαφέρον, η προστασία με βάση τις διατάξεις για τον αδικαιολόγητο πλουτισμό είναι αμφίβολη.

Είναι αμφίβολο κυρίως αν θα πληρούται η προϋπόθεση του πραγματικού και συγκεκριμένου του πλουτισμού, εάν δε το αίτημα της αγωγής αφορούς την απόδοση του ονόματος, είναι αμφίβολο εάν θα γινόταν δεκτό.

Μη γνήσια διοίκηση αλλοτρίων

Προστασία με βάση τις διατάξεις για τη μη γνήσια διοίκηση αλλοτρίων (739 ΑΚ) είναι ενδεχόμενη στις περιπτώσεις που συνεργαζόμενοι με το δικαιούχο του διακριτικού γνωρίσματος κατοχυρώσουν χωρίς εξουσιοδότηση όνομα διαδικτύου που προσβάλλει το διακριτικό γνώρισμα. Εάν υπάρχει εξουσιοδότηση είναι δυνατόν να θεμελιωθεί προστασία στις διατάξεις για τη γνήσια διοίκηση αλλοτρίων (736 ΑΚ επ.) και τις διατάξεις για την εντολή(722, 723 ΑΚ)

Προστασία της προσωπικότητας

Αποτελεί ίσως την πλέον ενδιαφέρουσα εκδοχή στην προστασία των διακριτικών γνωρισμάτων. Οι διατάξεις 57επ ΑΚ μπορούν, κατά πάσα πιθανότητα, να παράσχουν αποτελεσματική προστασία. Ας σημειωθεί εδώ η ειδική διάταξη για την προστασία του ονόματος (58 ΑΚ).

Για την ακρίβεια, η εντύπωση που δημιουργείται είναι ότι λίγο απέχει η νομολογία από το να δεχθεί την προστασία διακριτικού γνωρίσματος με βάση τις προβλέψεις για την προστασία της προσωπικότητας του ΑΚ.

.

10.9 **Συμπέρασμα**

Γεγονός είναι ότι η νομολογία έως τώρα δεν έτυχε να αντιμετωπίσει ιδιαίτερα περίπλοκες υποθέσεις.

Η πρόθεση κατάχρησης του ονόματος από τους καθ' ων ήταν μάλλον ευχερώς διαπιστώσιμη.

Το γεγονός αυτό δεν θα πρέπει να μειώσει τη σημασία της αποφασιστικής αντίδρασης των δικαστηρίων υπέρ κατοχυρωμένων διακριτικών γνωρισμάτων.

Θα μπορούσε να ειπωθεί ότι στις έως τώρα αποφάσεις, το δικαστήριο παραμέρισε την αρχή της χρονικής προτεραιότητας στην καταχώρηση ονομάτων διαδικτύου προς το σκοπό της προστασίας νομικά ισχυρότερων διακριτικών γνωρισμάτων .Ορθότερο θα ήταν να ειπωθεί ότι το δικαστήριο εφάρμοσε την αρχή της χρονικής προτεραιότητας συνολικά στο χώρο των συναλλαγών χωρίς να απομονώνει το διαδίκτυο.

Θα ήταν περισσότερο αποτελεσματική η προστασία εάν τα δικαστήρια δέχονταν ότι και η απλή καταχώρηση ενός ονόματος διαδικτύου συνιστά μορφή χρήσης και προσβολή του διακριτικού γνωρίσματος στο βαθμό που αποκλείεται η δυνατότητα του νόμιμου δικαιούχου να κατοχυρώσει το διακριτικό γνώρισμα ως όνομα διαδικτύου.

Αυτή φαίνεται να είναι η άποψη του δικαστηρίου στην υπόθεση ΕΛΕΞ Μον Πρ Αθηνών 1250/2000, ΕΕμπΔ 2000, σελ. 386. Κρίθηκε ότι η αιτούσα αδυνατούσε να δημιουργήσει ανάλογη με της καθ' ης σελίδα στο διαδίκτυο.

10.10 **Δικαστική επιδίωξη προστασίας**

Η δικαστική προστασία παρουσιάζει σημαντικές αδυναμίες.

Το πρώτο πρόσφορο μέτρο προστασίας είναι η απόφαση ασφαλιστικών μέτρων, η οποία εκδίδεται σε τρεις έως τέσσερις μήνες, και με την οποία διατάσσεται κατά κανόνα η προσωρινή παύση της χρήσης του ονόματος στο διαδίκτυο, αλλά όχι και η λήξη της καταχώρησης, η οποία θα δώσει τη δυνατότητα στο δικαιούχο του διακριτικού γνωρίσματος να το κατοχυρώσει για λογαριασμό του, όπως είναι, πιθανότατα, και η τελική του πρόθεση.

Με βάση την πολιτική της ΕΕΤΤ και του ΙΤΕ-ΙΠ απαιτείται για τη λήξη της καταχώρησης, απόφαση μετά από τακτική αγωγή.

Αν και η πολιτική αυτή είναι τυπικά ορθή, ενόψει της ταχύτατης ανάπτυξης του διαδικτύου, θα ήταν εύλογο να προωθούνταν μία ταχύτερη διαδικασία ή να γινόταν η λήξη της καταχώρησης με την απόφαση ασφαλιστικών μέτρων και να μετετίθετο το βάρος της αποτροπής της λήξης στον ηττηθέντα κατά τη διαδικασία των ασφαλιστικών μέτρων ή με προσωρινή διαταγή.

Ας σημειωθεί ότι είναι μάλλον φρόνιμο να στρέφονται η αίτηση ασφαλιστικών μέτρων και η αγωγή και εναντίον της ΕΕΤΤ και/ ή του ΙΤΕ-ΙΠ, με σκοπό να διατυπωθεί συγκεκριμένη διαταγή του δικαστηρίου, όπως αυτή στην περίπτωση της BMG (ΜονΠρωτΑθ 1318/8-2-2001) που υποχρεώνει προσωρινά το δεύτερο των καθ' ων (ΙΤΕ-ΙΠ) να διαγράψει από τους καταλόγους του το όνομα περιοχής, όσο και αν η προσωρινή διαγραφή δύσκολα γίνεται κατανοητή.

10.11 **Διαιτητική επίλυση διαφορών**

Στην ανωτέρω απόφαση της ΕΕΤΤ προβλεπόταν η δυνατότητα διαιτητικής επίλυσης των διαφορών μεταξύ χρηστών και μεταξύ χρηστών και διαχειριστή της ονοματοδοσίας, με διαιτητή την ΕΕΤΤ. Η πρόβλεψη αυτή δεν έχει ενεργοποιηθεί έως σήμερα.

Εκτιμάται ότι παρουσιάζονται σημαντικά προβλήματα στο ενδεχόμενο διαιτητικής επίλυσης των διαφορών. Θα απαιτούνταν ίσως ρητή νομοθετική εξουσιοδότηση, εάν θεωρηθεί ότι δεν θα αρκούσε Προεδρικό Διάταγμα για τη σύσταση μόνιμης διαιτησίας.

Γεγονός είναι ότι, ενόψει των μεγάλων ελλείψεων σε προσωπικό και σε σχετική εμπειρία, το ενδεχόμενο διαιτητικής επέμβασης φαντάζει απίθανο. Η διαιτητική παρέμβαση θα έπρεπε ίσως να συνδυαστεί με τη δυνατότητα άσκησης πιέσεων προς τα εμπλεκόμενα μέρη.

Κάτι τέτοιο θα ήταν δυνατόν μόνο εάν και τα μέρη ήταν επιχειρήσεις εποπτευόμενες από την ΕΕΤΤ, για παράδειγμα επιχειρήσεις παροχής υπηρεσιών διαδικτύου.

Εξάλλου από την ελληνική εμπειρία φαίνεται πως οι περισσότεροι χρήστες που κάνουν κατάχρηση των δυνατοτήτων καταχώρησης του διαδικτύου είναι ευκαιριακά παραβάτες, οι οποίοι δύσκολα θα δέχονταν να υπαχθούν σε καθεστώς διαιτησίας.

10.12 **Γενικό συμπέρασμα**

Από τα έως τώρα αναφερόμενα συνάγεται ότι η στάση των ελληνικών δικαστηρίων σε ζητήματα προστασίας διακριτικών γνωρισμάτων από καταχωρήσεις στο διαδίκτυο είναι γενικά ικανοποιητική.

Οι ισχύουσες διατάξεις για την προστασία του ανταγωνισμού, την προστασία του σήματος και της προσωπικότητας παρέχουν προς το παρόν προστασία στους δικαιούχους, η οποία όμως ίσως να μην ανταποκρίνεται επαρκώς στις ιδιαιτερότητες του διαδικτύου, λόγω κυρίως της ταχύτητας με την οποία αναπτύσσεται και της ανεπάρκειας των προβλέψεων για τη διαχείριση της ονοματοδοσίας από τους αρμόδιους φορείς.

Το αίτημα αποτελεσματικότερης ρύθμισης και διαχείρισης των προβλημάτων που είναι δυνατόν να ανακύψουν είναι παραπάνω από ώριμο, όπως και η ρύθμιση του διαδικτύου γενικότερα. Σε κάποιες χώρες (Ιταλία) προωθήθηκαν νομοθετικές ρυθμίσεις για τη διευθυνσιοδότηση και την προστασία διακριτικών γνωρισμάτων στο διαδίκτυο.

Η έκδοση ενός σύγχρονου κανονιστικού κειμένου για τη διαδικασία καταχώρησης και τις αρχές που πρέπει να τη διέπουν είναι αναγκαία για τον ελληνικό χώρο.

Απαιτείται ειδική ρύθμιση για την ταχύτερη διευθέτηση αμφισβητήσεων επί ονομάτων διαδικτύου, όπως διαφαίνεται από τις προσπάθειες σε διεθνές επίπεδο. Απαιτείται επίσης ιδιαίτερη μελέτη της φυσιογνωμίας των συναλλασσομένων, των οποίων τα δικαιώματά ίσως θίγονται, διότι θα πρέπει να εξεταστεί εάν, για παράδειγμα, ενδείκνυται να είναι διαφορετική

η αντιμετώπιση των επιχειρήσεων που δραστηριοποιούνται κυρίως ή αποκλειστικά μέσω διαδικτύου και για τις οποίες ο αποκλεισμός από το διαδίκτυο θα έχει ιδιαίτερα σοβαρές συνέπειες.

Θα μπορούσαν εξάλλου να αποφευχθούν πιθανές αμφισβητήσεις ονομάτων με την επιβολή υποχρεώσεων όσον αφορά το περιεχόμενο των ιστοσελίδων, όπως, για παράδειγμα, να αναφέρεται ότι δεν αφορούν την πιθανώς θιγόμενη δραστηριότητα. Η αντιμετώπιση, τέλος, του θέματος της προστασίας διακριτικών γνωρισμάτων στο διαδίκτυο σε διεθνές επίπεδο μπορεί να παράσχει χρήσιμες κατευθύνσεις στον Έλληνα νομικό.

11 ΗΛΕΤΡΟΝΙΚΕΣ ΣΥΝΝΑΛΑΓΕΣ

Η συνεχώς αυξανόμενη εμπορευματοποίηση του Internet, και η χρήση του Web έχουν ωθήσει τις επιχειρήσεις στην εύρεση μεθόδων και συστημάτων πληρωμών για την υποστήριξη του Ηλεκτρονικού Εμπορίου.

Η πρακτική εφαρμογή του Ηλεκτρονικού Εμπορίου στο σύγχρονο επιχειρηματικό περιβάλλον απαιτεί την ύπαρξη συστημάτων ηλεκτρονικών πληρωμών μέσο των οποίων θα διεκπεραιώνονται ηλεκτρονικά οι οφειλές των εμπλεκόμενων μερών. Ήδη έχουν υιοθετηθεί διάφορα συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες ηλεκτρονικό χρήμα κλπ) κατάλληλα για την εξυπηρέτηση των συναλλαγών.

Στα συστήματα ηλεκτρονικών συναλλαγών εντάσσεται κάθε μέθοδος που χρησιμοποιείται για να εξυπηρετήσει την πραγματοποίηση αγορών μέσω του Internet. Ορίζοντας τις ηλεκτρονικές συναλλαγές με αυτό τον τρόπο, μπορούμε να συμπεριλάβουμε σε αυτές -εκτός από τις αμιγώς ψηφιακές- και κάποιες παραδοσιακές μεθόδους.

Έτσι, σύστημα ηλεκτρονικών συναλλαγών θεωρούνται όχι μόνο η χρήση πιστωτικών καρτών, το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές, αλλά και το έμβασμα, η αντικαταβολή, η μεταφορά χρημάτων σε λογαριασμό κ.ά.

Κοινό χαρακτηριστικό των παραπάνω μεθόδων είναι ότι μπορούν να ενσωματωθούν στη λειτουργία ενός online καταστήματος εξυπηρετώντας τις αγοραπωλησίες και το εν γένει ηλεκτρονικό εμπόριο.Υπάρχουν διεθνώς περισσότερα από 100 διαφορετικά συστήματα ηλεκτρονικών συναλλαγών, άλλα λιγότερο και άλλα περισσότερο επιτυχημένα

Ένα από τα πιο σημαντικά ζητήματα που σχετίζονται άμεσα με τη χρήση και τη διάδοση του Ηλεκτρονικού Εμπορίου αφορά το επίπεδο ασφάλειας των ηλεκτρονικών συναλλαγών.

11.1 **Ψηφιακό Χρήμα**

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξόφλησης μικροποσών μέσο του Internet. Ένας τέτοιος μηχανισμός μπορεί να αποτελέσει το επόμενο βήμα στις εφαρμογές ηλεκτρονικών πληρωμών. Σε ένα σύστημα ψηφιακού χρήματος, το νόμισμα δεν είναι τίποτα άλλο παρά μια σειρά από ψηφία..

Ένας χρήστης μπορεί να κάνει ανάληψη ψηφιακού χρήματος από μια τράπεζα μεταφέροντας το ποσό αυτό στον ηλεκτρονικό του υπολογιστή. Το ψηφιακό χρήμα που παραχωρείται από την τράπεζα σημαδεύετε κατάλληλα για λόγους εγκυρότητας και ασφάλειας. Σε περίπτωση αγοράς προϊόντων μέσο του Internet, ο αγοραστής ξαποστέλνει στον προμηθευτή το αντίτιμο σε ψηφιακό χρήμα. Ο τελευταίος με τη σειρά του, προωθεί στην τράπεζα τη ψηφιακή-ροή που έλαβε προκειμένου να διερευνηθεί κατά πόσο η ροή αυτή αποτελεί έγκυρη χρηματο-ροή ή όχι.

Για να διασφαλίσει ότι κάθε χρηματο-ροή (token) χρησιμοποιείται μόνο μια φορά, η τράπεζα καταγράφει τον σειριακό αριθμό κάθε token που ξοδεύεται Αν ο σειριακός αριθμός του token υπάρχει ήδη στην βάση δεδομένων, τότε η τράπεζα έχει εντοπίσει κάποιον που προσπάθησε να χρησιμοποιήσει περισσότερες από μια φορές το token και θα, πληροφορήσει τον έμπορο ότι αυτή η χρηματική μονάδα είναι άχρηστη.

Μία εναλλακτική λύση που αναπτύχθηκε από την DigiCash επιτρέπει στους χρήστες να διατηρήσουν την ανωνυμία τους. Ο εν λόγω μηχανισμός, που ονομάζεται «blind signature», επιτρέπει στον αγοραστή να λάβει ηλεκτρονικό χρήμα από μια τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα του αγοραστή με τα tokens που του διανέμονται. Η τράπεζα πρέπει να εκτιμήσει το token που λαμβάνει από τον έμπορο, μέσο της ψηφιακής στάμπας που έχει αρχικά τοποθετηθεί στα tokens του χρήστη αλλά η τράπεζα δεν μπορεί να καταλάβει ποιος έκανε την πληρωμή.

Οι βασικές απαιτήσεις για την ασφαλή διεξαγωγή του Ηλεκτρονικού Εμπορίου είναι η Εμπιστευτικότητα (Confidentiality), η Ακεραιότητα (Integrity), και ο Έλεγχος Αυθεντικότητας (Authentication).

Εμπιστευτικότητα (Confidentiality).

Η εμπιστευτικότητα είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy) καθώς και της προστασίας των μυστικών πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και παρέχεται μέσο κρυπτογράφησης.

Σε ένα ηλεκτρονικό περιβάλλον θα πρέπει να υπάρχει η βεβαιότητα ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται παραμένει αναλλοίωτο.

Ακεραιότητα (Integrity).

Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται και παρέχεται μέσο ψηφιακής υπογραφής. Τα δεδομένα που αποστέλλονται ως μέρος της συναλλαγής πρέπει να είναι μη τροποποιήσιμα κατά τη διάρκεια της μεταφοράς και αποθήκευσής τους στο δίκτυο.

Έλεγχος Αυθεντικότητας (Authentication).

Η διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα, αλλά και η βεβαιότητα ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο κατά την μεταφορά οριοθετούν την έννοια του ελέγχου αυθεντικότητας .

Σύμφωνα με τον παραπάνω ορισμό η πιστοποίηση της ταυτότητας των επιχειρήσεων που συμμετέχουν σε μία συναλλαγή είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να μπορεί να πεισθεί για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται μέσο ψηφιακής υπογραφής.

Εξουσιοδότηση (Authorization).

Η εξουσιοδότηση αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στον λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.

Εξασφάλιση (Assurance).

Η εμπιστοσύνη, ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνονται. Για παράδειγμα, μια από τις απαιτήσεις του πελάτη είναι η βεβαιότητα ότι ο έμπορος με τον οποίο συναλλάσσεται είναι νόμιμος και έμπιστος.

Μη αποποίηση ευθύνης (Non-repudiation).

Κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή.

11.2 Πιστωτικές

Οι πιστωτικές κάρτες αποτελούν παγκοσμίως το δημοφιλέστερο μέσο διεκπεραίωσης συναλλαγών στο Διαδίκτυο. Η ευκολία στη χρήση τους, το γεγονός ότι επιτρέπουν στους εμπλεκομένους να συναλλάσσονται online χωρίς πολλές διατυπώσεις, όπως και το ότι μπορούν να χρησιμοποιηθούν για αγορές σε ολόκληρο τον κόσμο, τις καθιστούν το πιο ελκυστικό διαδικτυακό μέσο πληρωμής.

Παρουσιάζουν ωστόσο και ορισμένα μειονεκτήματα.

Κατά πρώτον οι απάτες, καθώς συχνά καταγράφονται κρούσματα μη εξουσιοδοτημένης χρήσης πιστωτικών καρτών στο Διαδίκτυο, υπεξαίρεσης αριθμών, υποκλοπής κωδικών κ.λπ.

Κατά δεύτερον, οι περιορισμοί στην απόκτησή τους, καθώς ο κάτοχος θα πρέπει να έχει συμπληρώσει το 18ο έτος της ηλικίας του και να διαθέτει τραπεζικό λογαριασμό με κάποιο σεβαστό ποσό και την οικονομική άνεση για να πληρώνει συνδρομές, προμήθειες κ.λπ.

Σε μια παραδοσιακή συναλλαγή με πιστωτική κάρτα, ο προμηθευτής καταγράφει τα στοιχεία, της πιστωτικής κάρτας του πελάτη δημιουργώντας ένα έγγραφο συναλλαγής.

Το εν λόγω έγγραφο υπογράφεται από τον αγοραστή και προωθείται στη συνέχεια, στην τράπεζα για διεκπεραίωση. Στο τέλος η τράπεζα χρεοπιστώνει τους αντίστοιχους λογαριασμούς ενημερώνοντας τα εμπλεκόμενα μέρη για την συναλλαγή που έγινε.

Σε ένα μηχανισμό ηλεκτρονικής πληρωμής με χρήση πιστωτικής κάρτας, ακολουθείται περίπου το ίδιο σενάριο με αυτό που αναφέρθηκε στην περίπτωση της ηλεκτρονικής επιταγής. Επιπλέον το σενάριο αυτό, εμπλουτίζεται με μηχανισμούς ασφάλειας (π.χ. έλεγχος ταυτότητας πελάτη και εμπόρου). Το γεγονός αυτό έχει οδηγήσει στην ύπαρξη μιας γκάμας συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες. Δύο από τα χαρακτηριστικά που προσδιορίζουν και διαφοροποιούν τα συστήματα αυτά, είναι το επίπεδο της ασφάλειας των συναλλαγών, και το λογισμικό που απαιτείται από όλα τα εμπλεκόμενα μέρη (αγοραστής προμηθευτής, τράπεζα).

Κατά τη διάρκεια μιας on-line συναλλαγής, τα στοιχεία της πιστωτικής κάρτας ενός αγοραστή μπορούν να μεταφερθούν με δύο τρόπους. Ο πρώτος τρόπος θεωρείται μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο (ή την τράπεζα) σε μη κρυπτογραφημένη μορφή. Η μέθοδος αυτή κρίνεται ως μη ασφαλής γιατί κατά τη μεταβίβαση των στοιχείων μπορεί να παρεισφρήσει κάποιος εισβολέας και να τροποποιήσει τα στοιχεία, της συναλλαγής ή ακόμη και να τα υποκλέψει. Ο δεύτερος τρόπος, θεωρείται πιο ασφαλής και προβλέπει την κρυπτογράφηση όλων πληροφοριών που σχετίζονται με τη πληρωμή πριν την αποστολή τους στον έμπορο (ή την τράπεζα) μέσο του Internet .

Για την αποφυγή της παρεμβολής κάποιου τρίτου κατά την διεξαγωγή των συναλλαγών μεταξύ του πελάτη και του εμπόρου, μια καλή επιλογή αποτελεί εκείνος ο συνδυασμός web browser και web server που θα υποστηρίζει το πρωτόκολλο Secure Sockets Layer (SSL).

Η χρησιμοποίηση web servers και web browsers που υποστηρίζουν το πρωτόκολλο SSL, εξασφαλίζει την προστασία των δεδομένων από κάποιον τρίτο. Δεν εγγυάται όμως ότι τα δεδομένα αυτά δεν θα χρησιμοποιηθούν σκόπιμα από τον έμπορο.

Για την αποφυγή εξαπάτησης του πελάτη από τον έμπορο (για. παράδειγμα, χρήση των στοιχείων της πιστωτικής κάρτας από τον έμπορο για την διεξαγωγή μη εξουσιοδοτημένων αγορών), θα μπορούσε να χρησιμοποιηθεί ένας ανεξάρτητος φορέας διασφάλισης των συναλλαγών

γνωστός ως Έμπιστη Τρίτη Οντότητα (ΕΤΟ). Μία ΕΤΟ μεσολαβεί ανεξάρτητα στην όλη διαδικασία, αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας επικυρώνοντας τη συναλλαγή .

11.3 Το πρόγραμμα Η/Υ ως μέσο διακίνησης και διασφάλισης της περιουσίας

Το πρόγραμμα Η/Υ λειτουργεί στην παραγωγική διαδικασία και ως μέσο διασφάλισης και διακίνησης περιουσιακών στοιχείων. Η χρήση κωδικής κάρτας (cashcard) και του μυστικού της κωδικού αριθμού (PIN) με σκοπό την ανάληψη χρημάτων από τερματικό υπολογιστή τράπεζας ήταν από τις πρώτες περιπτώσεις όπου εμφανίστηκε αυτή η λειτουργία του προγράμματος.

Ο χρήστης της κάρτας και του μυστικού αριθμού της χρεώνει τον αντίστοιχο τραπεζικό λογαριασμό χωρίς την παρεμβολή ανθρώπου.

Οι τραπεζικές εργασίες από απόσταση (homebanking, telebanking), με τις οποιες είναι δυνατή η μεταφορά οποιουδήποτε χρηματικού ποσού από ένα λογαριασμό σε άλλον χωρίς τη μεσολάβηση ανθρώπου παρά μόνο εκείνου που αποφασίζει και εκτελεί τη μεταφορά, αποτελούν ακόμα μία περίπτωση. Η χρήση μίας ιστοσελίδας στο διαδίκτυο και ενός μυστικού κωδικού αριθμού καθιστούν εικονική την παρουσία ενός πελάτη σε μια τράπεζα, αφού υπάρχει και λειτουργεί μόνο μέσα στο διαδίκτυο.

Με τον τρόπο αυτό διενεργούνται χρεοπιστώσεις ενός ή περισσότερων τραπεζικών λογαριασμών με οποιοδήποτε ποσό χωρίς την παρεμβολή ανθρώπινου στοιχείου. Η από απόσταση πρόσβαση σε αγαθά και υπηρεσίες, μέσω υπολογιστή και προγράμματος το οποίο υποκαθιστά τον πωλητή, είναι ένας άλλος τομέας όπου το πρόγραμμα λειτουργεί ως μέσο διακίνησης και διασφάλισης της περιουσίας.

Όταν κάποιος κάνει χρήση στο διαδίκτυο μίας ιστοσελίδας «εικονικής» βιτρίνας καταστήματος, μπορεί να αγοράσει ένα αγαθό, π.χ ένα βιβλίο, και να χρεώσει έναν τραπεζικό λογαριασμό πιστωτικής κάρτας, χωρίς την παραμικρή παρεμβολή ανθρώπινου στοιχείου. Το πιστωτικό όριο της

κάρτας ελέγχεται από το κατάλληλο πρόγραμμα που συνδέει την εκδότρια τράπεζα της κάρτας και την επιχείρηση που πουλάει το αγαθό. Εφόσον εγκριθεί η χορήγηση πίστωσης, θεωρείται συναφθείσα η σύμβαση, ο λογαριασμός της κάρτας χρεώνεται και έπειτα παρεμβαίνει το ανθρώπινο στοιχείο, το οποίο, αφού ελέγξει τα παραπάνω, αποστέλλει το αγαθό στον αγοραστή.

Σήμερα, αναπτύσσονται διεθνώς όλο και περισσότερα συστήματα διακίνησης περιουσιακών στοιχείων, κυρίως χρήματος, με πλήρη αυτοματισμό, όπως για παράδειγμα η λειτουργία της ηλεκτρονικής φορτωτικήςκαι το σύστημα των άϋλων τίτλων .Η τάση είναι η περαιτέρω αυτοματοποίηση όλων των συστημάτων πληρωμών.

Τα κύρια χαρακτηριστικά αυτών των συστημάτων είναι η πλήρης αυτοματοποίηση των περιουσιακών μετατοπίσεων και η διασφάλιση της νομιμότητας χρήσης αυτών μόνο με τη χρήση ενός μυστικού κωδικού που «διαβάζεται» και «αναγνωρίζεται» από το πρόγραμμα του Η/Υ.

Στα ηλεκτρονικά αυτά συστήματα παράγονται και διακινούνται ανθρώπινες δηλώσεις βουλήσεως μέσω του κατάλληλου προγραμματισμού. Ο παράγων άνθρωπος δεν παρεμβαίνει για την ανταλλαγή των σχετικών δηλώσεων, παρά μόνο στην αρχική φάση του προγραμματισμού και κατόπιν για τον έλεγχο της ήδη επελθούσης περιουσιακής μετατόπισης.

Έπεται, ότι τα ανωτέρω αυτοματοποιημένα συστήματα διακίνησης της περιουσίας μέσω Η/Υ έχουν αποκτήσει ιδιαίτερη σημασία στη σύγχρονη κοινωνία. Καταλαμβάνουν μεγάλο μέρος των συναλλαγών και είναι βέβαιο ότι θα εκτοπίσουν εξολοκλήρου τα παραδοσιακά συστήματα διακίνησης χρήματος. Το κυρίαρχο υλικό στοιχείο των σύγχρονων αυτοματοποιημένων συστημάτων διακίνησης χρήματος είναι το πρόγραμμα Η/Υ, υπό την ιδιότητά του να διακινεί και να διασφαλίζει την περιουσία.

Η ιδιότητα αυτή του προγράμματος θα μπορούσε αναμφίβολα να χαρακτηριστεί ως ουσιώδες στοιχείο του σύγχρονου κοινωνικού χώρου, ώστε να μπορεί να συζητηθεί και η προστασία του ως εννόμου αγαθού. Η διαφύλαξη της ακεραιότητας αυτής της ιδιότητας- λειτουργίας του

προγράμματος Η/Υ αποτελεί προϋπόθεση για την ασφαλή διακίνηση αγαθών και υπηρεσιών σε ολόκληρο τον πλανήτη.

Συνεπώς, θα νομιμοποιούνταν ο Έλληνας και διεθνής νομοθέτης να τυποποιήσουν ως έγκλημα τη χωρίς δικαίωμα χρήση της ιδιότητας του προγράμματος να διακινεί και να διασφαλίζει την περιουσία.

Η πράξη που συνιστά βλάβη για την ανωτέρω ιδιότητα του προγράμματος είναι η χρήση του χωρίς δικαίωμα. Η χρήση αυτή μπορεί να αφορά είτε την εξωτερική είτε την εσωτερική λειτουργία του προγράμματος.

Η επίδραση στην εσωτερική λειτουργία του συνίσταται στην αλλαγή της προσχεδιασμένης ροής του προγράμματος, με τη χρησιμοποίηση προγραμμάτων-ιών ή με ηλεκτρομαγνητικά μέσα.

Κατά μία άποψη, η επίδραση στην εξωτερική λειτουργία αφορά την τροφοδοσία του προγράμματος με δεδομένα, ανεξάρτητα εάν αυτά ανταποκρίνονται στην πραγματικότητα ή όχι, αρκεί να γίνεται η εισαγωγή τους χωρίς δικαίωμα.

Η βλάβη που προκαλείται για το προστατευόμενο έννομο αγαθό

Για την αναγκαιότητα να αποτελεί ένα υλικό αντικείμενο-ουσιώδες στοιχείο του κοινωνικού χώρου, ώστε να τυποποιηθεί ως αξιόποινη η προσβολή του.

Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου,

Το αγαθό «πρόγραμμα» από τις ανωτέρω πράξεις, αποτελεί όρο συγκεκριμένου κινδύνου για άλλα έννομα αγαθά που συνδέονται με αυτό, όπως η περιουσία, το υπόμνημα, το απόρρητο και άλλα.Έπεται λοιπόν η δυνατότητα του νομοθέτη να τυποποιήσει τη χωρίς δικαίωμα χρήση του προγράμματος, είτε με είτε χωρίς την απαίτηση να προσβάλλει αυτή και άλλο έννομο αγαθό.

Σε αρκετές περιπτώσεις, εταιρίες που παράγουν συστήματα ηλεκτρονικών πληρωμών όπως η Cybercash, η Verifone η First Virtual

χρησιμοποιούν μηχανισμούς με τους οποίους παρέχουν υπηρεσίες ΕΤΟ. Η Cybercash και η Verifone χρησιμοποιούν το μηχανισμό των wallet. Ο μηχανισμός αυτός μεταφέρει τον κρυπτογραφημένο αριθμό της πιστωτικής κάρτας από τον έμπορο στον δικό τους επεξεργαστή για τον έλεγχο αυθεντικότητας και την έγκριση της συναλλαγής.

Η εταιρία First Virtual εκδίδει κάποιο Virtual PIN στον πελάτη που το χρησιμοποιεί αντί του αριθμού της πιστωτικής κάρτας . Αφού λάβει τις πληροφορίες των πωλήσεων από τον έμπορο, η First Virtual μετατρέπει το virtual PIN στον αριθμό λογαριασμού της πιστωτικής κάρτας, προκειμένου να διεκπεραιωθεί η πληρωμή.

Σε αυτή την περίπτωση, η ηλεκτρονική ολοκλήρωση των συναλλαγών παρουσιάζει το εξής πλεονέκτημα έναντι του παραδοσιακού τρόπου πληρωμής με πιστωτική κάρτα: κρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας και με την μεσολάβηση μιας Τρίτης Έμπιστης Οντότητας, όπως η Cybercash ή η First Virtual, η επεξεργασία των στοιχείων αυτών δεν γίνεται από τον έμπορο, οπότε και εξαλείφεται ο κίνδυνος απάτης από την πλευρά του τελευταίου.

Στο σημείο αυτό, θα πρέπει να σημειωθεί ότι παρά την πρόοδο που έχει σημειωθεί στα συστήματα ηλεκτρονικών πληρωμών με χρήση πιστωτικών καρτών, εξακολουθούν να υπάρχουν ακόμη ορισμένα προβλήματα.

Το σημαντικότερο πρόβλημα που εξακολουθεί να υφίσταται ακόμη είναι η τυποποίηση. Θα πρέπει να υιοθετηθεί μια κοινά αποδεκτή μέθοδος διεκπεραίωσης των ηλεκτρονικών συναλλαγών στο Internet που θα επιτρέπει την επικοινωνία μεταξύ των διαφορετικών τύπων λογισμικού των συναλλασσομένων μερών.

Η εξασφάλιση ή όχι αυτής της διαλειτουργικότητας θα καθορίσει και την μελλοντική πορεία των ηλεκτρονικών συστημάτων πληρωμών μέσο πιστωτικής κάρτας.

Παρά τις ανωτέρω ενστάσεις, η πρωτοκαθεδρία των πιστωτικών καρτών στις δικτυακές συναλλαγές δεν μπορεί να αμφισβητηθεί. Ελάχιστα είναι τα ηλεκτρονικά καταστήματα που δεν τις δέχονται ως μέσο πληρωμής. Σχεδόν το σύνολο των e-shops παγκοσμίως κάνουν αποδεκτές όλες τις κάρτες

τύπου Visa και MasterCard, ενώ αρκετά ακόμη δέχονται και άλλα είδη καρτών (λ.χ. American Express). Οι πιστωτικές κάρτες μπορούν να εξυπηρετήσουν όλα τα είδη ηλεκτρονικών καταστημάτων και η ενσωμάτωσή τους στους τρόπους πληρωμής κρίνεται απαραίτητη. Βασική προϋπόθεση ομαλής λειτουργίας είναι οι πληρωμές με πιστωτική κάρτα να πραγματοποιούνται σε περιβάλλον ασύμμετρης κρυπτογράφησης και υψηλής ασφάλειας 128 bit, έτσι ώστε τα κρίσιμα δεδομένα των καρτών να μη διαρρέουν.

Υπεύθυνοι για αυτό είναι οι ιθύνοντες του ηλεκτρονικού καταστήματος, που οφείλουν να λαμβάνουν τις μέγιστες δυνατές προφυλάξεις.

Τέσσερις είναι οι πιο πρόσφορες λύσεις προκειμένου να μπορέσει το ηλεκτρονικό σας κατάστημα να υποστηρίξει ασφαλείς συναλλαγές με πιστωτικές Visa και MasterCard:

1. Απευθυνθείτε στις τράπεζες που παρέχουν υπηρεσίες ηλεκτρονικών συναλλαγών. Κάποιες τράπεζες έχουν ήδη αναπτύξει σύστημα ηλεκτρονικών συναλλαγών για πιστωτικές Visa και MasterCard, σε περιβάλλον ασύμμετρης **Σφάλμα! Η αναφορά της υπερ-σύνδεσης δεν είναι έγκυρη.** και υψηλής ασφάλειας 128bit. Τη στιγμή που ο πελάτης δηλώσει πρόθεση να προβεί σε αγορά από το κατάστημα συμπληρώνοντας τη σχετική φόρμα για τη χρέωση της πιστωτικής του κάρτας, μεταφέρεται αυτόματα στον server της τράπεζας, όπου σε ασφαλές περιβάλλον συμπληρώνει τα απαραίτητα στοιχεία.

Ακολούθως, η τράπεζα αναλαμβάνει την εκκαθάριση της συναλλαγής: ελέγχει την ορθότητα των στοιχείων της κάρτας, το πιστωτικό υπόλοιπο κ.λπ. και κατόπιν, εφόσον δοθεί η σχετική έγκριση, προχωρά στη χρέωση της κάρτας και πιστώνει το ποσό στον πωλητή, αφού αφαιρέσει τη συμφωνημένη προμήθεια. Από την πλευρά του, ο πωλητής (έμπορος) μπορεί να ενημερώνεται συνεχώς για τις δοσοληψίες και την κατάσταση των online παραγγελιών.

Το κόστος για τις παραπάνω υπηρεσίες διακρίνεται σε κόστος διασύνδεσης με το σύστημα (από 0 - 300 ευρώ), σε κόστος ετήσιας συντήρησης του συστήματος (από 150 - 300 ευρώ) και στην τραπεζική

προμήθεια που αποτελεί και το βασικό έσοδο των τραπεζών. Η προμήθεια αυτή ανέρχεται στο 3% περίπου της αξίας κάθε αγοραπωλησίας. Επισημαίνεται ότι για τα ποσά προμήθειας χρήσης και συντήρησης μπορεί να γίνει διαπραγμάτευση, ανάλογα και με τον τζίρο που θα πραγματοποιεί το ηλεκτρονικό κατάστημα.< υπηρεσιών παροχής εταιρία κάποια σε

2.Απευθυνθείτε>(ISP), που να ειδικεύεται στο ηλεκτρονικό εμπόριο. Υπάρχουν αρκετές εταιρίες στην Ελλάδα που αναπτύσσουν ολοκληρωμένες λύσεις δημιουργίας και φιλοξενίας e-shop. Αναλαμβάνουν εξολοκλήρου τη δημιουργία του ηλεκτρονικού καταστήματος, και μέσα στο όλο πακέτο υπηρεσιών που παρέχουν περιλαμβάνεται και η διαχείριση των ηλεκτρονικών συναλλαγών με πιστωτικές κάρτες, σε ασφαλές περιβάλλον και χωρίς την επαφή προμηθευτή - καταναλωτή. Χαρακτηριστικό παράδειγμα είναι το εικονικό εμπορικό κέντρο Agora (www.agora.gr), που έχει δημιουργηθεί από την Hellas On Line και φιλοξενεί αρκετά ηλεκτρονικά καταστήματα.

Το κόστος για τη διαχείριση των ηλεκτρονικών συναλλαγών με πιστωτική κάρτα περιλαμβάνεται στο συνολικό κόστος ανάπτυξης του ηλεκτρονικού καταστήματος, παρέχεται δηλαδή από τις εταιρίες στο πακέτο υπηρεσιών και γι' αυτό δεν μπορεί εύκολα να υπολογιστεί. Αυτό που πρέπει να τονιστεί είναι ότι η συντριπτική πλειονότητα των ISP δεν πρόκειται να παράσχει υπηρεσίες ηλεκτρονικών συναλλαγών χωρίς να έχει προηγηθεί η αγορά ολόκληρου του πακέτου από τον ενδιαφερόμενο.

3.Απευθυνθείτε στο Internet και στις ξένες εταιρίες που αναλαμβάνουν να εξυπηρετήσουν τις ηλεκτρονικές συναλλαγές με πιστωτική κάρτα, έναντι προμήθειας, η οποία συνήθως κυμαίνεται μεταξύ 2,5 και 3% για κάθε αγορά.

Τέτοια συστήματα είναι, μεταξύ άλλων, τα www.ibill.com, www.paypal.com, www.charge.com και www.internetsecure.com. Η εισαγωγή σας σε κάποιο από αυτά τα συστήματα μπορεί να γίνει μέσω Διαδικτύου, με την από μέρους σας συμπλήρωση μιας φόρμας εκδήλωσης ενδιαφέροντος. Κατόπιν, οι εταιρίες αυτές αναλαμβάνουν τη διαχείριση των συναλλαγών με πιστωτικές κάρτες σε ασφαλές περιβάλλον και

πιστώνουν, ανά τακτά χρονικά διαστήματα, τα έσοδα από τις πωλήσεις στο λογαριασμό του εμπόρου.

4.« Κάν' το μόνος σου». Οι λύσεις που προηγήθηκαν είναι διαμεσολαβητικού χαρακτήρα. Ένας μεσάζοντας δηλαδή (εταιρία ή χρηματοπιστωτικός οργανισμός) παρεμβάλλεται μεταξύ προμηθευτή και αγοραστή, διαχειρίζεται τη συναλλαγή με ασφάλεια και εισπράττει προμήθεια για τις υπηρεσίες του.Υπάρχει όμως και η λύση να κάνετε εσείς όλες τις απαιτούμενες ενέργειες και να διαχειρίζεστε τις παραγγελίες χωρίς την παρέμβαση τρίτων.

Το σημαντικότερο προαπαιτούμενο για κάτι τέτοιο είναι η απόκτηση ψηφιακού πιστοποιητικού. Την ύπαρξη του πιστοποιητικού υποδηλώνει ένα κίτρινο λουκέτο που εμφανίζεται στη σελίδα του browser κάτω δεξιά, ενώ η σελίδα ανοίγει, στο address bar, ως https:// και όχι http://. Το πιστοποιητικό εξασφαλίζει ότι η συναλλαγή με τον πελάτη θα πραγματοποιηθεί στο υψηλότερο δυνατό επίπεδο ασφαλείας (128 bit).

Ο πιο γνωστός προμηθευτής ψηφιακού πιστοποιητικού είναι η εταιρία VeriSign (www.verisign.com). Το κόστος για την αγορά πιστοποιητικού είναι σημαντικό, ξεκινά δε από περίπου 1.000 ευρώ για χρονική περίοδο ενός έτους και αυξάνεται ανάλογα με τις λειτουργικές απαιτήσεις του ηλεκτρονικού καταστήματος. Αφού αποκτηθεί το πιστοποιητικό, απομένει η συνεργασία με την τράπεζα στην οποία τηρείτε λογαριασμό, για την πίστωση των χρημάτων από τις παραγγελίες

.

11.4 **Συμβουλές**

Τα φαινόμενα απάτης μέσω online χρήσης πιστωτικών καρτών δεν είναι ιδιαίτερα συχνά, ωστόσο υπάρχουν. Ο μικρομεσαίος επιχειρηματίας, πάντως, δεν έχει να φοβάται εάν είναι προσεκτικός και ακολουθεί ορισμένους απλούς κανόνες.

Η διαδικασία επαλήθευσης των στοιχείων μιας πιστωτικής κάρτας αρχίζει με την είσοδο της κάρτας στο τερματικό ή με την πληκτρολόγηση του κωδικού της αριθμού.

Η διαδικασία αυτή ουσιαστικά ελέγχει το αν η κάρτα έχει αναφερθεί ως κλεμμένη και αν η παρεχόμενη πίστωση επιτρέπει τη συγκεκριμένη συναλλαγή.

Είναι γεγονός ότι το Διαδίκτυο καθιστά τις απάτες που σχετίζονται με τη χρήση πιστωτικών καρτών ευκολότερες. Στο Internet κυκλοφορούν λίστες κλεμμένων αριθμών ή και προγραμμάτων που παράγουν νέους κωδικούς αριθμούς πιστωτικών καρτών.

Επιπλέον, η έλλειψη επαφής πρόσωπο με πρόσωπο στο Διαδίκτυο τείνει να κάνει τους απατεώνες τολμηρότερους.

Οι τρέχουσες τεχνικές για την πρόληψη της απάτης μέσω πιστωτικών καρτών, που επικεντρώνονται στον έλεγχο των υπογραφών στο πίσω μέρος της κάρτας, των ολογραμμάτων ή και την τυπωμένη εικόνα του κατόχου της, δεν μπορούν να λειτουργήσουν στις online συναλλαγές, όπου ο κάτοχος δεν είναι παρών (συναλλαγή τύπου CNP, cardholder not present), δεδομένου ότι ο έμπορος δεν μπορεί να δει την πιστωτική κάρτα και να ελέγξει την υπογραφή.

Οι online συναλλαγές μέσω πιστωτικών καρτών εμπίπτουν στην κατηγορία MOTO (Mail Order /Telephone Order, παραγγελία ταχυδρομείου/τηλεφωνική παραγγελία), ή αλλιώς CNP.

Οι περισσότερες εμπορικές συναλλαγές μέσω πιστωτικών καρτών καθιστούν τον έμπορο 100% υπεύθυνο για απάτες που πραγματοποιούνται μέσω αυτού του τύπου συναλλαγής. Σε περιπτώσεις online απάτης μέσω κλεμμένων καρτών που έχουν διεξαχθεί στο εξωτερικό, οι επιχειρηματίες δεν βρίσκουν την αναμενόμενη αρωγή των αστυνομικών αρχών. Αυτό οφείλεται στο γεγονός πως οι Αρχές θεωρούν πολύ μικρά τα ποσά που διακυβεύονται (κυρίως όταν πρόκειται για λίγες δεκάδες ευρώ).

Επίσης, σε περιπτώσεις διεθνών συναλλαγών, υπάρχουν εμπόδια που σχετίζονται με την αρμοδιότητα των εκάστοτε εθνικών αστυνομικών αρχών.Τέτοιου είδους προβλήματα όμως δεν πρόκειται να αντιμετωπίσει ένας προσεκτικός επιχειρηματίας. Υπάρχουν αρκετές δικλείδες ασφαλείας και μέθοδοι που διασφαλίζουν την καλή πίστη των συναλλαγών μέσω καρτών, ορισμένες από τις οποίες παραθέτουμε:

1. Πρέπει να υπάρχει ταύτιση της διεύθυνσης που δηλώνει ο πελάτης με τη διεύθυνση αποστολής του προϊόντος. Όσο υπερβολικό κι αν ακούγεται, πολλές επιχειρήσεις του εξωτερικού δεν δέχονται να αποστείλουν προϊόντα σε διεύθυνση διαφορετική από αυτήν που έχει δηλωθεί στην πιστωτική κάρτα του καταναλωτή. Σε περίπτωση που ο πελάτης επιθυμεί η παράδοση να γίνει σε διεύθυνση διαφορετική από τη δική του, θα πρέπει να γίνεται κατόπιν ειδικής συνεννόησης.

2. Να είστε προσεκτικοί σε παραγγελίες πελατών οι οποίοι παρέχουν διεύθυνση ηλεκτρονικού ταχυδρομείου δωρεάν υπηρεσίας. Πολλές online επιχειρήσεις του εξωτερικού δεν δέχονται παραγγελίες από πελάτες με email του τύπου username @yahoo.com, username @hotmail.com κ.λπ. Αυτό γίνεται διότι απλούστατα ο ιδιοκτήτης ενός ελεύθερου λογαριασμού email παραμένει ανώνυμος. Εάν ένας απατεώνας διαθέτει κλεμμένο κωδικό πιστωτικής κάρτας και κλεμμένη διεύθυνση κατοικίας, θα χρειαστεί και μια ηλεκτρονική διεύθυνση η οποία δεν μπορεί να ανιχνευθεί.

3. Ελέγξτε το δικτυακό τόπο του πελάτη, εάν υπάρχει και εάν είναι εφικτό. Είναι πιθανό να βρείτε το URL του πελάτη απλά πληκτρολογώντας www. μπροστά από το δεύτερο μέρος της διεύθυνσης ηλεκτρονικού ταχυδρομείου του.Για παράδειγμα, εάν ένας πελάτης παρέχει μια διεύθυνση ηλεκτρονικού ταχυδρομείου username @domain.com, πληκτρολογήστε www. domain.com.

Είναι αρκετά πιθανό να εντοπίσετε με αυτό τον τρόπο το site του.

Εκεί θα πρέπει να ελέγξετε αν πρόκειται για δικτυακό τόπο υπό κατασκευή ή για site το οποίο παρέχει στοιχεία επικοινωνίας διαφορετικά από αυτά της κατατεθείσας παραγγελίας.

4. Προσέξτε τις ασυνήθιστες παραγγελίες. Οι επιτήδειοι συνηθίζουν να κάνουν παραγγελίες που διαφέρουν σημαντικά από αυτές ενός απλού (και νόμιμου) πελάτη, όπως για παράδειγμα ακριβά προϊόντα ή πολύ μεγάλες ποσότητες, και συχνά εμφανίζονται διατεθειμένοι να πληρώσουν πολύ περισσότερα χρήματα ώστε να λάβουν το εμπόρευμα ταχύτερα. **5. Τηλεφωνήστε στον πελάτη εάν έχετε αμφιβολίες.** Ένα σύντομο τηλεφώνημα μπορεί να είναι αρκετό ώστε να εξασφαλίσει το έγκυρο της

συναλλαγής.

6. Συλλέξτε όσο το δυνατόν περισσότερα στοιχεία για την παραγγελία: τη διεύθυνση του πελάτη και τον αριθμό τηλεφώνου, την τράπεζα που εξέδωσε την πιστωτική κάρτα και τη διεύθυνση IP του υπολογιστή από τον οποίο έγινε η παραγγελία. Βέβαια αυτό έρχεται σε αντίθεση με την πολιτική του να μη ζητάμε περισσότερα από τα απαραίτητα στοιχεία για τον πελάτη, ωστόσο οφείλετε να διασφαλίσετε τη νομιμότητα της συναλλαγής.

7. Προειδοποιήστε τους επισκέπτες του ηλεκτρονικού σας καταστήματος **για τις μεθόδους που χρησιμοποιείτε** κατά της απάτης, καθώς και τις συνέπειές της. Δείξτε ότι έχετε τον τρόπο να εντοπίσετε τους επιτήδειους και πως είστε διατεθειμένοι να τους «κυνηγήσετε».

8. Εάν χρησιμοποιείτε κάποια υπηρεσία λήψης και εκτέλεσης παραγγελιών σε πραγματικό χρόνο (real time service), βεβαιωθείτε ότι είναι αξιόπιστη.

9. Χρησιμοποιήστε κάποια προηγμένη υπηρεσία η οποία θα μπορέσει να σας βοηθήσει στον εντοπισμό των επίδοξων απατεώνων ή/και στην αποτροπή τους. Υπηρεσίες όπως η CyberSource αυτοματοποιούν όλους τους ελέγχους που καλείστε να διεξάγετε προκειμένου να εξασφαλίσετε τη νομιμότητα και την αξιοπιστία των συναλλαγών σας.

Εάν βρίσκεστε σε επαγρύπνηση και δεν αφήνετε τις online παραγγελίες που λαμβάνετε στην… τύχη τους, τότε η επιχείρησή σας δεν πρόκειται να αντιμετωπίσει σοβαρό πρόβλημα με τη χρήση πιστωτικών καρτών.

Οι οικονομικές συναλλαγές μέσω Διαδικτύου, και δη με τη χρήση πιστωτικής κάρτας, έχουν ακόμη μεγάλο περιθώριο διάδοσης στο μέλλον, καθώς η έλλειψη εμπιστοσύνης στα ηλεκτρονικά μέσα αποτρέπει σήμερα μεγάλο μέρος των χρηστών από το να πραγματοποιούν τις αγορές τους online. Προστατεύοντας λοιπόν το ηλεκτρονικό σας κατάστημα από ύποπτες συναλλαγές με πλαστές ή κλεμμένες πιστωτικές κάρτες ή άλλες απάτες, ουσιαστικά συμβάλλετε στην ενίσχυση του αισθήματος ασφάλειας των χρηστών και κατά συνέπεια στη διάδοση των ηλεκτρονικών συναλλαγών.

Τρεις Εναλλακτικοί τρόποι για ηλεκτρονικές αγορές χωρίς τη χρήση πιστωτικής κάρτας

Νέες «πόρτες» για ασφαλείς ηλεκτρονικές συναλλαγές δίνουν τώρα οι τράπεζες για όσους φοβούνται να χρησιμοποιήσουν την πιστωτική τους κάρτα, προσδοκώντας σε αύξηση του τζίρου μέσω του ηλεκτρονικού εμπορίου. Ο φόβος της ψηφιακής απάτης - κυρίως μέσω πιστωτικών καρτών - λειτουργεί αποτρεπτικά, μειώνοντας τον τζίρο των ηλεκτρονικών καταστημάτων, αλλά και τις προμήθειες των τραπεζών.

Έτσι, το τελευταίο διάστημα οι τελευταίες δίνουν στους πελάτες τους τρεις εναλλακτικούς τρόπους προκειμένου να κάνουν ψηφιακές αγορές με ασφάλεια και ανωνυμία. Προπληρωμένες πιστωτικές κάρτες, χρεωστικές κάρτες αλλά και ειδικές ηλεκτρονικές τράπεζες είναι το «διαβατήριο» για ασφαλέστερες οικονομικές συναλλαγές.

1.Προπληρωμένες πιστωτικές

Οι ελεγχόμενες απώλειες σε περίπτωση κλοπής είναι το βασικό πλεονέκτημα που προσφέρουν οι προπληρωμένες πιστωτικές κάρτες που το τελευταίο διάστημα έχουν κάνει την εμφάνισή τους στην ελληνική αγορά. Σε αντίθεση με τις «παραδοσιακές» πιστωτικές, μπορούν να «φορτωθούν» με συγκεκριμένο ποσό, το οποίο χρησιμοποιεί ο κάτοχός τους για κάθε είδους αγορές, ψηφιακές και μη.

Δηλαδή, αν κάποιος θέλει για παράδειγμα να αγοράσει από το Ίντερνετ βιβλία αξίας 100 ευρώ, μπορεί να αγοράσει μια προπληρωμένη κάρτα αντίστοιχης αξίας, να πραγματοποιήσει τη συναλλαγή και στη συνέχεια να την αφήσει χωρίς υπόλοιπο μέχρι την επόμενη αγορά του.

2. Χρεωστικές κάρτες

Η δεύτερη εναλλακτική για ασφαλέστερες ηλεκτρονικές συναλλαγές περνά μέσα από τις χρεωστικές κάρτες, τις οποίες σήμερα διαθέτουν σχεδόν όλα τα χρηματοπιστωτικά ιδρύματα στους καταθέτες τους. Πρόκειται για τις κάρτες τύπου Electron Visa, οι οποίες - εκτός από την ανάληψη μετρητών - μπορούν να χρησιμοποιηθούν και για συναλλαγές. Σε αυτή την περίπτωση, το ποσό της αγοράς αφαιρείται από τον τραπεζικό λογαριασμό με τον οποίο είναι συνδεδεμένες. Το «μυστικό» για να εξασφαλιστεί πλήρως ο καταναλωτής είναι να ανοίξει στην τράπεζα με την οποία συνεργάζεται έναν νέο τραπεζικό λογαριασμό με μηδενικό υπόλοιπο και να ζητήσει την έκδοση χρεωστικής κάρτας τύπου Electron Visa. Στη συνέχεια, και ανάλογα με την αγορά που θέλει να κάνει, μεταφέρει στον λογαριασμό αυτόν μόνο το συγκεκριμένο ποσό.

3. Ηλεκτρονικές τράπεζες

Ο τρίτος δρόμος για την πραγματοποίηση ηλεκτρονικών συναλλαγών με ασφάλεια - και μάλιστα χωρίς να καταφύγει καν στο πλαστικό χρήμα - είναι η στροφή στις διαδικτυακές τράπεζες που το τελευταίο διάστημα έχουν κάνει την εμφάνισή τους. Η διαδικασία έχει ως εξής: ο πελάτης επισκέπτεται την ιστοσελίδα της ηλεκτρονικής τράπεζας (π.χ. www.neteller.com ή www.paypal.com) και δημιουργεί εκεί έναν λογαριασμό.

Στη συνέχεια, τον τροφοδοτεί με χρήματα, είτε με την πιστωτική του κάρτα, είτε με έμβασμα από κάποια τράπεζα. Από εκεί και πέρα, για τις διαδικτυακές του συναλλαγές χρησιμοποιεί τα στοιχεία της ηλεκτρονικής τράπεζας και το υπόλοιπο που υπάρχει σε αυτήν. Έτσι, δεν κινδυνεύει να πέσουν στα χέρια επιτήδειων ούτε τα στοιχεία του τραπεζικού του λογαριασμού ούτε ο αριθμός της πιστωτική του κάρτας.

Πρότυπα Ηλεκτρονικών Πληρωμών

Παρά την ύπαρξη αρκετά ισχυρών συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες, θα πρέπει να αναπτυχθεί κάποιο κοινό πρότυπο που να επιτρέπει στα συστήματα πληρωμών να μπορούν να επικοινωνήσουν μεταξύ τους. Η έλλειψη διαλειτουργικότητας που παρατηρείται σήμερα ίσως να ελαττώσει την αποδοχή των συστημάτων ηλεκτρονικών πληρωμών.

Παρόλα αυτά υπάρχουν ήδη, δύο σημαντικά πρότυπα υπό ανάπτυξη, τα οποία θα καταστήσουν την διαλειτουργικότητας αυτών των συστημάτων πιο εύκολη.

Το πρώτο από αυτά αφορά το **Secure Electronic Transactions (SET),** που αναπτύχθηκε από την **Visa** και την **MasterCard**. Το SET χρησιμοποιεί τα λεγόμενα ψηφιακά πιστοποιητικά για, την πιστοποίηση της ταυτότητας των συμμετεχόντων σε μια συναλλαγή. Επίσης, κρυπτογραφεί τις πληροφορίες των πιστωτικών καρτών πριν την μετάδοση τους στο Internet.

Το δεύτερο πρότυπο αφορά **το Joint Electronic Payments lnitiative (JEPI)**, που αναπτύχθηκε από την CommerceNet και το World Wide Web Consortium. Το JEPI αποτελεί μια προσπάθεια για προτυτοποίηση των διαφορετικών μηχανισμών πληρωμών, πρωτοκόλλων και μεταφοράς.

Τέτοια παραδείγματα μηχανισμών πληρωμών περιλαμβάνουν: πιστωτικές κάρτες, χρεωστικές κάρτες, Ψηφιακό χρήμα και ηλεκτρονικές επιταγές.Τα πρωτόκολλα πληρωμών περιλαμβάνουν το STT και το SEPP. Στην ουσία ορίζουν την μορφή του μηνύματος και την διαδικασία, που απαιτείται για την ολοκλήρωση της πληρωμής.

Το JEPI παρέχει τη δυνατότητα στον πελάτη να χρησιμοποιήσει μια μόνο εφαρμογή και μια μόνο διεπαφής χρήστη για την διεκπεραίωση των συναλλαγών

Ηλεκτρονικές Επιταγές

Μία έντυπη επιταγή είναι ουσιαστικά μία εντολή μεταφοράς κεφαλαίων από ένα λογαριασμό σε έναν άλλο. Η εντολή αυτή αποστέλνεται αρχικά

στον αποδέκτη των κεφαλαίων, ο οποίος με τη σειρά του, παρουσιάζει την επιταγή στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Μια ηλεκτρονική επιταγή έχει όλα τα χαρακτηριστικά που διαθέτει μια έντυπη επιταγή και χρησιμοποιείται σαν ένα μήνυμα προς την τράπεζα του αποστολέα για την μεταφορά κεφαλαίων από ένα λογαριασμό σε ένα άλλο. Σε αντιστοιχία, με την παραδοσιακή διαδικασία, η ηλεκτρονική επιταγή αποστέλνεται αρχικά στον αποδέκτη ο οποίος την υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Από άποψη ασφάλειας, η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη επιταγή. Και αυτό, γιατί ο αποστολέας, μπορεί να προστατέψει τον εαυτό τον από μία απάτη. Αυτό γίνεται με την κωδικοποίηση του αριθμού του λογαριασμού του με το δημόσιο κλειδί της τράπεζας, χωρίς έτσι να αποκαλύπτει τον αριθμό τον λογαριασμού του στον έμπορο. Το FSTC αποτελεί μια συνεργασία, τραπεζών και πιστωτικών οργανισμών, που έχουν υλοποιήσει μια, ηλεκτρονική επιταγή.

Στηριγμένη στην παραδοσιακή επιταγή, η επιταγή του FSTC επιτρέπει την ψηφιακή υπογραφή του αποδέκτη. Για την προσθήκη μεγαλύτερης ευελιξίας σε αυτό το σύστημα πληρωμών, το FSTC προσφέρει στους χρήστες διάφορες επιλογές επιταγών ανάλογα με τις ανάγκες του χρήστη. Οι ηλεκτρονικές επιταγές μπορούν να παραδοθούν είτε με άμεση παράδοση μέσο ενός δικτύου ή μέσο ηλεκτρονικού ταχυδρομείου.

Σε κάθε περίπτωση, τα υπάρχοντα τραπεζικά κανάλια, μπορούν να εκκαθαρίσουν τις πληρωμές, μέσο των δικτύων τους. Κάτι τέτοιο οδηγεί σε μια ικανοποιητική αναβάθμιση της υπάρχουσας τραπεζικής υποδομής και του Internet.

12 ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ

12.1 Phishing

Το Phising είναι μια νέα μέθοδος εξαπάτησης των καταναλωτών ενός οργανισμού,συνήθως κερδοσκοπικού, και συνίσταται κυρίως στην απατηλή υφαρπαγή των εμπιστευτικών πληροφοριών των καταναλωτών, όπως προσωπικά ή ευαίσθητα δεδομένα, οικονομικά δεδομένα κλπ, με σκοπό την παράνομη χρήση τους από τον Phisher για την πρόκληση βλάβης ξένης περιουσίας.

Με τη βοήθεια κυρίως της απρόσκλητης εμπορικής επικοινωνίας-το γνωστό Spam-ή χρησιμοποιώντας bots για την αυτοματοποιημένη στόχευση των υποψήφιων θυμάτων τους ή άλλες παρόμοιες μεθόδους, οι Phishers, εμφανιζόμενοι κυρίως στο διαδίκτυο ως εκπρόσωποι ενός οργανισμού τα χαρακτηριστικά του οποίου έχουν αντιγράψει παράνομα, προβαίνουν σε δόλιες πράξεις ή παραλείψεις με τις οποίες πείθουν τα στοχευμένα θύματά τους, τα οποία ενδέχεται να είναι άδηλα ν' αποκαλύψουν ή εισάγουν σε σύστημα ηλεκτρονικών υπολογιστών στοιχεία της ταυτότητάς τους καιεμπιστευτικές πληροφορίες με σκοπό να χρησιμοποιήσουν οι Phishers αυτές τις πληροφορίες για να προσπορίσουν στον εαυτό τους ή τρίτον παράνομο περιουσιακό όφελος προξενώντας βλάβη σε περιουσιακά στοιχεία των θυμάτων τους .

- *Η ονομασία Phising αναφέρεται χρησιμοποιούμενη για πρώτη φορά το 1996 από χάκερς που έκλεβαν ή παράνομα ιδιοποιούνταν τους λογαριασμούς νομίμων χρηστών της εταιρίας America Online (AOL) με παράνομη χρήση κωδικών πρόσβασης που ανήκαν σε ανυποψίαστους χρήστες-συνδρομητές της AOL.*
- *Η πρώτη αναφορά στο Διαδίκτυο για το Phising έγινε σε news-group χάκερς γνωστό ως alt.2600 τον Ιανουάριο του 1996 και η πρώτη αναφορά των μέσων ενημέρωσης στο Phising χρονολογείται τον Μάρτιο του 1997.*

Οι επιθέσεις Phising συνίστανται σ’ ένα μείγμα δόλιας χρήσης τεχνολογικών μέσων αποβλέποντας στην εξαπάτηση των καταναλωτών και εφαρμοσμένων μηχανιστικών πρακτικών εξαπάτησης.

Σε όλες τις περιπτώσεις επιθέσεων Phising, ο Phisher υποδύεται τον εκπρόσωπο έμπιστης πηγής πληροφοριών που, δήθεν, σχετίζεται με το θύμα, προκειμένου να πείσει το θύμα να του αποκαλύψει εμπιστευτικές πληροφορίες ή να προβεί σε πράξεις αποκάλυψης της ταυτότητας του θύματος.

Συνήθως ο Phisher επικοινωνεί με το υποψήφιο θύμα του και ισχυρίζεται ότι εργάζεται σε τράπεζα ή άλλη εταιρία που μπορεί να σχετίζεται με τον λήπτη της επικοινωνίας δίνοντάς του όλες τις απαραίτητες λεπτομέρειες για την πιστοποίησή του ονοματεπώνυμο, αριθμός εργαζομένου, τηλέφωνο για επιβεβαίωση των στοιχείων του κλπ.

Εν συνεχεία, ο Phisher ενημερώνει τον λήπτη της επικοινωνίας του ότι, δήθεν, η πιστωτική του κάρτα ή ο τραπεζικός λογαριασμός του έχουν καταχωρηθεί σε λίστα παρακολούθησης για ασυνήθιστη συναλλακτική συμπεριφορά.

Κατά την επικοινωνία του, ο Phisher επιχειρεί ν’ αλιεύσει, ρωτώντας το θύμα του, κάθε πληροφορία που θα μπορούσε εν συνεχεία να χρησιμοποιήσει για να απαλείψει κάθε αμφιβολία του θύματος για την ταυτότητα του προσώπου με το οποίο επικοινωνεί.

Αφού επιτύχει την πλάνη του θύματος αναφορικά με την ταυτότητα του Phisher με παράσταση ψευδών γεγονότων ως αληθινών ή αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, ο Phisher οδηγεί το θύμα σε πράξεις περιουσιακής διάθεσης, από τις οποίες άμεσα ή έμμεσα αποκομίζει περιουσιακό όφελος ο Phisher επί ζημία του διαθέτοντος.

Η επικοινωνία στις επιθέσεις Phising μπορεί να διεξαχθεί με ηλεκτρονικό ταχυδρομείο, με χρήση πλαστών διαδικτυακών τόπων, με εργαλεία στιγμιαίας επικοινωνίας, με τηλεφωνική επικοινωνία, και με χρήση παραβιασμένων ως προς την ασφάλειά τους διακομιστές-servers.

Οι περισσότερες επιθέσεις Phising συνήθως γίνονται με χρήση ηλεκτρονικού ταχυδρομείου.

Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις

Phising με ηλεκτρονικό ταχυδρομείο περιλαμβάνουν:

1. χρήση ηλεκτρονικής αλληλογραφίας που μοιάζει να έχει σταλεί από έμπιστη πηγή

2. χρήση αντίγραφων ηλεκτρονικής αλληλογραφίας στα οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks

3. χρήση HTML ηλεκτρονικής αλληλογραφίας στην οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks

4. χρήση ιών (viruses) και σκουληκιών (worms) συνημμένων σε ηλεκτρονική αλληλογραφία

5. χρήση αντι-spam εργαλείων

6. χρήση εξατομικευμένης ηλεκτρονικής αλληλογραφίας

7. χρήση ηλεκτρονικής αλληλογραφίας με τροποποιημένη ένδειξη αποστολέα «Mail From:» σε συνδυασμό με χρήση Open Mail Relays διακομιστών για την απόκρυψη της προέλευσης της ηλεκτρονικής αλληλογραφίας

Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phising με χρήση πλαστών διαδικτυακών τόπων περιλαμβάνουν:

1. Εισαγωγή παραπλανητικών hyperlinks σε δημοφιλείς διαδικτυακούς τόπους

2. Χρήση παραπλανητικών γραφικών ή διαφημιστικών πινακίδων (banners κλπ) με σκοπό να δελεάσουν του επισκέπτες του διαδικτυακού τόπου που ταπεριέχει για να κάνουν click σ’ αυτά

3. Χρήση διαδικτυακών bugs ικανών να ιχνηλατήσουν την επισκεψιμότητα και συμπεριφορά των καταναλωτών στο διαδικτυακό τόπο που τα περιέχει

4. Χρήση pop-ups ή frameless windows για τη μεταμφίεση της αληθινής προέλευσης του ηλεκτρονικού μηνύματος του Phisher

5. Ενσωμάτωση κακόβουλου λογισμικού κώδικα μέσα σε ιστοσελίδα ή διαδικτυακό τόπο που εκμεταλλεύεται μια γνωστή αδυναμία ασφαλείας

των browsers των καταναλωτών και εγκαθιστά στο υπολογιστικό σύστημα των λογισμικό της επιλογής του Phisher (π.χ. Key-loggers Screen-grabbers, Back-doors Trojan Horses Wabbits Viruses WormsSpyware Exploits Rootkits, Dialers, κλπ). κατάχρηση προδιαγραφών σχέσεων εμπιστοσύνης δημιουργημένων στα πλαίσια λογισμικών browsing-φυλλομετρητών ιστοσελίδων στο Διαδίκτυο-με σκοπό τη διείσδυση στα υπολογιστικά συστήματα των καταναλωτών και την τοποθέτηση εγκεκριμένων εκτελέσιμων λογισμικών προγραμμάτων-site-authorized scriptable components στις περιοχές αποθήκευσης δεδομένων των υπολογιστικών συστημάτων των καταναλωτών.

Το **Phising** (αλίευση στοιχείων ή «ψάρεμα») είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά e-mails.

Μπορούν να οδηγήσουν στην κλοπή των αριθμών πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών λογαριασμών ή άλλων προσωπικών δεδομένων.

Οι επιτήδειοι της ηλεκτρονικής απάτης σας πλησιάζουν με ψεύτικα προσχήματα και προσπαθούν να σας πείσουν να κοινοποιήσετε σημαντικές προσωπικές σας πληροφορίες όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης ή δεδομένα του λογαριασμού σας.

Οι απάτες ψαρέματος μπορεί να γίνουν αυτοπροσώπως ή μέσω τηλεφώνου ενώ διακινούνται μέσω ανεπιθύμητων e-mails, pop-up windows ή άμεσων μηνυμάτων (Instant messaging).Να τονίσουμε πως δεν είναι ασφαλές να εισάγετε προσωπικές ή οικονομικές πληροφορίες σε pop-up windows (αναδυόμενα παράθυρα). Μια κοινή τεχνική **Phising** είναι το άνοιγμα ενός false pop-up window όταν κάποιος κάνει click σε ένα **Phising** e-mail.

Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεστε. Ακόμη και εάν το pop-up window φαίνεται πολύ επίσημο ή διακηρύσσει πως είναι ασφαλές, θα πρέπει να αποφεύγετε να εισάγετε ευαίσθητα προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελέγξετε την πιστοποίηση ασφάλειας.

Το πιστοποιητικό ασφαλείας της τοποθεσίας αντιστοιχεί στο όνομα της τοποθεσίας. Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο είναι ένα σημάδι επειδή το κλειστό λουκέτο υποδεικνύει πως η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών που εισάγετε (όπως ο αριθμός της πιστωτικής σας κάρτας ή άλλη πληροφορία ταυτοποίησης).

Όμως, το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο. Για να διασφαλίσετε τη γνησιότητά του κάντε διπλό κλικ για να διαπιστώσετε το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το «Issued to» (Εκδόθηκε για), θα πρέπει να αντιστοιχεί με το όνομα της τοποθεσίας.

Εάν το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως «Spoofed» (πλαστή) τοποθεσία. Εάν δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο μην εισαγάγετε προσωπικά δεδομένα. Αν και το λογισμικό προστασίας από ιούς δεν μπορεί να σας αποτρέψει να ανοίξετε ένα spoofed e-mail ή να κάνετε click σε επικίνδυνα links, μπορεί εντούτοις να σταματήσει ιούς ή λογισμικό υποκλοπής που θα προέλθει από τέτοιες ενέργειες.

Κάποιο spoofed e-mail μπορεί να σας οδηγήσει σε τοποθεσίες Web που εγκαθιστούν στον υπολογιστή σας λογισμικό το οποίο συνεχίζει να καταγράφει τις πληροφορίες που εισάγετε όπως τον κωδικό πρόσβασης, πληροφορίες σύνδεσης και δεδομένα του λογαριασμού. Αυτού του είδους το ανεπιθύμητο λογισμικό συχνά καλείται Spyware (λογισμικό υποκλοπής) ενώ μπορεί να περιέχει ακόμη και ιό.

Στις απάτες μέσω Phising συνηθίζονται οι γενικές προσφωνήσεις όπως «Αγαπητέ πελάτη» αντί για το όνομά σας. Σας ζητούν να κάνετε click σε κάποιο link, με φρασεολογία που δίνει την εντύπωση του επείγοντος ή σας ζητούν να επιβεβαιώσετε κάποιες προσωπικές σας πληροφορίες.

Όταν χρησιμοποιείτε πιστωτική κάρτα, μπορεί να γίνετε ευάλωτοι σε πιθανή απάτη πληρώνοντας μέσω Internet, μέσω τηλεφώνου ή ακόμη και αυτοπροσώπως σε κάποιο κατάστημα της γειτονιάς σας.

Γι' αυτό κάθε φορά που πληρώνετε με πιστωτική κάρτα, οι επιχειρήσεις θα πρέπει να επιβεβαιώνουν τα στοιχεία του λογαριασμού σας πριν σας παρέχουν αγαθά και υπηρεσίες.

Δυστυχώς, επειδή τα στοιχεία της πιστωτικής σας κάρτας αποθηκεύονται σε μεγάλους υπολογιστές, οι διακομιστές μπορούν να γίνουν στόχος διαφόρων hackers οι οποίοι αναζητούν τρόπους για να εισχωρήσουν στο σύστημα και να ανακτήσουν στοιχεία τα οποία κατόπιν θα τα χρησιμοποιήσουν για να διαπράξουν κάποια απάτη εις βάρος σας.

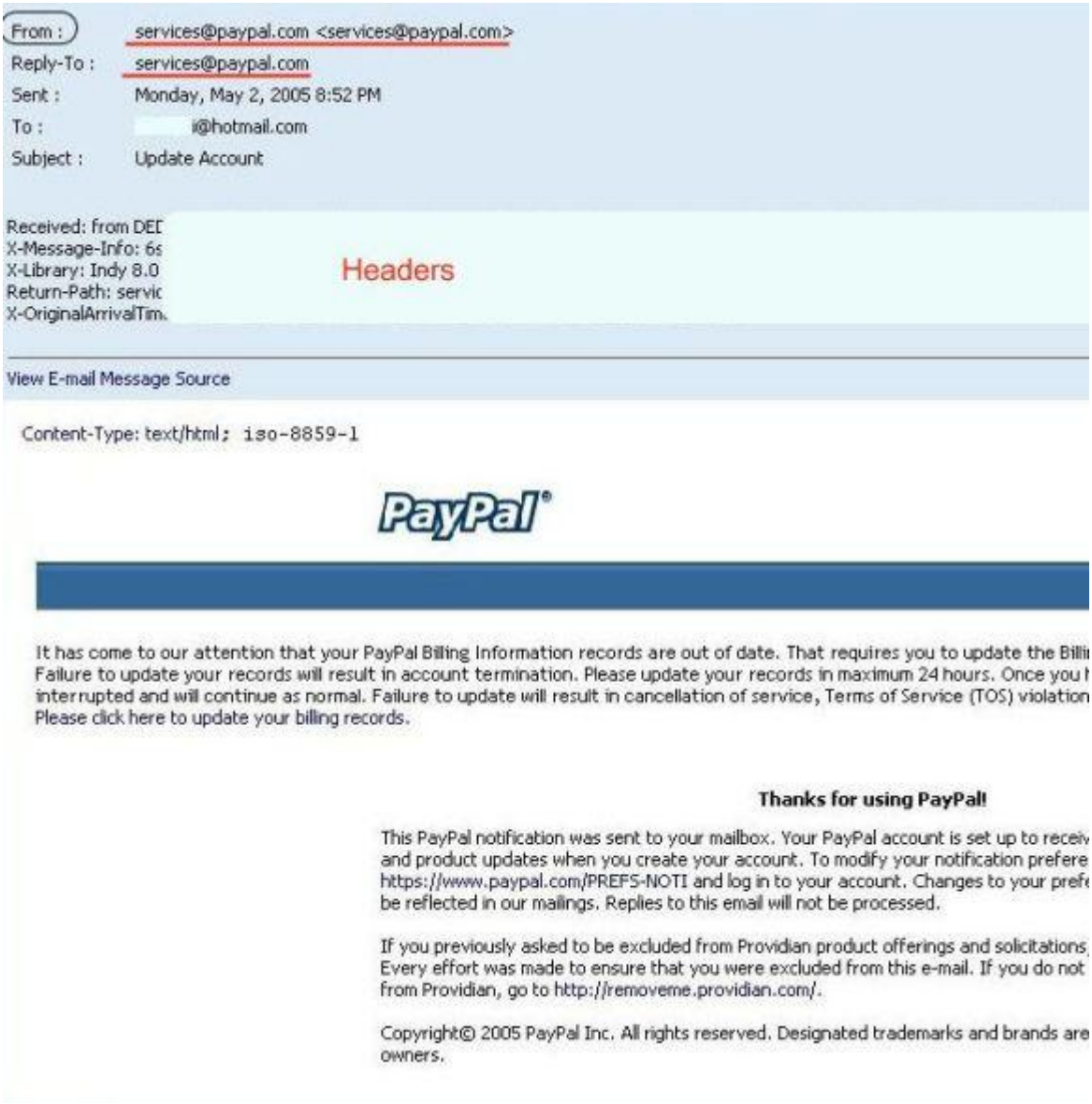
Απάτη – Phishing

Phishing = Ψάρεμα. Emails που φαίνονται να προέρχονται από μεγάλες και γνωστές εταιρίες, με όλα τα γραφικά και το κατάλληλο επίσημο κείμενο, προσπαθούν να σας ψαρέψουν και να σας πείσουν ότι πρέπει να εισάγετε τα στοιχεία του λογαριασμού σας για εξακρίβωση ή για να αποφευχθεί κάποιο σοβαρό πρόβλημα.

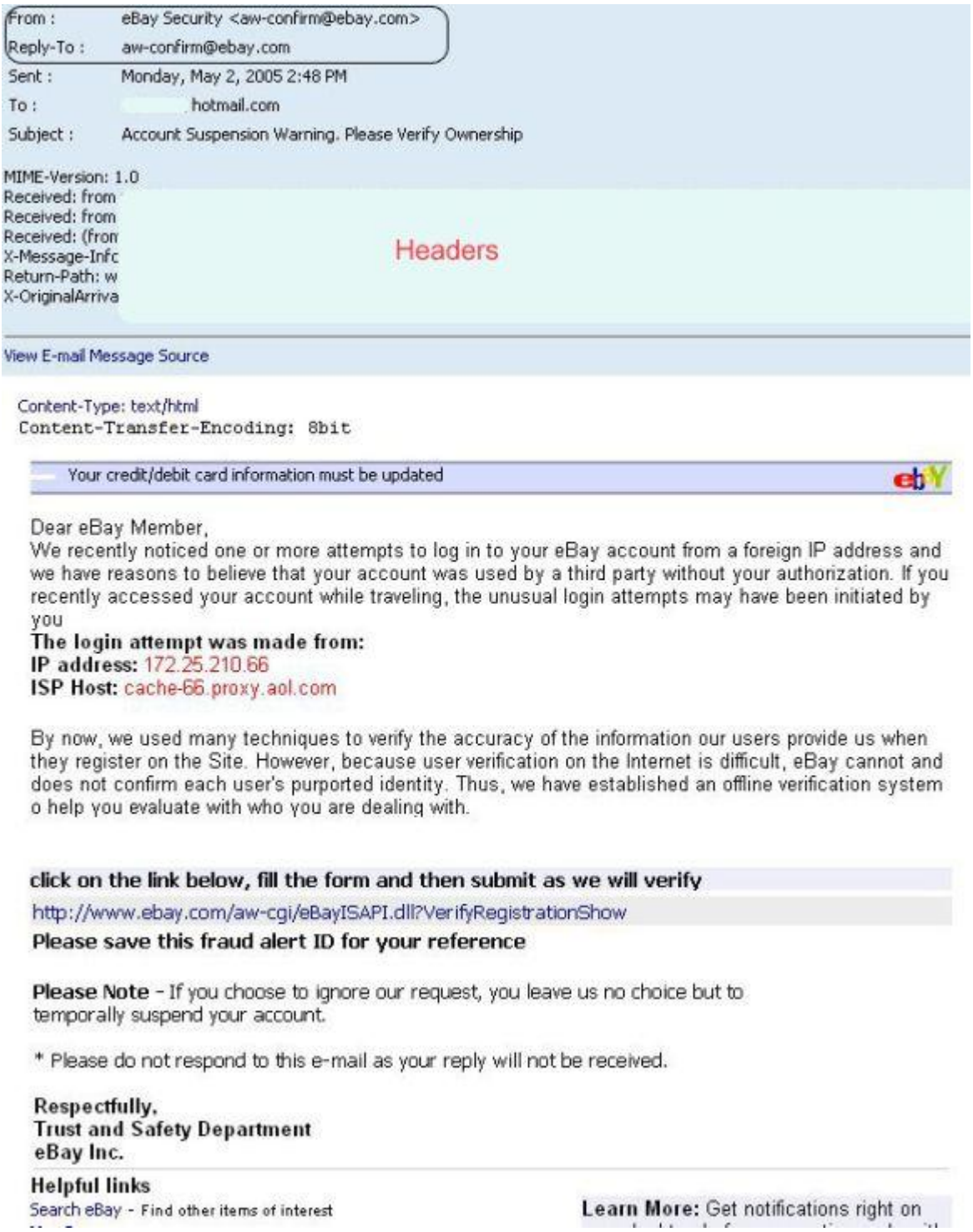
Αυτό το είδος απάτης είναι πολύ καλά σχεδιασμένο και στοχεύει σε κωδικούς από πελάτες των amazon, ebay, citybank, paypal και άλλων μεγάλων εταιριών. Δυστυχώς πολλοί αφελείς έχουν πέσει θύμα τέτοιων Phishing email με αποτέλεσμα να αδειάσουν οι λογαριασμοί τους από τους ηλεκτρονικούς εγκληματίες.Η επιτυχία των phishing email βασίζεται σε ψυχολογικούς τρόπους παραπλάνησης ανθρώπων που είναι αφελείς και δεν έχουν τις κατάλληλες γνώσεις.

Αυτός ο ψυχολογικός τρόπος παραπλάνησης και καθοδήγησης των θυμάτων λέγεται «κοινωνική μηχανική»(social engineering) και έχει χρησιμοποιηθεί κατά καιρούς από hackers με διάφορες παραλλαγές. Πολλές φορές μάλιστα η κοινωνική μηχανική αποδεικνύεται πιο αποτελεσματική από τεχνολογικά μέσα (κατασκοπευτικά προγράμματα και ιούς) γιαυτό και χρησιμοποιείται ευρέως.

Παράδειγμα PHISHING που μιμείται την εταιρία Paypal:



Παράδειγμα PHISHING που μιμείται την εταιρία Ebay:



From : eBay Security <aw-confirm@ebay.com>
Reply-To : aw-confirm@ebay.com
Sent : Monday, May 2, 2005 2:48 PM
To : hotmail.com
Subject : Account Suspension Warning. Please Verify Ownership

MIME-Version: 1.0
Received: from
Received: from
Received: (from
X-Message-Info
Return-Path: w
X-OriginalArriva

Headers

View E-mail Message Source

Content-Type: text/html
Content-Transfer-Encoding: 8bit

Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify

http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow

Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest

Learn More: Get notifications right on

12.2 Pharming

Η υποκλοπή με την μέθοδο Pharming («παραπλάνηση») είναι η ανακατεύθυνση του browser σε spoofed web Pages. Pharming συμβαίνει όταν hackers ανακατευθύνουν την κίνηση του Internet από μία Web page σε μια άλλη πανομοιότυπη έτσι ώστε να σας ξεγελάσουν και να καταχωρήσετε το username σας και το password στη βάση δεδομένων της spoofed web Page.

Web pages τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων,κατά τις οποίες hackers προσπαθούν να αποσπάσουν προσωπικά δεδομένα με σκοπό να βρουν πρόσβαση σε τραπεζικούς λογαριασμούς και να κλέψουν το ψηφιακό ID σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Το Pharming, η χρήση δηλαδή διαφόρων spoofed Web pages πιθανόν να θυμίζει τις απάτες Phising από e-mails, όμως η παραπλάνηση είναι πιο ύπουλη αφού μπορεί να κατευθυνθείτε σε μία spoofed Web page χωρίς να το γνωρίζετε. Εώς σήμερα έχουν γίνει αρκετές επιθέσεις γεγονός που έχει αρχίσει να ανησυχεί αρκετά κυβερνήσεις και επιχειρήσεις.

Με τη χρήση μιας διαδικασίας που ονομάζεται DNS Poisoning κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι ISP (Internet Service Providers) για να κάνουν routing (να δρομολογήσουν δηλαδή) τη διαδικτυακή κίνηση και μπορεί να κάνει τροποποιήσεις σε κάποιο σημείο έτσι ώστε να εκτρέπεστε σε μια spoofed Web page πριν αποκτήσετε πρόσβαση σε αυτή που τελικά επιθυμούσατε.

Κάποιες εταιρίες υποστηρίζουν πως το λογισμικό firewall που χρησιμοποιούν προστατεύει και από το Pharming**.**

Κάποιοι πάροχοι υπηρεσιών διαδικτυακής ασφάλειας πιστεύουν πως οι πελάτες τους που καθοδηγούν όλη τους την διαδικτυακή κίνηση μέσω των δικών τους, ασφαλών, διακομιστών είναι και προστατευμένοι από επιθέσεις παραπλανήσεις.

Η φύση της παραπλάνησης υποδεικνύει το αντίθετο αλλά ανεξάρτητα από το τι υποστηρίζει η κάθε εταιρεία είναι καλή ιδέα να αναζητά κάποιος προσεκτικά τα προϊόντα ασφαλείας πριν επενδύσει και εμπιστευτεί κάποιες λύσεις λογισμικού. Δεν μπορείτε να αναγνωρίσετε μία spoofed Web page απλά μετακινώντας τον cursor πάνω από τα link και παρατηρώντας εάν ο κώδικας σας οδηγεί σε κάποιο εμφανώς άσχετο σημείο εκτός της Web page! Τις περισσότερες φορές τουλάχιστον.

Οι spoofed web pages που χρησιμοποιούνται στις απάτες Pharming συνήθως «πλαστογραφούν» τα link τους έτσι ώστε να μοιάζουν ακριβώς με αυτά που αναμένετε να δείτε. «Πλαστογραφούν» ακόμη και τον κώδικα που εμφανίζεται όταν το mouse περάσει πάνω από αυτά. Επίσης, οι spoofed Web pages πιθανόν να αλλάζουν τον κώδικα των δικών τους links αρκετά συχνά και για διάφορους λόγους όπως όταν αναβαθμίζουν το λογισμικό τους, την πλατφόρμα του server ή τις μεθόδους ανάλυσης των στατιστικών κίνησης της Web page.

12.3 **Scam**

Μέχρι πρόσφατα οι επαγγελματίες απατεώνες περιορίστηκαν στη χρήση αργών και αναποτελεσματικών τηλεφωνημάτων και έντυπων αγγελιών για να προωθήσουν τις απάτες τους. Σήμερα, τα ίδια χαρακτηριστικά που κάνουν το Internet τόσο βολικό για όσους αναζητούν εργασία δηλαδή η παγκοσμιότητα, η ευχρηστία και η ταχύτητα διευκολύνουν τους επίδοξους hackers να επιδίδονται σε απάτες με θέμα την απασχόληση διατρέχοντας μικρότερο κίνδυνο.

Δημιουργώντας ψεύτικες αγγελίες θέσεων εργασίας που μοιάζουν με τις αληθινές και συχνά, δημοσιεύοντάς τις σε νόμιμες ιστοσελίδες εύρεσης εργασίας, οι απατεώνες ελπίζουν να παραπλανήσουν τους πρόθυμους και ανυποψίαστους που αναζητούν εργασία και να τους πείσουν να τους στείλουν προσωπικά στοιχεία . (πχ. για όσους γνωρίζουν μία τέτοια εταιρία είναι η Mystery Shopper)

Αυτές οι ψεύτικες αγγελίες εύρεσης εργασίας γίνονται όλο και πιο κομψές και συχνά χρησιμοποιούν συνηθισμένη εικόνα ή πειστικά εταιρικά λογότυπα και φρασεολογία.Πολλές φορές διαθέτουν και links προς spoofed Web pages που εμφανίζονται ως Web pages πραγματικών εταιρειών.

Κάποιες φορές ακόμα χρεώνουν για υπηρεσίες που δεν θα παρέχουν ποτέ. Τυπικά, μετά από μερικές ημέρες, οι απατεώνες «κλείνουν» το Scam και εξαφανίζονται.Ακόμα, εκτός από τη σάρωση προσωπικών Web pages και τη δημοσίευση ανακοινώσεων σε δημόσιες Web pages, οι επαγγελματίες απατεώνες συχνά εμφανίζονται ως γραφεία ευρέσεως εργασίας και στέλνουν ανεπιθύμητα e-mails (ή Spam) σε πιθανούς υποψηφίους που διαθέτουν ευκαιρίες απασχόλησης ή νόμιμα γραφεία ευρέσεως εργασίας.

Ένας επαγγελματίας απατεώνας τέτοιου είδους θα προσπαθήσει να κερδίσει την εμπιστοσύνη του θύματος, χρησιμοποιώντας ψεύτικο προσωπικό για να αποσπάσει προσωπικά στοιχεία, ακόμη και από το τηλέφωνο.

Είναι σημαντικό να θυμάστε ότι τέτοια στοιχεία δεν προβλέπεται ποτε να ζητούνται online**.** Οι εταιρίες γνωρίζουν ότι αυτά θα σας ζητηθούν μόνον σε προσωπικό interview.

12.4 **Blog**

Η πρακτική του Blogging μεγαλώνει δραματικά ιδίως ανάμεσα στους έφηβους τα τελευταία χρόνια.Σύμφωνα με κάποιες πρόσφατες μελέτες, τα μισά από τα Blogs διεθνώς, σήμερα, δημιουργούνται από εφήβους με δύο στους τρεις να δημοσιοποιούν την ηλικία τους, τρεις στους πέντε να αποκαλύπτουν την τοποθεσία τους και έναν στους πέντε να αποκαλύπτει το πλήρες όνομα του.

Αυτό συμβαίνει χωρίς να λέγεται ότι υπάρχουν πιθανοί κίνδυνοι από τη δημοσιοποίηση αυτού του τύπου προσωπικών δεδομένων. Και καθώς πολλοί δημιουργούν όλο και περισσότερα Blogs, οδηγούνται σε έναν αυξανόμενο ανταγωνισμό μεταξύ τους για να τραβήξουν την προσοχή.

Μερικές φορές αυτό μπορεί να οδηγήσει τους Bloggers να δημοσιεύσουν ακαταλληλο υλικό όπως προκλητικές εικόνες των εαυτών τους ή των φίλων τους.Μπορείτε να θεωρείτε πως ό,τι δημοσιεύεται στο Internet (άρα και στα Blogs) είναι μόνιμο. Οποιοσδήποτε μπορεί στο Internet να εκτυπώσει ένα όποιοδήποτε Blog ή να το αποθηκεύσει στον υπολογιστή του ή να το κάνει copy/paste και να το χρησιμοποιήσει όπως θέλει.Οι δικτυακοί τόποι για Blogging (blogspot, wordpress κ.α.) είναι μία η άλλη γνωστό ότι είναι public domain συνεπώς δεν υφίσταται copyright.

12.5 **Spam**

Spam είναι μια δικτυακή κατάχρηση, φάρσα ή ακόμα και απάτη. Με τον όρο Spam μπορούμε να χαρακτηρίσουμε ενέργειες που σχετίζονται με κατάχρηση email (spam email), messengers (spim), blogs (sblogs), forum, κινητά τηλέφωνα, μηχανές αναζήτησης κτλ.

Η κατάχρηση αυτή γίνεται συνήθως, αλλά όχι αποκλειστικά, με σκοπό να διαφημιστούν ιστοσελίδες, προϊόντα ή υπηρεσίες και έχει κριθεί παράνομη για διάφορους λόγους. Πρώτον είναι ενοχλητική και επίμονη. Οι όγκοι τέτοιων διαφημίσεων είναι μεγάλοι και σπαταλούν τον πολύτιμο χρόνο μας.

Ενώ μπορεί να περιμένουμε σημαντικά email, τα spam καθιστούν δύσκολο να ξεχωρίσουμε τα χρήσιμα από τις διαφημίσεις και χρεώνεται ο λογαριασμός μας στον ΟΤΕ περισσότερο, αφού αναγκαζόμαστε να μένουμε online περισσότερο.Επίσης, τέτοια email μπορεί να περιέχουν κακόγουστες φάρσες, επικίνδυνες απάτες, κακόβουλα προγράμματα (ιοί, σκουλήκια κτλ) και άλλο παράνομο υλικό.

Αυτή η ενοχλητική αλληλογραφία αποτελείται από emails που στέλνονται μαζικά σε χιλιάδες διευθύνσεις email ανά τον κόσμο. Οι spammer, αυτοί που στέλνουν τα email δηλαδή, χρησιμοποιούν διάφορους τρόπους, κυρίως βασιζόμενη στην τεχνολογία, για να εντοπίσουν διευθύνσεις email που υπάρχουν στον ίντερνετ.Σαρώνουν λοιπόν το διαδίκτυο με ειδικά προγράμματα που συλλέγουν διευθύνσεις και τις

αποθηκεύουν σε μεγάλες λίστες. Ακόμα και emails που χρησιμοποιούνται στις λίστες των DNS μπορούν να εντοπισθούν.

Εκτός από αυτούς τους τρόπους όμως, μπορεί και να μαντεύουν το email βασιζόμενοι σε ένα domain όνομα ή σε εφαρμογές που χρησιμοποιούν λεξικά. Οι λίστες των spammer μπορεί να πουληθούν και σε άλλους επαγγελματίες του είδους.

Για τους αρχάριους του ίντερνετ είναι μερικές φορές δύσκολο να συνειδητοποιήσουν ότι αυτά τα email δεν απευθύνονται σε αυτούς προσωπικά και πέφτουν πιο εύκολα θύματα σε τέτοιες ηλεκτρονικές απάτες.

Γι'αυτό χρησιμοποιώντας το ίντερνετ δε πρέπει να ξεχνάμε την κοινή λογική που θα μας συνόδευε σε οποιαδήποτε άλλη μας δραστηριότητα.

Σκοπός των email spam και μερικά από τα είδη που έχουν παρατηρηθεί, είναι τουλάχιστον ένας από τους παρακάτω:

Είδη ηλεκτρονικού spam:

Διαφήμιση	**Διάδοση Malware**	**Εξακρίβωση email**
	Φάρσα-Hoax	**Προσηλυτισμός**
Nigeria C.	**Flooding**	**DoS**

Το e-mail Spam είναι ανεπιθύμητο διαφημιστικό e-mail.Εάν λάβετε ένα e-mail που πιθανόν να είναι ανεπιθύμητο, δεν θα πρέπει να απαντήσετε σε αυτό, να το κάνετε click ή να το προωθήσετε.

Εάν είναι δυνατόν θα πρέπει να το αναφέρετε και να το διαγράψετε χωρίς να το ανοίξετε ή να κάνετε click σε κάποιο link μέσα σε αυτό. Το Spam είναι ενοχλητικό γιατί πιθανόν να εμπεριέχει (fraud) απάτη ή να μολύνει τον υπολογιστή σας με ιό ή άλλο κακόβουλο λογισμικό.

Τώρα όσον αφορά το downloading.Κάντε λήψη με προσοχή. Πρώτα να σκέφτεστε και μετά να κάνετε click. Αναρωτηθήκατε ποτέ εάν είναι ασφαλές να ανοίξετε ένα λογιστικό φύλλο που λάβατε attached από

κάποιον συνάδελφο (σε μια εταιρία π.χ.) ή να «κατεβάσετε» ένα όμορφο μικρό screensaver από το Internet ή να κάνετε λήψη μουσικών αρχείων ή αρχείων βίντεο από τον υπολογιστή ενός αγνώστου; Πριν το επιχειρήσετε, σκεφτείτε σοβαρά την πιθανότητα κινδύνου για τον υπολογιστή σας ή το δίκτυο της εταιρείας. Για να προστατέψετε τον υπολογιστή σας από πιθανούς κινδύνους απαιτείται λίγη προνοητικότητα, λίγη προσοχή και αυστηρή προσήλωση στον κανόνα:

Εάν έχετε αμφιβολίες, αποθηκεύστε το πριν την λήψη.

Στη διαδικασία λήψης αρχείων downloading συμπεριλαμβάνεται η εγκατάσταση προγραμμάτων από CD, το άνοιγμα εικόνων ή η σύνδεση σε τοποθεσίες Web από ηλεκτρονικά μηνύματα, αντιγραφή εγγράφων Word ή λογιστικών φύλλων Excel από το δίκτυο της εταιρείας, η ενημέρωση λογισμικού που απαιτείται από το Internet ή η μεταφορά μουσικών αρχείων από έναν υπολογιστή στην άλλη άκρη του κόσμου.Αυτά τα αρχεία μπορεί να είναι αυτό που αναμένατε αλλά μπορεί να είναι και εντελώς επικίνδυνα. Κακόβουλο λογισμικό (λέγεται επίσης και Malware) είναι το λογισμικό το οποίο μπορεί να βλάψει τον υπολογιστή σας. Μπορεί να περιέχει viruses, worms, trojans, hi-jackers, προγράμματα υποκλοπής ή και άλλα ενοχλητικά προγράμματα.

Η απελευθέρωση ενός ιού μπορεί να προκαλέσει την καταστροφή δεδομένων στον υπολογιστή σας ή να επιτρέψει την πρόσβαση τρίτων σε αυτόν, στο δίκτυο και σε όλους τους υπολογιστές που είναι συνδεδεμένοι σε αυτό. Αυτό μπορεί να έχει καταστροφικό αντίκτυπο ειδικά εάν ο ιός καταστρέψει σημαντικές πληροφορίες, όπως καταλόγους διευθύνσεων ή άλλες εμπιστευτικές πληροφορίες.

Οι πιο γνωστές μορφές προγραμμάτων υποκλοπής μπορούν να αλλάξουν τη συμπεριφορά του υπολογιστή σας, να τον καθυστερούν υπερβολικά και να του προκαλέσουν ανεπανόρθωτη βλάβη (δεν θα φτιάχνει ούτε με format). Κατά τ' άλλα το λογισμικό KeyLogger θα κάνει remote τον υπολογιστή σας και θα τον χρησιμοποιεί όσο και όποτε θέλει, σαν να είσασταν εσείς. Περισσότερο επικίνδυνο είναι το γεγονός ότι τα προγράμματα υποκλοπής μπορούν να παρακολουθήσουν της συνήθειες

περιήγησης, να αποσπάσουν passwords καθώς επίσης και να επιτρέψουν σε κάποιον εισβολέα να πάρει τον έλεγχο του υπολογιστή σας.

Κακόβουλο λογισμικό μπορεί να εγκατασταθεί στον υπολογιστή χωρίς να το γνωρίζετε ή χωρίς να συναινείτε ή μπορεί να είναι ενσωματωμένο σε κάποιο πρόγραμμα που σκοπεύετε να κάνετε λήψη από το ίντερνετ

Για παράδειγμα, ενώ εσείς πιστεύετε πως κάνατε λήψη ενός παιχνιδιού, ανακαλύπτετε πως το «παιχνίδι» βρήκε στον υπολογιστή τον αριθμό της πιστωτικής σας κάρτας και το έστειλε σε κάποιον εισβολέα. Κάποια είδη κακόβουλου λογισμικού εξαπλώνονται όταν αποστέλλουν ηλεκτρονικά μηνύματα από έναν «μολυσμένο» υπολογιστή σε κάθε ηλεκτρονική διεύθυνση που βρίσκουν.

Με βάση έγκυρα sites στην Αμερική τα οποία μετρούν την κίνηση στο Internet και κάποιους υπολογισμούς, το 80% ολόκληρης της κίνησης των e-mails είναι ανεπιθήμυτα.

Πολλοί λένε πως δεν υπάρχουν ανεπιθύμητα «σύγχρονα» μηνύματα. Λάθος.

Όπως μπορείτε να λάβετε ανεπιθύμητα μηνύματα στο mailbox σας, έτσι μπορείτε να λάβετε και ανεπιθύμητα synchronous μηνύματα (Instant messaging, Messenger, IRC κ.ά), τα οποία συχνά αναφέρονται ως Spim. Αυτά τα synchronous μηνύματα μπορεί να προέρχονται από κάποιον τελείως άγνωστο σας ή και από ανθρώπους που γνωρίζετε. Μπορεί επίσης να περιέχουν και επικίνδυνους ιούς. Εάν λάβετε μια ηλεκτρονική κάρτα από κάποιον που δεν γνωρίζετε, θα πρέπει να την διαγράψετε.

Πώς θα αποφύγετε το SPAM

Για να αποφεύγουμε το spam πρέπει να προστατεύουμε το email μας και να προσέχουμε να μη το δημοσιεύουμε σε σελίδες του ίντερνετ. Οι spammers χρησιμοποιούν «διαδικτυακά ρομπότ» που σκανάρουν το διαδίκτυο για ηλεκτρονικές διευθύνσεις και τις αποθηκεύουν στα αρχεία τους. Αυτές τις διευθύνσεις μετά τις πουλάνε σε άλλους spammers.

Αν παρατηρήσετε προσεκτικά την ιστοσελίδα μου, δε θα βρείτε πουθενά το email μου σαν link παρά μόνο σαν αρχείο εικόνας. Ένας άλλος τρόπος προστασίας του email είναι να μη χρησιμοποιείτε το σύμβολο @ αλλά να περιγράφετε το email όπως ακούγεται (ηχητικά) πχ «myemail at yahoo dot com» όπου at=@, dot=.΄Αν θέλετε να χρησιμοποιήσετε αρχείο εικόνας, μπορείτε να φτιάξετε ένα στην ιστοσελίδα: http://www.privacysig.com/

Ένα άλλο πρόβλημα είναι ότι αν ο ηλεκτρονικός υπολογιστής ενός φίλου σας μολυνθεί από κάποιο κατασκοπευτικό πρόγραμμα, το πιό πιθανό είναι να καταγράψει όλα τα email που έχει ο φίλος σας αποθηκευμένα στον Η/Υ του και να τα ενσωματώσει στις «διευθνείς» spam λίστες. Έτσι δε φτάνει να προστατεύετε εσείς το email σας.

Πρέπει να μάθουμε όλοι να σεβόμαστε το απόρρητο της ηλεκτρονικής διεύθυνσης email και να το διαχειριζόμαστε σαν ένα νούμερο τηλεφώνου που δε θα αποκαλύπταμε πουθενά χωρίς την άδεια του ιδιοκτήτη.

Προστατεύστε τα email των φίλων σας

Σαν απλοί χρήστες μη στέλνετε email μαζικά σε λίστες φίλων σας χωρίς να χρησιμοποιείτε την επιλογή **bcc**. Θα το έχετε παρατηρήσει ότι στην αποστολή ενός email έχετε το πεδίο προς, θέμα, αλλά και τα πεδία cc**,** bcc**.** CC **(**carbon copy**)** σημαίνει δηλαδή καρμπόν αντίγραφο και BCC **(**blind carbon copy**)** σημαινει «τυφλό» καρμπόν αντίγραφο. Στο πεδίο bcc μπορείτε να γράφετε τη λίστα με τα email των φίλων σας, έτσι ώστε να μην είναι ορατά για τα υπόλοιπα μέλη και να προστατεύονται έτσι τα δεδομένα τους. Ένας ακόμα τρόπος που ακολουθούν πολλοί είναι το να έχουμε μια απλή δωρεάν ηλεκτρονική διεύθυνση (webmail: yahoo, hotmail, gmx κτλ) που χρησιμοποιείται σε εγγραφές στο ιντερνετ (messenger, message boards, φόρουμ, clubs κτλ) και το επίσημο email το οποίο προστατεύουμε. Αυτή είναι μια πολύ καλή τακτική.

Διαφορετικά, ο μόνος τρόπος να προστατευτούμε από το spam και μια τακτική που αναγκάζονται να χρησιμοποιούν εταιρίες των οποίων το email είναι πολύ γνωστό, είναι τα διάφορα εμπορικά και μη προγράμματα anti-spam.

Παρόλαυτά, εγώ εδώ δε θα προτείνω κάποια προγράμματα Antispam γιατί ούτε μέσα από αυτά μπορεί κανείς να εγγυηθεί ότι δε θα λάβει ανεπιθύμητη αλληλογραφία ή το οτι θα λειτουργίσουν σωστά τα φίλτρα του και δεν θα εμποδίσει χρήσιμη αλληλογραφία να κατεβεί.

Όπως και να το κάνουμε το spam δε μπορούμε τα το αποφύγουμε τελείως με κανένα τρόπο, όσο δεν υπάρχουν αυστηροί νόμοι για τη καταπολέμησή του και όσο δεν εφαρμόζονται. Αν και σε πολλές χώρες υπάρχουν τέτοιοι νόμοι, δυστυχώς δεν εφαρμόζονται. Ακόμα χειρότερα οι περισσότεροι internet providers δεν συμβάλλουν στον αγώνα κατά του spam και δεν προσφέρουν abuse email διευθύνσεις καταγγελιών. Το 90% από τις φορές που έχω προσπαθήσει να καταδιώξω και να εντοπίσω αυτούς που στέλνουν τα spam, σκοντάφτω σε ασιατικούς providers που δεν έχουν δεσμεύσεις και δεν υπόκειται σε Antispam νόμους.

Όπως φαίνεται υπάρχει μια μεγάλη μερίδα ανθρώπων ανά τον κόσμο που στη κυριολεξία ζει και πλουτίζει από την ανεπιθύμητη αλληλογραφία και ίσως αυτός να είναι ο μεγαλύτερος λόγος για τον οποίο δεν υπάρχουν αποτελεσματικά μέτρα κατά της.

12.6 **Διαφήμιση**

Τα spam email που περιέχουν διαφημίσεις είναι τα πιο συνηθισμένα και ονομάζονται επίσημα «μη ζητηθείσα εμπορική επικοινωνία» (unsolicited email).Είναι ενοχλητικά γιατί φουσκώνουν το inbox μας με περιττές διαφήμισης ιστοσελίδων ή προϊόντων και επίσης καταλαμβάνουν χώρο, χρόνο και bandwidth καθώς κατεβαίνουν στον υπολογιστή μας.

Η μη ζητηθείσα εμπορική αλληλογραφία είναι παράνομη σύμφωνα με το νόμο για την «Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα».

Αυτός ο νόμος προβλέπει (άρθρο 9 του Ν.2774/1999):Η με οποιοδήποτε τηλεπικοινωνιακό μέσο απ΄ ευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών επιτρέπεται μόνον στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους**.**

Αυτό σημαίνει ότι και η τακτική telemarketing ορισμένων εταιριών, όπως κάποιων τραπεζών που προσπαθούν να πουλήσουν πιστωτικές κάρτες από το τηλέφωνο, είναι παράνομη και θα έπρεπε να τιμωρείται.

Την επόμενη φορά λοιπόν που κάποιος πωλητής θα σας πάρει τηλέφωνο χωρίς τη ρητή συγκατάθεσή σας, επικαλεστείτε τον νόμο προστασίας προσωπικών δεδομένων και μη τον αφήσετε να σπαταλήσει τον χρόνο σας.

Επίσης να προσέχετε που δίνετε τα στοιχεία σας, γιατί πολλές εταιρίες τα πουλάνε σε άλλες για να σας ενοχλούν με διαφημίσεις. Όταν όμως τα δίνετε από μόνοι σας από το τηλέφωνο, είναι σας να δίνετε τη «ρητή συγκατάθεσή σας».

12.7 **Διάδοση Malware**

Ιοί και άλλα προγράμματα που περιέχουν βλαβερό κώδικα στέλνονται συννημένα σε email. Θα έχετε ακούσει τη συνηθισμένη συμβουλή «μην ανοίγετε συννημένα από ανθρώπους που δε γνωρίζετε».

Πρέπει κανείς να λάβει υπόψη του ότι είναι πολύ εύκολο να παραποιηθεί και να πλαστογραφηθεί η διεύθυνση του πραγματικού αποστολέα.

«Θα πλαστογραφούσε ένας spammer τη διεύθυνση ενός φίλου μου;»Ναι. Έχει συμβεί και δεν είναι σπάνιο φαινόμενο. Πιό πιθανό όμως είναι να έχει κολλήσει κάποιος φίλος σας ένα σκουλήκι (worm) το οποίο στέλνει τον εαυτό του αυτόματα σε όλες τις αποθηκευμένες επαφές του προγράμματος αλληλογραφίας (outlook express, outlook, thunderbird κτλ).

Κακόβουλα προγράμματα μπορούν να περιέχονται και στο κώδικα HTML του email με τη μορφή κάποιου script. Σε αυτή την περίπτωση αρκεί η απλή προεπισκόπιση του email για να κολλήσει κανείς ιό. Η λύση είναι να απενεργοποιήσουμε τον κώδικα HTML στο πρόγραμμα αλληλογραφίας.

12.8 Εξακρίβωση Email

Οι spammers στέλνουν συχνά emails τα οποία περιέχουν ένα πρόγραμμα που ενημερώνει τον αποστολέα αν ο λογαριασμός email είναι ενεργός. Όταν σιγουρευτούν συνεχίζουν να στέλνουν SPAM emails και κρατάνε τη διεύθυνση email στα αρχεία τους. Για αυτό τον σκοπό χρησιμοποιούνται και τα αρχεία εικόνας.

Ο τρόπος αντιμετώπισης είναι πάλι η απενεργοποίηση του κώδικα HTML και το μπλοκάρισμα της εμφάνισης των εικόνων.

Φάρσα - Hoax

Ένα ακόμα επικίνδυνο spam το οποίο είναι δυστυχώς αρκετά διαδεδομένο είναι το HOAX. Αυτά είναι email που φαίνεται να περιέχουν πληροφορίες για τον πιο επικίνδυνο ιό και μας καλούν να προωθήσουμε το μήνυμα σε όλα τα άτομα στη λίστα μας. Τέτοια hoax στέλνονται συχνά και μέσω των messengers, δεν περιέχουν ποτέ αξιόπιστες πληροφορίες και σκοπό έχουν να σπείρουν τον τρόμο και τον πανικό ανάμεσα σε άπειρους χρήστες.

Να βασίζεστε μόνο σε επίσημες πληροφορίες που μπορείτε να βρείτε σε επίσημες και γνωστές ιστοσελίδες κατασκευαστών antivirus. Εκτός του ότι δεν είναι αστείο να σπέρνουμε τον πανικό με το να προωθούμε τέτοια γελοία email, μαζικές προωθήσεις δημιουργούν μεγάλα προβλήματα και αστάθειες στα δίκτυα.

Παράδειγμα HOAX 1:

A MEMBER OF AOL BY THE SCREEN NAME OF ZZ331MIGHT TRY TO SEND YOU A VIRUS WHICH COULD CRASH YOUR COMPUTER SYSTEM.

HIS TRICK: HE INNOCENTLY IM's YOU HELLO, WAITS 30 SECONDS, THEN IM's YOU AGAIN, WAITS ANOTHER 30 SECONDS, AND THEN WRITES..."WHAT THE FU**,

WHY AREN'T YOU ANSWERING"DO NOT REPLY TO HIS IM's, NOR READ ANY OF HIS E-MAIL BECAUSE ONCE YOU REPLY, YOUR
COMPUTER WILL FREEZE AND THATS HOW YOU KNOW YOUR HARD DRIVE IS BEING WIPED OUT. SO PLEASE BE VERY VERY CAREFUL!!!!

PLEASE PASS THIS ON TO EVERY ONE YOU KNOW!!!

Παράδειγμα HOAX 2:

Outbreak: I'm infecting you with t-virus, my code is «random numbers». Forward this to «phone number» to get your own code and chance to win prizes.
More at «website URL»

Φάρσα-HOAX για το κινητό τηλέφωνο:

Μια καινούργια φάρσα που σπέρνει την αμηχανία στους χρήστες κινητών τηλεφώνων είναι η ακόλουθη:

«Αν σας τηλεφωνήσουν στο κινητό σας από κάποιον που θα σας πει ότι είναι τεχνικός εταιρείας, και κάνουν έλεγχο στο τηλέφωνό σας και θα πρέπει να πατήσετε #90 ή 09# ή οποιοδήποτε άλλο νούμερο κλειστε το τηλέφωνο χωρίς να πατήσετε άλλο νούμερο.

Πρόκειται για κάποια εταιρεία-απάτη που χρησιμοποιεί κάποια συσκευή, η οποία μόλις πατήσετε τα παραπάνω νούμερα, μπορεί να μπει στην κάρτα SIM και να παίρνουν τηλέφωνα με δική σας χρέωση. Προωθήστε το μήνυμα σε όσους περισσότερους μπορείτε.»

Η παραπάνω φάρσα είχε εμφανιστεί για πρώτη φορά στη γερμανία το 1999, με ακριβώς το ίδιο κείμενο. Η γερμανική εταιρία κινητής τηλεφωνίας T-Mobil (T-D1) τότε είχε δηλώσει επίσημα ότι κάτι τέτοιο δεν είναι δυνατόν τεχνικά στο δίκτυό της γιατί:

στη γερμανία δεν ισχύει το reverse charging το δίκτυο δεν υποστηρίζει πρόσβαση σε κάρτα SIM κατά τη διάρκεια κλήσης. Επίσης υπάρχει μια λειτουργία για την πιστοποίηση του κινητού, η οποία μαζί με το κρυπτογραφικό κλειδί δεν επιτρέπει την πρόσβαση στην κάρτα με το

συνδιασμό 9009.η κάρτα SIM προστατεύεται από τον κωδικό PIN.Στην ερώτησή μου αν κάτι τέτοιο είναι τεχνικά δυνατόν στα ελληνικά δίκτυα, η vodafone μου απάντησε με το παρακάτω email:

«Αγαπητή κα Κοντίνη,

σε απάντηση του τελευταίου e-mail σας θα θέλαμε να σας ενημερώσουμε ότι, και στο παρελθόν έχει αναφερθεί κάτι ανάλογο το οποίο όταν διερευνήθηκε διαπιστώθηκε ότι δεν ήταν πραγματικό γεγονός, δεν έχει καταγραφεί και διαπιστωθεί γιατί απλά δεν ισχύει κάτι τέτοιο. Ηταν μια κακόγουστη φάρσα.

Τεχνικά και δικτυακά δεν υπάρχει απολύτως καμμία πρόσβαση στην κάρτα sim του συνδρομητη με οποιαδήποτε χρήση κωδικών ή άλλων ενεργειών εξ αποστάσεως έτσι όπως περιγράφεται. Σε καμμία περίπτωση δεν ισχύει ότι αναφέρεται. Παρακαλούμε μην διστάσετε αν έχετε κάποια άλλη ερώτηση ή απορία.

Στην διάθεση σας για οποιαδήποτε διευκρίνιση.

Ευχαριστούμε που επικοινωνήσατε μαζί μας.

Kyriacos Maragos Customer Service Support Analys Customer Services»

Το email που έστειλα ήταν το παρακάτω:

«Γειά σας,

Είμαι συνδρομητής της vodafone και με απασχολούν τα παρακάτω. Έχω στείλει ήδη ένα email στο γραφείο υποστήριξης της Vodafone αλλά δεν έλαβα απάντηση.

Έλαβα ένα email το οποίο μάλλον περιέχει ψευδείς πληροφορίες. Θα ήθελα όμως να μου επιβεβαιώσετε σαν επίσημη πηγή ότι το παρακάτω δεν ισχύει, και ότι κάτι τέτοιο είναι τεχνικά αδύνατον:

«Αν σας τηλεφωνήσουν στο κινητό σας από κάποιον που θα σας πει ότι είναι τεχνικός εταιρείας, και κάνουν έλεγχο στο τηλέφωνό σας και θα πρέπει να πατήσετε #90 ή 09# ή οποιοδήποτε άλλο νούμερο, κλείστε το τηλέφωνο χωρίς να πατήσετε κάποιο αριθμό.

Πρόκειται για κάποια εταιρεία-απάτη που χρησιμοποιεί κάποια συσκευή, η οποία μόλις πατήσετε τα παραπάνω νούμερα, μπορεί να μπει στην κάρτα SIM και να παίρνουν τηλέφωνα με δική σας χρέωση.

Προωθήστε το μήνυμα σε όσους περισσότερους μπορείτε.

Επίσης θα ήθελα να ρωτήσω:

-Επιτρέπει η vodafone reverse calling;

-Υποστηρίζει το δίκτυο πρόσβαση σε κάρτα σιμ κατα τη διάρκεια κλήσης;

-Μπορεί να διαβαστεί το κρυπτογραφικό κλειδί της κάρτας απο απόσταση;

Παρακαλώ ενημερώστε με για να μπορέσω να ενημερώσω και εγώ τους αναγνώστες μου. Η απάντηση σας μπορεί να δημοσιευτεί στην ιστοσελίδα μου www.itsecurity.gr που αναλύει θέματα για την ηλεκτρονική ασφάλεια.

Ευχαριστώ
Αγγελίνα Κοντίνη

Τα προγράμματα dialer (στο εξής dialers) είναι λογισμικό το οποίο μπορεί να μεταδοθεί μέσω διαδικτύου και να εγκατασταθεί στον ηλεκτρονικό σας υπολογιστή.Αυτό που κάνουν οι dialers, αφού εγκατασταθούν στον υπολογιστή σας είναι να αλλάξουν τις ρυθμίσεις (settings) του modem σας από μία συγκεκριμένη σύνδεση στο διαδίκτυο σε μία άλλη. Συνήθως η αλλαγή είναι από το συνήθη αριθμό του παροχέα Internet (ISP) που χρησιμοποιείτε, σε έναν αριθμό αυξημένης χρέωσης, είτε αυτός είναι της σειράς 90XXXXXXXX είτε αριθμός στο εξωτερικό (00XXXXXXXXX).

Οι dialers μπορεί να είναι ένας νόμιμος και βολικός τρόπος για να πληρώσει ο χρήστης πρόσβαση σε ειδικό περιεχόμενο μέσω του διαδικτύου (π.χ. λογισμικό, παιχνίδια, SMS logos, ερωτικό περιεχόμενο),αντί χρήσης πιστωτικής κάρτας.

Στην περίπτωση αυτή, ο χρήστης αντί να χρησιμοποιήσει πιστωτική κάρτα για τη χρέωσή του ειδικού περιεχομένου κάποιου διαδικτυακού

τόπου,χρεώνεται για το περιεχόμενο αυτό στο λογαριασμό του τηλεφώνου του,μέσω των αριθμών αυξημένης χρέωσης, όπως ακριβώς συμβαίνει και με τις υπηρεσίες προστιθέμενης αξίας αυξημένης τιμολόγησης που καλεί από το τηλέφωνό του (π.χ. Audiotex).

Ο τρόπος με τον οποίο οφείλουν να λειτουργούν οι νόμιμοι dialer,προστατεύοντας τον καταναλωτή, είναι ο ακόλουθος: αν προσπαθήσετε να επισκεφτείτε μία ιστοσελίδα η οποία προσφέρει ειδικό περιεχόμενο με αυτόν τον τρόπο, θα εμφανιστεί στην οθόνη σας ένα παράθυρο διαλόγου το οποίο σας ρωτά αν θέλετε να κατεβάσετε το συγκεκριμένο πρόγραμμα dialer.

Επίσης σας ενημερώνει για το είδος της υπηρεσίας την οποία πρόκειται να χρησιμοποιήσετε και για τη χρέωσή της. Αν επιλέξετε «yes»,το λογισμικό του dialer εγκαθίσταται στον υπολογιστή σας.

Το λογισμικό αλλάζει τον αριθμό σύνδεσής σας στο διαδίκτυο με αυτόν της αυξημένης χρέωσης, ενώ εσείς έχετε τη δυνατότητα πρόσβασης στο ειδικό περιεχόμενο ενώ χρεώνεστε με αυξημένη τιμολόγηση.

Καθ’ όλη τη διάρκεια πρόσβασης στο ειδικό περιεχόμενο, υπάρχει στην οθόνη σας ένδειξη ότι χρησιμοποιείται σύνδεση στο διαδίκτυο αυξημένης χρέωσης.

Στη συνέχεια, μόλις αποσυνδεθείτε από τη συγκεκριμένη ιστοσελίδα, odialer απεγκαθίσταται από τον υπολογιστή σας, και η σύνδεση του modem επιστρέφει στον αριθμό του παροχέα Internet (ISP) που χρησιμοποιείτε.

Ποιο είναι το πρόβλημα

Το πρόβλημα ξεκινά όταν ο χρήστης δεν γνωρίζει ότι έχει «κατεβάσει»(download) έναν dialer από το διαδίκτυο ή όταν δεν γνωρίζει τι κάνει αυτός ο dialer τον οποίο έχει κατεβάσει.

Η απάτη μέσω dialers συμβαίνει όταν ο διαδικτυακός τόπος δεν καθιστά σαφές για τον χρήστη ότι με τις ενέργειές του, οδηγείται στην εγκατάσταση λογισμικού στον ηλεκτρονικό του υπολογιστή ή ότι η σύνδεσή του στο διαδίκτυο θα αλλάξει, όχι μόνο για την πρόσβαση σε ειδικό περιεχόμενο, αλλά σε πιο συχνή ή και μόνιμη βάση. Οι dialers αυτοί μπορεί να πραγματοποιούν συνέχεια κλήσεις προς έναν αριθμό αυξημένης

χρέωσης, εις βάρος του χρήστη, κατά τη διάρκεια όλου του εικοσιτετραώρου, ακόμα και κάθε λίγα λεπτά, αρκεί ο υπολογιστής να είναι αναμμένος.

Υπάρχει ακόμα η πιθανότητα, κάποιοι dialers να φτάσουν στον χρήστη ως συνημμένα (attachment) σε κάποιο ηλεκτρονικό μήνυμα (e-mail). Αυτοί δεν είναι εύκολο να ανιχνευθούν, και εγκαθίστανται χωρίς να ζητήσουν τη συγκατάθεση του χρήστη.Απάτες τέτοιου είδους μπορεί ακόμα να σιγήσουν τους ήχους κλήσης(dialing) στο διαδίκτυο που κάνει το modem σας για να αποκρύψουν το γεγονός ότι το modem πραγματοποιεί μία κλήση.

Πρόσφατα, το πρόβλημα με τις απάτες μέσω dialers έχει πάρει σημαντικές διαστάσεις και στην Ελλάδα.

Ήδη, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχει λάβει μεγάλο αριθμό καταγγελιών από χρήστες διαδικτύου, οι οποίες αφορούν την υπέρογκη και εν αγνοία τους χρέωσή τους για κλήσεις σε αριθμούς της σειράς 90XXXXXXXX ή αριθμούς του εξωτερικού (00XXXXXXXXXXX), ενώ αυτές οι κλήσεις συνδέονται με την πρόσβασή τους στο διαδίκτυο.

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, στην προσπάθειά της να αντιμετωπίσει το πρόβλημα αυτό στα πλαίσια των αρμοδιοτήτων της, εξετάζει την κατάρτιση Κώδικα Δεοντολογίας για τις Υπηρεσίες Προστιθέμενης Αξίας Αυξημένης Τιμολόγησης, στα πλαίσια του οποίου ρυθμίζονται και θέματα που αφορούν τους dialers και η θέσπιση κανόνων λειτουργίας οι οποίοι θα εξασφαλίσουν την προστασία των χρηστών από παράνομους dialers.

Πώς θα καταλάβετε ότι έχει εγκατασταθεί στον Η/Υ σας ένας dialerdialer;

Στη συνέχεια θα βρείτε μερικές συμβουλές για πιθανούς τρόπους με τουςοποίους μπορείτε να καταλάβετε ότι έχει εγκατασταθεί στον Η/Υ σας και λειτουργεί ένας dialer:

Θα ακούσετε το modem σας να αποσυνδέεται και να πραγματοποιεί νέα κλήση (εκτός εάν ο dialer έχει σιγήσει τους ήχους κλήσης).Είναι πιθανόν, η ταχύτητα της σύνδεσής σας με το Internet να είναι πολύ χαμηλότερη από ότι συνήθως. Μπορεί να υπάρχουν άλλοι λόγοι γι' αυτό, αλλά ξεκινήστε εξετάζοντας τη σύνδεσή σας (dial up settings).

Θα λάβετε έναν απρόσμενα υψηλό λογαριασμό τηλεφώνου, στον οποίο θα βρείτε κλήσεις σε άγνωστους αριθμούς υψηλής χρέωσης ή εξωτερικού.

Είναι πιθανόν, παρά το γεγονός ότι θα είστε συνδεδεμένοι στο διαδίκτυο, να μην μπορείτε να στείλετε ηλεκτρονικά μηνύματα (e-mails)

Τι μπορείτε να κάνετε για να προφυλαχτείτε;

Στη συνέχεια θα βρείτε μερικές συμβουλές οι οποίες έχουν ως στόχο την προστασία σας από κακόβουλες ενέργειες dialer:

Να κλείνετε τον Η/Υ σας όταν δεν τον χρησιμοποιείτε.Ποτέ μην ανοίγετε attachments ηλεκτρονικών μηνυμάτων αν δεν γνωρίζετε τι είναι, διότι θα μπορούσε να είναι ένας κακόβουλος dialer.

Μπορείτε να απευθυνθείτε στον ISP σας ο οποίος θα σας συμβουλεύσει όσον αφορά τη χρήση συγκεκριμένων προγραμμάτων για την προστασία σας.

Εξετάζετε συχνά τις παραμέτρους σύνδεσης του Η/Υ σας με το διαδίκτυο για να βεβαιώνεστε ότι ο αριθμός που καλεί το modem σας για να συνδεθεί είναι ο σωστός. Να είστε επιφυλακτικοί όταν επιλέγετε με το ποντίκι σας (click) σε αναδυόμενα παράθυρα (pop-up windows) που εμφανίζονται ξαφνικά στην οθόνη σας. Αν έχετε αμφιβολία για το αν επιθυμείτε να δείτε το συγκεκριμένο περιεχόμενο, πάντα να επιλέγετε με το ποντίκι σας την απάντηση «no» ή να κλείνετε το παράθυρο.

Να είστε ιδιαίτερα επιφυλακτικοί αν κατά την περιήγησή σας.Στο διαδίκτυο μεταφερθείτε σε κάποια ιστοσελίδα την οποία δεν περιμένατε.

Να έχετε δυνατά την ένταση του modem σας έτσι ώστε να ακούσετε τους ήχους στην περίπτωση που το modem σας αποσυνδεθεί και επιχειρεί να πραγματοποιήσει και πάλι κλήση.Αν προσέξετε κάποιο εικονίδιο στην

επιφάνεια εργασίας σας που σας φαίνεται άγνωστο, εξετάστε το και σβήστε ο,τιδήποτε δεν αντιστοιχεί σε έγκυρες εφαρμογές.

Σε αυτήν την περίπτωση δεν θα σβήσετε μόνο τα εικονίδια αλλά θα απεγκαταστήσετε (uninstall) και τις σχετικές εφαρμογές.

Ενημερώστε την οικογένειά σας για την απειλή των κακόβουλων dialers και ελέγξτε τη χρήση του διαδικτύου από τα παιδιά σας

Μπορείτε να ζητήσετε από τον ΟΤΕ να σας ενεργοποιήσει την υπηρεσία της φραγής για εξερχόμενες κλήσεις προς αριθμούς αυξημένης χρέωσης και αριθμούς εξωτερικού.

Στην περίπτωση που έχετε προεπιλογή φορέα μπορείτε εναλλακτικά να ζητήσετε από τον προεπιλεγμένο σας πάροχο να σας ενεργοποιήσει την υπηρεσία της φραγής για εξερχόμενες διεθνείς κλήσεις.

Οι περισσότεροι dialers ανιχνεύονται από τα πρόσφατα αντιικά προγράμματα. Βεβαιωθείτε ότι το αντιικό σας πρόγραμμα παρέχει αυτή τη δυνατότητα και φροντίστε να το ενημερώνετε συστηματικά. Μπορείτε να εντοπίσετε την ύπαρξη ήδη εγκατεστημένων ή προς εγκατάσταση dialers στον Η/Υ σας με λογισμικό το οποίο θα εντοπίσει τα ύποπτα προγράμματα, θα σας περιγράψει τι κάνουν και στη συνέχεια θα σας βοηθήσει να τα απεγκαταστήσετε.

Τέτοιο λογισμικό (είτε ελεύθερο, είτε με πληρωμή) μπορείτε να βρείτε στο διαδίκτυο.Επίσης, σημειώνουμε ότι στην περίπτωση όπου η σύνδεσή σας με το διαδίκτυο είναι αποκλειστικά με ευρυζωνική σύνδεση (ADSL) δεναπειλείστε από προγράμματα dialers, όπως περιγράφηκαν πιο πάνω.

Η Απάτη των Dialer-1

- Η απάτη λειτουργεί ως εξής : Μια ιστοσελίδα δελεάζει τον επισκέπτη, συνήθως με ανακοινώσεις για γυμνές φωτογραφίες επώνυμων γυναικών ή για καυτά videos on-line κ.ά., οι οποίες υπηρεσίες μάλιστα διαφημίζονται έντονα και τονίζεται ότι παρέχονται δωρεάν.
- Μόλις ο χρήστης κάνει κλικ σ’ ένα συγκεκριμένο σημείο, εγκαθίσταται αυτόματα στον υπολογιστή του και χωρίς αυτός να το γνωρίζει, ένα ειδικό πρόγραμμα, με αποτέλεσμα αντί για αστική κλήση στον τοπικό provider (ο γνωστός ΕΠΑΚ, 8962…) να γίνεται εκτροπή και

διεθνής κλήση σύνδεσης και μάλιστα υπερπόντια, με πολλαπλάσιο φυσικά κόστος.

Η Απάτη των Dialer-2

- Για παράδειγμα, ο χρήστης αντί για 0,17 – 0,35 € την ώρα, χρεώνεται με 2,50 € ανά λεπτό. Οι δημιουργοί παρόμοιων ιστοσελίδων έχουν κάνει συμβάσεις με τους τηλεπικοινωνιακούς οργανισμούς των χωρών αυτών και μοιράζονται τα κέρδη από τις υπέρογκες χρεώσεις των ανυποψίαστων χρηστών.
- Είναι ποινικό αδίκημα;
- Πάντως έχει γίνει ποινική δίωξη στην Ελλάδα σε βαθμό κακουργήματος το έτος 2004 για μια τέτοια υπόθεση. Οι τηλεφωνικές εταιρείες ισχυρίζονται ότι δεν φέρουν καμία ευθύνη για τις υποθέσεις αυτές και η μόνη παραχώρηση που μπορούν να κάνουν προς τους παθόντες είναι να αποπληρώσουν τα χρέη τους σε δόσεις.

12.9 Προσηλυτισμός

Κατά καιρούς έχουν εμφανιστεί κύματα Spam email που σαν στόχο έχουν τη διάδοση μιας ρατσιστικής, εξτρεμιστικής ή θρησκευτικού περιεχομένου ιδεολογίας.

12.10 Flooding

Flooding σημαίνει πλημμυρίζω και είναι ένας όρος που χρησιμοποιείται για να περιγράψει το πλημμύρισμα των λογαριασμών email.

Στόχος τους είναι να παραλύσουν ένα δίκτυο ή έναν email provider και τα email που στέλνονται είναι συνήθως άδεια, χωρίς κανένα περιεχόμενο.

Παραβίαση σε ιστοσελίδες

iFrame

Εκμεταλλευόμενοι οι κακόβουλοι κενά ασφαλείας,εγκαθιστούν κώδικα (iFrame) σε σελίδες ενός νόμιμου site. Κάθε φορά που το επισκέπτεται κάποιος χρήστης, οκώδικας ενεργοποιείται και μπορεί να εκτρέπει το χρήστη σε πλαστή σελίδα αντιγράφει τα στοιχεία που δίνει ο χρήστης και τα αποστέλλει σε κακόβουλο site εκτελεί πρόγραμμα που κατεβάζει malware στο τερματικό του χρήστη (π.χ. Italian Job) οδηγεί σε παράνομο site που ελέγχει το τερματικό τουχρήστη και, αναλόγως των κενών ασφαλείας πουανιχνεύει,το εγκαθιστά το ανάλογο malware. Τον Μάιο 2008, 200.000 σελίδες μολύνθηκαν μαζικά με τύπου iFrame κώδικα.

Παραβίαση σε ιστοσελίδες

Κοινωνικά Portals (Social Networking)

MySpace

Διαφημιστικό Banner στο MySpace περιείχε κώδικα που εκμεταλλευόταν κενό ασφαλείας του Internet Explorer.Video καλλιτέχνη περιείχε κώδικα που οδηγούσε το χρήστη σε πλαστό site και κατέβαζε malware στο τερματικό του Facebook. Στο Wall του Facebook**,** που χρησιμοποιείται από μέλη για ανταλλαγή μηνυμάτων,video,φωτογραφιών κ.λπ., τοποθετήθηκε μήνυμα απόφίλο» που καλεί τα μέλη να πατήσουν το link και να δουν σχετικό video από το Googlevideo από το Google. Ο χρήστης οδηγείται σε ένα πλαστό site που τον καλεί να κατεβάσει μία νέα έκδοση του Flash Player. Αντί αυτού ένα malware κατεβαίνει στο τερματικό του Αντί αυτού, ένα malware κατεβαίνει στο τερματικό του.

Webmail (Google, Hotmail, Yahoo)

Εύκολο να γίνει reset το password και να αποκτήσει κάποιος πρόσβαση στο λογαριασμό e mail του χρήστη πρόσβαση στο λογαριασμό e-mail του χρήστη.Πρόσφατα, παραβιάστηκε το webmail της κ. Palin.

12.11 Skimming

Ηλεκτρονική υφαρπαγή των δεδομένων που βρίσκονται αποθηκευμένα στη μαγνητική πάστα των τραπεζικών καρτών& δημιουργία κλωνοποιημένων καρτ΄βν.

12.11.1 Skimming σε ATM

- **Τρόπος δράσσης**

Κατασκευή ή προμήθεια από το διαδύκτιο, των ηλεκτρονικών μηχανισμών παγίδευσης. Επιλογή ATM στόχου, συνήθως σε πολυ σ χνα στο σημείο. Εγκατάσταση μηχανισμου παγίδευσης, η οποία διαρκεί λίγα δευτερόλεπτα.

Ο μηχανισμός αποσύρεται από το ATM και με τη χρήση ηλεκτρονικού υπολογιστή μεταφέρονται τα προσωπικά δεδομένα των καρτών που υφαρπάχθηκαν.

Κατασκευή καρτών κλωνών και πραγματοποίηση συναλλαγών σε ελλάδα και εξωτερικο.

- **Δράστες**

Η πλειονότητα των δραστών είναι υπήκοοι Ρουμανίαςκαι Βουλγαρίας. Σε μικρότερο βαθμό συναντόντε με άτομα αλλων εθνικοτήτων.

Σε δύο υποθόσεις έχουν συλληφθεί και κατηγορηθεί έλληνες. Οι δράστες ανήκουν κατά κύριο λόγο σε οργανωμένες εγκληματικές ομάδες.

Ø Δομή εγκληματικών ομάδων (Ε.Ο.)

Ακολουθείται ιεραρχική δομή.

Οι κεφαλές της Ε.Ο. βρίσκονται στη Χώρα καταγωγής (πυρήνας).

Συντονίζουν τις μετακινίσεις τωνυπολοόπων μελών και φροντίζουν για την κάλυψητων εξόδων.

Ομάδες συνεργών τους διαμοιράζονται σε διάφορες χώρες, αναπτύσσοντας κοινωνική και οικονομική δραστηριότητα και τοπικά δίκτυα συνεργατών, έτοιμες να δράσουν (μεσαία επιχειρησιακά κύτταρα). Μικρότερες ομάδες ομοεθνών τους, συγκροτούνται περιστασιακά και δραστηριοποιούνται σε διάφορες Χώρες, κατευθυνόμενοι από τα μέλη της Ε.Ο. που έχουν εγκατασταθεί εκεί (εκτελεστικά όργανα).

Επιβολή του νόμου

Μετά το έτος 2006, οι δράστες κατηγορούνται επιπρόσθετα και για παραβίαση του Νόμου για τη Προστασία των Προσωπικών Δεδομένων (άρθρο 22 §§4 & 6 Ν. 2472/1997), η οποία αποτελεί κακούργημα, με αποτέλεσμα :

1. για κάθε υπόθεση μετά την Αστυνομική έρευνα,διατάσσεται Κύρια Ανάκριση και διενεργείται επισταμένη έρευνα ,οι δράστες προφυλακίζονται & επιβαρύνονται οικονομικά με μεγάλα έξοδα της υπεράσπισάς τους

2. αποτροπή επαναδραστηριοποίησης

3.επιβολή ποινών κάθειρξης άνω των 5 ετών

Συλήψεις

Από το Σεπτέμβριο του έτους 2006 έως και σήμερα, από το Τμήμα Οικονομικών Εγκλημάτων έχουν συλληφθεί 36 άτομα (35 άνδρες & 1 γυναίκα), τα οποία εμπλέκονταν σε 18 υποθέσεις SKIMMING.

Οι δράστες προφυλακίσθηκαν,ενώ για δύο εκ των υποθέσεων χουν εκδοθεί αποφάσεις δικαστηρίου, σύμφωνα με τις οποίες επιβλήθηκαν σε 4αλλοδαπούς ποινές κάθειρξης.

Ο δρόμος του χρήματος

Μέχρι και σήμερα δεν έχουν προκύψει στοιχεία σχετικά με την κατάληξη των χρηματικών ποσόν που προέρχονται από την παράνομη δραστηριάτητα του skimming.

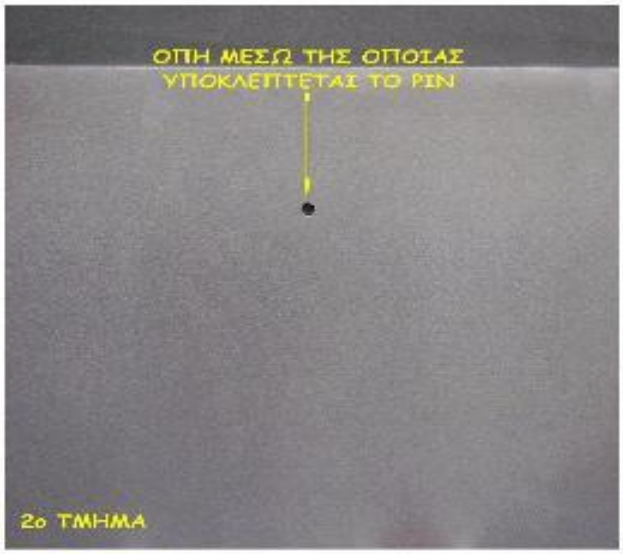
Ο συνήθης τρόπος μεταφοράς αυτών είναι μέσω διεθνών εταιρειών μεταφοράς χρημάτων (WESTERNUNION, MONEY GRAM κ.α.) ή με την απόκρυψή τους σε λεωφορεία ή ιδιωτικά αυτοκίνητα.

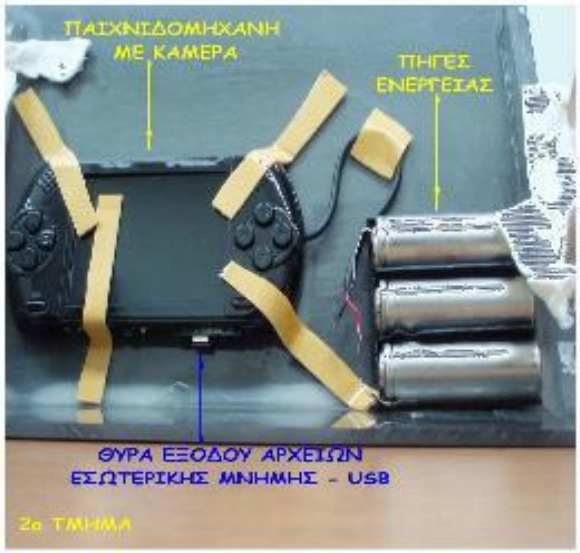
12.12 Skimming σε POS

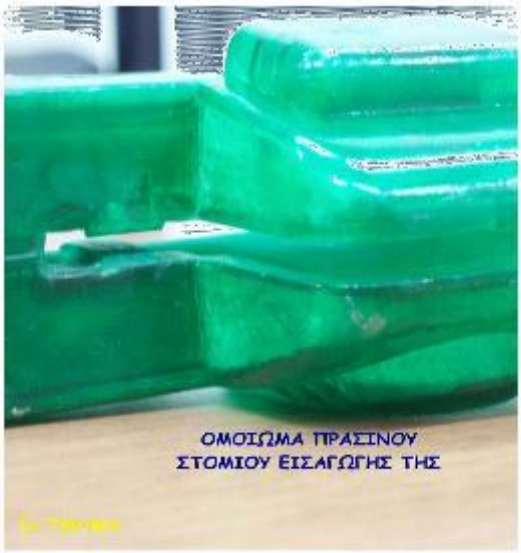
Με τον τρόπο αυτό πέτυχαν να πιστωθεί στους λογαριασμούς τους συνολικό χρηματικό ποσό που ξεπερνάει τα 14.100.000 €.

Από τα χρήματα αυτά κατάφεραν και εκταμίευσαν το ποσό των 1.200.000 € περίπου, μέχρι τη στιγμή που έγιναν αντιληπτοί από τις Τράπεζες. Οι δράστες ισχυρίζονταν κλοπή του POS και άγνοια της απάτης, εκμεταλλευόμενοι την αδυναμία εντοπισμού του σημείου όπου αυτό λειτουργεί.


1ο ΤΜΗΜΑ
2ο ΤΜΗΜΑ


ΟΠΗ ΜΕΣΩ ΤΗΣ ΟΠΟΙΑΣ
ΥΠΟΚΛΕΠΤΕΤΑΙ ΤΟ PIN
2ο ΤΜΗΜΑ

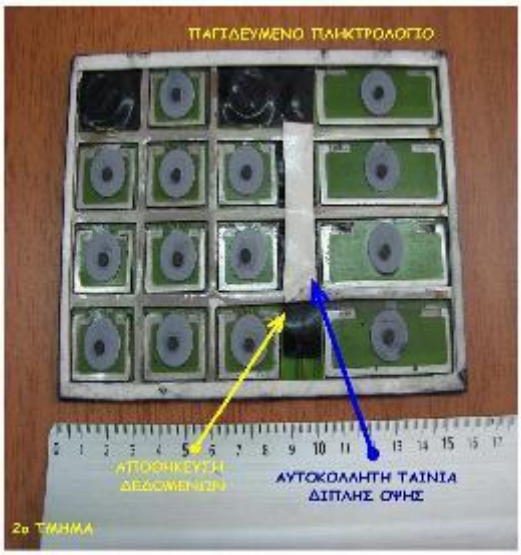

ΠΑΙΧΝΙΔΟΜΗΧΑΝΗ
ΜΕ ΚΑΜΕΡΑ
ΠΗΓΕΣ
ΕΝΕΡΓΕΙΑΣ
ΘΥΡΑ ΕΞΟΔΟΥ ΑΡΧΕΙΩΝ
ΕΣΩΤΕΡΙΚΗΣ ΜΝΗΜΗΣ - USB
2ο ΤΜΗΜΑ


ΟΜΟΙΩΜΑ ΠΡΑΣΙΝΟΥ
ΣΤΟΜΙΟΥ ΕΙΣΑΓΩΓΗΣ ΤΗΣ

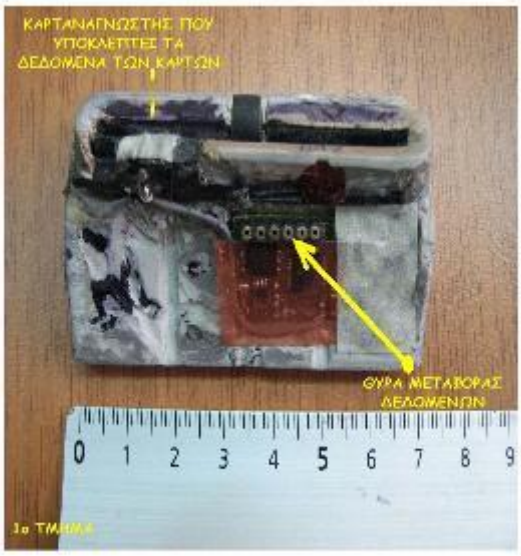

2ο ΤΜΗΜΑ
1ο ΤΜΗΜΑ


2ο ΤΜΗΜΑ
1ο ΤΜΗΜΑ


ΠΑΓΙΔΕΥΜΕΝΟ ΠΛΗΚΤΡΟΛΟΓΙΟ
2ο ΤΜΗΜΑ


ΠΑΓΙΔΕΥΜΕΝΟ ΠΛΗΚΤΡΟΛΟΓΙΟ
ΑΠΟΘΗΚΕΥΤΗ ΔΕΔΟΜΕΝΩΝ
ΑΥΤΟΚΟΛΛΗΤΗ ΤΑΙΝΙΑ ΔΙΠΛΗΣ ΟΨΗΣ
2ο ΤΜΗΜΑ


ΠΑΓΙΔΕΥΜΕΝΟ ΣΤΟΜΙΟ ΕΙΣΑΓΩΓΗΣ ΤΗΣ ΚΑΡΤΑΣ
1ο ΤΜΗΜΑ


ΚΑΡΤΑΝΑΓΝΩΣΤΗΣ ΠΟΥ
ΥΠΟΚΛΕΠΤΕΙ ΤΑ
ΔΕΔΟΜΕΝΑ ΤΩΝ ΚΑΡΤΩΝ
ΘΥΡΑ ΜΕΤΑΦΟΡΑΣ
ΔΕΔΟΜΕΝΩΝ
0 1 2 3 4 5 6 7 8 9
1ο ΤΜΗΜΑ


ΠΗΓΗ ΕΝΕΡΓΕΙΑΣ
1ο ΤΜΗΜΑ


εισοδος κάρτας / insert card
1ο ΤΜΗΜΑ


1ο ΤΜΗΜΑ


2ο ΤΜΗΜΑ


ΕΡΧΕΤΑΙ ΜΕ ΚΑΘΕ ΣΑΣ ΑΓΟΡΑ
2ο ΤΜΗΜΑ


PHOTO 1


PHOTO 2


PHOTO 4


PHOTO


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
ΟΙ ΔΥΟ ΔΡΑΣΤΕΣ
ΠΛΗΣΙΑΖΟΥΝ


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
ΤΟΠΟΘΕΤΕΙ ΤΟΝ
ΚΑΡΤΑΝΑΓΝΩΣΤΗ

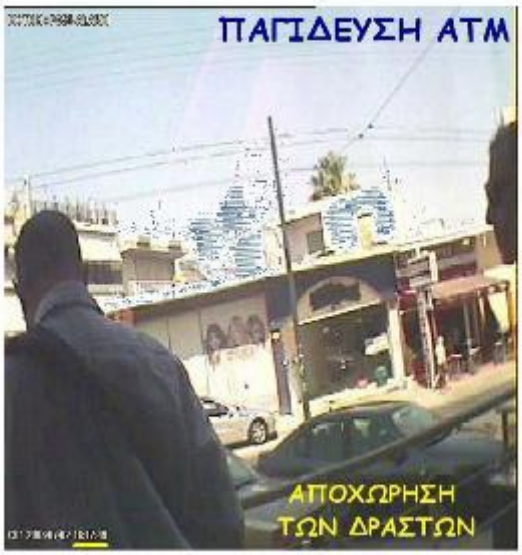

ΠΑΓΙΔΕΥΣΗ ΑΤΜ
Ο ΣΥΝΕΡΓΟΣ ΤΟΥ
ΕΛΕΓΧΕΙ ΤΟ ΧΩΡΟ


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
ΑΠΟ ΤΟ ΣΑΚΙΔΙΟ ΩΜΟΥ
ΒΓΑΖΕΙ ΤΟ 2ο ΤΜΗΜΑ


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
ΤΟ ΤΟΠΟΘΕΤΕΙ ΠΑΝΩ
ΑΠΟ ΤΟ ΠΛΗΚΤΡΟΛΟΓΙΟ


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
ΕΛΕΓΧΟΣ ΓΙΑ ΤΗ ΣΩΣΤΗ
ΕΠΙΚΟΛΛΗΣΗ ΤΟΥ
ΚΑΡΤΑΝΑΓΝΩΣΤΗ


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
Η ΠΑΓΙΔΕΥΣΗ
ΟΛΟΚΛΗΡΩΘΗΚΕ ΣΕ 1 ΛΕΠΤΟ


ΠΑΓΙΔΕΥΣΗ ΑΤΜ
ΑΠΟΧΩΡΗΣΗ
ΤΩΝ ΔΡΑΣΤΩΝ


ΑΠΕΓΚΑΤΑΣΤΑΣΗ
ΜΗΧΑΝΙΣΜΟΥ
ΠΑΓΙΔΕΥΣΗΣ
ΟΙ ΔΥΟ ΔΡΑΣΤΕΣ
ΠΛΗΣΙΑΖΟΥΝ


ΑΠΕΓΚΑΤΑΣΤΑΣΗ
ΜΗΧΑΝΙΣΜΟΥ
ΠΑΓΙΔΕΥΣΗΣ
ΑΠΟΚΟΛΛΗΣΗ
1ου ΤΜΗΜΑΤΟΣ


ΑΠΕΓΚΑΤΑΣΤΑΣΗ
ΜΗΧΑΝΙΣΜΟΥ
ΠΑΓΙΔΕΥΣΗΣ
ΑΠΟΚΟΛΛΗΣΗ
1ου ΤΜΗΜΑΤΟΣ

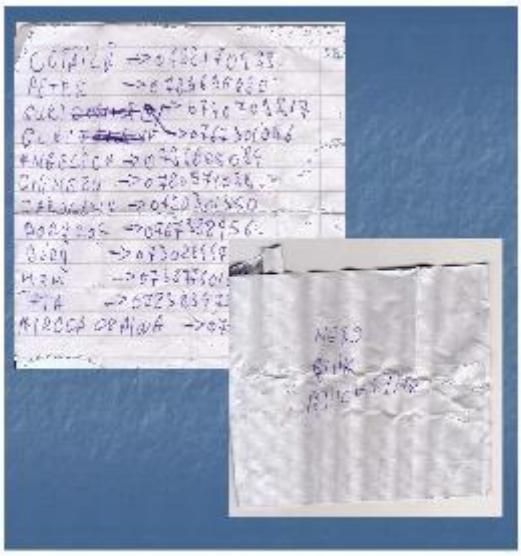

ΑΠΕΓΚΑΤΑΣΤΑΣΗ
ΜΗΧΑΝΙΣΜΟΥ
ΠΑΓΙΔΕΥΣΗΣ
ΑΠΟΚΟΛΛΗΣΗ
2ου ΤΜΗΜΑΤΟΣ


ΑΠΕΓΚΑΤΑΣΤΑΣΗ
ΜΗΧΑΝΙΣΜΟΥ
ΠΑΓΙΔΕΥΣΗΣ
ΟΛΟΚΛΗΡΩΣΑΝ
ΣΕ 21 ΔΕΥΤΕΡΟΛΕΠΤΑ

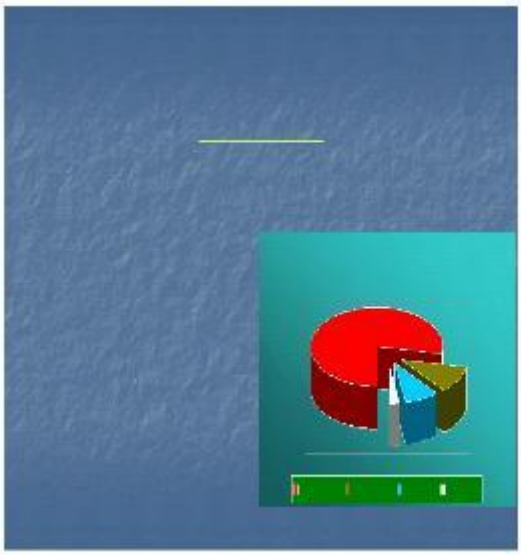

UNIVERSAL CARD
CartaCi
ΚΑΤ' ΟΙΚΟΝ ΕΡΕΥΝΑ
[redacted]
α/α 22 26


ΚΑΤ' ΟΙΚΟΝ ΕΡΕΥΝΑ
[redacted]
α/α 22-26


ΚΑΤ' ΟΙΚΟΝ ΕΡΕΥΝΑ
[redacted]
α/α 22-26




easyJet
IBERIA
IBERIA



ΒΙΒΛΙΟΓΡΑΦΙΑ

http://fusmoker.blogspot.com/2007/05/part-no1-internet.html

http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-DomainNames-Introduction.html

http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html

http://www.cnc.uom.gr/services/WEB_DECEPTION.pdf

http://homoecumenicus.com/greek_copyright_law.htm

http://homoecumenicus.com/copyright_law7.htm

http://library.panteion.gr:8080/dspace/bitstream/123456789/697/1/athanasopoulou.pdf

http://www.marinos.com.gr/bbpdf/pdfs/msg50.pdf

http://www.ictplus.gr/default.asp?pid=51&frID=3&la=1

http://62.1.43.74/8Ekdiloseis/UplFiles/synedria%20kai%20imerides%20eet/25-9-08/ragos.pdf

http://venus.cslab.aueb.gr/portal/index.php/p-categoriesmenu-99/-categoriesmenu-102/3651---------

http://www.scribd.com/doc/8029354/-Creative-Commons

http://dlib.ionio.gr/ctheses/0304tab475/Katsira_Copyright.doc

http://utopia.duth.gr/~kdrakato/thesis/chapter5.doc.

http://www.saferinternet.gr/Portals/0/docs/conference_speeches/Ioannis_Konstas.pdf.

http://www.apodimos.com/arthra/08/Mar/TO_HLEKTRONIKO_EGGLHMA_TOY_INTERNET_KAI_MORFES_TOY/index.htm

http://www.astinomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=111&lang=

http://www.diaplous.org/library/nomothesia.php

http://www.elesme.gr/elesmegr/periodika/t19/t19_03.htm

http://www.diaplous.org/library

http://www.theartofcrime.gr/

http://dspace.lib.uom.gr/bitstream/2159/3769/1/TheodwridisM

sc2008.pdf

http://www.eett.gr/opencms/export/sites/default/EETT/Electronic_Communications/DomainNames/PAROYSIASH.ppt.

http://www.domaintalk.gr/uploads/documents/Sxediagramma.pdf

http://www.itsecurity.gr/spam.html

www.lawnet.gr

www.asxetos.gr

www.ictplus.gr

www.go-online.gr

www.ipodcrates.com/archives/500

www.circe.de/content/view/23/258/lang.gr

www.opi.gr

www.aepi.gr

http://utopia.duth.gr

www.diaplus.org

www.eett.gr