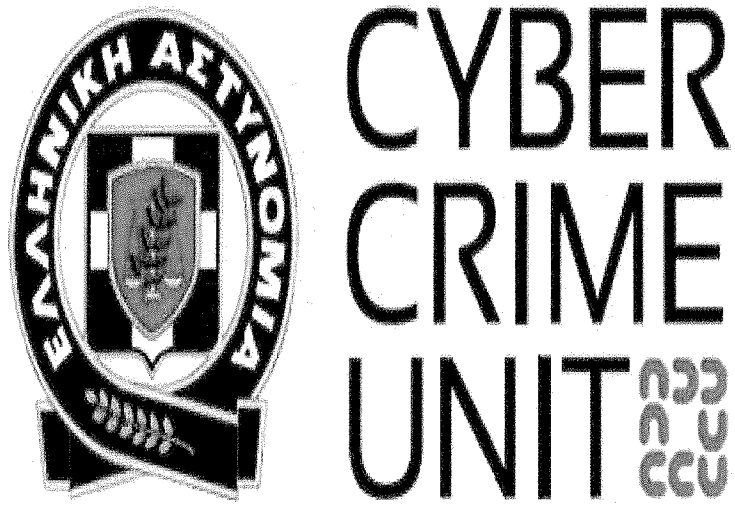
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΡΕΒΕΖΗΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗ



ΘΕΜΑ: ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ, ΕΚΤΑΣΗ ΤΟΥ ΠΡΟΒΛΗΜΑΤΟΣ, ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΝΟΜΟΘΕΣΙΑ.

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΡΙΑ: ΠΑΡΑΣΚΕΥΗ ΠΑΠΠΑ

ΣΠΟΥΔΑΣΤΕΣ: ΤΙΚΟΥ ΦΩΤΕΙΝΗ: Α.Μ.12475

ΓΕΙΤΟΝΑ ΒΑΣΙΛΙΚΗ: Α.Μ.11353

ΜΑΙΟΣ 2014

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά , θα θέλαμε να ευχαριστήσουμε την Κ. Παρασκευή Παππά , για τη συνεργασία της και τις συμβουλές της καθ' όλη τη διάρκεια της πτυχιακής μας.

Επίσης , να πούμε ένα μεγάλο ευχαριστώ στον Κ. Αριστείδη Αναγνωστάκη για τη βοήθεια του.

Τέλος , ευχαριστούμε πάρα πολύ τις οικογένειές μας για την υποστήριξή τους όλων αυτών των ετών .

KEYWORDS

Cybercrime, hacker, internet, crime, addiction, prevention, safety, electronic crime, phrasing, fishing

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το πρόβλημα των ηλεκτρονικών εγκλημάτων[1] εμφανίστηκε στη δεκαετία του 1970 στις τεχνολογικά ανεπτυγμένες χώρες και λίγο αργότερα αναπτύχθηκε στις ανεπτυγμένες και στις αναπτυσσόμενες χώρες. Σήμερα τα ηλεκτρονικά εγκλήματα αυξάνονται συνεχώς. Οι ηλεκτρονικοί υπολογιστές στις νέες μορφές εγκληματικότητας μπορούν:

- Να χρησιμοποιηθούν οι ίδιοι για να γίνει μια εγκληματική πράξη
- Να καταστούν οι ίδιοι το προσβαλλόμενο αντικείμενο της εγκληματικής πράξης
- Το αντικείμενό τους να τύχει εγκληματικής προσβολής

Με την εφαρμογή της πληροφορικής έπρεπε να θεσμοθετηθούν νόμοι ως προς τη νομική λειτουργία των υπολογιστών και του διαδικτύου. Οι νομικοί αυτοί κανόνες, οι δικαστικές αποφάσεις , που σχετίζονται με υποθέσεις σχετικά με την προβατική συμπεριφορά στον τομέα της πληροφορικής και η ανάλογη θεωρία που αναπτύσσεται αποτελούν ένα νέο είδος δικαίου. Το δίκαιο της πληροφορικής .

Ένα βασικό πρόβλημα που υπάρχει στο δίκαιο πληροφορικής είναι η προστασία της πνευματικής ιδιοκτησίας των προϊόντων λογισμικού, των δημιουργών καθώς και η παράνομη χρήση και αντιγραφή λογισμικού. Στα περισσότερα κράτη υπάρχουν αρμόδιοι φορείς που απονέμουν διπλώματα ευρεσιτεχνίας στους παραγωγούς, ενώ έχουν θεσπίσει διατάξεις για την προστασία πνευματικής ιδιοκτησίας . Οι διατάξεις για την κυκλοφορία προϊόντων της πληροφορικής υπάγονται στο «ενοχικό δίκαιο» όπου καλύπτουν δύο βασικές κατηγορίες συμβάσεων:

1. Τη σύμβαση πώλησης ,εγκατάστασης και συντήρησης υλικού
2. Τη σύμβαση προμήθειας άδειας χρήσης και τεχνικής υποστήριξης

Τη δεκαετία του 1980 το ηλεκτρονικό έγκλημα μεταδόθηκε με μεγαλύτερη ταχύτητα με αποτέλεσμα να αρχίσουν οι νομικές και οι εγκληματολογικές προσεγγίσεις προς τη νέα μορφή εγκληματικότητας . Ο όρος «computer crime» δηλώνει την παράνομη κατοχή δεδομένων που είναι αποθηκευμένα στον υπολογιστή. Για τη νομική κάλυψη του ηλεκτρονικού εγκλήματος δόθηκα αρκετοί ορισμοί για το τι είναι έγκλημα. Ο Parker (1976) διακρίνει τρεις τύπους ηλεκτρονικού εγκλήματος

1. Την κατάχρηση υπολογιστών (computer abuse)
2. Το έγκλημα διά μέσω υπολογιστών (computer crime)
3. Το έγκλημα σχετιζόμενο με τους υπολογιστές (computer related crime)

[1] Πτυχιακή Στούρη Βασιλική <<έγκλημα στο διαδίκτυο>> διπλωματική εργασία

Οι κυριότεροι λόγοι της εγκληματολογικής συμπεριφοράς[2] θεωρούνται ότι είναι οι εξής :

- Η ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου (e-commerce)
- Η ευκολία των συναλλαγών μέσου πλαστού χρήματα
- Η ευκολία τραπεζικών και συναλλαγματικών πράξεων από απόσταση
- Η ευκολία παρουσίας νέων προϊόντων, χωρίς τη δοκιμή του για τον αποκλεισμό ή τη μείωση λάθους.
- Η παγκοσμιοποίηση της επικοινωνίας και της πληροφορίας
- Διάπραξη εγκλήματος από απόσταση χωρίς να εκτίθεται σε κίνδυνο ο δράστης
- Η δυσχέρεια των αστυνομικών για να ανακαλύψουν ή να αποκαλύψουν κάποιο έγκλημα
- Η απειρία των αρχών σε νέες μορφές εγκληματικότητας
- Το ανύπαρκτο εγκληματικό πλαίσιο

Ο Lasik (1991) διατυπώνει τρία διαφορετικά προβλήματα που σχετίζονται με τα ηλεκτρονικά εγκλήματα :

1. Στο πρώτο πρόβλημα αν πραγματικά υπάρχει το ηλεκτρονικό έγκλημα , θεωρώντας ως εξωπραγματική τη θέση ότι «το ηλεκτρονικό έγκλημα είναι πλάσμα της φαντασίας»
2. Το δεύτερο πρόβλημα αναφέρεται στο ποινικό δίκαιο αν δηλαδή μπορεί να θέσει το ηλεκτρονικό έγκλημα κάτω από κοινωνικό έλεγχο, πράγμα αδύνατο λόγω της δημιουργίας νέων κοινωνικών συνθηκών.
3. Το τρίτο πρόβλημα αναφέρεται στο εύρος του ηλεκτρονικού εγκλήματος και στο τι είναι λογικό και αναγκαίο να περιλαμβάνεται στο εύρος αυτό.

Το 1986 ο ΟΡΓΑΝΙΣΜΟΣ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΑΝΑΠΤΥΞΗΣ (ΟΟΣΑ) ανέθεσε σε μια ομάδα ειδικών να μελετήσει τις νέες εκφάνσεις του ηλεκτρονικού εγκλήματος, να επεξεργαστεί τα δεδομένα και τα καθορίσει την υπόσταση του προβλήματος. Η συγκεκριμένη μελέτη αναφέρει «το ηλεκτρονικό έγκλημα ως κάθε παράνομη , ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή την μετάδοση δεδομένων» Ο ορισμός αυτός υπερέχει των προϋπαρχόντων.

ΣΚΟΠΟΣ ΕΡΓΑΣΙΑΣ

Η εργασία έχει σκοπό τη μελέτη των ηλεκτρονικών εγκλημάτων . Πως δηλαδή εκδηλώνονται και πως αντιμετωπίζονται σε νομικό και τεχνικό επίπεδο.

[2] Πτυχιακή Στούρη Βασιλική <<έγκλημα στο διαδίκτυο>> διπλωματική εργασία

Επίσης , παρουσιάζονται διάφορες μορφές ηλεκτρονικών εγκλημάτων σε όλο τον κόσμο , κάποια πρόσφατα παραδείγματα , οι αντιμετώπισής τους από τις αρχές και τεχνικά μέτρα τα οποία λαμβάνονται.

Τέλος παρουσιάζονται κάποιες πρακτικές οι οποίες θα πρέπει να εφαρμόζονται από όλους για αποφυγή παραπλανήσεων.

ΚΕΦΑΛΑΙΟ 1

1.1 Τι είναι το διαδίκτυο

Το διαδίκτυο είναι[3] ένα παγκόσμιο δημόσιο δίκτυο υπολογιστών στο οποίο οι άνθρωποι μπορούν να προσχωρήσουν και να χρησιμοποιήσουν στις πολλαπλάσιες υπηρεσίες όπως η διανομή των πληροφορούντο World Wide Web (www) είναι μια από τις σημαντικότερες υπηρεσίες του Διαδικτύου οπού υπάρχουν πληροφορίες σχεδόν για οτιδήποτε επιθυμήσουν να ψάξουν στις μηχανές αναζήτησης μηχανές αναζήτησης χρησιμοποιούνται για να κοιτάξουν γρήγορα μέσω των διαθέσιμων πηγών πληροφορίας ενώ μπορεί να κάνει την ανακάλυψη αυτών των πληροφοριών ένα εύχρηστο παιχνίδι Επιπλέον το Διαδίκτυο προσφέρει υπηρεσίες επικοινωνίας οπού οι άνθρωποι μπορούν να χρησιμοποιήσουν για να έρθουν σε επαφή με τους φίλους και την οικογένεια που μπορεί να ζουν σε μια διαφορετική χωρά. Τέτοιες υπηρεσίες επικοινωνίας περιλαμβάνουν MSN,Skype και το yahoo. Τέλος το Διαδίκτυο, μπορεί να προσφέρει υπηρεσίες για κατέβασμα στον υπολογιστική μετάβαση στον υπολογιστή μπορεί να περιλαμβάνει μουσική, κινηματογράφο και άλλα προγράμματα.

Η υπηρεσία Web(παγκόσμιος ιστός) είναι[4] ένα παγκόσμιο σύστημα παροχής πληροφοριών, το οποίο λειτουργεί στο Internet και έχει τα παρακάτω χαρακτηριστικά:

- Στηρίζεται στην εφαρμογή της τεχνολογίας υπερκειμένου(Hypertext). Το υποκείμενο επιτρέπει την ανάγνωση πληροφοριών οργανωμένων σε σελίδες με μη γραμμικό τρόπο, όπως η ανάγνωση των βιβλίων.
- Η ύπαρξη ειδικών σημείων, των συνδέσμων(Hyperlinks), ενσωματωμένων στις
- πληροφορίες που περιέχει ένα υπερκείμενο, επιτρέπει τη μη σειριακή μετάβαση
- από ένα σημείο σε άλλο και από μία σελίδα σε άλλη. Τυπικό παράδειγμα
- εφαρμογής του υπερκειμένου είναι τα συστήματα on line βοήθειας(help), που
- υπάρχουν σε όλες τις εφαρμογές των Microsoft Windows.

- Η υπηρεσία Web στηρίζεται σε γραφικό περιβάλλον και υποστηρίζει και άλλες μορφές πληροφορίας εκτός από το απλό κείμενο, όπως γραφικά, ήχο, βίντεο.
- Επίσης, ενσωματώνει εφαρμογές πολυμέσων.

- Η υπηρεσία Web προσπελαύνεται ανεξάρτητα από τον τύπο του υπολογιστή που χρησιμοποιείται. Η πρόσβαση επιτυγχάνεται μέσω μίας εφαρμογής, η οποία αποκαλείται πλοηγός(Browser).Η εφαρμογή αυτή υπάρχει σε εκδόσεις για όλους τους τύπους υπολογιστών.

- Οι πληροφορίες που παρέχει η υπηρεσία Web είναι κατανεμημένες σε χιλιάδες εγκαταστάσεις (Η/Υ) σε ολόκληρο τον κόσμο. Κάθε εγκατάσταση και κάθε σελίδα πληροφοριών που αυτή περιέχει αναγνωρίζεται από μία μοναδική διεύθυνση. Η διεύθυνση αυτή ονομάζεται διεύθυνση ομοιόμορφου εντοπισμού πόρων (Uniform Resource Locator ή URL).

- Η υπηρεσία Web είναι δυναμική. Οι πληροφορίες που δημοσιεύονται είναι δυνατόν να ενημερώνονται ανά πάσα στιγμή από τους ανθρώπους που τις δημοσίευσαν.

- Η υπηρεσία Web είναι διαλογική. Ο χρήστης <<συνομιλεί>> με τον Web Server όταν επιλέγει, μέσω ενός συνδέσμου, μία σελίδα ή μία άλλη εγκατάσταση. Επίσης, πολλές σελίδες περιέχουν διαλογικές φόρμες, που συμπληρώνονται με στοιχεία από τους αναγνώστες και αποστέλλονται στον Web Server, από όπου προήλθαν.

1.2 Θετικά από τη χρήση του διαδικτύου

Η χρήση Διαδικτύου προσφέρει[5] ποικίλα οφέλη στον καθένα που είναι πρόθυμος να το χρησιμοποιήσει τεράστιο ποσό διαθέσιμης πληροφορίας και οι πολλές χρήσεις που κάποιος μπορεί να έχει μέσω του Διαδικτύου το έχουν κάνει το πολυτιμότερο εργαλείο στις διάφορες θέσεις της ζωής ενός ατόμου. Το Διαδίκτυο έχει ένα τεράστιο ποσοστό δημοσιεύσεων που προστίθενται καθημερινά και εξελίσσεται ως η ισχυρότερη πηγή πληροφορίας Επίσης η χρήση του Διαδικτύου έχει κάνει τις εργασίες ευκολότερες και απλές, στόχοι που θα έπαιρναν ένα τεράστιο χρονικό διάστημα πριν ενώ τώρα θέλουν μόνο μερικά λεπτά. Επιπλέον το Διαδίκτυο έχει γίνει ένα μεγάλο εργαλείο για τις τράπεζες, που προσφέρουν την πιθανότητα να κάνουν συναλλαγές γρήγορα και ακίνδυνα. Προσφέρουν επίσης, μία ισχυρή πηγή για αγορές και ευκολία να παραδώσει τα προϊόντα σας κατευθείαν στο σπίτι σας. Επιπλέον η διαδεδομένη χρήση του Διαδικτύου έχει ανοίξει νέους τομείς εργασιών σε όλες τις χώρες και έχει επεκτείνει τις διαθεσιμότητες εργασίας από το σπίτι. Τέλος Διαδίκτυο είναι ένα από τα πολυτιμότερα εργαλεία στην εκπαίδευση δεδομένου ότι παρέχει ένα τεράστιο ποσό πληροφοριών και είναι μια μέγιστη πηγή αναφοράς για τους εκπαιδευτικούς και τους σπουδαστές. Οι ηλεκτρονικές βιβλιοθήκες είναι εξαιρετικά σημαντικές για τους φοιτητές πανεπιστημίου και των ΤΕΙ που ψάχνουν επιστημονικές πληροφορίες για τις σειρές μαθημάτων τους.
Ένα άλλο σημαντικό όφελος του Διαδικτύου είναι η δυνατότητά του να ελαχιστοποιεί τις αποστάσεις και να παρέχει τις υπηρεσίες επικοινωνίας αποτελεσματικά και χωρίς οποιοδήποτε κόστος.
Γενικά το Διαδίκτυο είναι ένα πολύ-εργαλείο με εφαρμογές σε κάθε πτυχή της ζωής κάποιου.

[3]http://www.cyberethics.info

[4]http://www.kathimerini.gr

[5]www.cyberethics.info

1.2.1 Έρευνα: Οι ελληνικές επιχειρήσεις λένε <<ναι>> στο Διαδίκτυο

Η πρόσβαση των ελληνικών επιχειρήσεων στο Διαδίκτυο έχει πλέον φθάσει[6] στο 91%, μία στις τέσσερις χρησιμοποιεί πια το Facebook και τα άλλα κοινωνικά δίκτυα για την προβολή τους ενώ ένα ανάλογο ποσοστό (24%) παρέχουν στο προσωπικό τους εταιρικές φορητές συσκευές (<<έξυπνο>> κινητό, τάμπλετ, λάπτοπ κ.α),σύμφωνα με νέα έρευνα του Παρατηρητηρίου της Κοινωνίας της Πληροφορικής ΑΕ. Η μελέτη που διεξήχθη στο πρώτο τρίμηνο του 2013,διαπίστωσε ότι οι επιχειρήσεις στην Ελλάδα θεωρούν απαραίτητη τόσο τη χρήση όσο και την παρουσία τους στο Διαδίκτυο.

Σε αυτό το πλαίσιο παρατηρείται επίσης μια σημαντική διεύρυνση της χρήσης του Διαδικτύου στις συναλλαγές των εγχώριων επιχειρήσεων με το Δημόσιο(επτά στις δέκα υποβάλλουν ηλεκτρονικά τις εργοδοτικές εισφορές και τις δηλώσεις ΦΠΑ), ενώ παράλληλα η προώθηση των επιχειρήσεων μέσα από τα κοινωνικά δίκτυα είναι σε συνεχή ανοδική πορεία. Επιπλέον, από την ερεύνα προκύπτει ότι υπάρχει σημαντική ανάπτυξη του ηλεκτρονικού εμπορίου στην Ελλάδα, καθώς και ότι πληθώρα επιχειρήσεων συνεχίζουν να επενδύουν σε νέες τεχνολογίες ,παρά την κρίση.

Έξι στις δέκα εταιρίες ανεξαρτήτως μεγέθους(ποσοστό 61%) στην αρχή του 2013 είχε δική της ιστοσελίδα, προβάλλοντας τα προϊόντα και τις υπηρεσίες τους, ποσοστό το οποίο αγγίζει 78% για τις επιχειρήσεις που απασχολούν πάνω από δέκα άτομα, ενώ μία στις δύο μικρότερες εταιρίες(ποσοστό 52,4%) έχει πια την ιστοσελίδα της.

Τον Ιανουάριο του 2013, το 96,5% των ελληνικών εταιριών με πάνω από δέκα εργαζόμενους είχαν πρόσβαση στο Ιντερνέτ, ενώ το αντίστοιχο ποσοστό για τις εταιρίες με λιγότερα από δέκα άτομα ήταν 88,1%(από όπου προκύπτει μέσο ποσοστό 90,9% στο σύνολο της χώρας). Το 3,7% των εταιριών είχαν εταιρικό ιστολόγιο (Blog).

Το 37,8% των μεγαλύτερων εταιριών(με περισσότερους από 10 υπαλλήλους) παρέχει για εταιρικούς σκοπούς φορητές συσκευές στο προσωπικό, ενώ το ποσοστό αυτό πέφτει στο 17% για τις μικρότερες επιχειρήσεις(με λιγότερους από 10 υπαλλήλους),από όπου προκύπτει μέσο ποσοστό 24% για το σύνολο της χώρας.

Όσον αφορά το ηλεκτρονικό εμπόριο, το 2012 το 6,1% των επιχειρήσεων δέχτηκαν online παραγγελίες που αντιπροσώπευαν το 7,5% του συνολικού τζίρου τους. Το μεγαλύτερο ποσοστό(σχεδόν 40%)αφορούσε τον κλάδο ξενοδοχείων-εστίασης. Από την άλλη, οι ελληνικές επιχειρήσεις έκαναν οι ίδιες ηλεκτρονικές παραγγελίες σε ποσοστό 12,5%, οι περισσότερες από τον κλάδο <<επιστημονικών, επαγγελματικών και τεχνικών δραστηριοτήτων>> (σχεδόν το 24%).

Οι ελληνικές εταιρίες, σύμφωνα με τη μελέτη, υστερούν σε σχέση με τις άλλες ευρωπαϊκές όσον αφορά την ηλεκτρονική μάθηση/εκπαίδευση(eLearning), προτιμώντας ακόμα τις πιο παραδοσιακές μεθόδους <<πρόσωπο με πρόσωπο>>. Μόνο το 8% των εταιριών καταφεύγει στο Διαδίκτυο για την κατάρτιση του προσωπικού του, οι περισσότερες (ποσοστό 37,5%) από τον χρηματοπιστωτικό και ασφαλιστικό κλάδο.

[6]http://icteval.ktpae.gr/

Όσον αφορά τις επενδύσεις σε νέες τεχνολογίες στην Ελλάδα, ο κλάδος <<ενημέρωσης-επικοινωνίαςς>> ξεχωρίζει (με ποσοστό 65%). Γενικότερα, περισσότερες από μία στις τρεις εταιρίες οποιουδήποτε κλάδου(σχεδόν το 37%) επένδυσαν πέρυσι σε νέες τεχνολογίες.

Εξάλλου, σχεδόν μία στις πέντε εγχώριες εταιρίες (το 19%) ανέφεραν ότι αντιμετώπισαν προβλήματα ασφάλειας με τη χρήση του Διαδικτύου, γι' αυτό λαμβάνουν τα κατάλληλα μέτρα προστασίας.

1.2.2 στατιστικά στοιχεία του διαδικτύου στην Ελλάδα

Σωρεία καταγγελιών για παράνομο περιεχόμενο ή δραστηριότητα στο ιντερνέτ[7] υπέβαλλαν οι Έλληνες καταναλωτές και το 2014, με την πλειοψηφία τους να αφορά την παραβίαση προσωπικών δεδομένων, καθώς και οικονομικές απάτες μέσω Διαδικτύου. Ο συνολικός αριθμός καταγγελιών που υποβλήθηκαν στην Ελληνική Ανοιχτή Γραμμή Safe Line στη διάρκεια του 2014, διαμορφώθηκε σε 3.435, ενώ το 2013 οι αναφορές είχαν ανέλθει 3.904.

Παρά το γεγονός ότι ο συνολικός αριθμός παρουσιάζει μικρές διακυμάνσεις από έτος σε έτος, οι καταγγελίες των χρηστών γίνονται, πλέον πιο ποιοτικά στοχευόμενες από παρελθόντα έτη.

Το 35% του συνόλου έφτασαν οι καταγγελίες για παραβίαση προσωπικών δεδομένων σύμφωνα με τα στοιχεία που δημοσιοποίησε η Safe Line η κατηγορία που διακρίνεται από το μεγάλο αριθμό καταγγελιών που την αφορά είναι αυτή της παραβίασης Προσωπικών Δεδομένων με ποσοστό 35% (από 34% το 2013).

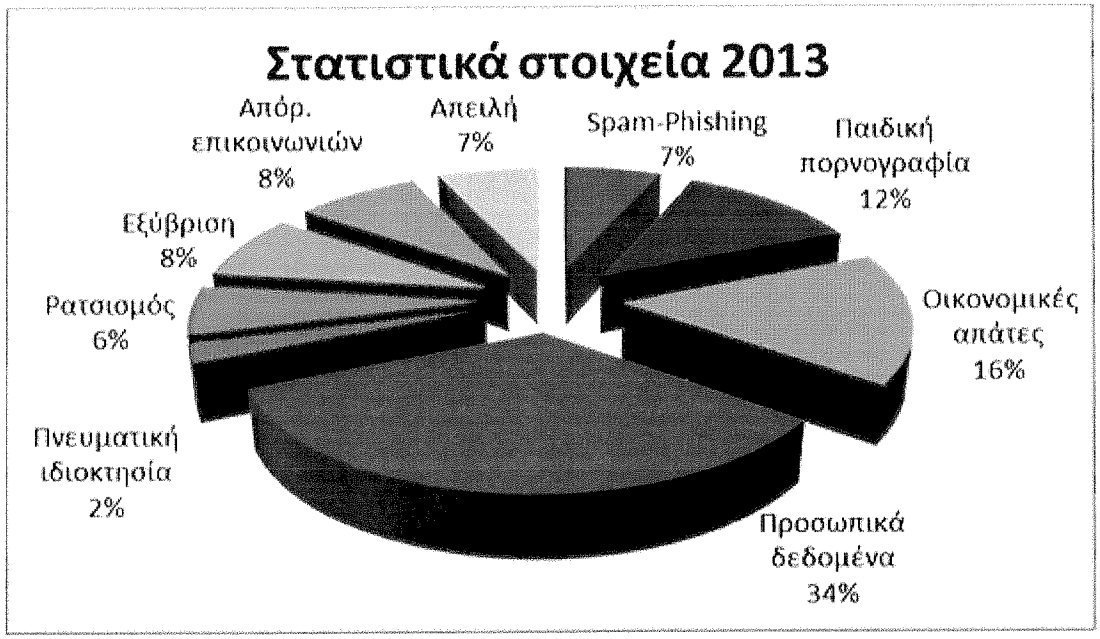
Εντυπωσιακό χαρακτηρίζει η Safe Line το εύρημα ότι η κατηγορία της παιδικής πορνογραφίας, με 20% από 12% το 2013, καταλαμβάνει το δεύτερο μεγαλύτερο ποσοστό καταγγελιών το 2014.Για πρώτη φορά φέτος το ποσοστό αυτό έφτασε στο 20%, οκτώ ποσοστιαίες μονάδες αυξημένο συγκριτικά με το περσινό έτος. Στην τρίτη θέση των ζητημάτων που αφορούν το Διαδίκτυο και συγκέντρωσαν τις περισσότερες καταγγελίες στην Ελλάδα το 2014,βρίσκονται οι οικονομικές απάτες με ποσοστό 18% (έναντι 16% ένα χρόνο νωρίτερα).

Επιπλέον σύμφωνα με τα στατιστικά δεδομένα της Ανοιχτής Γραμμής Safe Line, το 7% των αναφορών που έλαβε, το 2014, αφορούσαν σε απειλές, που έλαβαν χώρο στο Διαδίκτυο.

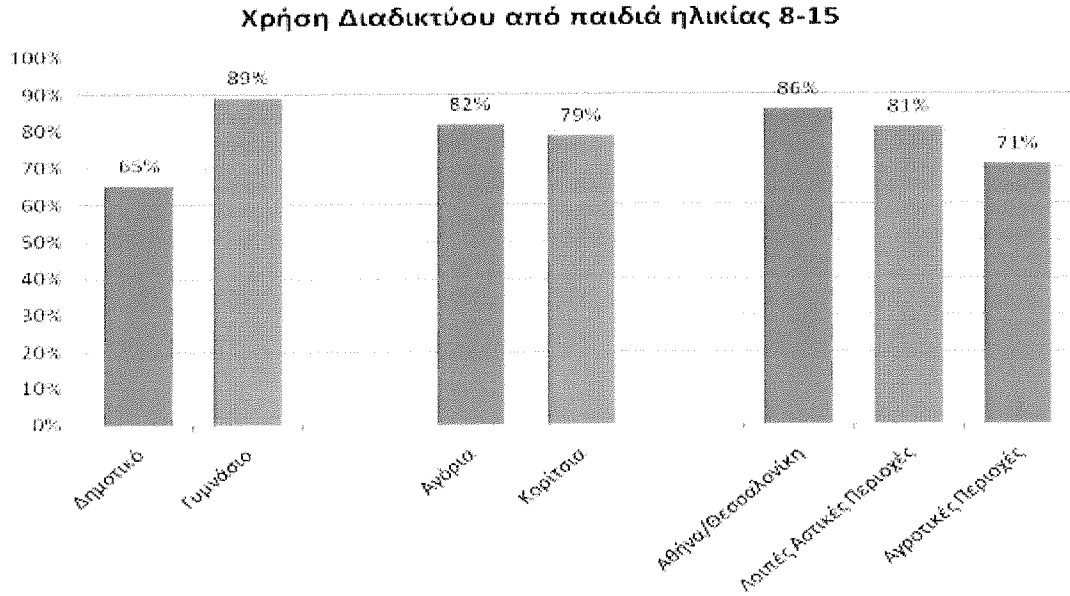
Εγκλήματα, όπως ο ρατσισμός ,η εξύβριση ή η συκοφαντική δυσφήμιση ή παραβίαση του απορρήτου των επικοινωνιών και η παραβίαση πνευματικής ιδιοκτησίας ακολουθούν με χαμηλότερα ποσοστά.

[7]http://www.kathimerini.gr

(Πηγή:Safe line)
Στατιστικά στοιχεία Διαδικτύου 2013, σχήμα 1.2.2 , εικόνα 1



Χρήση διαδικτύου παιδιών , σχήμα 1.2.2, εικόνα 2



[8]http://www.polispress.gr/plithora-katangelion-stin-ellada-gia-paranomoperiechomeno-i-drastiriotita-sto-diadiktio-to-2014/ σχήμα 1.2.2, εικόνα 1

[9]http://techblog.gr/wp-content/uploads/2009/10/kpt-internet-8-12.j,σχήμα 1.2.2, εικόνα 2

1.3 Ηλεκτρονικό ταχυδρομείο

Ακόμη ένας άλλος τρόπος επικοινωνίας είναι[10] το ηλεκτρονικό ταχυδρομείο(E-m, ail):
Τα ηλεκτρονικά ταχυδρομεία είναι μια άλλη μορφή επικοινωνίας που σήμερα έχει αντικαταστήσει την παραδοσιακή και χειρόγραφη πιστολέτα ηλεκτρονικά ταχυδρομεία είναι επιστολές που μπορούν να σταλούν μέσω Διαδικτύου και μπορούν να φτάσουν σχεδόν αμέσως και χωρίς κόστος ηλεκτρονικά ταχυδρομεία είναι ένα βασικό μέρος κάθε επιχείρησης και κάθε πρόσωπο που πρέπει να επικοινωνήσει με ανθρώπους που ζουν μακριά.

Επίθεση στο ηλεκτρονικό ταχυδρομείο
Το πρωτόκολλο SMTP (Simple Mail Transfer Protocol) αποτελεί το TCP/IP πρωτόκολλο επικοινωνίας των MTA (Mail Transfer Agents) της υπηρεσίας του ηλεκτρονικού ταχυδρομείου. Το κυριότερο πρόγραμμα που χρησιμοποιείται και αποτελεί πηγή του προβλήματος είναι το send mail (σε Berkeley UNIX συστήματα). Πιο πρόσφατα προγράμματα με μεγαλύτερη ασφάλεια έχουν δημιουργηθεί τόσο για UNIX όσο και για Windows λειτουργικά συστήματα.
Στη κατηγορία αυτή περιέχονται προβλήματα που προκύπτουν από τη προβληματική χρήση του SMTP.

Τέτοια προβλήματα είναι το mail spoofing (απόκρυψη αποστολέα ή αλλαγή διεύθυνσης του), mail bombs (μεγάλος όγκος μηνυμάτων σε συγκεκριμένο παραλήπτη), bin mail, mail trace, mail abuse. Ένα ακόμα πρόβλημα το οποίο αναπτύσσεται όλο και περισσότερο σήμερα και μπορεί να κατηγοριοποιηθεί κάτω από τον ευρύτερο όρο mail, είναι το spamming, που είναι η παράνομη χρήση mail relays για την αποστολή μηνυμάτων ακατάλληλου ή αδιάφορου περιεχομένου σε ένα μεγάλο αριθμό χρηστών.

1.4 Τρόποι αντιμετώπισης για ιούς

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη-ορισμένοι,μάλιστα,ιοί είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την δημιουργία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιικο (antivirus).
Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος αντιικά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από τον χρήστη και παραμένουν ως διαδικασίες στη μνήμη (memory resident),ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνια προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση ,ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων αντιικά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να καθαρίσουν τυχόν μολυσμένα αρχεία που εντοπίζουν.

[10]el.wikipedia.org

1.4.1 A vast free antivirus

A vast free antivirus: Δημοφιλές λογισμικό προστασίας από ιούς[11] για την προστασία του υπολογιστή λογισμικό μπορεί να ανιχνεύσει και να αφαιρέσει ιούς, Trojans, worms, spywares και άλλα επικίνδυνα αρχεία.A vast σαρώνει το σύστημα και επιτρέπει να ενημερώνουμε τις παλαιότερες εκδόσεις του λογισμικού. Το λογισμικό παρέχει την ανωνυμία όταν είναι συνδεδεμένο σε δίκτυο και ασφαλή διαμονή στο διαδίκτυο.A vast έχει επίσης πολλές χρήσιμες λειτουργίες ,όπως η απομακρυσμένη πρόσβαση ηλεκτρονικό κατάστημα, τη δημιουργία δίσκου διάσωσης ,ανοίγοντας το πρόγραμμα περιήγησης από τις επεκτάσεις χαμηλή βαθμολογία, κτλ. Το λογισμικό έχει λειτουργικό και εύκολο στη χρήση interface.

Κύρια χαρακτηριστικά :

- Προστασία κατά των διαφόρων τύπων των απειλών
- Ικανότητα να ενημερώνεται εγκατεστημένες εφαρμογές
- Απομακρυσμένη πρόσβαση
- Λειτουργική και φιλικό προς το χρήστη interface.

ΚΕΦΑΛΑΙΟ 2

2.1 Τι είναι έγκλημα

Έγκλημα είναι κατά τον ορισμό του ποινικού κώδικα[12] μια πράξη άδικη η οποία τιμωρείτε από το νόμο ΠΚ 14. Το έγκλημα είναι η έννοια του ποινικού δικαίου. Κάποια στοιχεία της έννοιας του ορισμού που προκύπτουν είναι:

- Πράξη ή παράλειψη (ενέργεια)
- Άδικη (αντιτιθέμενη στο νόμο)
- Καταλογιστώ

Το ποινικό δίκαιο αποτελεί το σύνολο των κανόνων δικαίου που ρυθμίζουν τον τρόπο άσκησης της ποινικής εξουσίας μιας πολιτείας από θεσμοθετημένα όργανα όπως προβλέπει κάθε Σύνταγμα της κάθε χώρας.

2.2 Ηλεκτρονικό έγκλημα

Το ηλεκτρονικό έγκλημα εμφανίστηκε πρώτα στις ανεπτυγμένες χώρες το 1970 και λίγο αργότερα δεν άργησε να φτάσει και στις αναπτυσσόμενες χώρες. Έχουνε δοθεί αρκετοί ορισμοί για το ηλεκτρονικό έγκλημα. Για παράδειγμα ένας ορισμός από τους Forester και Morrison του 1994 όρισαν το Ηλεκτρονικό Έγκλημα (Computer Crime) σαν «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της».

[11] http://el.wikipedia.org,

[12]http://el.wikipedia.org

Υιοθετώντας μια τριπλή προσέγγιση (Αγέλης, 2000) που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

1. μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
2. μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
3. μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν είναι: e-Crime cybercrime, Computer-Crime internet related crime, και hitech-crime .Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου.
Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notepad κλπ

2.3 Δίωξη ηλεκτρονικού εγκλήματος

Οι πρώτες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος[13,14] , ιδρύθηκαν στις Ηνωμένες πολιτείες της Αμερικής , καθότι από εκεί ξεκίνησε το hacking στα μέσα τις δεκαετίας του 70 και αναπτύχθηκε τόσο η τεχνολογία των ηλεκτρονικών υπολογιστών όσο και το διαδίκτυο. Σήμερα στις Η.Π.Α λειτουργούν υπηρεσίες αντιμετώπισης και δίωξης του ηλεκτρονικού εγκλήματος σε κάθε πολιτεία οι οποίες έχουν τοπική αρμοδιότητα. Οι απειλές όμως που προβάλουν από το οργανωμένο ηλεκτρονικό έγκλημα , μέσω του κυβερνοχώρου, οδήγησαν στη σύστασης της US-CERT170 (united states computer emergency readiness team) μιας εθνικής υπηρεσίας που φέρνει την κύρια ευθύνη για την ασφάλεια των Η.Π.Α από επιθέσεις που μπορεί να προκύψουν από τον κυβερνοχώρο. Η US-CERT170 αποτελεί το επιχειρησιακό κομμάτι της NCSD (national cyber security division) η οποία με

τη σειρά της υπάγεται στο υπουργείου εσωτερικών. Οι κύριες αρμοδιότητες της US-CERT170 :

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

[13] Ηλεκτρονικό Έγκλημα - Ελληνική Αστυνομία www.astynomia.gr

[14] e-crimenews, www.e-crime.gr

Σε επίπεδο εξέτασης ψηφιακών τεκμηρίων[15] , το ομοσπονδιακό γραφείο ερευνών , διαθέτει το πιο σύγχρονο εργαστήριο στον κόσμο. Το εξειδικευμένο προσωπικό της computer analysis and response team εξοπλισμένο με τα απαιτούμενα εργαλεία υλικού και λογισμικού , εξετάζει πάση φύσεως ψηφιακά δεδομένα και υπολογιστικά συστήματα έχοντας τη δυνατότητα για ανάκτηση και ανάλυση αρχείων σπάσιμο κωδικών , προσδιορισμό του χρόνου και σειράς δημιουργίας των αρχείων κ.α. Στην Αγγλία έχει ιδρυθεί μονάδα ηλεκτρονικού εγκλήματος στην Μητροπολιτική Αστυνομία , για την αντιμετώπιση των απειλών με ηλεκτρονικούς υπολογιστές , που οριοθετούνται από το ισχύον νομικό πλαίσιο και ειδικότερα , την computer Misuse Act 1990 . Επίσης, στον Καναδά έχει ιδρυθεί η integrated technological crime unit royal Canadian mounted police . Στην Αυστραλία έχει συσταθεί το Australian High Tech Crime Centre 176 υπαγόμενο στην ομοσπονδιακή αστυνομία. Σκοπός τους είναι ο συντονισμός των εθνικών προσπαθειών για την πάταξη ηλεκτρονικού εγκλήματος , καθότι αναγνωρίζεται ότι, η αντιμετώπισή του δυσχεραίνεται από το πλήθος εμποδίων νομικών και μη . Για το σκοπό αυτό συνεργάζεται και με άλλες υπηρεσίες στον κόσμο , με τις οποίες μπορεί από κοινού να ερευνήσουν υποθέσεις παράνομης δραστηριότητας στο διαδίκτυο και να ανταλλάξουν τεχνογνωσία.

Δίωξη ηλεκτρονικού εγκλήματος του ιντερνέτ από την καλύτερη υπηρεσία του κόσμου και μορφές ηλεκτρονικού εγκλήματος

Όλοι μας και ιδιαίτερα εκείνη που χρησιμοποιούν το ιντερνέτ γνωρίζουμε τη ραγδαία εξέλιξη της τεχνολογίας, την ανάπτυξη της πληροφορικής και την ευρύτατη χρήση του διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύλλογο των καθημερινών δραστηριοτήτων, την παραγωγική διαδικασία στις συναλλαγές, στην εκπαίδευση , στη διασκέδαση, ακόμα και στον τρόπο σκέψεις του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές οι οποίες κατά κανόνα βελτιώνουν την ποιότητα ζωής μας , υπάρχουν και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας . Οι νέες αυτές μορφές εγκληματικότητας έχουν θεσμοθετηθεί με τον όρο <<ηλεκτρονικό έγκλημα>>.

2.4 Το πρώτο καταγεγραμμένο ηλεκτρονικό έγκλημα

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα[16], χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία [1]. Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών , οι ευκαιρίες για την ανάπτυξη της ηλεκτρονικής εγκληματικότητας πολλαπλασιάζονται.

[15] e-crimenews www.e-crime.gr

[16]Κωνσταντίνα *Λιανού <<έγκλημα και διαδίκτυο>>, διπλωματική εργασία*

2.5 Γνήσια ηλεκτρονικά εγκλήματα

Τα κυριότερα και πιο διαδεδομένα εγκλήματα[17] που περιλαμβάνονται σε αυτήν την κατηγορία είναι [1]:

- Κακόβουλες εισβολές σε δίκτυα (hacking, cracking).
- Ανεπιθύμητη αλληλογραφία (spamming).
- Ηλεκτρονικό «Ψάρεμα» (phishing - harming).
- Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - Trojan horses). Piracy) .
- Απάτη με τη Νιγηριανή Επιστολή (Nigerian scam)
- Πειρατεία ονομάτων χώρου (domain names)
- Επιθέσεις Άρνησης Εξυπηρέτησης (Dos, Denial of Service).

2.5.1 Κακόβουλες εισβολές σε δίκτυα

Υπάρχουν 2 κατηγορίες κακόβουλων εισβολών σε δίκτυα, το **hacking** και το **cracking**.

Το **hacking**[18] είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα. Η έννοια του hacking είναι ευρεία.

Μπορεί να αφορά από το νομικό και έγκριτο πληροφορικό προγραμματισμό έως μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να οριστούν ως παράνομες και εγκληματικές. Η εισβολή στο δίκτυο ακόμα και αν δεν είναι κακόβουλη, θα λέγαμε ότι ενέχει κακόβουλο χαρακτήρα. Αυτό γιατί ο επιτιθέμενος ή αλλιώς hacker, εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του, εντοπίζει πιθανά αδύνατα σημεία του και έτσι μπορεί στη συνέχεια αν θέλει να διαπράξει κακόβουλη επίθεση ή ακόμα και να διαθέσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει στην επίθεση. Η δράση των hackers δεν είναι πάντα καταστροφική και συνδεδεμένη με εγκληματικές πράξεις βανδαλισμού, αλλά μια πτυχή των παραβιάσεων σχετίζεται με την ανάγκη επίδειξης των τεχνικών δυνατοτήτων τους. Όπως σε μια πραγματική μάχη, έτσι και στο ιντερνέτ το βασικότερο πράγμα πριν από μια επίθεση είναι η συλλογή πληροφοριών για τον αντίπαλο. Συνοπτικά ως χάκερ (hacker) μπορεί να ορισθεί το άτομο εκείνο το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών Γενικά υπάρχουν τρεις (3) κατηγορίες hacker:

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

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

3) **Grey hat-Hackers** : Εδώ μπαίνουμε στην γκρίζα ζώνη του ιντερνέτ. Σε αυτή την κατηγορία ανήκουν χάκερ που παραβιάζουν τον νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Μπορεί να ανακαλύψουν κενά ασφαλείας ξένων δικτύων ή προγραμμάτων και να τα σπάσουν για να αποδείξουν την αδυναμία τους. Αυτοί οι χάκερ είναι επί το πλείστο μικρής ηλικίας, ξεκινούν σε ηλικία 15 χρονών και φτάνουν στο αποκορύφωμα των γνώσεων τους ως φοιτητές. Οι ίδιοι δεν θεωρούν τον εαυτό τους εγκληματία ακόμα και αν παραβιάζουν νόμους γιατί δεν καταστρέφουν ούτε δημιουργούν ζημία στα συστήματα που εισβάλουν. Θεωρούν τον εαυτό τους ερευνητές της τεχνολογίας και σε κάποιες περιπτώσεις ενημερώνουν ακόμα και το κοινό ή τους διαχειριστές συστημάτων για τυχόν προβλήματα ασφάλειας [3].
Από την άλλη το **cracking**[19] αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, η αλλαγή των σχετικών κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους. Βασικός σκοπός είναι η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς [4].

2.5.2 Ανεπιθύμητη αλληλογραφία (spamming)

Η **ανεπιθύμητη αλληλογραφία** ή **spamming** είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο

[17] Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία,

[18]www.it.security.gr/hacker

[19]www.it.security.gr/ cracking.html. www.sch.gr/

παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα. Παρά το γεγονός ότι ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για αυτόν που το λαμβάνει. Η αλληλογραφία αυτή θα μπορούσε να χαρακτηριστεί «απρόκλητη» καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας [5].

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του spamming[21] :

• **Απρόκλητο**: Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα η οποία θα δικαιολογούσε ή θα προκαλούσε τη σχέση αυτή.

• **Εμπορικό**: Το **spamming** αφορά την αποστολή μηνυμάτων με εμπορικό σκοπό κατά κύριο λόγο, σκοπεύοντας την προβολή και διαφήμιση προϊόντων και υπηρεσιών και εν συνεχεία διεύρυνση πελατολογίου και πραγματοποίηση πωλήσεων.

• **Μαζικό**: Το **spamming** συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών.

Για να προστατευτεί ο χρήστης που λαμβάνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει, και αυτό γιατί υπάρχει πιθανότητα να εμπεριέχει απάτη ή να «μολύνει» με κακόβουλο λογισμικό τον ηλεκτρονικό υπολογιστή του. Κρίνεται σκόπιμο κάθε χρήστης να εγκαταστήσει στον Η/Υ ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων όπως επίσης να αποφεύγει να δίνει την ηλεκτρονική του διεύθυνση σε οποιονδήποτε τη ζητήσει.

[20]Κωνσταντίνα Λιανού, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία,

[21]www.it.security.gr/spamming

Για να προστατευτεί ο χρήστης :

- -Μην δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου
- -Μη δίνετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σε οργανισμούς που δεν εμπιστεύεστε τρεις κατηγορίες ηλεκτρονικού ψαρέματος, το **phishing**, το **vishing** και το **pharming**.

Στην περίπτωση του **phising** ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα email, αποστολέας του οποίου φαίνεται να είναι η τράπεζα του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρεται σε προβλήματα σε Η.Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί. Το email αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας, οποίος όμως δεν είναι πραγματικός και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα [6-7].

-Μην απαντάτε στα spam.

-Αναφέρατε κάθε μήνυμα spam που δέχεστε.

-Διαδώστε τη γνώση σας και την εμπειρία σας σχετικά με τα spam.

2.5.3 Ηλεκτρονικό «Ψάρεμα» (phising – pharming)[22]

Υπάρχουν τρεις κατηγορίες ηλεκτρονικού ψαρέματος, το **phishing**, το **vishing** και το **farming**. Στην περίπτωση του **phising** ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα email, αποστολέας του οποίου φαίνεται να είναι η τράπεζα του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρεται σε προβλήματα σε Η.Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί. Το email αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας, οποίος όμως δεν είναι πραγματικός και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα [Από την άλλη vishing είναι η προσαρμογή του ηλεκτρονικού ψαρέματος (vishing) σε αυτούς που χρησιμοποιούν το τηλέφωνο ή το Crime (Crime over IP tools). Ο χρήστης

[22] www.pharming-fishing.gr

λαμβάνει e-mail ή SMS με το οποίο του ζητείται να καλέσει έναν αριθμό χωρίς χρέωση με στόχο να επιβεβαιώσει τα στοιχεία του. Μπορεί ακόμα να λάβει ένα τηλέφωνο με μαγνητοφωνημένο μήνυμα που να του ζητά να εισάγει τα προσωπικά του στοιχεία.

Τέλος pharming είναι[23] η εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name), που επιτρέπει σε έναν hacker να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Οι δράστες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστόχωρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Οι δράστες δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν προγράμματα που στην πραγματικότητα επαναδρομολογούν την κυκλοφορία των δεδομένων. Με παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα που είναι αντίγραφο της γνήσιας. Έτσι, ο χρήστης καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα, ενώ στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Η.Υ Σε άλλες περιπτώσεις, οι δράστες αποστέλλουν μέσω e-mail προγράμματα, τα οποία μετά την εγκατάστασή τους στον υπολογιστή του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία τους ενδιαφέρουν. Κατόπιν τα χρησιμοποιούν προκαλώντας περιουσιακή ζημία στο θύμα [8].

2.5.4 Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται σε προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν

[23]Πτυχιακή Λιανού Κωνσταντίνα <<έγκλημα και διαδίκτυο>>, διπλωματική εργασία

[24]www. it security.gr 8 www.pharming-fishing.gr

(**viruses**), τα **ηλεκτρονικά σκουλήκια** (**worms**) καθώς και οι **δούρειοι ίπποι** (**Trojan horses**).[25]

προσωπικά στοιχεία. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι **ηλεκτρονικοί ιοί**

Ο **ιοί** είναι προγράμματα Η/Υ που έχουν σχεδιαστεί με σκοπό να μολύνουν άλλα προγράμματα με αντίγραφά τους [5]. Επειδή δε έχουν την δυνατότητα να αναπαράγονται συνεχώς μπορεί να μεταδοθούν από ένα σύστημα σε άλλο , με σκοπό να εκτελέσουν την αποστολή τους η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων , την διαγραφή αρχείων ή το σβήσιμο του συνόλου των σκληρών δίσκων. Ουσιαστικά ένας ιός είναι ένας βλαβερός εκτελέσιμος κώδικας , ο οποίος επιζεί με το να «κολλάει» ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα. Έχουν παρασιτική συμπεριφορά, καθώς επιζούν με το «μολύνουν άλλα αρχεία, ακολουθώντας έτσι πιστά την ανάλογη συμπεριφορά (ο τρόπος που ζουν και πολλαπλασιάζονται) των οργανικών ιών. Σήμερα ο συνηθέστερος τρόπος μετάδοσης των ιών είναι η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου (e-email). Ξεκίνησαν σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικανικών πανεπιστημίων όπως του M.I.T. ή εταιριών προϊόντων υψηλής τεχνολογίας όπως XEROX, BELL κλπ.

Σύμφωνα με τον Kyas (1997) και με βασικά κριτήρια το προσβαλλόμενο μέρος του Η/Υ καθώς επίσης και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί, έχουμε τον παρακάτω διαχωρισμό [7]:

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

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

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

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

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

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

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

Από την άλλη ένας **δούρειος ίππος** αποτελείται από δύο (2) μέρη, το server και το client . Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτόν το μέρος server. Στη συνέχεια, αφού εκτελεστεί το μέρος client στον υπολογιστή του επιτιθέμενου και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή λέγονται droppers.

Οι **δούρειοι ίπποι** επικοινωνούν με τον client μέσω διαφόρων θυρών (ports) του υπολογιστή τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας (firewall) [5]. Είναι προγράμματα που ενώ φαίνονται να λειτουργούν κανονικά παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. Έτσι ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού , αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδίκτυο.

Στις περισσότερες των περιπτώσεων, ένας **δούρειος ίππος** δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Κερκόπορτα (trapdoor) είναι ένα μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης [9].

Επίσης τα **σκουλήκια** είναι και αυτά προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για τον λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν

[25]Πτυχιακή Λιανού Κωνσταντίνα <<έγκλημα και διαδίκτυο>>, διπλωματική εργασία

κάποιο καταστρεπτικό πρόγραμμα δηλαδή έναν ιό στα διάφορα συστήματα το δικτύου αυτού. Η διαφορά τους από τους ιούς είναι ότι δεν χρειάζεται ανθρώπινη παρεμβολή για την ενεργοποίηση τους [5].

2.5.5 Πειρατεία ονομάτων χώρου (Domain crime, gr)[26,27]

Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Μέσο (εισιτήριο) για την είσοδο στο διαδίκτυο αποτελεί το «**Domain name**» (όνομα πεδίου ή όνομα χώρου), το οποίο κατ' ουσία επιτελεί ρόλο ηλεκτρονικής διευθύνσεως ή «κυβερνοδιευθύνσεως», επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως. Το «**Domain name**» αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το πρώτο μέρος είναι κοινό για όλα τα «Domain crime, » και αποτελείται από τα αρκτικόλεξα «http://www» (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο). Το δεύτερο μέρος (second level Domain – SLD) ή Μεταβλητό Πεδίο αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το κατ' εξοχήν όνομα, την κατ' εξοχήν διαδικτυακή διεύθυνση. Το τρίτο μέρος αποτελεί το επονομαζόμενο top level Domain (TLD), που δηλώνει το είδος της τοποθεσίας (ιστοθέτησες) ή τη γεωγραφική προέλευση, όπως «.com» για όσους ασκούν εμπορική δραστηριότητα, «.edu» για εκπαιδευτικούς οργανισμούς, «.org» για οργανισμούς, «.net» για παροχές υπηρεσιών διαδικτύου, «.gov» για κυβερνητικούς οργανισμούς, «.int» για διεθνείς οργανισμούς, «.gr» για τη χώρα αρχειακής καταχωρίσεως του «**Domain name**» του χρήστη, εν προκειμένω για την Ελλάδα [10]. Το «**Domain name**» δεν μπορεί κατ' αρχήν να ταυτιστεί με την εμπορική επωνυμία, τον διακριτικό τίτλο και το εμπορικό σήμα. Πρέπει, ωστόσο, να αποδίδεται σ' αυτό λειτουργία τόσο διακριτικού τίτλου όσο και σήματος, κατά έμμεσο τρόπο, όταν αυτό

[26]Πτυχιακή Λιανού Κωνσταντίνα <<έγκλημα και διαδίκτυο>> διπλωματική εργασία

[27] www.en.wikipedia.org/domain_name

χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση στο διαδίκτυο, διότι, έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία. Η ευχέρεια ελεύθερης χρήσεως οποιασδήποτε ονομασίας, όσο γνωστή και φημισμένη και αν είναι, από τον πρώτο τυχόντα, θα προκαλούσε τεράστιες ή ανεπανόρθωτες ζημίες στην επιχείρηση που καθιερώθηκε στις συναλλαγές με την επίμαχη ονομασία. Για τη διαφύλαξη έτσι των νομίμων συμφερόντων των παραπάνω επιχειρήσεων, θα πρέπει να αποδοθεί στο «**Domain name**» μια οιονεί λειτουργία διακριτικού τίτλου και σήματος. Τούτο ενισχύεται και από το ότι οι κάτοχοι «**Domain crime**» στην πράξη εμφανίζονται στο διαδίκτυο με τα διακριτικά γνωρίσματα που τους κατέστησαν γνωστούς στον υλικό κόσμο, δηλαδή χρησιμοποιούν το όνομα, την επωνυμία ή το σήμα τους, δεδομένων μάλιστα των περιορισμένων ορίων παροχής «Domain **crime,** » για κάθε χρήση αλλά και της επιβαλλόμενης συντομίας γι' αυτού του είδους την επικοινωνία. Δεδομένων όλων αυτών, το **domain name** απολαμβάνει έννομη προστασία απέναντι σε αυτούς που προσπαθούν να το ιδιοποιηθούν ασκώντας **domain name piracy**.

2.5.6 Απάτη με τη Νιγηριανή επιστολή

Η Νιγηριανή απάτη[28] είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e- email) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη [7]. Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το

[28]Πτυχιακή Λιανού Κωνσταντίνα <<έγκλημα και διαδίκτυο>>, διπλωματική εργασία

σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-email . Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Ξεκινάει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

2.5.7 Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)[29]

Οι επιθέσεις άρνησης εξυπηρέτησης (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου, για παράδειγμα ενός διακομιστεί ιστοσελίδας(web server) ή ενός διακομιστεί αρχείων(file server). Ο υπολογιστής- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου πλήθους των «ψεύτικων» αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου (κάνοντας τες σαφώς χαμηλότερες έως και μηδενικές) καθώς επίσης την ακεραιτοτήτων δεδομένων και τη γενικότερη λειτουργία του συστήματος [1]. Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι:

• Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο

• Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες.

• Υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες.

[29]Πτυχιακή Λιανού Κωνσταντίνα <<έγκλημα και διαδίκτυο>>, διπλωματική εργασία

2.6 Ρόλος ηλεκτρονικού υπολογιστή[30]

Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ,ο οποίος μπορεί:

- Να αποτελεί τον στόχο κάποιας επίθεσης.
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης.
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Αν θέλαμε να ορίσουμε το «Ηλεκτρονικό Έγκλημα» θα μπορούσαμε να πούμε ότι γενικότερα είναι κάθε παράνομη δραστηριότητα που για την διάπραξη αλλά και για την αντιμετώπισή της απαιτείται η τεχνολογική γνώση. Ο ορισμός του ηλεκτρονικού εγκλήματος έχει να κάνει με την οπτική γωνία από την οποία εξετάζεται. Αυτή η πολυμορφία του εγκλήματος είναι που δυσχεραίνει και τον νομοθέτη, ο όποιος αποφεύγει να του προσδώσει έναν ορισμό και είτε αφήνει αυτήν την αρμοδιότητα στα δικαστήρια και στην παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

Με απλά λόγια θα μπορούσαμε να πούμε ότι ως ηλεκτρονικό έγκλημα θεωρούνται οι εγκληματικές πράξεις που γίνονται με την χρήση υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης χωρίζονται σε δύο κατηγορίες. Τα εγκλήματα που τελούνται με τη χρήση υπολογιστών (computer time) και σε κυβερνοεγκλήματα (cyber crime) αν προέρχονται μέσω διαδικτύου.

2.7 Firewall και router: Απαραίτητες δικλείδες ασφαλείας.

Σε συνδυασμό με τα μέτρα πρόληψης απέναντι σε ιούς και spyware, πρέπει να τονιστεί η σημασία τόσο του Firewall,όσο και των σωστών ρυθμίσεων προστασίας του modem η router που χρησιμοποιούμε για πρόσβαση στο διαδίκτυο. Το Firewall αποτελεί το απαραίτητο τείχος προστασίας του υπολογιστή από επιτήδειους που προσπαθούν να επικοινωνήσουν με τον υπολογιστή. Η εύρεση ενός καλού αξιόπιστου Firewall δεν είναι δύσκολη υπόθεση αφού κυκλοφορούν πολλές διαφορετικές εκδόσεις που μπορούν να εξυπηρετήσουν από τον <<ανυποψίαστο>> μέχρι τον επαγγελματία χρήστη. Ταυτόχρονα, ένα από τα πρώτα πράγματα που πολλοί χρήστες συχνά αγνοούν όταν αποκτήσουν πρόσβαση στο διαδίκτυο, είναι η ρύθμιση του router που χρησιμοποιούν ώστε να προστατεύσουν το οικιακό τους δίκτυο. Ειδικά όταν χρησιμοποιείται ασύρματο router,είναι επιτακτική η ενεργοποίηση κωδικό τρόπο αυτό περιορίζεται η πρόσβαση μόνο στους υπολογιστές που κάνουν χρήση του κωδικού ,η που συνδέονται με καλώδιο εντός του σπιτιού.

Η μη χρήση κωδικού ασφαλείας του ασύρματου δικτύου εκτός του επιτρέπει την πρόσβαση σε ανεπιθύμητους υπολογιστές, κυριότερα δίνει την δυνατότητα σε κάποιον ακόμη και με στοιχειώδεις γνώσεις διεισδύσει στο διαδίκτυο μας, να αλλάξει τις ρυθμίσεις και να δημιουργήσει γενικότερα προβλήματα στην πρόσβασή μας στο internet.

[30]https://electroniccrime.wordpress.com/category

ΚΕΦΑΛΑΙΟ 3

3.1 Μορφές κυβερνοεγκλήματος [31]

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime... and Punishment?» κατατάσσει τα αδικήματα που

(κυβερνώ)κυκλοφορίας, Τροποποίηση και Κλοπή δεδομένων, Εισβολή και Σαμποτάζ διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα κατηγορίες. Παρεμπόδιση Πλαστογραφία και Απάτη.

Κύριες μορφές Κυβερνοεγκλήματος που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ

1. Απάτες μέσω Διαδικτύου

2. Παιδική πορνογραφία

3. Cracking και hacking

4. Διακίνηση-πειρατεία λογισμικού

5. Πιστωτικές κάρτες

6. Διακίνηση ναρκωτικών

7. Έγκλημα στα chat rooms

3.1.1 Απάτη στο διαδίκτυο

Αποτελεί τη ηλεκτρονική έκφανση της συμβατικής μορφής της απάτης. Μπορεί να συντελεστεί με διάφορους τρόπους και μεθόδους. Κυρίως οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά e-mail, αποστέλλοντας Νιγηριανές Επιστολές ή ενημέρωση για κέρδη στο Ισπανικό Λόττο. Επίσης πολλές απάτες πραγματοποιούνται με τη χρήση πιστωτικών καρτών. Οι χρεώσεις της πιστωτικής κάρτας των πολιτών που τις αγορές τους δεν τις έκαναν οι ίδιοι. Κάποιος κακόβουλος χρήστης δημιουργεί μια ψεύτικη ιστοσελίδα, καταφέρνοντας να συγκεντρώσει στοιχεία αθώων ανθρώπων , βάζοντάς τους να κάνουν τις αγορές τους. Σε πολλές περιπτώσει ο πολίτης δίνει μόνος του τα προσωπικά του στοιχεία, λαμβάνοντας μηνύματα από το ηλεκτρονικό ταχυδρομείο που έχει λογαριασμό και του ζητούνται τα στοιχεία του, όπως το ονοματεπώνυμο, αριθμός λογαριασμού και άλλα και έτσι γίνεται θύμα εξαπάτησης. Επίσης, η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες στο διαδίκτυο, που τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό και για να φανούν πιστικοί χρησιμοποιούν μεγάλα ονόματα εταιρειών όπως για παράδειγμα Microsoft, yahoo και άλλες. Αυτό γίνεται βέβαια για

[31] https://electroniccrime.wordpress.com

να ζητήσουν από τους υποτιθέμενους κερδισμένους χρήματα, για να μπορέσουν να πληρώσουν κάποιους φόρους ή έξοδα που μπορεί να έχουν. Τέλος, μπορεί πάλι σε τυχαία επιλογή να σταλθεί μήνυμα σε κάποιον πολίτη και να του εξηγεί ότι κάποιος κάτοικος μεγάλης περιουσίας απεβίωσε κ έχει αφήσει μια τεράστια κληρονομιά, στην οποία δεν υπάρχει κανένας κληρονόμος, αν θέλει να λάβει αυτό το χρηματικό ποσό θα πρέπει να δημιουργήσει έναν τραπεζικό λογαριασμό στο εξωτερικό.

Τρόποι αντιμετώπισης

θα πρέπει να είμαστε βέβαιοι ότι ο υπολογιστής δεν έχει προσβληθεί από κακόβουλο λογισμικό, όπως για παράδειγμα από το <<Δούρειο ίππο>> που καταγράφει τα προσωπικά δεδομένα που καταχωρείται σε φόρμες του διαδικτύου. Να ενημερωθούμε για τους τρόπους προστασίας που αφορά τέτοιου είδος λογισμικό, μπορούμε να χρησιμοποιήσουμε το antivirus από το εμπόριο.
Μπορούμε να εγκαταστήσουμε ανεπιθύμητη αλληλογραφία και αν μας στείλουν μήνυμα στα εισερχόμενα να το διαγράψουμε χωρίς να το διαβάσουμε.

Ακόμη κάποιος οργανισμός ή κάποια τράπεζα δε θα επικοινωνούσε μαζί μας μέσω ηλεκτρονικού ταχυδρομείου. Τα στοιχεία που μπορεί αν μας ζητήσουν είναι προσωπικά και θα πρέπει να είμαστε εκεί εμείς οι ίδιοι, άρα αν συμβεί κάτι τέτοιο θα πρέπει να ενημερώσουμε τον οργανισμό ή την εταιρεία.
Πριν καταχωρήσουμε στοιχεία μας σε κάποιο λογαριασμό στο διαδίκτυο, θα πρέπει να κοιτάξουμε ότι είναι η επίσημη σελίδα και ότι αρχίζει με https://. Καλύτερα να το πληκτρολογούμε εμείς.

Να μη κάνουμε κλικ με το ποντίκι σε διευθύνσεις που μας δίνονται e mails γιατί θα μας πηγαίνουν σε εικονικές ιστοσελίδες όμοιες με τις πρωτότυπες, που προσπαθούν να μας αποσπάσουν τα προσωπικά μας δεδομένα.

Να αποφεύγουμε να κάνουμε ηλεκτρονικές συναλλαγές από άλλους υπολογιστές (π.χ. ιντερνέτ καφέ) Να μην έχουμε κωδικούς με ονόματα και ημερομηνίες που μπορεί να μαντέψει κάποιος

3.1.2 Παιδική πορνογραφία

Αναφέρεται στη διακίνηση παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου[32] που μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσων. Τα παιδιά είναι αθώα και ευάλωτα και δε μπορούν να επιβιώσουν μόνα τους. Είναι περίεργα στο να μαθαίνουν καινούρια πράγματα και να εξελίσσονται. Η πορνογραφία ανηλίκων είναι μια μορφή οικονομικής εκμετάλλευσης της γενετήσιας ζωής που είναι ενάντια στην ατομική αξιοπρέπεια και την εξέλιξή του.

[32] https://electroniccrime.wordpress.com

Το **άρθρο 348 Α** του ποινικού κώδικα διώκεται ως έγκλημα πορνογραφίας[33,34] όταν αναφέρεται σε ανήλικο και επιχειρεί να προστατέψει τους ανήλικους οι οποίοι διατρέχουν κίνδυνο, από εκείνους που δε διστάζουν να εκμεταλλεύονται παιδιά προκειμένου να κερδοσκοπήσουν, χωρίς να νοιάζονται για το τι προκαλούν. Σε αυτές
τις περιπτώσεις εγκλημάτων και συγκεκριμένα σε κακουργήματα, πρέπει η διωκτική αρχή να δραστηριοποιείται με προσοχή ώστε να αποφεύγονται οι εν θερμώ (κατά)διώξεις κατά προσώπων, τα οποία κρίνονται ως ύποπτα τέλεσης των υπαγόμενων στη συγκεκριμένη διάταξη πράξεων, εξ αιτίας της μεγάλης σημασίας των συνεπειών κατά του δράστη τέλεσης των πράξεων, που υπάγονται στο πραγματικό της διάταξης αυτής.

Σχετική νομοθεσία: **Ν. 3064/2002** (για πρώτη φορά εισήχθη στον Ελληνικό Ποινικό Κώδικα το άρθρο 348Α, το οποίο μεταξύ άλλων αφορούσε στη «διακίνηση παιδικής πορνογραφίας μέσω Διαδικτύου»), **Ν. 3625/2007 και Ν. 3666/2008** ο οποίος και συμπεριέλαβε το έγκλημα του 348Α στις περιπτώσεις άρσης του απορρήτου των επικοινωνιών.Πέρα όμως από τη διακίνηση παιδικής πορνογραφίας, οι ανήλικοι χρήστες έρχονται να αντιμετωπίσουν και άλλων παράνομες πράξεις όπως είναι η προσβολή της γενετήσιας αξιοπρέπειας. Αυτού του είδους η πράξη ποινικοποιείται βάσει του 337 άρθρο του Ποινικού Κώδικα και δυστυχώς λαμβάνει χώρα καθημερινά. Σύμφωνα με όσα ορίζει η διάταξη στην παράγραφο 3 που προστέθηκε με το **Ν. 3727/2008:**

«Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα 15 έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.» **Ο νομοθέτης εδώ, με τον όρο *«ή άλλου επικοινωνιακού μέσου»*** Οι διαστάσεις ου εγκλήματος σε διεθνές και ελληνικό επίπεδο Για να γίνουν αντιληπτές οι διαστάσεις του προβλήματος , παρατίθενται μερικά στατιστικά στοιχεία

- Ο τζίρος της βιομηχανία της παιδικής πορνογραφίας στο διαδίκτυο υπερβαίνει τα τρία δισεκατομμύρια ευρώ ετησίως
- Ο αριθμός των ιστοσελίδων που φιλοξενούν πορνογραφικό περιεχόμενο με πρωταγωνιστές ανηλίκους , ακόμη και βρέφη, υπολογίζεται ότι αυξήθηκε την τελευταία δεκαετία κατά 345%
- Η ημερήσια επισκεψημότητα ορισμένων τέτοιων σελίδων είναι 150.000, ιδιαίτερα υψηλά αριθμός , δεδομένου το τεράστιου ποσού που απαιτείται για να έχει πρόσβαση κάποιος σε αυτές
- περισσότερες από μία πορνογραφικές εικόνες ανηλίκων διακινούνται στο διαδίκτυο και άλλες εικόνες ταχυδρομούνται ηλεκτρονικά ημερησίως.
- Έχει χαρακτηριστεί <<παράδοξο>> το πώς μια από τις τόσες μεγάλες επιτεύξεις του περασμένου αιώνα , το ιντερνέτ από δημοκρατικό <<forum ελεύθερης ανταλλαγής απόψεων>> κατέστη φορέας σεξουαλικής κακοποίησης παιδιών και παιδοφιλίας. Η δημιουργία του ιντερνέτ δε συνιστά

[33] http://www.saferinternet.gr

[34] www.e-crime.gr

σε καμιά περίπτωση το μόνο λόγο τη ύπαρξης του φαινομένου της παιδικής πορνογραφίας . Η πορνογραφία ανηλίκων συνιστά στις μέρες μια εγκληματική δραστηριότητα, που εντάσσετε στο πλαίσιο του οργανωμένου εγκλήματος και ειδικότερα με αυτή ασχολούνται κυκλώματα που είτε την έχουν σαν αποκλειστικό τομέα της δραστηριότητας τους είτε ασχολούνται με το human trafficking εν γένει.

Το προφίλ του δράστη της παιδικής πορνογραφία στο διαδίκτυο[35,36]

Οι προσπάθειες που έχουν σημειωθεί ως σήμερα για την αντιμετώπιση του ειδεχθούς εγκλήματος του υπό εξέταση φαινομένου είναι επίμονες. Τα κρούσματα πορνογραφίας ανηλίκων αυξάνονται με γοργούς ρυθμούς. Η τεχνολογική ανάπτυξη των τελευταίων ετών και πιο συγκεκριμένα η εισαγωγή ηλεκτρονικών υπολογιστών και του διαδικτύου στην καθημερινή ζωή, έχει συμβάλει σε αυτόν, καθώς η χρήση του διαδικτύου παρέχει την ευκαιρία για πρόσβαση στις τεράστιες ποσότητες πορνογραφικών εικόνων που διακινούνται στον πλανήτη. Επίσης καθιστά την παιδική πορνογραφία εύκολα προσβάσιμη άμεσα σε οποιαδήποτε χρόνο και τόπο , παρέχοντας ανωνυμία στους χρήστες της. Η χρήση του διαδικτύου προσφέρει ακόμη εικόνες υψηλής ποιότητας , κρατά αναλλοίωτη την ποιότητα του αναπαριστάμενου υλικού και <<παρέχει μια ποικιλία σχηματικών απεικονίσεων (εικόνων, βίντεο φωνής) , καθώς επίσης τη δυνατότητα πορνογραφικής απόλαυσης τους σε πραγματικό χρόνο και με διαντιδραστικές εμπειρίες >>. Εάν κανείς περιπλανηθεί στους διάφορους δικτυακούς τόπους του κυβερνοχώρου, ενδέχεται αν έρθει αντιμέτωπος με έναν πραγματικό <<θησαυρό>> , δεδομένου του κόστους του πορνογραφικού υλικού εν γένει . ο αριθμός του πορνογραφικού υλικού, εικόνων και βίντεο είναι ανυπολόγιστος, ενώ ανάμεσά τους υπάρχει και απέραντο υλικό για τους παιδόφιλους

Η πλειονότητα του τελευταίου απεικονίζει ανήλικους, ακόμη και βρέφη από οχτώ μηνών εώς δεκαεπτά ετών σε άσεμνες στάσεις και ερωτικές περιπτύξεις είτε μεταξύ τους είτε με ενήλικα πρόσωπα, ενώ υφίσταται υλικό ακόμη και για αρρωστημένα μυαλά.

Σύμφωνα με έρευνα που έγινε στο ινστιτούτο εγκληματολογίας στην Αυστραλία, οι δράστες του εγκλήματος της πορνογραφίας ανηλίκων στο διαδίκτυο τίθεται σε κατηγορίες ανάλογα με τα κριτήριά τους ξεκινώντας από αυτόν που δεν έχει άμεση σχέση με το ανήλικο και καταλήγοντας σε αυτούς που επιδιώκουν τη σεξουαλική συναναστροφή με αυτόν. Περιγράφονται οχτώ τύποι δραστών

1) Ο πρώτος αποτελεί άτομο που κάνει χρήση του διαδικτύου και δίχως τη θέλησή του, συναντά πορνογραφικό υλικό και παρά το γεγονός ότι δε το επιδίωξε, δέχεται να το κρατήσει.
2) Ο δεύτερος αποτελεί άτομο που φαντασιώνεται σεξουαλικά ανηλίκους, αποτυπώνει σε ψηφιακή μορφή κείμενα τις φαντασιώσεις του στον υπολογιστεί του ή κάνει προσωπική χρήση ψηφιακών φωτογραφιών, χωρίς να τις διανέμει σε άλλους .
3) Το τρίτο είναι ο << αλιευτείς>> που επιζητεί πορνογραφικό υλικό πορνογραφίας ενεργά επικοινωνώντας και με άλλους χρήστες

[35] Παιδική Πορνογραφία - ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
[36] www.pi.ac.cy/InternetSafety/sec_kindinoi_pornografia.html

4) Τον τέταρτο τον χαρακτηρίζει η ανασφάλεια και γι' αυτό τον αποκαλούν <<επισφαλή>> συλλέκτη ο οποίος κάνει χρήση πορνογραφικού υλικού το οποίο βρίσκεται σε δικτυακούς τόπους ή chat rooms όπου δεν απαιτούνται κωδικοί ασφαλείας, εγγραφές και οτιδήποτε άλλο για να αποκτήσει πρόσβαση
5) Ο επόμενο τύπος σε σχέση με τον προηγούμενο χρησιμοποιεί εχέγγυα.

3.1.3 Hacking και cracking

Hacker και cracker[37,38] είναι εκείνος που έχει πρόσβαση σε ένα δίκτυο υπολογιστών . Ο πρώτος έχει σκοπό να προκαλέσει ζημιά ή να πάρει κάποιο οικονομικό όφελος , ενώ ο δεύτερος το αντίθετο. Είναι άτομα με υψηλές γνώσεις στον τομέα τον υπολογιστών και επικοινωνιών. Ο όρος Hacking θα μπορούσαμε να πούμε ότι είναι μια τέχνη η οποία αποτελείται από εξαιρετικά άτομα. Αυτό που τους κοινή το ενδιαφέρον είναι η εσωτερικοί μηχανισμοί του συστήματος . η εμπορευματοποίηση του λογισμικού ευθύνεται άμεσα για την εμφάνιση Hacking στην εγκληματική του μορφή . Πολλοί κάνουν χρήση πληροφοριών που είναι σε ψηφιακή μορφή, έτσι κάποιος καλός χρήστης Hacker μπορεί εύκολα να έχει πρόσβαση και να πάρει οποιαδήποτε πληροφορία θέλει. Ανάμεσα στους Hacker και cracker έχει δημιουργηθεί μια κόντρα. Τους crackers τους χωρίζουμε σε τέσσερεις βασικές κατηγορίες

1) Στους εγκληματίες οι οποίοι εκμεταλλεύονται τις αδυναμίες των συστημάτων και μπορούν να μπούνε σε τραπεζικά συστήματα κάνοντας «ηλεκτρονικές ληστείες». Δε χρησιμοποιούν απλοποιημένες μεθόδους.
2) Στους ειδικοί που είναι ενημερωμένοι σε θέματα υπολογιστή, σε επικοινωνίες δεδομένων και τηλεπικοινωνίες. Μπορούν να μπούνε να σπάσουνε το σύστημα και μετά να αποσυρθούνε.
3) Στους βάνδαλους, είναι εκείνοι που μπαίνουν σε δίκτυα ή σε υπολογιστές και αφήνουν μηνύματα ή διαγράφουν αρχεία. Ξεκινούν από παιχνίδια και στο τέλος γίνονται ζημιές.
4) Στους swappers αποτελούνται από άτομα νεαρής ηλικίας, γνωρίζουν αρκετά γύρω από τους υπολογιστές. Θεωρούν τους εαυτούς τους έξυπνους και όχι κλέφτες. Χρειάζονται λιγότερα κίνητρα για να καταστρέψουν .

3.1.4 Πιστωτικές κάρτες

Μια μορφή ηλεκτρονικής απάτης, γνωστής ως "ψάρεμα" (phishing), είναι η αποστολή ψεύτικων μηνυμάτων από αποστολείς ανεπιθύμητης αλληλογραφίας, τα οποία μοιάζουν να είναι έγκυρα και ότι προέρχονται από γνωστές τοποθεσίες στο Web ή από εταιρείες που εμπιστεύονται οι παραλήπτες, όπως εταιρείες έκδοσης πιστωτικών καρτών, τράπεζες ή φιλανθρωπικούς οργανισμούς. Σκοπός των ψεύτικων μηνυμάτων είναι να ξεγελάσουν τους καταναλωτές ώστε να παρέχουν προσωπικά στοιχεία. Δυστυχώς, πολλοί ανυποψίαστοι. παραλήπτες πέφτουν θύματα αυτών των τακτικών και χωρίς τη γνώση τους παρέχουν προσωπικά στοιχεία:

[37]www.it.security.gr/ hacker.html. και www.it.security.gr/ cracking.html

[38]Πτυχιακή Στουρή Βασιλική, <<έγκλημα στο διαδίκτυο>> διπλωματική εργασία

- Αριθμός κοινωνικής ασφάλισης.
- Κωδικός πρόσβασης ή PIN.
- Αριθμός τραπεζικού λογαριασμού.
- Αριθμός κάρτας ΑΤΜ ή πιστωτικής.
- Κωδικός επαλήθευσης πιστωτικής κάρτας ή τιμή επαλήθευσης κάρτας.

Αριθμός τηλεφώνου και διεύθυνση. Οι εγκληματίες χρησιμοποιούν αυτές τις πληροφορίες [39] ποικιλοτρόπως για να επωφεληθούν οικονομικά. Συνηθισμένη πρακτική είναι η υποκλοπή ταυτότητας.

Ο εγκληματίας κλέβει τα προσωπικά σας στοιχεία, αναλαμβάνει την ταυτότητά σας και μπορεί να κάνει τα εξής:

- Να κάνει αίτηση και να βγάλει πιστωτικές κάρτες στο όνομά σας.
- Να αδειάσει τον τραπεζικό σας λογαριασμό και να χρησιμοποιήσει τις πιστωτικές σας κάρτες στο μέγιστο όριο.
- Να μεταφέρει χρήματα από το λογαριασμό όψεως στο λογαριασμό ταμιευτηρίου και να χρησιμοποιήσει αντίγραφο της κάρτα αναλήψεων για να
- βγάλει χρήματα από το λογαριασμό σας σε μηχανήματα ΑΤΜ σε όλο τον κόσμο.

Οι πιστωτικές κάρτες είναι ευρείας αποδοχής από το καταναλωτικό κοινό καθώς η χρήση τους είναι εύκολη, ασφαλής και εγγυάται γρήγορες συναλλαγές. Παρά το γεγονός ότι θεωρούνται ένα ασφαλές μέσο πληρωμών, υπάρχουν περιπτώσεις απάτης των κατόχων των πιστωτικών καρτών. Ιδιαίτερα στις ηλεκτρονικές συναλλαγές όπου ο κάτοχος της κάρτας δεν είναι παρών, οι απάτες είναι ευκολότερες καθώς ο έμπορος δεν μπορεί να ελέγξει την υπογραφή του κατόχου.

Εκτός από την κλοπή της κάρτας που είναι ο πιο απλός τρόπος απάτης, υπάρχουν αρκετές εξελιγμένες μορφές απάτης όπως:

1) κλωνοποίηση ιστότοπου
2) ιστοσελίδες με ψεύτικες υπηρεσίες
3) πρόγραμμα υπηρεσίας πιστωτικών καρτών
4) κλοπή πληροφοριακών πιστωτικών καρτών (skimming)

1) ΚΛΩΝΟΠΟΙΗΣΗ ΙΣΤΟΤΟΠΟΥ

Η μέθοδος αύτη αναφέρεται στη δημιουργία εικονικών ιστοσελίδων πραγματικών ηλεκτρονικών καταστημάτων. Ο χρήστης πιστεύοντας ότι βρίσκεται στην αυθεντική ιστοσελίδα αγοράζει προϊόντα κοινοποιώντας τα στοιχεία της κάρτας του. Η χρέωση γίνεται κανονικά αλλά η παραγγελία δεν αποστέλλεται ποτέ.

2)ΙΣΤΟΣΕΛΙΔΕΣ ΜΕ ΨΕΥΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

Οι ιστότοποι αυτοί παρέχουν δωρεάν υπηρεσίες ή προϊόντα μόνο με την παροχή

[39]Πτυχιακή Στουρή Βασιλική, <<έγκλημα στο διαδίκτυο>> διπλωματική εργασία

στοιχείων από την πιστωτική κάρτα τα οποία στη συνέχεια τα προμηθεύουν σε απατεώνες.

3)ΠΡΟΓΡΑΜΜΑΤΑ ΔΗΜΙΟΥΡΓΙΑΣ ΑΡΙΘΜΩΝ ΠΙΣΤΩΤΙΚΩΝ ΚΑΡΤΩΝ

Τα προγράμματα αυτά δημιουργούν αριθμούς πιστωτικών καρτών που χρησιμοποιούνται ήδη και είναι βασιζόμενα σε αλγόριθμους Kuhn. Οι αριθμοί που δημιουργούνται, αξιοποιούνται ανάλογα.

4)ΚΛΟΠΗ ΠΛΗΡΟΦΟΡΙΩΝ ΠΙΣΤΩΤΙΚΩΝ ΚΑΡΤΩΝ (SKIMMING)

Το skimming είναι η κλοπή πληροφοριών από τις πιστωτικές κάρτες και συμβαίνει κατά τη χρήση της σε μια νόμιμη συναλλαγή. Ο απατεώνας κλέβει τον αριθμό της πιστωτικής κάρτας είτε με φωτοτυπία της κάρτας είτε με μια ηλεκτρονική συσκευή (skimmer) που αποθηκεύει αριθμούς καρτών.

3.1.5 Πειρατεία λογισμικού

Πειρατεία λογισμικού[40] είναι η κλοπή προγραμμάτων λογισμικού με την παράνομη αντιγραφή ή πλαστογράφηση γνήσιων προϊόντων και τη διανομή πλαστών και παράνομων αναγεγραμμένων προϊόντων. Μπορεί να χαρακτηριστεί τόσο η μη συστηματική αντιγραφή προϊόντων χωρίς νόμιμη άδεια χρήσης από ιδιώτες ή επιχειρήσεις , όσο και διανομή ή μεταπώληση προϊόντων λογισμικού, χωρίς τη νόμιμη άδεια χρήσης.

<u>Δικαιώματα πνευματικής ιδιοκτησίας</u>

Πνευματική ιδιοκτησία είναι το δικαίωμα ιδιοκτησίας ιδεών , προϊόντων του πνεύματος , καθώς και ο έλεγχος της υλικής ή εικονικής παρουσίασης αυτών των ιδεών ή προϊόντων. Το λογισμικό είναι πνευματική ιδιοκτησία, όπως είναι η μουσική, οι ταινίες . Όπως οι μουσικοί, οι συγγραφείς, οι παραγωγοί λογισμικού χρησιμοποιούν τους νόμους πνευματικής ιδιοκτησίας για να προστατέψουν τη δουλειά τους και τις επενδύσεις τους σε αυτόν τον τομέα.. Η κλοπή πνευματικής ιδιοκτησίας αποτελεί φραγμό στην ανάπτυξη του κλάδου, την έρευνα και ανάπτυξη νέων προϊόντων και αποθαρρύνει νέες εταιρείες να εισέλθουν σε αυτόν.

<u>Οι αρνητικές επιπτώσεις της πειρατείας λογισμικού με τους καταναλωτές</u>

- Στα πειρατικά προϊόντα σχεδόν πάντα λείπουν βασικά κομμάτια και τα εγχειρίδια οδηγιών και ποτέ δεν έχουν εγγύηση καλής λειτουργίας , τεχνική υποστήριξη και δυνατότητα αναβάθμισης .
- Πολύ συχνά τα πειρατικά προϊόντα έχουν προσβληθεί από ιούς οι οποίοι μπορούν να βλάψουν το σκληρό δίσκο και πολλές φορές ολόκληρο το δίκτυο.
- Χρησιμοποιώντας πειρατικά προϊόντα στο χώρο της δουλειάς εκθέτετε σε κινδύνους τον εαυτό σας και την επιχείρηση που εργάζεστε.

[41] Πτυχιακή Στουρή Βασιλική, <<έγκλημα στο διαδίκτυο>> διπλωματική εργασία

επιπτώσεις της πειρατείας για τους μεταπωλητές

Η πειρατεία λογισμικού έχει άμεσες αρνητικές επιπτώσεις για τους μεταπωλητές λογισμικού - προκαλώντας απώλειες πολλών δισεκατομμυρίων κάθε χρόνο. Επιπλέον, οι περισσότερες περικοπές σε επενδύσεις και ανθρώπινο δυναμικό που προκαλούνται από την πειρατεία και τον αθέμιτο ανταγωνισμό, γίνονται κυρίως στο δίκτυο μεταπώλησης.

Σύμφωνα με τη μελέτη για το έτος 2000 της Business Software Alliance (BSA) για την πειρατεία λογισμικού, η Ελλάδα παραμένει η χώρα με το μεγαλύτερο ποσοστό πειρατείας στην δυτική Ευρώπη , έχοντας 66% πειρατείας

- απώλειες για την Ελλάδα υπολογίζονται περίπου στα $62 εκατομμύρια δολάρια για το έτος 2000.

- Η Δανία και η Μεγάλη Βρετανία είναι οι δύο χώρες με τα χαμηλότερα ποσοστά πειρατείας στην Ευρώπη, στο 26%.
- Ο μέσος όρος για την Δυτική Ευρώπη κυμαίνεται στο 34%.
- Η Ανατολική Ευρώπη είναι η περιοχή με το υψηλότερο μέσο όρο πειρατείας παγκοσμίως με ποσοστό 63%.
- Η πειρατεία στην Βόρεια Αμερική μειώθηκε κατά 6 μονάδες τα τελευταίαχρόνια (25% το 2000 από 31% το 1994).
- Το Βιετνάμ με 97% έχει το υψηλότερο ποσοστό πειρατείας παγκοσμίως.

Η νομική βάση της αίτησης ασφαλιστικών μέτρων θεμελιώνεται στα πραγματικά περιστατικά που προέκυψαν από την προαναφερθείσα διερευνητική αγορά. Το Μονομελές Πρωτοδικείο Αθηνών, κατόπιν σχετικού αιτήματος της Microsoft χορήγησε προσωρινή διαταγή με την οποία διέταξε την προσωρινή απαγόρευση της εν γένει διαθέσεως πειρατικού λογισμικού από την ανωτέρω επιχείρηση.

3.1.6 Εγκλήματα ΣΤΑ CHAT ROOMS

Οι νέες τεχνολογίες αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας εκατομμυρίων πολιτών σε όλο τον κόσμο. [41] Το ιντερνέτ έχει μπει στη ζωή μικρών και μεγάλων και αποτελεί πλέον το μέσον στο οποίο καταφεύγουν όλες οι ηλικιακές ομάδες για να ενημερωθούν, να διασκεδάσουν, να αντλήσουν ή να ανταλλάξουν πληροφορίες, να αποκτήσουν γνώσεις, να επικοινωνήσουν. Αποτελεί το σύγχρονο μέσον εκείνο που χρησιμοποιείται με τόση συχνότητα και για τόσες πολλές ώρες όσο κανένα άλλο. Το ιντερνέτ έχει σίγουρα αλλάξει τον χαρακτήρα και τον τρόπο επικοινωνίας εκατομμυρίων ανθρώπων, μηδέ εξαιρουμένων των Ελλήνων. Τα θετικά του είναι ανεκτίμητα, ωστόσο υπάρχει και η αρνητική πλευρά του, την οποία οι χρήστες πρέπει να γνωρίζουν.

Το «σερφάρισμα» στο διαδίκτυο κρύβει κινδύνους από τους οποίους ο χρήστης μπορεί να προστατευθεί, αρκεί να είναι ενημερωμένος γι' αυτούς. Η ασφαλής

[41] Πτυχιακή Στουρή Βασιλική, <<έγκλημα στο διαδίκτυο>> διπλωματική εργασία

πλοήγηση είναι ότι ο ΚΟΚ για τους οδηγούς που αν δεν τον γνωρίζουν είναι ανά πάσα στιγμή εν δυνάμει θύματα της ασφάλτου. Όσο οι χρήστες του ιντερνέτ αυξάνονται, και αυξάνονται καθημερινά, τόσο αυξάνονται και οι περιπτώσεις ηλεκτρονικών εγκλημάτων.

Το παραδοσιακό έγκλημα έχει μεταλλαχτεί και ηλεκτρονικά. Όλα σχεδόν τα αδικήματα του Ποινικού Κώδικα έχουν μεταφερθεί και στο διαδίκτυο. Απάτες, κλοπές, συκοφαντικές δυσφημήσεις, αλλά και τέλεση εγκλημάτων των οποίων η αφετηρία βρίσκεται σε κάποια ηλεκτρονική πύλη, όπως: βιασμοί, δολοφονίες, παιδοφιλία, παιδεραστία.

Η πιο ευάλωτη ηλικιακή ομάδα είναι τα παιδιά και οι έφηβοι. Αυτή η ομάδα μάλιστα, είναι και κείνη που σερφάρει περισσότερες ώρες καθημερινά. Τα chat rooms αποτελούν την κερκόπορτα του ηλεκτρονικού εγκλήματος. Γι' αυτό και η είσοδος μικρών παιδιών σε αυτά είναι απαγορευτική.

Αυτή τη στιγμή το 93% των εφήβων είναι στο διαδίκτυο. Δηλαδή το target group 13-18 ετών. Όλα αυτά τα νέα παιδιά θα πρέπει να καταλάβουν ότι υπάρχουν και όρια στην πλοήγησή τους. Κάποιος όμως οφείλει να τα ενημερώσει. Και αν και οι γονείς τους έχουν άγνοια κινδύνου είναι δύσκολο να τα προστατεύσει κάποιος τρίτος.

3.2 Παραδοσιακά (συμβατικά) εγκλήματα που τελούνται και χωρίς τη χρήση Η/Υ ή και του Διαδικτύου

Στην κατηγορία αυτή εντάσσονται εγκλήματα[42] που προϋπήρχαν της πληροφορικής τεχνολογίας δηλαδή εγκλήματα του κοινού Ποινικού Κώδικα τα οποία τελούνται και χωρίς τη χρήση Η/Υ και Διαδικτύου. Η τεχνολογία έχει δώσει δυνατότητες για νέους και πιο πρόσφορους τρόπους τέλεσης τους.

Τα κυριότερα εγκλήματα αυτής της κατηγορίας είναι τα εξής:

- Ξέπλυμα χρήματος .
- Πειρατεία Λογισμικού.
- Παιδική Πορνογραφία .
- Διαδικτυακή Τρομοκρατία .

3.2.1 Ξέπλυμα χρήματος

Ο όρος «ξέπλυμα χρήματος» χρησιμοποιείται για να περιγράψει τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων (βρώμικο χρήμα) υπόκεινται σε μία σειρά

[42]Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο

διαδικασιών οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα) [5].

Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια [11]:

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

Έτσι λοιπόν, βλέπει κανείς ένα παραδοσιακό έγκλημα του ποινικού κώδικα να διαπράττεται με τη βοήθεια πλέον της τεχνολογίας και των νέων μέσων που αυτή προσφέρει, με σύγχρονους τρόπους και μεθόδους πάντα όμως με τον ίδιο επιδιωκόμενο σκοπό.

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

3.2.2 Πειρατεία λογισμικού

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

[43]Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο

Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι εξής:

Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια [11]:

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

Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες.

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

Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών .

Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες

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

2) **Πλαστογράφηση ή αλλιώς πλήρης απομίμηση του προϊόντος**: Η παράνομη αναπαραγωγή και πώληση λογισμικού με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, επαναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Η αυξανόμενη επιλογή του εμπορίου μέσω ιντερνέτ έχει αυξήσει και τις πιθανότητες να βρεθούν οι καταναλωτές αντιμέτωποι με το πρόβλημα της χρήσης πλαστών προϊόντων. Η όλο και περισσότερο εξελιγμένη τεχνολογία που χρησιμοποιούν οι πλαστογράφοι, απαιτείται ξεχωριστή άδεια για κάθε υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα. εκδηλώνεται δε ως εξής:

καθιστούν ακόμα και τους πιο απαιτητικούς καταναλωτές συχνά ανήμπορους να

[44]Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο

διακρίνουν το νόμιμο λογισμικό από το πλαστό. Το πλαστό λογισμικό συνήθως κατασκευάζεται και προωθείται με τρόπο ώστε να μοιάζει και να ανταγωνίζεται το αυθεντικό προϊόν.

3.2.3 Παιδική πορνογραφία[45]

Σύμφωνα με το «Προαιρετικό Πρωτόκολλο της Σύμβασης για τα δικαιώματα του Παιδιού για την εμπορία παιδιών, την παιδική πορνεία και την παιδική πορνογραφία» και συγκεκριμένα στο άρθρο 2, «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».

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

Με τη χρήση του διαδικτύου:

• Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτότητά του.

• Υπάρχει προσβασιμότητα του επίμαχου υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος.

• Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων. • Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κλπ) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.

Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα

[45]Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο

οργανωμένη «επιχειρηματική» δραστηριότητα. Αποτελεί προϊόν μιας επικερδέστατης επιχείρησης καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλουν διόλου ευκαταφρόνητα ποσά.

Οι επιπτώσεις εις βάρος των ανηλίκων[46], μπορούν να ειδωθούν από πολλές οπτικές γωνίες. Οι ανήλικοι μετατρέπονται σε θύματα των ενηλίκων, αποφέροντάς τους ιδιαίτερα υψηλά κέρδη, εφόσον μετατρέπονται σε εμπορεύσιμα είδη υψηλής αξίας. Επιπλέον μετατρέπονται σε «μέσα» ικανοποίησης των σεξουαλικών τους ορέξεων. Όμως υπάρχει και ένας άλλος κίνδυνος για τους ανηλίκους, που δεν είναι τόσο φανερός όσο οι προηγούμενοι, αλλά που είναι όμως εξίσου σοβαρός και ικανός να προκαλέσει ανεπανόρθωτες βλάβες, κυρίως ως προς τη σεξουαλική τους ωρίμανση. Ο ανήλικος από την πλευρά του, είναι ικανότατος χρήστης των υπολογιστών και συνήθης επισκέπτης του διαδικτύου. Εξαιτίας λοιπόν κάποιων φυσικών γνωρισμάτων του νεαρού της ηλικίας του, όπως της έντονης περιέργειας και του ατίθασου του χαρακτήρα του, μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου. Έτσι μπορεί εύκολα ένας ανήλικος να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετάσχει στην παραγωγή του, πειθόμενος από αυτούς που γνώρισε δια μέσου του ιστού [1].

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

1. Κατασκευή υλικού πορνογραφίας (κινηματογραφική λήψη, μοντάζ, επεξεργασία εικόνων κλπ).
2. Κατοχή πορνογραφικού υλικού δηλαδή φυσική εξουσίαση επί του υλικού.
3. Προμήθεια και αγορά υλικού (πραγματική μετακίνηση του πορνογραφικού υλικού στην κατοχή του δράστη).
4. Μεταφορά πορνογραφικού υλικού
5. Κυκλοφορία πορνογραφικού υλικού (διακίνηση, διάθεση, πώληση) [13].

Έχουμε λοιπόν δύο εκφάνσεις της παιδικής πορνογραφίας στο διαδίκτυο: από τη μία τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο

[46]Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο

την πραγματοποίηση κέρδους και από την άλλη την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.3.2.4 Διαδικτυακή τρομοκρατία Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες» [14]. Η χρήση του διαδικτύου[44] παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα: Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους. Οι ενέργειες τους δύσκολα εντοπίζονται. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρόντας την ανωνυμία του. Με τη χρήση λοιπόν του Διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων. Ένα παράδειγμα είναι το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που είναι Ένα παράδειγμα είναι το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που είναι ύποπτος ότι βρίσκεται πίσω από τον βομβαρδισμό των Αμερικανικών βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφήτου καταλόγου των καταζητούμενων του FBI. Στον Chameleon δόθηκαν 1000 $ προκαταβολικά για την ανταλλαγή με το software και θα έπαιρνε επιπλέον 10.000 $ με την πρόοδο της εργασίας. Ευτυχώς το FBI τον συνέλαβε προτού να έχει την ευκαιρία να διανέμει τα στοιχεία.

[47]Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο

ΚΕΦΑΛΑΙΟ 4

4.1 Νομοθεσία και ηλεκτρονικό έγκλημα

Νομική προσέγγιση του Διαδικτύου [48,49]

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί η νομική ρύθμιση του Διαδικτύου, ενός χώρου τεράστιου και αχανούς, με δυσδιάκριτα όρια και απεριόριστες δυνατότητες ανταλλαγής πληροφοριών [1]. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες μέσω του Διαδικτύου υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιαδήποτε προσπάθειας ρύθμισης του Διαδικτύου [16].
Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:
Το Διαδίκτυο είναι ανοικτό σε όλους και απαιτείται ρύθμιση του για τον έλεγχο του παράνομου περιεχομένου του.
Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.
Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της.
Οι περισσότεροι χρήστες απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους έναντι επιθέσεων κακόβουλων χρηστών

Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα:

[48] Λιανού Κωνσταντίνα, «Έγκλημα και Διαδίκτυο», Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο,

[49] Καρακώστας Ι., «Δίκαιο & Internet. Νομικά ζητήματα στο Διαδίκτυο

Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις .
Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.
Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια θα έρχεται πάντα αντιμέτωπη με το ζήτημα της λογοκρισίας.
Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις.
Το Διαδίκτυο, με άξονα τη βασική του χρήση ως μέσο επικοινωνίας, απασχόλησε το νομοθέτη, ιδιαίτερα από το χρονικό σημείο που άρχισε να αναπτύσσεται και να επεκτείνεται. Στην Ελλάδα ως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον Ο.Τ.Ε.. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες [17]. Το τοπίο στη συνέχεια διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας, η οποία κατήργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιοδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες [1].

Στην Ελλάδα ιδρύθηκε ρυθμιστική αρχή, η «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων», με αποστολή τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η αρχή αυτή έχει τη δυνατότητα να ελέγχει τους πάροχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους [12].

4.2 Ελληνική νομοθεσία

Ο νόμος 1805/88 αφορά εγκλήματα που γίνονται με ηλεκτρονικούς υπολογιστές (computer crime) και σε βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον διαδικτύου (internet). Στην ελληνική νομοθεσία[47] δεν υπάρχει κάποιος νόμος που να αναφέρεται σε θέματα διαδικτύου και να ρυθμίζει τη συμπεριφορά χρηστών στο διαδίκτυο.

[50] Καρακώστας Ι., «Δίκαιο & Internet. Νομικά ζητήματα στο Διαδίκτυο

Η Ελλάδα συνεργάζεται :

- Με άλλα κράτη της Ευρωπαϊκής ένωσης
- Συμβούλιο της Ευρώπης
- Άλλων διεθνών οργανισμών

Άρθρο 370Β[51]

1. Όποιος αντιγράφει, αποτυπώνει , χρησιμοποιεί, αποκαλύπτει σε τρίτον ή παραβιάζει στοιχεία και προγράμματα υπολογιστών τα οποία είναι απόρρητα , τιμωρείται με φυλάκιση τριών (3) μηνών.
2. Αν ο δράστης είναι η υπηρεσία είναι στην υπηρεσία , επιβάλλεται φυλάκιση ενός έτους .
3. Αν πρόκειται για στρατιωτικό ή για απόρρητο που αφορά την ασφάλεια του κράτους , τιμωρείται σύμφωνα με την παράγραφο 1 κατά το άρθρο 146 και 147.

Άρθρο 370Γ[52]

1. Όποιος αντιγράφει ή χρησιμοποιεί υπολογιστή τιμωρείται με φυλάκιση μέχρι 6 μήνες και χρηματική ποινή διακοσίων ενενήντα ευρώ (290) έως και πέντε χιλιάδες εννιακόσια ευρώ (5900)
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή και παραβιάστηκαν, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον 29 ευρώ. Αν η πράξη

αναφέρεται σε διεθνείς σχέσεις ή την ασφάλεια του κράτους , τιμωρείται κατά το άρθρο 148.

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

[51] Τεχνική Νομοθεσία Για Μηχανικούς Πληροφορικής ...
[52] el.wikibooks.org/wiki/Τεχνική_Νομοθεσία.../Ηλεκτρονικό_Έγκλημα

Άρθρο 386Α

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό

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

4.3 Νομοθεσία διαδικτυακών εγκλημάτων στην αλλοδαπή

Στην Αγγλία από τον Φεβρουάριο του 2001, οι hacker, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες.

Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

4.4 Παγκόσμια νομοθεσία για το ηλεκτρονικό έγκλημα[53]

ΗΠΑ Το 1948 θεσπίστηκε το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα. Ωστόσο, στο νομοθέτημα αυτό δεν ήταν διακριτός ο προσδιορισμός των ορίων δικαιοδοσίας των δικαστηρίων και αυτό αποτελούσε το σημαντικότερο πρόβλημα. Επίσης, δεν υπήρχε ορολογία σχετική με την τεχνολογία των ηλεκτρονικών υπολογιστών. Τέλος η νομοθεσία αυτή αφορούσε στην προστασία των κρατικών υπολογιστικών συστημάτων από τη μη εξουσιοδοτημένη πρόσβαση για την αποφυγή διαρροής απόρρητων πληροφοριών που θα μπορούσαν να βλάψουν τις ΗΠΑ. Τα παραπάνω ήταν ο λόγος για την αναθεώρηση του νομού το 1986. Στην αναθεώρηση χρησιμοποιείται πιο σαφής ορολογία και διαφαίνεται η προσπάθεια αντιμετώπισης περιπτώσεων άρνησης εξυπηρέτησης αλλά ακόμα και ο αναθεωρημένος νόμος κάνει λόγο περί προστασίας των κρατικών υπολογιστικών συστημάτων. Το 1994 γίνεται σημαντική τροποποίηση του νόμου κατά την οποία: Η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικούς υπολογιστές που χρησιμοποιούνται στο διαπολιτειακό εμπόριο Αφαιρέθηκε ο όρος «μη εξουσιοδοτημένη πρόσβαση», κάτι το όποιο σημαίνει ότι οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχθούν Συγκεκριμένες μορφές επικίνδυνων και σκόπιμων ενεργειών θεωρούνταν πλέον παράνομες όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης Τέλος το 1996 το νόμο αυτό έρχεται να ολοκληρώσει η National Information Infrastructure Protection Act. Η πιο σημαντική διάταξη προβλέπει ότι κάθε μεμονωμένος χρηστής που θα εισέρχεται σε έναν προστατευόμενο υπολογιστή θα είναι υπεύθυνος όχι μονό για τις ενέργειές του αλλά και για τις συνέπειες αυτών. Σε περίπτωση που ο χρηστής έχει εξουσιοδότηση για αυτό το σύστημα τότε θα είναι ποινικά υπεύθυνος μονό όταν θα έχει εγκληματικές προθέσεις.

ΑΥΣΤΡΑΛΙΑ Στην Αυστραλία θεσμοθετείται ο νομός Crime Act 1914 που θέτει σα βασικές μορφές ηλεκτρονικού εγκλήματος: α) την παράνομη πρόσβαση σε δεδομένα που βρίσκονται σε κρατικό ηλεκτρονικό υπολογιστή β) την καταστροφή δεδομένων δεδομένα που βρίσκονται σε κρατικό ηλεκτρονικό υπολογίστηκα γ) την πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης και δ) την καταστροφή δεδομένων σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης. Σήμερα ισχύει ο νομός The Cybercrime Act 2001 και αποτελεί τροποποίηση του Crime Act 1914. ο νομός προβλέπει τρεις βασικές κατηγορίες ηλεκτρονικού εγκλήματος: α) μη εξουσιοδοτημένη πρόσβαση, μετατροπή και φθορά δεδομένων, με σκοπό τη διάπραξη σοβαρού εγκλήματος, β) μη εξουσιοδοτημένη τροποποίηση δεδομένων που οδηγεί σε φθορά δεδομένων, γ) μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών. Ωστόσο, ο νομός αυτός δημιούργησε τέσσερις νέες μορφές εγκλημάτων: α) μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευόμενων δεδομένων, β) παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ, γ) κατοχή ή έλεγχος δεδομένων, με σκοπό την διάπραξη ηλεκτρονικών αδικημάτων και δ) παραγωγή, προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος.

ΑΓΓΛΙΑ Στην Αγγλία η πρώτη νομοθεσία για το ηλεκτρονικό έγκλημα ψηφίστηκε το 1990 Computer Misuse Act και αποτελεί πρότυπο νομοθεσίας και για άλλες χώρες. Η νομοθεσία αυτή διακρίνει τρεις βασικές κατηγορίες εγκλημάτων: α) μη εξουσιοδοτημένη πρόσβαση, σε πληροφορίες που είναι αποθηκευμένες σε ηλεκτρονικό υπολογιστή, β) μη εξουσιοδοτημένη πρόσβαση με σκοπό τη διάπραξη αδικημάτων και γ) μη εξουσιοδοτημένη τροποποίηση πληροφοριών, αποθηκευμένων τη νομοθεσία και τον τρόπο απονομής δικαιοσύνης.

ΑΡΓΕΝΤΙΝΗ Στην Αργεντινή δεν υπάρχει κάποιο νομοθετικό πλαίσιο που να αφορά στο ηλεκτρονικό έγκλημα. Η ποινική αντιμετώπιση των περιπτώσεων αυτών γίνεται σύμφωνα με τον κοινό Ποινικό Κώδικα. Η δίωξη των ηλεκτρονικών εγκλημάτων γίνεται με διασταλτική ερμηνεία των ισχυουσών διατάξεων.

ΚΙΝΑ Στην Κίνα υπάρχει σχετική νομοθεσία για το ηλεκτρονικό έγκλημα. Καθιστά παράνομη οποιαδήποτε δραστηριότητα έχει να κάνει με τη διασπορά ιών ή αλλού κακόβουλου λογισμικού σε συστήματα ηλεκτρονικών υπολογιστών. Παράνομη θεωρείται επίσης και η πώληση συστημάτων προστασίας υπολογιστών χωρίς άδεια. Αξίζει να ειπωθεί πως η νομοθεσία της Κίνας πάνω σε αυτή τη μορφή εγκλήματος καταδικάζει την δημιουργία, την αναπαραγωγή και τη διάδοση υλικού που θα κλονίσει την εθνική ενότητα, όπως επίσης απαγορεύεται η παραποίηση της αλήθειας και η διάδοση οποιασδήποτε φήμης που θα βλάψει τη συνοχή της κοινωνίας.

ΔΙΕΘΝΕΙΣ ΠΡΟΣΠΑΘΕΙΕΣ Η Interpol ήταν η πρώτη που προσέγγισε το θέμα του ηλεκτρονικού εγκλήματος σε διεθνές επίπεδο. Ωστόσο κι άλλες απόπειρες έγιναν με σημαντικότερη αυτή του OECD – Ο.Ο.Σ.Α., του Οργανισμού των Ηνωμένων Εθνών και της Group of Eight - «Ομάδα των Οκτώ». OECD – Ο.Ο.Σ.Α. : Ο Οργανισμός για

την Οικονομική Συνεργασία και Ανάπτυξη το 1983 διόρισε μια επιτροπή για το ζήτημα του ηλεκτρονικού εγκλήματος, για τη δημιουργία και την τροποποίηση των ποινικών διατάξεων στα κράτη-μέλη του οργανισμού. Η επιτροπή κατέληξε σε ένα κείμενο που λειτούργησε ως κοινός παρανομαστής μεταξύ των διαφορετικών νομικών προσεγγίσεων, που εξετάστηκαν στα κράτη – μέλη. Το κείμενο που συνέταξε απαγόρευε την εισαγωγή, την τροποποίηση, τη διαγραφή και την απόκρυψη των δεδομένων με σκοπό την παράνομη μεταφορά κεφαλαίων, τη διάπραξη πλαστογραφίας και την παρεμπόδιση λειτουργίας ενός υπολογιστή ή δικτυού. Εκτός των άλλων απαγορεύει και την πρόσβαση σε σύστημα Η/Υ χωρίς άδεια. Οργανισμός Ηνωμένων Εθνών: τα Ηνωμένα Έθνη στο 8ο Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών παρουσίασε ένα ψήφισμα σχετικά με τη νομοθεσία του ηλεκτρονικού εγκλήματος. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος εκδόθηκε το 1994 και αντιμετωπίζει συνολικά το ζήτημα αυτό. Με αυτό το τρόπο προτείνει λύσεις που θα μπορέσουν να βοηθήσουν στο πρόβλημα της νομοθεσίας. Είναι η πρώτη συστηματική προσπάθεια σε διεθνές επίπεδο νομοθετικής προσέγγισης του εγκλήματος. Group of Eight - Ομάδα Οκτώ: Την ομάδα των Οκτώ συνθέτουν οι οκτώ ισχυρότερες χώρες του κόσμου οι οποίες δημιούργησαν το 1997 μια Υποομάδα για το Έγκλημα Υψηλής Τεχνολογίας. Η Υποομάδα αυτή με τη συμμέτοχη των υπουργών εσωτερικών και δικαιοσύνης των οκτώ χωρών, κατέληξε σε «Δέκα Αρχές» και «Δέκα Τομείς Δράσης» με σκοπό τη διασφάλιση της ενιαίας αντιμετώπισης του εγκληματικού φαινόμενου, σε όλες τις χώρες του κόσμου. Επιπρόσθετα ή Ομάδα των Οκτώ ίδρυσε κι ένα δίκτυο συνεχούς λειτουργίας με σκοπό τη συνεργασία μεταξύ των χώρων σε επίπεδο ερευνών για εγκλήματα υψηλής τεχνολογίας.

4.5 Πνευματικά Δικαιώματα

Στον κόσμο του διαδικτύου υπάρχει ένα θέμα το όποιο προβληματίζει ιδιαίτερα κι έχει να κάνει με την προστασία των πνευματικών δικαιωμάτων και το κατά πόσο μπορούν να διασφαλιστούν αυτά τα δικαιώματα στον εικονικό κόσμο του internet. Τα βασικά ζητήματα για την προστασία των πνευματικών δικαιωμάτων είναι η προστασία αυτών σε έργα που δημοσιεύονται στο διαδίκτυο και η προστασία των βάσεων δεδομένων και των προγραμμάτων Η/Υ. Η μετατροπή της πληροφορίας σε ψηφιακή μορφή δίνει τη δυνατότητα εύκολης και γρήγορης αναπαραγωγής της. Η πληροφορία ενσωματώνεται σε πρότυπα όπως mp3 μειώνοντας σημαντικά τον όγκο της, κάτι που κάνει ακόμα πιο εύκολη τη μετάδοση της μέσω δικτύων. Η μορφή mp3 συναντάται στην διάδοση μουσικών κομματιών ή βιντεοταινιών χωρίς φυσικά την έγκριση του δημιουργού. Αυτό είναι ίσως η πιο γνωστή και διαδεδομένη μορφή παραβίασης πνευματικών δικαιωμάτων. Εκτός από αυτό, ένα δεύτερο βασικό ζήτημα είναι και οι σύνδεσμοι που παραπέμπουν απευθείας σε σελίδες που περιλαμβάνουν προστατευόμενα έργα και συνιστούν την παραβίαση των πνευματικών δικαιωμάτων. Έγινε λόγος και για την παραβίαση πνευματικών δικαιωμάτων των βάσεων

[53] http://invenio.lib.auth.gr/record/115622/files/ptuxiaki.pdf?version=1

δεδομένων, επίσης καθημερινή μορφή παραβίασης πνευματικών δικαιωμάτων. Συνήθη παραδείγματα είναι τα ψηφιακά λεξικά και εγκυκλοπαίδειες. Για να μπορέσει να αντιμετωπιστεί το πρόβλημα της προστασίας των πνευματικών δικαιωμάτων στις βάσεις δεδομένων θα πρέπει να γίνει προσέγγιση της εννοίας της βάσης δεδομένων, το αν είναι δυνατή η προστασία μεμονωμένων στοιχείων μιας βάσης ως προς το περιεχόμενο αλλά και τη δομή της. Εκτός από τη βάση δεδομένων, χρήζουν προστασίας και τα προγράμματα των Η/Υ. Ένα πρόγραμμα Η/Υ είναι μια σειρά από εντολές ή οδηγίες που χρησιμοποιούνται από τον Η/Υ και είναι γραμμένα σε τρία επίπεδα: στην γλώσσα προγραμματισμού, η οποία αποτελείται από σύνθετα σύμβολα, τα οποία ακολούθου συγκεκριμένους κανόνες στον κώδικα πηγής, η κατοχή του όποιου αποτελεί πλήρη απόδειξη των πνευματικών δικαιωμάτων στον κώδικα μηχανής, ο όποιος χρησιμοποιεί μονό δύο σύμβολα, το 0 και το 1. Ο προβληματισμός είναι στο εάν τα παραπάνω μέρη θα πρέπει να προστατεύονται με βάση τη νομοθεσία και τα πνευματικά δικαιώματα ή αν θα πρέπει να θεωρηθούν ως ευρεσιτεχνίες και να προστατευτούν από την αντίστοιχη νομοθεσία.

4.6 Απόρρητο και προσωπικά δεδομένα[54]

Τα προσωπικά δεδομένα και η προστασία του απορρήτου είναι ένα θέμα αμφισβητούμενο στο χώρο του διαδικτύου. Καθημερινά ζητούνται τα προσωπικά δεδομένα από οργανισμούς κι επιχειρήσεις για εμπορικούς και διαφημιστικούς λόγους. Ο χρήστης του διαδικτύου δίνει πληροφορίες για τα προσωπικά δεδομένα του με μια σχετική ευκολία χωρίς να το αντιλαμβάνεται πολλές φόρες. Δίνει πληροφορίες σχετικά με την προσωπικότητά του, τις προτιμήσεις του μέχρι και πληροφορίες ταυτότητας και αριθμούς πιστωτικών καρτών. Η ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί ένα συνδυασμό διεθνών συνθηκών, συνταγματικών διατάξεων, διατάξεων

του κοινού ποινικού δίκαιου και νομών που έχουν εκδοθεί βάση κοινοτικών οδηγών.

4.7 Νομοθεσία και Ηλεκτρονικό Εμπόριο

Για το ηλεκτρονικό εμπόριο έχει γίνει λόγος κι έχει τονισθεί η σημασία του από πλευρά νόμιμου χρηστή και εγκληματία. Το ηλεκτρονικό εμπόριο γνωρίζει ιδιαίτερη ανάπτυξη κι αποτελεί ανασταλτικός παράγοντας από πλευράς χρηστών – πελατών αλλά και των επιχειρήσεων αυτής της μορφής αλλά παράλληλα αποτελεί κατασταλτικό παράγοντα για το συμβατικό εμπόριο. Ωστόσο χρήζει κι αυτό ιδιαίτερης προσοχής και νομοθεσίας. Το νομοθετικό πλαίσιο για το «συμβατικό εμπόριο» δεν μπορεί να εφαρμοστεί στην περίπτωση του ηλεκτρονικού, αφού πρόκειται για έναν εικονικό κόσμο χωρίς τη φυσική παρουσία των συναλλασσόμενων κάτι που κάνει αμφισβητούμενη την εγκυρότητα της συναλλαγής. Η Ευρωπαϊκή Κοινότητα έχει εκδώσει μια σειρά από οδηγίες που ρυθμίζουν τα θέματα του ηλεκτρονικού εμπορίου. Σκοπός των οδηγιών αυτών είναι η ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ κρατών – μελών,

περιοριζόμενη από θεμελιώδεις ανάγκες για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρεπείας και την προστασία των ανηλίκων και της ανθρώπινης αξιοπρεπείας και την προστασία του καταναλωτή και της δημόσιας υγείας. Όσο αφόρα στο ηλεκτρονικό εμπόριο ρυθμίζεται στο Ελληνικό δίκαιο με το Ποινικό Δίκαιο 131/2003 στο όποιο ενσωματώθηκε η οδηγία 2000/31/ΕΚ. Οι πιο σημαντικές διατάξεις περιλαμβάνονται : στο άρθρο 6 το όποιο ρυθμίζει το ζήτημα της μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου, βάσει του όποιου, οι πάροχοι των υπηρεσιών αυτών υποχρεούνται να τηρούν και να συμβουλεύονται τακτικά μητρώα επιλογών, όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες. Στα άρθρα 8-10 που αναφέρονται στις ηλεκτρονικές συμβάσεις και τους τρόπους ηλεκτρονικής παραγγελίας. Γενικά, επιτρέπεται η κατάρτιση ηλεκτρονικών συμβάσεων, εξαιρούμενων περιπτώσεων που αφορούν θεμελίωση ή μεταβίβαση εμπράγματων δικαιωμάτων επί ακινήτων, που εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο και όσες, εκ του νομού, απαιτείται προσφυγή σε δημοσιές αρχές, δικαστήρια ή επαγγέλματα που ασκούν δημόσια εξουσία. Η ηλεκτρονική παραγγελία θεωρείται έγκυρη όταν ο παροχέας ενημερώσει τον πελάτη για τις λεπτομέρειες της σύμβασης και μετά την παραγγελία, αποστείλει και ηλεκτρονικό μήνυμα επιβεβαίωσης. Στο άρθρο 20, το όποιο εξαιρεί την εφαρμογή του Διατάγματος από ορισμένες δραστηριότητες όπως π.χ. το φορολογικό τομέα και θέματα που ήδη ρυθμίζονται με το νόμο περί προστασίας των προσωπικών δεδομένων. Όσο αφόρα στα ηλεκτρονικά έγγραφα ισχύει η εφαρμογή του άρθρου 3 που εξομοιώνει τα ηλεκτρονικά με τα συμβατικά έγγραφα. Βεβαία στα ηλεκτρονικά έγγραφα δεν υφίσταται ιδιόγραφη υπογραφή και επιπλέον υπάρχει μεγάλος αριθμός μεταβλητότητας. Το πρόβλημα της υπογραφής ρυθμίζουν οι διατάξεις του Ποινικού Κώδικα, κατά τις οποίες α) θα πρέπει η υπογραφή να συνδέεται μονοσήμαντα με τον υπογράφοντα, β) να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος, γ) να δημιουργείται με μέσα, τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και δ) να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπίσει οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων. Εκτός από την εξομοίωση των εγγράφων το άρθρο 3 εξομοιώνει και την ιδιόχειρη με την ψηφιακή υπογραφή.

4.8 Ποινική προσέγγιση του Ηλεκτρονικού Εγκλήματος– Μια μελέτη του συνηγόρου του καταναλωτή

"Η αντιμετώπιση της ηλεκτρονικής εγκληματικότητας, ανάλογα με τη μορφή που αυτή λαμβάνει, μπορεί να γίνει από το Ελληνικό δίκαιο συνδυάζοντας διάσπαρτες διατάξεις της κείμενης νομοθεσίας. Σε αυτές ανήκουν οι διατάξεις του Ποινικού Κώδικα περί απάτης με τη χρήση υπολογιστή, περί αθέμιτης πρόσβασης σε συστήματα πληροφοριών, υποκλοπής και παραβίασης απορρήτων, η ειδική νομοθεσία περί προστασίας προσωπικών δεδομένων (ν. 2472/1997 όπως τροποποιήθηκε με το ν. 3625/2007, ν. 3471/2006), η νομοθεσία περί διασφάλισης του απορρήτου των επικοινωνιών (ν. 3674/2008), οι κανονιστικές αποφάσεις διοικητικών

αρχών όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και ούτω καθεξής. Ειδικότερα, το άρθρο 5 του ν. 1805/1988, προσέθεσε στο άρθρο 386 του Ποινικού Κώδικα περί απάτης το ειδικό άρθρο 386Α που αναφέρεται στην απάτη με υπολογιστή. Σύμφωνα με το άρθρο αυτό, όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία, επηρεάζοντας τα αρχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές φυλάκισης που προβλέπονται για την απάτη. Ανάλογα με τη βαρύτητα του αδικήματος, οι ποινές αυτές μπορούν να ανέρχονται από φυλάκιση τουλάχιστον τριών μηνών έως φυλάκιση τουλάχιστον τριών ετών αν η ζημία που προκλήθηκε είναι ιδιαίτερα μεγάλη. Υπό συγκεκριμένες προϋποθέσεις, η διαδικτυακή εγκληματικότητα, στο μέτρο που οδηγεί σε παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας, παραβίαση επαγγελματικών απορρήτων ή παράνομη αντιγραφή προγραμμάτων ηλεκτρονικού υπολογιστή, τιμωρείται και από τα άρθρα 370Α και 370Β του Ποινικού Κώδικα, που προβλέπουν αντίστοιχες ποινές φυλάκισης κατά των δραστών. Πρόσφατα, ο νόμος 3674/2008 ψηφίστηκε για να ενισχύσει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, θεσπίζοντας ειδικές υποχρεώσεις u964 του παρόχου υ-πηρεσιών για την ασφάλεια δικτύου και συγκεκριμένες διαδικασίες άρσης του απορρήτου υπό την εποπτεία της ΑΔΑΕ. Παράλληλα, ο νόμος αυτός προσέθεσε νέο άρθρο 292Α στον Ποινικό Κώδικα που τιμωρεί τα εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών με φυλάκιση τουλάχιστον ενός έτους και χρηματικές ποινές που αρχίζουν από είκοσι χιλιάδες (20.000) Ευρώ και αυξάνονται ανάλογα με τη βαρύτητα του παραπτώματος και την ιδιότητα του δράστη. Ο ίδιος νόμος τροποποίησε ακόμα το άρθρο 370Α του Ποινικού Κώδικα θεσπίζοντας αυστηρές κυρώσεις, που μπορούν να φθάσουν ως κάθειρξη μέχρι δέκα ετών για όσους παραβιάζουν το απόρρητο της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας. Τέλος, θέσπισε διοικητικές κυρώσεις (χρηματικά πρόστιμα, ανάκληση αδειών κλπ) κατά των εκπροσώπων εταιριών παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών. Προς την ίδια κατεύθυνση, το άρθρο 348 Α του Ποινικού κώδικα, που προστέθηκε με το άρθρο 6 του ν. 3064/2002 τιμωρεί με φυλάκιση και χρηματικές ποινές την πορνογραφία ανηλίκων, οποιοσδήποτε και αν είναι ο υλικός φορέας αποτύπωσης του πορνογραφικού υλικού. Παρόμοιες κυρώσεις προβλέπονται από την ισχύουσα ειδική νομοθεσία περί προστασίας καταναλωτή, σε ότι αφορά ειδικότερα τις εξ αποστάσεως συμβάσεις πρόσβασης σε υπηρεσίες ηλεκτρονικού εμπορίου. Η νομοθεσία αυτή απαγορεύει τις παραπλανητικές εμπορικές πρακτικές (ν. 2251/1994 όπως ισχύει μετά την τροποποίηση του από το ν. 3587/2007), ενώ προβλέπει επίσης διοικητικές κυρώσεις κατά των παραβατών. Αντίστοιχες διοικητικές, αστικές και ποινικές κυρώσεις προβλέπονται επίσης κατά των παραβατών, όπως προαναφέρθηκε, από τη νομοθεσία περί προστασίας προσωπικών δεδομένων (ν. 2472/1997 όπως ισχύει και 3471/2006). Τέτοιες πράξεις ηλεκτρονικής παραβατικότητας μπορούν ακόμα να συνιστούν πλαστογραφία, εξύβριση, δυσφήμιση, προσβολή της νομοθεσίας

περί απορρήτου, του ν. 2121/1993 περί πνευματικής ιδιοκτησίας ή του ν. 3431/2006 περί ηλεκτρονικών επικοινωνιών. Στην Ελλάδα το spam ρυθμίζεται από το αρ. 11 του ν. 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/ ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Σύμφωνα με το άρθρο αυτό η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς. Εκτός από την ποινική προστασία και την ειδική νομοθεσία του τομέα που προβλέπει προσφυγή στις αρμόδιες αρχές, ο χρήστης που έπεσε θύμα ηλεκτρονικής απάτης μπορεί θεωρητικά να στραφεί δικαστικά κατά του προβολέα ζητώντας αποζημίωση με βάση το άρθρο 914 του Αστικού Κώδικα περί αδικοπραξίας. Πλην όμως, στις περισσότερες περιπτώσεις εγκλημάτων του κυβερνοχώρου, η ταυτότητα και η χώρα εγκατάστασης των προβολέων είναι άγνωστη ενώ οι δράστες εξαφανίζονται μετά την εγκληματική πράξη τους. Επίσης ο τόπος διάπραξης του κυβερνοεγκλήματος είναι συχνά αμφισβητούμενος, αν π.χ. η τεχνική υποδομή τέλεσης του εγκλήματος, ήτοι ο εξυπηρετητής (server) που φιλοξενεί την απατηλή ιστοσελίδα είναι εγκατεστημένος στην αλλοδαπή, οπότε είναι ενδεχόμενο να μην μπορούν να εφαρμοστούν οι προβλεπόμενοι Ελληνικοί νόμοι που τιμωρούν αποκλειστικά εγκλήματα τελούμενα στην Ελλάδα. Η διεθνής διάσταση των εγκλημάτων του κυβερνοχώρου απαιτεί τη διεθνή συνεργασία. Η Διεθνής Σύμβαση του Συμβουλίου της Ευρώπης (Νοέμβριος 2001), που έχει υπογραφεί και από την Ελλάδα, εντάσσεται σε αυτήν την προοπτική. Εκτός όμως ότι δεν έχει ακόμα κυρωθεί από όλες τις χώρες η Σύμβαση αυτή έχει τύχει αρκετής διεθνούς κριτικής για ασάφεια των περιγραφομένων εγκλημάτων και προβλήματα εφαρμογής. Προς την ίδια κατεύθυνση εντάσσονται οι σχετικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης για την καταπολέμηση διακίνησης επιβλαβούς και παράνομου περιεχομένου μέσω ιντερνέτ, που στοχεύουν στη δημιουργία συνθηκών ασφαλούς χρήσης του Διαδικτύου μέσω αυτορρύθμισης και κωδίκων δεοντολογίας. Η πρόληψη υποστηρίζεται επίσης από τη λειτουργία ειδικών τηλεφωνικών γραμμών (hotlines), όπου οι χρήστες μπορούν να καταγγείλουν προβατική συμπεριφορά προς τις αρμόδιες διωκτικές αρχές των κρατών- μελών. Ο Ευρωπαϊκός Οργανισμός για την ασφάλεια ENISA, έχει επίσης εκδώσει δύο εκθέσεις για την ασφάλεια και μέτρα καταπολέμησης της ανεπιθύμητης εμπορικής επικοινωνίας που εφαρμόζουν οι Πάροχοι Υπηρεσιών Διαδικτύου στην Ευρώπη. Παρά τη διεθνή κινητοποίηση και συνεργασία, η δυσκολία εντοπισμού των δραστών, η πιθανή αρνητική δημοσιότητα για το θύμα που συνοδεύει τη δημοσιοποίηση περιπτώσεων ηλεκτρονικής απάτης, σε συνδυασμό με την μικρή ταχύτητα ενεργοποίησης των διωκτικών μηχανισμών και απονομής δικαιοσύνης, καθώς και το κόστος της, είναι συνήθως αποτρεπτικοί παράγοντες διεκδίκησης της βλάβης από τον ζημιωθέντα καταναλωτή. Για το λόγο αυτό, η πρόληψη, η ευαισθητοποίηση και η λήψη μέτρων προστασίας κατά του ηλεκτρονικού εγκλήματος από τον

συνειδητοποιημένο καταναλωτή είναι προτιμότερη από την καταστολή τέτοιων πράξεων σε βάρος των συμφερόντων του" (Ο Συνήγορος του Καταναλωτή, 2008).

4.9 Αδυναμίες της νομοθεσίας[55,56]

Ο Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος της Δ/νσης Ασφάλειας Αττικής, Αστυνόμος Α΄ κ. Εμμανουήλ Σφακιανάκης παρατηρεί ότι "*οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες.* Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών." (Σε ειδική έρευνα που έγινε στη Βρετανία από την Επιτροπή Πρόβλεψης και Πρόληψης Εγκλήματος (Foresight Crime Prevention Panel) διαπιστώθηκε ό,τι το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα έχουν την τεχνογνωσία να υπερκεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο

4.10 Συνθήκη Βουδαπέστης

Στη συνθήκη της Βουδαπέστη, που υπέγραψε μεταξύ πολλών άλλων χωρών και η Ελλάδα υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.
2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.

3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.

4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

[54]http://invenio.lib.auth.gr/record/115622/files/ptuxiaki.pdf?version
[55]Τεχνική Νομοθεσία Για Μηχανικούς Πληροφορικής ...
[56] el.wikibooks.org/wiki/Τεχνική_Νομοθεσία.../Ηλεκτρονικό_Έγκλημα

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνεργεία, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση. Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος.

Στην Ευρωπαϊκή Ένωση ισχύουν:[57,58]

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

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

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

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

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

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

[57] Τεχνική Νομοθεσία Για Μηχανικούς Πληροφορικής ...
[58] el.wikibooks.org/wiki/Τεχνική_Νομοθεσία.../Ηλεκτρονικό_Έγκλημα

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

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

Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η συνεννόηση μεταξύ των κρατών και η εκπόνηση μιας αναλυτικής και αποτελεσματική στρατηγικής. Ο σκοπός αυτός επετέθη με το συνέδριο για το ηλεκτρονικό έγκλημα (convention on cybercrime) , του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23/11/01.

1.για τα δικαιώματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών . τέτοια αδικήματα είναι η παράνομη πρόσβαση , η παράνομη υποκλοπή , η επέμβαση σε δεδομένα , η επέμβαση σε συστήματα και η κακή χρήση συσκευών

2.για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.

3.για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας

4.για το αδίκημα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας

Επίσης, η συνθήκη περιέχει ρυθμίσεις για την συνεργασία , την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων . ακόμη τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοσύνης των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή Ένωση . Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του ηλεκτρονικού εγκλήματος .

4.11 Παράνομη διείσδυση σε δεδομένα[59]

Η χωρίς δικαιώματα διείσδυση- πρόσβαση σε συστήματα επεξεργασίας , δεδομένων έστω κι όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του ποινικού κώδικα

Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση των hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες

[59] Ηλεκτρονικό Έγκλημα - Ελληνική Αστυνομία www.astynomia.gr

για τη δημιουργία τους . Τέτοια είναι :

1. Η ανακοίνωση της επιτροπής με αριθμό com/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών
2. Πρόταση κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού οργανισμού για την ασφάλεια δικτύων και πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών .
3. Πρόταση απόφασης πλαισίου του συμβουλίου με αριθμό com/2002/0173 – CNS 2002/0086 για τις επιθέσεις κατά των
4. συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της
5. επίθεσης μέσω παράνομης πρόσβασης σε σύστημα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε σύστημα πληροφοριών

ΚΕΦΑΛΑΙΟ

5.1 Βασικές αρχές ασφαλείας

Οι στόχοι μιας υλοποιημένης ασφαλείας υπολογιστών συνήθως συνοψίζονται σε τρεις έννοιες, γνωστές με το αρκτικόλεξο CIA:
Εμπιστευτικότητα : η αρχή του εμπιστευτικότητας (confidentiality) προστατεύει ευαίσθητη πληροφορία από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή της . Η πληροφορία πρέπει να είναι εμφανής μόνο μεταξύ των νόμιμων άκρων μιας επικοινωνίας και όχι και σε αυτούς που πιθανά <<ακούνε>> το κανάλι της επικοινωνίας .

Ακεραιότητα : η αρχή του ακεραιότητα (integrity) εξασφαλίζει ότι η πληροφορία ή το λογισμικό είναι πλήρες , σωστό κ αυθεντικό με άλλα λόγια ότι δεν έχει υποστεί κάποια αλλαγή με κάποιον παράνομο τρόπο . θέλουμε να εξασφαλίσουμε ότι υπάρχουν κατάλληλοι μηχανισμοί στα σημεία , οι οποίοι μας προστατεύουν από τυχαία ή κακόβουλη τροποποίηση της αρχικής πληροφορίας.

Διαθεσιμότητα: η αρχή του διαθεσιμότητας (availability) εξασφαλίζει ότι η πληροφορία ή οι υπηρεσίες είναι προσπελάσιμες και λειτουργικές, όταν ζητηθούν από κάποιον ο οποίος είναι εξουσιοδοτημένος για πρόσβαση σε αυτές.

Με την αρχή αυτή σχετίζεται και η έννοια της εμπιστοσύνης: Η εμπιστοσύνη έχει να κάνει με το κατά πόσο μπορεί κάποιος χρήστης να εμπιστεύεται ένα υπολογιστικό σύστημα και να είναι εφησυχασμένος ότι το σύστημα κάνει αυτό που ισχυρίζεται και όχι κάποια άλλη ανεπιθύμητη ενέργεια.
Διαφορετικά συστήματα, που εξυπηρετούν διαφορετικούς σκοπούς, ρίχνουν μεγαλύτερο βάρος σε κάποια από τις τρεις αυτές αρχές.
Για παράδειγμα κάποιος πάροχος internet (ISP) ενδιαφέρεται περισσότερο να παρέχει στους χρήστες του availability.Ο στρατός από την άλλη ρίχνει περισσότερο βάρος στο confidentiality του δικτύου του, καθώς πρόσβαση στις πληροφορίες του πρέπει να έχουν λίγοι μόνο εξουσιοδοτημένοι χρήστες.
Εδώ μάλιστα υπάρχει και κατηγοριοποίηση πρόσβασης, καθώς διαφορετικά άτομα έχουν και διαφορετικού επιπέδου πρόσβαση σε πληροφορία. Οι περισσότερες επιχειρήσεις τώρα πρέπει να δίνουν έμφαση και στις τρείς αυτές αρχές, με ίσως λίγο μεγαλύτερη στο integrity των δεδομένων τους.

Εμπιστευτικότητα: Η αρχή του confidentiality (εμπιστευτικότητας) προστατεύει ευαίσθητη πληροφορία από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή της. Συνήθως χρησιμοποιείται κρυπτογραφία και έλεγχος πρόσβασης, ώστε να εξασφαλισθεί η εμπιστευτικότητα των δεδομένων. Η προσπάθεια που θα καταβληθεί για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων εξαρτάται από το πόσο ευαίσθητα είναι τα δεδομένα του.
Διάφορες εφαρμογές παρέχουν κρυπτογράφηση από άκρο σε άκρο, ωστόσο σε μια τέτοια περίπτωση υπάρχει το μειονέκτημα ότι καθένα από τα άκρα θα πρέπει να υποστηρίζει το ίδιο πρωτόκολλο κρυπτογράφησης.
Ιδεατά Ιδιωτικά Δίκτυα, γνωστά ως (VPNs), μπορούν να χρησιμοποιηθούν ως εναλλακτική λύση για δημιουργία ενός ασφαλούς καναλιού επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων.

Κρυπτογραφία μπορεί να χρησιμοποιηθεί και στο επίπεδο συνδέσμου μετάδοσης δεδομένων (data-link layer) του μοντέλου OSI, ωστόσο είναι δύσκολο στην

εφαρμογή του, καθώς απαιτεί κάθε ενδιάμεση συσκευή δικτύωσης στο μονοπάτι επικοινωνίας να συμμετέχει στην κρυπτογράφηση.
Προστασία με φυσικά μέσα εφαρμόζεται παράλληλα για να περιορίσει την μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά κέντρα η σε μέρη οπού υπάρχει δικτυακός εξοπλισμός.
Ένας βασικός λόγος που λαμβάνονται μέτρα περιορισμού της φυσικής πρόσβασης σε μέρη με δικτυακό εξοπλισμό είναι για να μειωθεί η πιθανότητα κάποιος να μπορεί να λαμβάνει πακέτα χωρίς να πρέπει.
Αυτό μπορεί να επιτευχθεί με χρήση προγραμμάτων λογισμικού τα οποία συλλαμβάνουν πακέτα τα οποία όμως δεν προορίζονταν για αυτά. Με τον τρόπο αυτό μπορεί κάποιος να υποκλέψει σημαντικές πληροφορίες, τόσο για τα δεδομένα όσο και για την ίδια την δομή του δικτύου.

Ακεραιότητα : Η αρχή του integrity (ακεραιότητα) εξασφαλίζει ότι η πληροφορία δεν έχει υποστεί κάποια αλλαγή με κάποιον παράνομο τρόπο κατά την μεταφορά της από τον αποστολέα στον παραλήπτη της. Επιθυμούμε να προστατέψουμε την πληροφορία να δεχθεί τροποποίηση από χρήστες ή εφαρμογές που δεν είναι εξουσιοδοτημένες να πράξουν κάτι τέτοιο, ή από χρήστες που είναι μεν εξουσιοδοτημένοι για προσπέλαση, αλλά τα δικαιώματά τους δεν τους επιτρέπουν να πραγματοποιήσουν καμιά τροποποίηση σε αυτήν. Για να μπορούμε να πούμε ότι ικανοποιείται η ακεραιότητα των δεδομένων μας πρέπει να εξασφαλίζεται ότι το μήνυμα που φτάνει σε έναν παραλήπτη είναι ίδιο με αυτό που έφυγε από τον αποστολέα. Το περιεχόμενο του μηνύματος πρέπει να είναι πλήρες και να μην έχει υποστεί καμιά αλλαγή σε κάποιον ενδιάμεσο κόμβο του δικτύου, και το κανάλι της επικοινωνίας είναι μεταξύ της νόμιμης πηγής και του σωστού προορισμού.
Η ακεραιότητα μιας σύνδεσης μπορεί να εξασφαλιστεί με χρήση κρυπτογραφίας και έλεγχο δρομολόγησης. Ισχυρές μέθοδοι εξασφάλισης της ακεραιότητας υπάρχουν όταν γίνεται χρήση hash συναρτήσεων, όπως ο αλγόριθμος MD5 ή ο Ασφαλής Hash Αλγόριθμος (SHA).Η ακεραιότητα επεκτείνεται και στο λογισμικό των δικτυακών συσκευών, μέσω των οποίων μεταφέρονται δεδομένα. Το λογισμικό πρέπει να πιστοποιείται ώστε να εξασφαλίζεται η προέλευσή του και η ορθή μεταφορά του στην κάθε συσκευή. Για παράδειγμα, όπως τα IP πακέτα έχουν ένα checksum με το οποίο ελέγχουν ότι δεν αλλοιώθηκε το πακέτο κατά την μεταφορά, έτσι και το λογισμικό των δικτυακών συσκευών της γνωστής εταιρίας CISCO συνοδεύεται από ένα

checksum. Όταν το λογισμικό εγκατασταθεί σε κάποια συσκευή τότε πρέπει να πιστοποιείται ότι το checksum που επιστρέφει το λογισμικό με αυτό που δίνει η εταιρία για το λογισμικό αυτό.
Έτσι εξασφαλίζεται η ορθή μεταφορά και εγκατάσταση του στην κάθε συσκευή.

Διαθεσιμότητα : Η αρχή του availability (διαθεσιμότητας) εξασφαλίζει ότι η πληροφορία ή οι υπηρεσίες είναι προσπελάσιμες και λειτουργικές, όταν ζητηθούν από κάποιον ο οποίος είναι εξουσιοδοτημένος για πρόσβαση σε αυτές. Η ανοχή σε σφάλματα, ο πλεονασμός, τα εφεδρικά αντίγραφα, οι διαδικασίας ανάκτησης, η ανθεκτικότητα και η εξισορρόπηση φορτίου είναι σχεδιαστικές αρχές του δικτύου, οι οποίες χρησιμοποιούνται για να εξασφαλιστεί η διαθεσιμότητα. Αν τα συστήματα δεν είναι διαθέσιμα όταν πρέπει, τότε οι έννοιες εμπιστευτικότητα και ακεραιότητα δεν έχουν καμία απολύτως σημασία. Επιθέσεις Άρνησης Εξυπηρέτησης (DoS) έχουν ως στόχο να εμποδίσουν την ομαλή λειτουργία ενός συστήματος και να το κάνουν, έστω και προσωρινά, μη διαθέσιμο. Τέτοιες επιθέσεις σε servers εταιριών που δραστηριοποιούνται στο διαδίκτυο μπορεί να σημαίνουν σημαντική απώλεια εσόδων, οπότε σε τέτοιες περιπτώσεις η διαθεσιμότητα είναι ο πρώτος στόχος. Το πρόβλημα.

με τις επιθέσεις DoS γίνεται σήμερα ακόμη μεγαλύτερο, καθώς εμφανίζεται συχνά μια νέα εκδοχή αυτού του τύπου επίθεσης, η DDoS (Distributed Denial of Service), η οποία είναι ακόμη πιο αποτελεσματική και δύσκολη στην αντιμετώπιση.

5.2 Τεχνικά μέτρα αντιμετώπισης ηλεκτρονικών εγκλημάτων

Για την μέθοδο ηλεκτρονικών εγκλημάτων επινοήθηκαν μια σειρά από μέθοδοι[60] που ασφαλίζουν και εξαλείφουν τις αδυναμίες του υπολογιστικού συστήματος .

- Τα φίλτρα προστασίας ελέγχουν το λογισμικό , επιτρέπουν την πρόσβαση στο σύστημα μόνο σε χρήστες που έχουν καταχωρηθεί ειδικά στους Η/Υ . Καθώς.

- οι χρήστες επιχειρούν να αποκτήσουν πρόσβαση στο σύστημα , τους ζητείται να βεβαιώσουν ότι έχουν ένα γνήσιο κωδικό πρόσβασης. Ένα φίλτρο προστασίας δρα κυρίως ως ένα εξελιγμένο ηλεκτρονικό σύστημα. Ένα φίλτρο είναι ένα πακέτο λογισμικού το οποίο μπορεί να αποκλείσει την προσπέλαση σε τόπους του κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο .
- Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού καθώς και από το πόσο ανανεωμένες είναι οι λίστες με τούς απαγορευμένους τόπους. Διαφορετικά φίλτρα είναι αποτελεσματικά στο να αποκλείουν την πρόσβαση σε τόπους με διαφορετικό περιεχόμενο. Για παράδειγμα, κάποιο φίλτρο μπορεί να είναι πιο αποτελεσματικό στο να

[60]Πτυχιακή Σερέτης Δημήτριος << Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών >>,διπλωματική εργασία

αποκλείει την πρόσβαση σε τόπους με πορνογραφικό περιεχόμενο, ενώ κάποιο άλλο να είναι πιο αποτελεσματικό σε περιεχόμενο με βία ή ρατσισμό.

- Κάποιοι από τους παροχής υπηρεσιών Διαδικτύου έχουν ήδη εγκαταστήσει λογισμικά φίλτρα στις υπηρεσίες τους. Σε αυτή την περίπτωση δεν είναι αναγκαία η εγκατάσταση άλλων φίλτρων.

Μερικά από τα πιο γνωστά λογισμικά φίλτρα είναι τα παρακάτω (σε αλφαβητική σειρά) :

- Crayon Crawler
- Cyberpatrol
- ICRA

- Η ταυτοποίηση του χρήστη αναγνωρίζει την ταυτότητα του χρήστη και δίνει την άδεια εισόδου . Η συγκεκριμένη μέθοδος συνιστά το πρώτο στάδιο αναγνώρισης , δηλαδή ο χρήστης για να εισέλθει στο σύστημα , πρέπει να δώσει ορισμένα στοιχεία , χωρίς τα οποία δεν είναι δυνατή η είσοδος του στον Η/Υ . Συνήθως απαιτείται ο χρήστης να συμπληρώσει το όνομά του και τον κωδικό πρόσβασης . Η ταυτοποίηση ή αλλιώς η αναγνώριση , έχει ορισθεί ως απαίτηση που ικανοποιεί την ιδιωτικότητα, αφενός μεν της εξωτερικής οντότητας που ζητά να αποκτήσει πρόσβαση σε μια υπηρεσία ή να προσπελάσει ένα σύνολο δεδομένων αυτής, αφετέρου των οντοτήτων των οποίων τα προσωπικά δεδομένα είναι αποθηκευμένα στο σύστημα.
- Συγκεκριμένα από την πλευρά της εξωτερικής οντότητας , η διαδικασία της αναγνώρισης ελέγχει αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι. Σε περίπτωση που δεν απαιτείται προστατεύεται η ιδιωτικότητά της αφού επιστρέφονται τα αντίστοιχα δεδομένα ή υπηρεσία που ζητήθηκε δίχως την παροχή προσωπικών δεδομένων από αυτή. Από την πλευρά της προστασίας των δεδομένων που είναι αποθηκευμένα σε ένα σύστημα , η διαδικασία της αναγνώρισης φροντίζει να μην επιτραπεί σε κανένα μη εξουσιοδοτημένο χρήστη ή πρόσβαση σε αυτά, προφυλάσσοντας έτσι την ιδιωτικότητα των κατόχων τους . το σύστημα αντιπαραβάλλει τα στοιχεία με αυτά που έχει αποθηκευμένα.
- και αν αναγνωρίσει τη συγκεκριμένη ταυτότητα επιτρέπει την είσοδο στα δεδομένα . Η αναγνώριση θα μπορούσε να χρησιμοποιηθεί σαν μέθοδος αντιμετώπισης ηλεκτρονικών εγκλημάτων όπως είναι το hacking .

Το δεύτερο στάδιο αναγνώρισης συνιστά η μέθοδος αυθεντικοποίησης που επαληθεύει την ταυτότητα του χρήστη . Η αυθεντικοποίηση είναι η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας . Σε ιδιωτικά και δημόσια δίκτυα η αυθεντικοποίηση υλοποιείται συνήθως με τη χρήση κωδικών πρόσβασης. Η αυθεντικοποίηση αποτελεί απαίτηση ασφάλειας ,παρά ιδιωτικότητας ενός συστήματος . Ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας . Έτσι μια οντότητα απαιτεί τη χρήση μιας υπηρεσίας από ένα πληροφοριακό σύστημα , θα πρέπει να εξετάζεται η υπηρεσία αυτή και ανάλογα να ζητείται η αυθεντικοποίηση ή μη της συγκεκριμένης οντότητας . Με αυτό τον τρόπο προστατεύεται και η ιδιωτικότητα της οντότητας αλλά και τα ευαίσθητα δεδομένα του συστήματος. Ο χρήστης με τη μέθοδο αυτή βεβαιώνει στο

- σύστημα ότι τα πραγματικά είναι ο ίδιος που ζητά την πρόσβαση. Έτσι διασφαλίζεται η χρήση του συστήματος από άτομα που τυχόν υπέκλεψαν ή κατά τύχη γνωρίζουν τα στοιχεία ταυτοποίησης . Συνήθως ο χρήστης χρησιμοποιεί κάτι που γνωρίζει (συναισθηματικά) ή κατέχει (μαγνητική
- κάρτα) ή τον χαρακτηρίζει (συσκευές αναγνώρισης δακτυλικών αποτυπωμάτων , φωνής) . Στο μέλλον η αυθεντικοποίηση του χρήστη θα βασίζεται στο αποτύπωμα της ίριδας . Έχουν ήδη σχεδιαστεί αλγόριθμοι με τη βοήθεια των οποίων είναι δυνατή η αναγνώριση της ίριδας χρησιμοποιώντας μια απλή ασπρόμαυρη κάμερα.

Η μέθοδος της εξουσιοδότησης που αποτελεί το τρίτο στάδιο αναγνώρισης , δίνει τη δυνατότητα στο υπολογιστικό σύστημα να αναγνωρίζει τις εργασίες και τα δεδομένα στα οποία έχει δικαίωμα πρόσβασης ο συγκεκριμένος χρήστης και το είδος των εργασιών που επιτρέπεται να εκτελέσει. Η εξουσιοδότηση είναι η διαδικασία μέσω της οποίας μια οντότητα αποκτά δικαιώματα (π.χ. χρήση, τροποποίηση , προσπέλαση κτλ) σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα. , ανάλογα με το ρόλο τους και τα δικαιώματα στο σύστημα .

Η εξουσιοδότηση όπως και η αυθεντικοποίηση , αποτελεί κυρίως απαίτηση πληροφοριακού συστήματος . Σε ένα σύστημα που υπάρχουν πολλοί χρήστες ο ασφάλειας

- Η εξουσιοδότηση όμως συντελεί στην ικανοποίηση της ιδιωτικότητας μιας και τα ευαίσθητα προσωπικά δεδομένα των χρηστών που βρίσκονται αποθηκευμένα σε ένα σύστημα.

πρέπει να μπορούν να τα προσπελάσουν μόνον εξουσιοδοτημένες χρήστες. Προστατεύοντας τα προσωπικά δεδομένα των χρηστών ενός συστήματος , προστατεύεται εν μέρει η ιδιωτικότητά τους . Η εξουσιοδότηση συχνά έπεται της αυθεντικοποίησης μιας και πρώτα πρέπει να αναγνωρισθεί θετικά μια

- οντότητα και μετά να της ανατεθούν τα αντίστοιχα δικαιώματα ανάλογα με το ρόλο της στο σύστημα .
- Η μέθοδος της κρυπτογράφησης στηρίζεται στη χρησιμοποίηση ενός αλγορίθμου , όπου τα δεδομένα μετασχηματίζονται σε κωδικοποιημένη μορφή πριν αποθηκευτούν ή αποσταλούν μέσω τηλεπικοινωνιακών γραμμών προς το κεντρικό ή άλλο σύστημα. Ο λήπτης της κρυπτογραφημένης πληροφορίας πρέπει να κατέχει τον αλγόριθμο αποκρυπτογράφησης για να μπορέσει να την αναγνωρίσει . Η κρυπτογράφηση θεωρείται ένα σημαντικό εργαλείο που προστατεύει τις πληροφορίες εμπιστευτικού χαρακτήρα. Τα μέτρα που διασφαλίζουν τη μέθοδο της κρυπτογράφησης είναι τα εξής:

- Η τακτική αλλαγή των κωδικών πρόσβασης
- Η χρησιμοποίηση αριθμητικών συστημάτων ελέγχου
- Η αναβάθμιση της γνησιότητας του λογισμικού
- Η παρακολούθηση των υπαλλήλων
- Η τήρηση λογιστικών αρχών και

- Η τακτική επιθεώρηση λογαριασμών μετρητών για μικρέ απώλειες , γιατί τα λογιστικά μικρά λάθη στους φακέλους του Η/Υ , χρησιμεύουν σαν καλοί δείκτες ότι κάποιος έχει εισέλθει στους λογαριασμούς .

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία .Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιοδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης , αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό , μέχρι να αποκρυπτογραφηθεί .

Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρήσουν την πληροφορία ασφαλή .Μια παραδοσιακή μέθοδος κρυπτογράφησης είναι η συμμετρική κρυπτογραφία η οποία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί με το ίδιο κλειδί. Το κλειδί θα πρέπει να παραμείνει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα σε πολλούς χρήστες και τις αυξημένες απαιτήσεις

αποκρυπτογράφηση. Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά . Το δημόσιο κλειδί είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ,ενώ το της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κλπ) Η ασύμμετρη κρυπτογραφία (ή κρυπτογραφία δημόσιου κλειδιού –pubic key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και να το κατέχει. Για να επιτευχθεί η εμπιστευτικότητα , ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη (που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί).

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημόσιου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια που αν κάποιος γνωρίσει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει τα άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευση της. Η διαφοροποίηση από την κρυπτογράφηση , έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και της επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού. Με την εφαρμογή της συνάρτησης καταμερισμού , από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η σύνοψή του, η οποία είναι μια σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits) . Η σύνοψη του μηνύματος είναι μια ψηφιακή αναπαράσταση του μηνύματος είναι μοναδική για το μήνυμα και το αντιπροσωπεύει .

Η συνάρτηση καταμερισμού είναι μονόδρομη , διότι από τη σύνοψη που δημιουργεί , είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης παράγει μια διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοση του έχει αλλοιωθεί. Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

- Η ηλεκτρονική υπογραφή, είναι ένα άλλο αντικείμενο που αφορά την ασφάλεια των πληροφοριών. Στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική σε κάθε μήνυμα. Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο

ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για αν κρυπτογραφήσει το μήνυμα , πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την. [60] ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφεί μπορεί να πλαστογραφηθεί , εάν ο δικαιούχος του ιδιωτικού κλειδιού δε το έχει υπό τον π

- πλήρη έλεγχό του (π.χ. χάσει το μέσο που έχει αποθηκευτεί το ιδιωτικό κλειδί). Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει 2 διαδικασίες : Τη δημιουργία της υπογραφής και την επαλήθευσή της

Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού δημιουργεί τη σύνοψη του μηνύματος που θέλει να στείλει . Ανεξάρτητα από το μέγεθος του μηνύματος αυτό που θα παραχθεί θα είναι μια συγκεκριμένου μήκους σειρά ψηφίων
2. Με το ιδιωτικό του κλειδί ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι μια σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η κρυπτογραφημένη σύνοψη προσαρτάται στο κείμενο και το μήνυμα με ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου .

Παραλήπτης

1. ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή
2. εφαρμόζοντας το μήνυμα που έλαβε στον ίδιο αλγόριθμο καταμερισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα , την κρυπτογραφημένη σύνοψη του μηνύματος .

4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί.

Η έννοια της κρυπτογράφησης και της ψηφιακής υπογραφής σχετίζονται με την απάτη μέσω ηλεκτρονικού ταχυδρομείου ή τοποθεσίας web το λεγόμενο ηλεκτρονικό ψάρεμα.

Μια άλλη έννοια που αφορά την προστασία του ηλεκτρονικού εγκλήματος είναι η ιδιωτικότητα . Όταν κάποιος άλλος χρησιμοποιεί μια τυπική εφαρμογή ηλεκτρονικής επεξεργασίας κειμένου, συνήθως δε σκέπτεται αν κάποιος βρίσκεται κοντά του και παρακολουθεί το κείμενο που παράγεται. Οι περισσότεροι χρήστες Η/Υ χρησιμοποιούν το διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου για επαγγελματικούς και προσωπικούς σκοπούς . Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου και του διαδικτύου και ειδικά συστήματα που αναφέρονται ως εξυπηρετητές διεκπεραιώνουν τις απαιτήσεις υπηρεσιών των χρηστών. Οι εξυπηρετητές διατηρούν δεδομένα των χρηστών που επισκέπτονται για διάφορους λόγους , όπως καλύτερη και γρηγορότερη παροχή υπηρεσίας την επόμενη φορά που

διάθεση του διαχειριστή των συστημάτων αυτών , τόσο για ανάγνωση όσο και για επεξεργασία . Η χρήση του διαδικτύου και του ηλεκτρονικού θα ζητηθούν οι ίδιες υπηρεσίες , διευκόλυνση των χρηστών στον τρόπο πρόσβασης στις υπηρεσίες αυτές κ.α. Τα στοιχεία αυτά διατηρούνται αποθηκευμένα για σημαντικό χρονικό διάστημα σε αρχεία καταγραφής (log files) τα οποία είναι στη ταχυδρομείου είναι δύο από τις πολλές υπηρεσίες που προσφέρονται σήμερα στους διάφορους χρήστες και μέσω των οποίων αυτοί αφήνουν εν αγνοία τους σημαντικό αριθμό των προσωπικών τους

δεδομένων, με αποτελέσματα να παραβιάζεται η ιδιωτικότητά τους. Κατά πόσο όμως γνωρίζουν οι σημερινοί χρήστες τον κίνδυνο της αποκάλυψης όλων αυτών των δεδομένων, των προσωπικών τους δεδομένων , σε τρίτους μη έμπιστους για αυτούς χρήστες; Η ιδιωτικότητά ως ένα ζήτημα κοινωνικό και νομικό, απασχόλησε κοινωνικούς επιστήμονες, φιλόσοφους και νομικούς . Με την αξιοποίηση Η/Υ , τα σύγχρονα πληροφοριακά συστήματα και τα δίκτυα επικοινωνιών , η ιδιωτικότητά των χρηστών κινδυνεύει.

- Οι τρόποι που θα πρέπει η ιδιωτικότητά να προστατεύεται σε μια δημοκρατική κοινωνία.
- Θέσπιση νόμων για την ιδιωτικότητά και την προστασία δεδομένων
- Εφαρμογών τεχνολογιών ενίσχυσης της ιδιωτικότητας που επιλέγονται και εφαρμόζονται από τους χρήστες .
- Εκπαίδευση των χρηστών και των επαγγελματιών πληροφόρησης σε θέματα ιδιωτικότητας
- Τήρηση επιχειρησιακών κανονισμών (κώδικες δεοντολογίας) που αφορούν σε πρακτικές εφαρμογής και υλοποίηση της ιδιωτικότητας .

5.3 Μέτρα προστασίας κατά την πρόσβαση στο διαδίκτυο[64]

Καθημερινά όλο και περισσότεροι άνθρωποι έχουν πρόσβαση στο διαδίκτυο αφού μέσω αυτού υπάρχουν τεράστιες δυνατότητες επικοινωνίας και πληροφόρησης με

σκοπό να ενημερώνονται για οτιδήποτε τους ενδιαφέρει, να ψάχνουν και να βρίσκουν πληροφορίες και αυτό γίνεται και μία καθημερινή συνήθεια για πολλούς χρήστες του διαδικτύου χωρίς όμως να λαμβάνουν υπόψη τους κινδύνους που μπορεί να προκύψουν από τη χρήση του διαδικτύου, έτσι κατά την πλοήγηση των χρηστών στο διαδίκτυο καλό είναι να λαμβάνονται ορισμένα μέτρα ασφαλείας. Ωστόσο, θα πρέπει να αποφεύγεται:

- η αποκάλυψη των προσωπικών ευαίσθητων δεδομένων σε τρίτους.
- να μην υπάρχει εμπιστοσύνη σε e-mail ή ιστοσελίδες που δεν έχουν αποδείξει την ταυτότητά τους.
- να αποφεύγεται η συμπλήρωση φορμών με οικονομικά στοιχεία, αριθμό ταυτότητας , αριθμό φορολογικού μητρώου, ημερομηνία γεννήσεως και λοιπά προσωπικά στοιχεία καθώς και η αποστολή τους μέσω ηλεκτρονικού ταχυδρομείου χωρίς να είναι κρυπτογραφημένες.

- να αποφεύγεται η επίσκεψη σε ύποπτα sites.
- όσο για τις on-line συναλλαγές, οι χρήστες θα πρέπει να βεβαιώνονται ότι το ηλεκτρονικό κατάστημα συναλλάσσονται είναι αξιόπιστο (ψηφιακά υπογεγραμμένο από κάποιο ανεξάρτητο φορέα ή αρχή πιστοποίησης), έχει καλή φήμη και εφαρμόζει μηχανισμού ς ασφαλείας όπως κρυπτογραφημένη επικοινωνία μέσω του πρωτοκόλλου SSL (Secure Socket Layer).

- εφόσον κριθεί αναγκαία η χρησιμοποίηση κάποιας οικονομικής κάρτας, καλό είναι αυτή η χρήση να γίνεται μέσω χρεωστικών καρτών ή προπληρωμένων πιστωτικών καρτών.
- οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί όσον αφορά τις πληροφορίες που αποκαλύπτουν. Υπάρχουν μέθοδοι υποκλοπής προσωπικών δεδομένων που δεν στηρίζονται σε τεχνολογικές αδυναμίες αλλά στην ικανότητα ενός επίδοξου hacker να αντλήσει προσωπικά στοιχεία από έναν ανυποψίαστο χρήστη πιο διάσημος hacker που χρησιμοποίησε τέτοιες μεθόδους είναι ο Kevin mitnick ο οποίος μέσω της πειθούς κατάφερνε να αποκαλύπτει ονόματα χρήσης (user names) και κωδικούς (passwords) από ανυποψίαστους χρήστες όπως γραμματείς και τεχνικούς.

5.4 Μέτρα προστασίας επιχειρήσεων(ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ)

Τίποτα δεν μπορεί να εξασφαλίσει απόλυτη προστασία από τους κινδύνους που συνεπάγεται η πλοήγηση στο Internet καθιστώντας την αναζήτηση ασφάλειας του Η/Υ
μια όλο και πιο περίπλοκη υπόθεση όχι μόνο για τους μεμονωμένους χρήστες του Διαδικτύου αλλά ακόμη και για τις επιχειρήσεις, ανεξαρτήτου μεγέθους. Τα μέτρα που μπορεί να πάρουν οι επιχειρήσεις για να αντιμετωπίσουν τους κινδύνους του διαδικτύου είναι:

- Ενημέρωση: Είναι δυνατή η παρακολούθηση δικτυακών τόπων με προγράμματα προστασίας και εγγραφή σε mailing list όπου μπορεί κανείς να ενημερωθεί μέσω ηλεκτρονικού ταχυδρομείου για τις νέες απειλές. Είναι βασικό να γνωρίζουν οι χρήστες τους κινδύνους πριν διαδοθούν ευρέως. Έτσι είναι σε θέση να τις αντιμετωπίζουν αποτελεσματικότερα.

[64]https://electroniccrime.wordpress.com/category

- Επιλογή <<δύσκολων>> συνθημάτων: Όταν τα συνθήματα και οι διάφοροι κωδικοί πρόσβασης είναι συνηθισμένοι και απλό να βρεθούν, οι hackers μπορούν εύκολα να εισβάλλουν στα υπολογιστικά συστήματα. Ένα ιδανικό και ασφαλές σύνθημα μπορεί να είναι ο συνδυασμός συμβόλων και αριθμών.

- Συχνή εναλλαγή συνθήματος: Με το εναλλάσσονται περιοδικά τα συνθήματα, ακόμη και να το βρουν οι hackers ,ήδη η επιχείρηση θα χρησιμοποιεί καινούργιο.
- Βεβαίωση ότι το υπάρχον πρόγραμμα προστασίας που υπάρχει έχει ενημερωθεί:
Οι εταιρίες λογισμικού προσφέρουν ανανεώσεις και συμπληρώματα στα προγράμματα ασφαλείας[61] που παρέχουν ώστε να είναι αντιμετωπίσιμοι οι νέοι κίνδυνοι. Οι επιχειρήσεις θα πρέπει τακτικά να ελέγχουν το πρόγραμμα ασφαλείας που διαθέτουν και να το ανανεώνουν για να μπορεί να αντιμετωπίζει τις απειλές που εμφανίζονται.

- Δοκιμή υπάρχοντος συστήματος για αδυναμίες: Η πραγματοποίηση τακτικών δοκιμών για τυχόν αδυναμίες του συστήματος μπορεί να γίνει τόσο μέσα από το δίκτυο της
εταιρίας όσο και με τα εργαλεία που μπορούν να βρεθούν στο Διαδίκτυο. Για παράδειγμα, είναι δυνατόν με ένα πρόγραμμα που <<σπάει>> συνθήματα να φανεί αν πρέπει να αλλαχθούν τα συνθήματα πρόσβασης των χρηστών της εταιρίας.
- Εκπαίδευση υπαλλήλων: Οι υπάλληλοι της επιχείρησης πρέπει να κατανοήσουν πόσο σημαντικό είναι εταιρικά στοιχεία και πληροφορίες να παραμένουν στα όρια της επιχείρησης και να μην κυκλοφορούν ευρέως στο Διαδίκτυο. Ακόμη θα πρέπει να εκπαιδευθούν για να μην ανοίγουν συννημένα αρχεία (file attachments) από πηγές που δεν γνωρίζουν, τα οποία αποτελούν το συνηθέστερο τρόπο να εισέλθει ένας ιός στον υπολογιστή.
- Ενημέρωση των προγραμμάτων και του λειτουργικού συστήματος: Μέσω της εγκατάστασης των τελευταίων ενημερώσεων και της ενημέρωσης προγραμμάτων και λειτουργικού συστήματος, τα υπολογιστικά συστήματα γίνονται πιο σταθερά άλλα και οι νέες συμπληρώσεις στα ήδη υπάρχοντα προγράμματα ασφαλείας λειτουργούν καλύτερα.
- Αντί-ίικά παντού: Όλα τα υπολογιστικά συστήματα, από τους φορητούς υπολογιστές μέχρι τους εξυπηρετητές (server) της επιχείρησης θα πρέπει να προστατεύονται από ιούς.

- Προστασία συστημάτων ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί η επιχείρηση: Η επιχείρηση έχει την δυνατότητα να επιλέξει σύστημα e-mail που μπορεί να <<μπλοκάρει>> ιούς που τυχόν περιέχονται σε mail που λαμβάνει.
- Δημιουργία εταιρικής πολιτικής ασφάλειας: Η καταγραφή της πολιτικής ασφαλείας της επιχείρησης και η ανανέωση της ανά τακτά χρονικά συστήματα μπορεί να ανταποκρίνεται καλύτερα σε νέες απειλές που προκύπτουν.

5.5 Προστασία των domain names

Η προστασία των domain names[65] προέρχεται ανάλογα με το περιεχόμενο του δεύτερου μέρους. Αν τη διαδικτυακή διεύθυνση αποτελεί ένα όνομα , τότε παρέχετε η

[64]https://electroniccrime.wordpress.com/category
[65]www.en.wikipedia.org/wiki/Domain_name.gr.

προστασία των άρθρων 57 και 58 ΑΚ . Αν πρόκειται για εμπορική επωνυμία , δηλαδή

με ένα όνομα με το οποίο ο έμπορος διαλέγει τις συναλλαγές του ή για διακριτικό τίτλο τότε μαζί με την προστασία του άρθρου 58 ΑΚ παρέχεται και η προστασία του άρθρου 13 του νόμου 146/1914 . Εφαρμόζεται κι όταν ένα domain name αποτελεί εικονικό κατάστημα που είναι γνωστό και επικρατεί στις ηλεκτρονικές συναλλαγές. Αν η ηλεκτρονική διεύθυνση ταυτίζεται με το σήμα και υπάρχει κίνδυνος σύγχυσης στις συναλλαγές παρέχεται η προστασία των άρθρων 4, 18 και 26 του νόμου 2239/1994 περί σημάτων .

5.6 Προστασία δεδομένων από ιούς[66]

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

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

5.7 Προστασία δεδομένου προσωπικού χαρακτήρα

Προσωπικά δεδομένα σύμφωνα με το νόμο 2472/1997 και την οδηγία 95/46/ΕΚ είναι κάθε πληροφορία που αναφέρετε στο πρόσωπο του κάθε ατόμου και το επάγγελμα του ατόμου , η οικογενειακή του κατάσταση , η ηλικία του, ο τόπος κατοικίας του, η φυλετική του προέλευση , τα πολιτικά του φρονήματα , η θρησκεία που πιστεύει , οι φιλοσοφικές του απόψεις η συνδικαλιστική του δράση , η υγεία του , η ερωτική του ζωή , και τυχόν ποινικές του διώξεις και καταδίκες.

Για την επεξεργασία και τη συλλογή προσωπικών δεδομένων είναι απαραίτητη άδεια από την αρχή προστασίας προσωπικών δεδομένων . Οι οδηγίες για τη χορήγηση άδειας επεξεργασίας αναλύονται στην κανονιστική πράξη 1/1999 ΑΠΠΔ σχετικά με την ενημέρωση υποκειμένων των δεδομένων κατ' άρθρο 11 Ν. 2472/1997και στην απόφαση 408.1998ΑΠΠΔ σχετικά με την ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα 'ίδιου τύπου.

Η συγκέντρωση και η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί έναν από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική σφαίρα και στην ιδιωτική ζωή των ατόμου. Κάθε δραστηριότητα του σύγχρονου ανθρώπου γίνεται καθημερινά αντικείμενο επεξεργασίας και ανάλυσης γεγονός που χρήζει αντιμετώπισης και νομικής κατοχύρωσης .

[66] Ηλεκτρονικό Έγκλημα - Ελληνική Αστυνομία www.astynomia.gr

Στην Ελλάδα και στην Ευρώπη ισχύουν πολλά νομοθετήματα που προστατεύουν τους πολίτες από την επεξεργασία προσωπικών δεδομένων σε διάφορους τομείς . Έτσι έχουμε :

Τον νόμο 2274/1999 , την οδηγία 97/66/ΕΚ , και την σύσταση 558.2003 που αναφέρονται στην ιδιωτική ζωή στον τηλεπικοινωνιακό τομέα. Την υπουργική απόφαση 80329.2003 , την οδηγία 2002 .58.ΕΚ , την σύσταση R(99)5 , το ψήφισμα 2003. C48 και τη σύσταση 2003.203 που αναφέρονται στην προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και συναλλαγές .

Όμως ισχύουν και γενικότερου περιεχομένου νομοθετήματα που είτε συστήνουν αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων όπως είναι στην Ελλάδα ¨η αρχή προστασίας προσωπικών δεδομένων ¨ (νόμος 2472/1997) και ¨αρχή διασφάλισης απορρήτου¨ (νόμος 3115.2003) και στην Ευρώπη ¨ο ευρωπαϊκός επόπτης προσωπικών δεδομένων¨ (απόφαση 1247.2002.ΕΚ) είτε ρυθμίζουν τη διαβίωση προσωπικών δεδομένων από την κοινότητα σε άλλες χώρες (απόφαση 2003.490, απόφαση του συμβουλίου 2004/644/ΕΚ)

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

5.8 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΟ Spam [67]

- Να μην απαντάτε ποτέ σ 'ένα spam e-mail και να μην κάνετε πουθενά κλικ, γιατί απλούστατα η απάντησή σας ή και η άρνησή σας θα επιβεβαιώσει την εγκυρότητα του δικού σας e-mail και έτσι το e-mail σας θα γίνει μία πολύτιμη πληροφορία για πολλούς spammers.
- Να έχετε μια πρόχειρη και μη συχνά χρησιμοποιούμενη ηλεκτρονική διεύθυνση, εκτός φυσικά από την κανονική, και να την δίνετε σε πρώτη ζήτηση έτσι ώστε να πηγαίνουν εκεί όλα τα ανεπιθύμητα e-mails.
- Αναζητήστε και εγκαταστήστε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails. Να ελέγχετε πάντα αν αυτά τα προγράμματα-φίλτρα κάνουν σωστά το μπλοκάρισμα των spam e-mails.
- Να μην κάνετε ποτέ προώθηση(forward) των spam e-mails σε φίλους ή και τρίτους, γιατί και αυτοί θα προστεθούν στην λίστα αποδοχής.
- Να μην παρασύρεστε ποτέ από δελεαστικούς τίτλους, όπως a very special message for you, earn money easily, urgent and confidential κ.ά.
- Να μην δημοσιεύεται την διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail).Η ύπαρξη της ηλεκτρονικής διεύθυνσης σε μια ιστοσελίδα, είναι σχεδόν σίγουρο ότι σύντομα θα φέρει πολλά μηνύματα spam στο γραμματοκιβώτιο σας.
- Να μην δίνετε εύκολα την διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail).

[67] http://www.e-crime.gr/p/1.html

Πρέπει να είστε προσεκτικοί όταν επισκεπτόσαστε διάφορους δικτυακούς τόπους και ζητείται η συμπλήρωση προσωπικών στοιχείων και στοιχείων επικοινωνίας, όπως είναι το e-mail. Θα πρέπει να διαβάσετε προσεκτικά τους όρους χρήσης και την πολιτική εχεμύθειας για την οποία δεσμεύεται ο δημιουργός της ιστοσελίδας.

- Να μην απαντάτε ποτέ στα spam e-mails ακόμα και στην υποτιθέμενη ένδειξη διαγραφής, γιατί έτσι διαπιστώνεται η εγκυρότητα της ηλεκτρονικής μας διεύθυνσης και επομένως θα αποτελούμε πολύτιμο στόχο για τους spammers.
- Να χρησιμοποιείται ειδικά προγράμματα-φίλτρα.

5.9 Συμβουλές για ασφαλείς οικονομικές συναλλαγές

Βασικές οδηγίες [68]

Καθώς το φαινόμενο της οικονομικής απάτης φαίνεται να έχει μεγαλώσει στην χώρα μας αφού σύμφωνα με τα στοιχεία που εξέδωσε η safe line βρίσκεται στην τρίτη θέση το φαινόμενο αυτό με ποσοστό 18% και αφόρα όλους διότι μπορεί κανείς εύκολα να πέσει θύμα από κάποιον επιτήδειο με πολλούς τρόπους όπως ψαρέματος κτλ. Οι οικονομικές απάτες είναι ένα μεγάλο ζήτημα και αφόρα όλο τον κόσμο που ασχολείται με το διαδίκτυο ακόμη και επιχειρήσεις και τράπεζες, ωστόσο ας δώσουμε κάποιες συμβουλές που πρέπει να προσέχουμε όλοι για να κάνουμε οικονομικές συναλλαγές μέσω διαδικτύου με ασφάλεια.

1.Αποφεύγετε να πραγματοποιείτε οικονομικές συναλλαγές μέσω διαδικτύου από internet cafe, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές. Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είναι βέβαιοι για το επίπεδο ασφάλειας.

2.Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείτε για τις διαδικτυακές συναλλαγές:
Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί.
Αποφεύγετε να χρησιμοποιείται ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα.
Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπής τους θα διευκολύνετε πολύ τους δράστες.
Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μία κάρτες σας.
Μην δίνετε τον κωδικό πρόσβασης σας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, μην τον δώσετε. Οι τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την αστυνομία.

3.Επικοινωνήστε με την τράπεζα σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία internet banking.

[68]http://www.astynomia.gr

4.Απενεργοποιήστε τη λειτουργία <<Αυτόματης Καταχώρησης>> του προγράμματος περιήγησης.[69] Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή , γεγονός που τους καθιστά έκθετους.

5.Κάνετε αγορές μόνο από γνωστές εταιρείες που σας παρέχουν εγγυήσεις ασφάλειας. Αν κάνετε συχνά αγορές από το διαδίκτυο, χρησιμοποιείτε μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.

6.Φροντίστε να διατηρείτε σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας..
Ειδικότερα:

Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείστε και κυρίως τις <<επιδιορθώσεις ασφαλείας>>. Πρόκειται για προγράμματα που εκδίδουν οι εταιρείες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείτε και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοσή του. Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές <<εισβολές>> που θα δεχτείτε κατά τις περιηγήσεις σας στο διαδίκτυο. Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.

7.Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου (e-mails):
Μην ανοίγετε τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι.
Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό σας.
Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μην στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μιας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail).Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.

8.Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζετε για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων.
Ειδικότερα:
Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και ειδοποιείστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά. Φροντίστε να καταστρέφετε όσα έγγραφα δεν σας χρειάζονται πλέον, όπως οι πιστωτικές και τραπεζικές κάρτες που ακυρώνετε, τα αντίγραφα των λογαριασμών σας ακόμα και τις αποδείξεις που λαμβάνετε από τα Α.Τ.Μ

[69]http://www.astynomia.gr

5.10 Επιπτώσεις του ηλεκτρονικού εγκλήματος

Ιδιαίτερη ανησυχία έχει προκαλέσει το ηλεκτρονικό έγκλημα[70,71] στους χρήστες του διαδικτύου, όπως χαρακτηριστικά δείχνει έρευνα του ευρωβαρομέτρου που δημοσιεύτηκε πρόσφατα [15].

Οι ευρωπαίοι πολίτες, κατά ποσοστό 76%, εκτιμούν ότι ο κίνδυνος να πέσει κανείς θύμα ηλεκτρονικού εγκλήματος αυξήθηκε το 2013 σε σχέση με το 2012. Εξάλλου, το 12% των χρηστών του Διαδικτύου έχει ήδη πέσει θύμα παραβίασης του λογαριασμού τους στα μέσα κοινωνικής δικτύωσης ή του ηλεκτρονικού τους ταχυδρομείου. Οι χρήστες του Διαδικτύου στην ΕΕ έχουν, σε ποσοστό 70%, εμπιστοσύνη στην ικανότητά τους να χρησιμοποιούν το Διαδίκτυο για αγορές ή τραπεζικές συναλλαγές, αλλά μόνο το 50% εξ αυτών επιλέγει τελικά να το χρησιμοποιήσει, λόγω των κινδύνων να πέσει θύμα ηλεκτρονικού εγκλήματος.

Οι δύο κύριες ανησυχίες σχετικά με τέτοιου είδους διαδικτυακές δραστηριότητες σχετίζονται με την κακή χρήση των προσωπικών δεδομένων (37% των ερωτηθέντων) και την ασφάλεια των πληρωμών μέσω του διαδικτύου (35%).

Η έρευνα αυτή δείχνει τις καταστροφικές επιπτώσεις του ηλεκτρονικού εγκλήματος στη χρήση του Διαδικτύου, καθώς πάρα πολλοί επιλέγουν να μην κάνουν χρήση όλων των δυνατοτήτων που προσφέρει. Αυτό βλάπτει τόσο την ψηφιακή οικονομία όσο και τις διαδικτυακές δραστηριότητες. Πρέπει να ενισχυθεί η συνεργασία, ώστε να φθάσουν οι αρχές στις ρίζες του οργανωμένου ηλεκτρονικού εγκλήματος. Πάντως, σύμφωνα με την κοινοτική δημοσκόπηση, όλο και περισσότεροι πολίτες της ΕΕ αισθάνονται ότι είναι καλά ενημερωμένοι για τους κινδύνους του ηλεκτρονικού εγκλήματος σε σχέση με το 2012 (44% έναντι 38%). Ωστόσο, φαίνεται ότι δεν συνάγουν πάντα όλα τα αναγκαία συμπεράσματα από τις σχετικές πληροφορίες.

Για παράδειγμα, λιγότεροι από τους μισούς χρήστες του διαδικτύου άλλαξαν κωδικό πρόσβασης στο διαδίκτυο κατά το προηγούμενο έτος (48% σε σύγκριση με 45% το 2012). Η έρευνα του Ευρωβαρομέτρου, στην οποία συμμετείχαν πάνω από 27.000 άτομα σε όλα τα κράτη μέλη, δείχνει επίσης ότι το 87% των ερωτηθέντων αποφεύγουν να αποκαλύπτουν προσωπικά δεδομένα στο διαδίκτυο. Οι περισσότεροι

[70]http://www.newsbeast.gr/technology/arthro/612029/oi-apeiles-kai-oi-epiptoseis-tou-

[71] ilektronikou-eglimatos-sti-hrisi-tou-diadiktuou

χρήστες εξακολουθούν να μην αισθάνονται καλά ενημερωμένοι σχετικά με τους κινδύνους του ηλεκτρονικού εγκλήματος, ενώ το 7% έχουν πέσει θύμα διαδικτυακής απάτης σε σχέση με την πιστωτική τους κάρτα ή τον τραπεζικό τους λογαριασμό.

ΚΕΦΑΛΑΙΟ 6

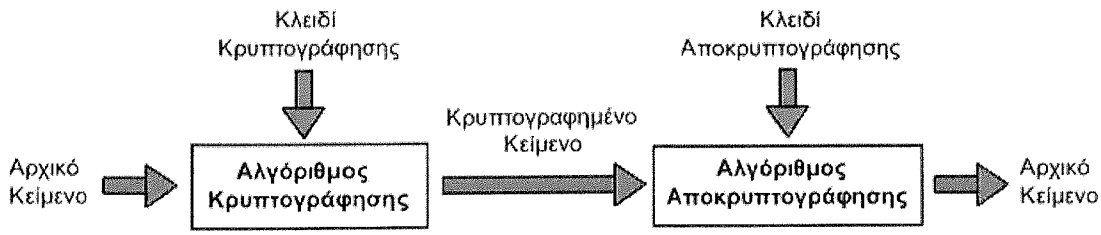
6.1 Κρυπτογραφία

Η κρυπτογραφία χρησιμοποιείται για να καλύψει την ανάγκη της εμπιστευτικότητας στο ηλεκτρονικό εμπόριο . Το κλειδί που χρησιμοποιεί είναι μια σειρά από bits συγκεκριμένου μήκους τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση .

Η κρυπτογραφία χωρίζεται στη συμμετρική κρυπτογραφία και στην ασύμμετρη κρυπτογραφία. Στην πράξη συνδυάζονται έτσι ώστε να χρησιμοποιούνται τα καλύτερα χαρακτηριστικά κάθε μεθόδου.

6.2 Κρυπτανάλυση

Η κρυπτανάλυση είναι η μελέτη για την επινόηση μεθόδων που εξασφαλίζουν την κατανόηση του νοήματος της κρυπτογραφημένης πληροφορίας, έχοντας ως άγνωστες ποσότητες τον κρυφό μετασχηματισμό, το κλειδί, με βάση το οποίο αυτός πραγματοποιήθηκε και το κρυπτογραφημένο μήνυμα. Βασικός στόχος της είναι, ανάλογα με της απαιτήσεις του αναλυτή κρυπτοσυστημάτων ή αλλιώς κρυπταναλυτή, να βρει το κλειδί, το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθά να αναγνώσει το (κρυφό) μήνυμα. (πηγή:wikipedia)



Ένα τυπικό σύστημα κρυπτογράφησης-αποκρυπτογράφησης , σχήμα 6.2

[72] http://el.wikipedia.org/wiki σχήμα 6.2

[73] Σημειώσεις κυρίου Αναγνωστάκη Καθηγητής Εφαρμογών Πληροφορικής Τμήμα Λογιστικής - Σχολή Διοίκησης και Οικονομίας - ΤΕΙ Ηπείρου

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με την βοήθεια ενός αλγόριθμου (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επι το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριεται σε bits. Γενικά ισχύει ο εξής κανόνας : όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Βασικές έννοιες

Ο αντικειμενικός στόχος της κρυπτογραφίας[74] είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω τον Κώστα και τη Βασιλική, να επικοινωνήσουν από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης-αποκρυπτογραφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων.
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος.
- Το E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση.
- Το D είναι η αντίστροφη συνάρτηση ή μετασχηματισμος αποκρυπτογράφησης.

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο P

6.3Κρυπτογράφηση (encryption)

ονομάζεται η διαδικασία μετασχηματισμού ενός μηχανήματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγόριθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη .

6.4 **Κρυπτογραφικός αλγόριθμος (cipher)**

είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

[74] Σημειώσεις κυρίου Αναγνωστάκη Καθηγητής Εφαρμογών Πληροφορικής Τμήμα Λογιστικής – Σχολή Διοίκησης και Οικονομίας - ΤΕΙ Ηπείρου

6.5 Μειονεκτήμα συμμετρικής κρυπτογραφίας [76]

- Ο αποστολέας και ο παραλήπτης γνωρίζουν το ίδιο μυστικό κλειδί
- Το κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση
- Θεωρείται γρήγορη και αποδοτική μέχρι ενός ορίου
- Προβληματική διαχείριση κλειδιών πάνω από δημόσια δίκτυα με πληθώρα χρηστών
- Αυθεντικότητα
- Αποποίηση ευθύνης

6.6 Αλγόριθμοι συμμετρικής κρυπτογράφησης

- DES
- 3DES
- AES
- RC2
- RC4
- RC5
- IDEA

6.7 Ασύμμετρη κρυπτογραφία

- Χρησιμοποιεί 2 κλειδιά ένα για την κωδικοποίηση και ένα για την αποκωδικοποίηση
- Δημόσιο κλειδί: είναι γνωστό σε όλους
- Ιδιωτικό κλειδί: παραμένει μυστικό
- Οποιοσδήποτε μπορεί να στείλει μήνυμα με το δημόσιο κλειδί αλλά το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί

[76] Σημειώσεις κυρίου Αναγνωστάκη Καθηγητής Εφαρμογών Πληροφορικής Τμήμα Λογιστικής – Σχολή Διοίκησης και Οικονομίας - ΤΕΙ Ηπείρου

- ❖ Ο αποστολέας στέλνει το μήνυμα του κρυπτογραφημένο με το δημόσιο κλειδί του παραλήπτη έτσι ώστε να παραμείνει εμπιστευτικό μέχρι να αποκρυπτογραφηθεί από τον παραλήπτη με το ιδιωτικό κλειδί του
- ❖ Ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί που μόνο αυτός το γνωρίζει (**αυθεντικότητα**)
- ❖ Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα της

6.8 Ασύμμετροι αλγόριθμοι [77]

- ❖ Ένας ασύμμετρος αλγόριθμος λειτουργεί ως μια μονόδρομη συνάρτηση (trap-door) δηλαδή είναι εύκολη η πραγματοποίηση μια λειτουργίας στην μια κατεύθυνση αλλά είναι δύσκολη ή αδύνατη η αντιστροφή της λειτουργίας
- ❖ Παράδειγμα: Είναι εύκολος ο πολλαπλασιασμός 2 ακεραίων αλλά είναι δύσκολο να βρεθούν οι αριθμοί που έδωσαν το γινόμενο αυτό. Αν από την άλλη όμως κάποιος γνωρίζει το γινόμενο και έναν από τους δύο αριθμούς τότε αποκαλύπτεται και ο άλλος αριθμός

6.9 Αλγόριθμοι ασύμμετρης κρυπτογράφησης

- ❖ Diffie-Hellman Key Exchange Algorithm
- ❖ RSA

6.10 Βήματα ασύμμετρης κρυπτογράφησης

- ❖ Ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας έναν κοινό αλγόριθμο κρυπτογράφησης και το ιδιωτικό του κλειδί.
- ❖ Στο αποτέλεσμα ο αποστολέας προσθέτει την ψηφιακή υπογραφή του και κρυπτογραφεί το συνολικό μήνυμα ξανά χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη.
- ❖ Ο παραλήπτης αποκρυπτογραφεί το μήνυμα που δέχεται χρησιμοποιώντας το δικό του ιδιωτικό κλειδί αποκαλύπτοντας την ταυτότητα του αποστολέα στο μήνυμα (**αυθεντικότητα**).

[77] Σημειώσεις κυρίου Αναγνωστάκη Καθηγητής Εφαρμογών Πληροφορικής Τμήμα Λογιστικής - Σχολή Διοίκησης και Οικονομίας - ΤΕΙ Ηπείρου

- ❖ Ο παραλήπτης αποκρυπτογραφεί το υπόλοιπο μήνυμα με το δημόσιο κλειδί του αποστολέα .
- ❖ Με αυτό τον τρόπο ο παραλήπτης διασφαλίζει ότι όποιος συνέθεσε το μήνυμα είχε πρόσβαση στο ιδιωτικό κλειδί του αποστολέα και ότι κανένας δεν τροποποίησε ή ανάγνωσε το μήνυμα κατά την διαδρομή

ΚΕΦΑΛΑΙΟ 7

ΠΑΡΑΔΕΙΓΜΑΤΑ

Πάνω από 40% των νέων έχουν απειληθεί μέσω internet για την προσωπική τους ζωή

Ιδιαιτέρως ανησυχητικά είναι τα αποτελέσματα έρευνας σχετικά με τους νέους και τις απειλές που δέχονται μέσα από τον κυβερνοχώρο. Η έρευνα διενεργήθηκε σε τελικό δείγμα 422 παιδιών ηλικίας 13-18 ετών (275 αγόρια και 147 κορίτσια) με ειδικά διαμορφωμένο έντυπο και ανώνυμο ερωτηματολόγιο με κριτήριο προεπιλογής τη χρήση του διαδικτύου το ελάχιστο μια φορά την εβδομάδα και ότι ο συμμετέχον έχει στην κατοχή του κινητό τηλέφωνο.
Τα αποτελέσματα που προκύπτουν από την έρευνα παρουσιάζονται στη συνέχεια του δελτίου και εμφανίζονται ως ποσοστό επί του συνολικού δείγματος ηλικίας 13 – 18ετών.
- 16% από τα αγόρια ηλικίας 13-18 ετών δηλώνουν ότι έχουν πέσει θύματα κυβερνοεκφοβισμού. Από αυτό το ποσοστό, το 9% δηλώνει ότι η πράξη έγινε μέσα από ιστοχώρο κοινωνικής δικτύωσης (BEBO, HI5, TWITTER), 6% δηλώνει ότι έγινε μέσω Instant Messaging Services και ένα 2% στο κινητό τους τηλέφωνο. - 32% είχαν δεχθεί εκφοβισμό με δημοσίευση στο διαδίκτυο προσωπικών τους φωτογραφιών, 11% λεκτικό – αποκάλυψη γεγονότων προσωπικού ενδιαφέροντος και ένα 3,5% δήλωσε ότι έγινε με χυδαίο λεξιλόγιο – ύβρεις. Ένα 10% των αγοριών απάντησε θετικά στην ερώτηση εάν έχουν εκφοβίσει μέσω διαδικτύου και νέων τεχνολογιών κάποιον συμμαθητή, φίλο ή γνωστό τους. Το πιο σημαντικό είναι ότι στο σύνολο του δείγματος ένα 42% απάντησε ότι ξέρουν ή έχουν ακούσει για κάποιον γνωστό που έχει πέσει θύμα εκφοβισμού μέσω διαδικτύου και νέων τεχνολογιών. Αναφορικά με το δείγμα των κοριτσιών τα ποσοστά ήταν λίγο πιο ψηλά με ένα 22%
να απαντά θετικά στο ότι έχει πέσει θύμα κυβερνοεκφοβιμού και ένα 9% να δηλώνει ότι γνώριζε τον εκφοβιστή του. Όταν ρωτήσαμε τα παιδιά αυτά να μας πούνε τους λόγους αυτού του φαινομένου το 13% μας απάντησε ότι έγινε για λόγους εκδίκησης, το 31% για να γελάσουνε και ένα 56% για δυσφήμιση. Η έρευνα διενεργήθηκε για λογαριασμό της οργάνωσης NEOI. Ο κυβερνοεκφοβισμός συνήθως γίνεται ανώνυμα και δεν περιορίζεται σε ηλικίες κάτω των 18 ετών. Η οργάνωση NEOI μέσα στα δύο χρόνια που ενεργά ενημερώνει για ηλεκτρονικούς κινδύνους έχει δεχθεί δεκάδες καταγγελίες από άτομα ηλικίας από 22 έως 45 χρόνων που έχουν πέσει θύματα εκφοβισμού στο διαδίκτυο. Η ψυχολόγος της οργάνωσης NEOI, κ. Όλγα Ζηκοπούλου αναφέρει: «Τα δεδομένα της παρούσας έρευνας, τα οποία συμφωνούν με τη διεθνή βιβλιογραφία, δείχνουν ότι

ο αριθμός των εφήβων που έχουν πέσει θύματα εκφοβισμού μέσω του διαδικτύου και της χρήσης νέων τεχνολογιών είναι σημαντικός.
Το γεγονός ότι παρουσιάζει μία αυξητική τάση καθιστά απαραίτητη την άμεση παρέμβαση για την πρόληψη και την αντιμετώπιση του προβλήματος. Με τη διάδοση της χρήσης του διαδικτύου και των ηλεκτρονικών μέσων επικοινωνίας από παιδιά σχολικής και εφηβικής ηλικίας ο εκφοβισμός δεν περιορίζεται πλέον στη σχολικήαυλή και στη γειτονιά. Δεν μπορούμε να πούμε με σιγουριά αν οι πιο «παραδοσιακές» μορφές του εκφοβισμού, που συναντώνται στα σχολεία, και οι πιο σύγχρονες μορφές, που διαπράττονται με τη χρήση των νέων τεχνολογιών, ταυτίζονται ή όχι, αλλά μπορούμε σίγουρα να εντοπίσουμε βασικές ομοιότητες και διαφορές. Το βασικό σημείο της διαφοράς τους είναι ότι οι νέες τεχνολογίες δίνουν εξαιρετική δύναμη σε αυτούς που επιλέγουν να διαπράξουν κάποια μορφή βίας μέσω αυτών, καθώς επιτρέπουν στα άτομα να αλλοιώσουν την ταυτότητά τους και να διατηρήσουν την ανωνυμία τους και αυτό συνήθως τα δίνει και τη δυνατότητα να γίνουν πιο σκληρά και επιθετικά. Επίσης, ο εκφοβισμός, μέσω της χρήσης των νέων τεχνολογιών, μπορεί να γίνει οποιαδήποτε στιγμή, σε οποιοδήποτε μέρος και μέσω της ταχύτατης διάδοσης, μπορεί να λάβει σε πολύ λίγο χρόνο πολύ μεγάλες διαστάσεις.
Ανεξάρτητα όμως από τις ομοιότητες και τις διαφορές, αυτό που είναι σημαντικό, και που αποδεικνύουν με απόλυτη σαφήνεια και συμφωνία τα ερευνητικά ευρήματα, είναι ότι τα παιδιά και οι έφηβοι, που με οποιοδήποτε τρόπο θυματοποιούνται από τους συνομηλίκους τους, βιώνουν κοινωνικο-συναισθηματικές δυσκολίες

παράδειγμα 1

Ασφαλής υπολογιστής είναι μόνο ο... κλειστός[78]

«Ιδιωτικός χώρος στο Ιντερνετ δεν υπάρχει», εξηγεί ο έμπειρος αστυνομικός και δίνει συμβουλές για το τι πρέπει να προσέχουν οι χρήστες του Διαδικτύου

Συνέντευξη στη Μαρία Ψαρά

Πριν από λίγα χρόνια, σε χώρα του εξωτερικού, η Αστυνομία κλήθηκε να αντιμετωπίσει τη δολοφονία ενός ασθενούς που λόγω σακχαρώδους διαβήτη νοσηλευόταν σε νοσοκομείο της χώρας. Υστερα από εντατικές έρευνες, εμβρόντητοι οι αστυνομικοί διαπίστωσαν πως ένας ανταγωνιστής του ασθενούς είχε πληρώσει χάκερ για να μπει στη βάση δεδομένων του νοσοκομείου και να... αλλάξει τα φάρμακα του άτυχου άνδρα... Ηταν η πρώτη δολοφονία μέσω Ιντερνετ, που συγκλόνισε την παγκόσμια κοινή γνώμη...

Το παραδοσιακό έγκλημα μετακομίζει στο Διαδίκτυο", εξηγεί ο επικεφαλής της Δίωξης Ηλεκτρονικού Εγκλήματος, Μανώλης Σφακιανάκης. Στη συνέντευξη που παραχώρησε στο FORUM, ο έμπειρος αστυνομικός υποδιευθυντής δηλώνει ότι "ιδιωτικός "χώρος" στο Ιντερνετ δεν υπάρχει", επιμένοντας ότι "δεν ξορκίζουμε το Ιντερνετ, αλλά γνωρίζουμε τους κανόνες του".

[78]http://cert.auth.gr/index.php/el/mnu-announce/101-interview-sfakianakis

παράδειγμα 2.

Σύλληψη παιδιάτρου στα Ιωάννινα

Στην Ελλάδα σχηματίστηκαν τρεις δικογραφίες και συνελήφθησαν τρία άτομα για κατοχή και διακίνηση πορνογραφικού υλικού ανάμεσα στα οποία και ο Βούλγαρος παιδίατρος στα Ιωάννινα.

«Κατά τη διάρκεια της επιχείρησης εντοπίσαμε συνολικά εβδομήντα επτά (78) χρήστες - δράστες, τα ηλεκτρονικά ίχνη των οποίων προκύπτουν σε τριάντα δύο (32) διαφορετικές χώρες του κόσμου. Πιο αναλυτικά, εκτός από τη χώρα μας, εντοπίσαμε ίχνη παιδόφιλων στη Γερμανία, Ρωσία, Η.Π.Α, Μεγάλη Βρετανία, Γαλλία, Πολωνία, Σουηδία, Κίνα, Τσεχία, Ιράν, Ολλανδία, Ιταλία, Ελβετία, Βραζιλία, Περού, Βενεζουέλα, Ουκρανία, Σαουδική Αραβία, Νότια Αφρική, Κολομβία και Γεωργία, Λίβανο, Σρι Λάνκα, Αυστραλία, Καναδάς, Πορτογαλία, Μεξικό, Μπαχάμες, Αυστρία, Σλοβενία και το Βέλγιο» τόνισε ο εκπρόσωπος Τύπου της ΕΛ.ΑΣ και πρόσθεσε: «Όσον αφορά στη χώρα μας, σχηματίσαμε τρεις αυτοτελείς δικογραφίες και συλλάβαμε με την αυτόφωρη διαδικασία στα Ιωάννινα και την Αττική τρία άτομα, από τα οποία δύο είναι ημεδαποί ηλικίας 34 και 25 ετών και ένας 47χρονος αλλοδαπός υπήκοος Βουλγαρίας.

»Σε βάρος τους ασκήθηκε ποινική δίωξη για πορνογραφία ανηλίκων, μέσω του διαδικτύου. Ειδικότερα, την 21-11-2013 μετά από διαδικτυακή έρευνα ταυτοποιήσαμε τη εγκληματική δράση 34χρονου ημεδαπού ο οποίος διακινούσε σκληρό παιδικό πορνογραφικό υλικό, μέσω ειδικού προγράμματος ανταλλαγής αρχείων PEER TO PEER (P2P), στο διαδίκτυο.

»Μετά από κατάλληλη αξιοποίηση των διαδικτυακών ευρημάτων και ιχνών του 34χρονου συλληφθέντα και σε συνεργασία με τις αρμόδιες Εισαγγελικές Αρχές, πραγματοποιήσαμε το χρονικό διάστημα από 28-11-2013 έως και 22-01-2014, στοχευμένη διαδικτυακή διεισδυτική έρευνα στο συγκεκριμένο πρόγραμμα ανταλλαγής αρχείων, με απώτερο στόχο την εύρεση και τον εντοπισμό και άλλων χρηστών, που κατείχαν και είχαν πρόσφορο προς διαμοιρασμό υλικό παιδικής πορνογραφίας.

»Επιπλέον, την 28-04-2014 συλλάβαμε στα Ιωάννινα το 47χρονο παιδίατρο, υπήκοο Βουλγαρίας. Σε έρευνα που πραγματοποιήθηκε στην οικία του, παρουσία Εισαγγελικού Λειτουργού, βρήκαμε αποθηκευμένα σε διάφορα ψηφιακά αποθηκευτικά μέσα, πλήθος αρχείων «σκληρού» υλικού παιδικής πορνογραφία. Ο παιδίατρος κατείχε κεντρικό ρόλο σε κλειστή ομάδα χρηστών του συγκεκριμένου προγράμματος ανταλλαγής αρχείων, τα μέλη της οποίας χρησιμοποιούσαν ιδιαίτερα τεχνάσματα, προγράμματα απόκρυψης ηλεκτρονικής ταυτότητας και κρυπτογράφησης, για να καλύπτουν την παράνομη δράση τους στο διαδίκτυο.

»Ακολούθως, την 25-04-2014 συλλάβαμε στην Αττική, τον 25χρονο, στο φορητό ηλεκτρονικό υπολογιστή του οποίου βρήκαμε αποθηκευμένα αρχεία (βίντεο και φωτογραφίες) με πορνογραφικό υλικό ανηλίκων» κατέληξε ο εκπρόσωπος Τύπου της ΕΛ.Α

παράδειγμα 3

Παραπλανητικά ηλεκτρονικά μηνύματα στο κινητό

Πρώτη ανάρτηση: 24/07/2013 Προσοχή: Τον κώδωνα του κινδύνου σε όλους τους πολίτες για παραπλανητικά ηλεκτρονικά μηνύματα στο κινητό στέλνει η Δίωξη Ηλεκτρονικού Εγκλήματος, με ανακοίνωση που εκδόθηκε από την ΕΛ.ΑΣ. Όπως έγινε γνωστό από την ανακοίνωση, το τελευταίο χρονικό διάστημα αποστέλλονται σε χρήστες κινητών τηλεφώνων sms για δήθεν κέρδη από διαγωνισμό, και συγκεκριμένα λοταρία, και ζητούν από τους «νικητές» να στείλουν ένα μήνυμα με προσωπικά στοιχεία στην διεύθυνση eurostakes@msn.com Όποιος κάνει το λάθος και επικοινωνήσει με τους επιτήδειους, μέσω του ηλεκτρονικού ταχυδρομείου, του ζητούν χρήματα για δήθεν προπληρωμή φόρων ή εξόδων εκταμίευσης των κερδών!

Σύμφωνα με την ανακοίνωση της αστυνομίας:

Ειδικότερα, το μήνυμα είναι γραμμένο στην αγγλική γλώσσα και αναφέρει: «Your Mobile Number has Won £1,500,000.00 in the Millions Mobile Award. To claim Funds, Kindly Email us: EML 424756, Your Name &Number to eurostakes@msn.com.

Παράδειγμα 4

Στις μέρες μας το διαδίκτυο έχει εξαπλωθεί σε μεγάλο βαθμό[75] και αυτό οφείλεται στις δυνατότητες πληροφόρησης και όχι μόνο. Για παράδειγμα ένα θέμα που αφορά όλους μας μέσω του διαδικτύου είναι κ οι οικονομικοί παράγοντες όπως απάτες (ηλεκτρονικό έγκλημα).

ΩΣΤΟΣΟ,ΠΛΑΣΤΟ EMAIL ΥΠΟΣΧΕΤΑΙ ΕΠΙΣΤΡΟΦΗ ΦΟΡΟΥ

Η διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας,

ενημερώνει τους χρήστες του διαδικτύου, ότι τις τελευταίες ημέρες παρατηρείται έξαρση αποστολής απατηλών μηνυμάτων ηλεκτρονικού ταχυδρομείου μεγάλο αριθμό χρηστών του διαδικτύου.

Με τα μηνύματα αυτά οι άγνωστοι δράστες προσπαθούν να εξαπατήσουν τους παραλήπτες, ώστε να τους αποσπάσουν ευαίσθητα προσωπικά δεδομένα και χρηματικά πόσα.

Ειδικότερα τα ανωτέρω μηνύματα ηλεκτρονικού ταχυδρομείου ενημερώνουν τους παραλήπτες, ότι έχουν επιστροφή φόρου εισοδήματος από το Υπουργείο Οικονομικών.

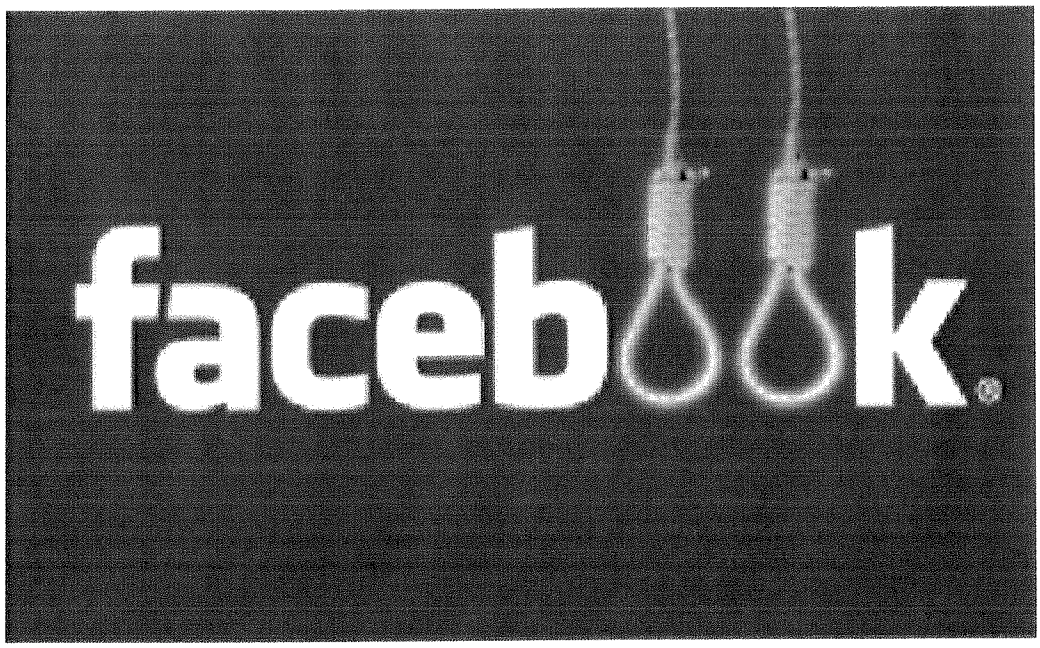
Στη συνέχεια, εφόσον ο παραλήπτης ανταποκριθεί, του ζητούν να καταχωρήσει σε ειδική φόρμα ευαίσθητες προσωπικές πληροφορίες όπως ονοματεπώνυμο, διεύθυνση κατοικίας ,αριθμό τηλεφώνου, αριθμό τραπεζικού λογαριασμού, ΑΦΜ, αριθμό πιστωτικής κάρτας κ.ά.

Επισημαίνεται ότι τα μηνύματα αυτά χρήζουν μεγάλη προσοχής, καθότι χρησιμοποιούν το λογότυπο Γενικής Γραμματείας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών και παρουσιάζονται εξαιρετικά αληθοφανή.

Καλούνται οι χρήστες που λαμβάνουν τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου να μην απαντούν να μην καταχωρούν και να μην στέλνουν προσωπικά δεδομένα καθότι σε καμιά περίπτωση δεν είναι αληθινά.

Επισημαίνεται ότι κανένας οργανισμός ή φορέας δεν ζητά πληροφορίες, όπως αριθμούς πιστωτικών καρτών, αριθμούς τραπεζικών λογαριασμών κ.α μέσω ηλεκτρονικού ταχυδρομείου.

[75]http://ipeirotika.gr/greece/item/4347-prosoxi-plasto-e-mail



Τα «μικρά γράμματα» του Facebook!

Το Facebook είναι ένα από τα πιο δημοφιλή social networking site (ιστοχώρος κοινωνικής δικτύωσης) παγκοσμίως. Το να είναι κανείς εγγεγραμμένος στο Facebook στην Ελλάδα, είναι MUST στις παρέες των νέων.

Χιλιάδες Νέοι και Νέες καθημερινά πλοηγούνται στις σελίδες του, δημιουργώντας προφίλ χρηστών, επικοινωνώντας με φίλους, προσθέτοντας προσωπικές λεπτομέρειες, αποθηκεύοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον τηλεφωνικό αριθμό του κινητού τους, προσωπικές φωτογραφίες, και πολλά άλλα προσωπικά δεδομένα.

Η ΜΚΟ **«Ν.Ε.Ο.Ι.»** (**Ν**έοι **Ε**υρωπαίοι **Ο**ργανωμένοι **Ι**κανοί) στην προσπάθειά της να ενημερώσει τους Νέους αναφορικά με τους κινδύνους του διαδικτύου, δέχτηκε το τελευταίο διάστημα πολλές ερωτήσεις από προβληματισμένους Νέους για τη διαφύλαξη των προσωπικών τους δεδομένων με την εγγραφή τους στο Facebook.

Οι περισσότεροι Νέοι δείχνουν «τυφλή» εμπιστοσύνη στην κοινότητα χρηστών του Facebook χρησιμοποιώντας το πραγματικό τους όνομα, διεύθυνση, ημερομηνία γέννησης, φωτογραφία κ.α., χωρίς προηγουμένως να έχουν διαβάσει τα «μικρά γράμματα» του Legal Notice (Όροι Χρήσης).

Σας παραθέτουμε μερικούς από τους βασικούς όρους που οι χρήστες πρέπει να γνωρίζουν ότι αυτομάτως συμφωνούν με την εγγραφή τους στο Facebook.

Οι όροι μπορούν να αλλάξουν οποτεδήποτε χωρίς προειδοποίηση. Αυτό είναι τυποποιημένο για έναν ιστοχώρο, αλλά στη συγκεκριμένη ιστοσελίδα, η δήλωση αυτή εμφανίζεται στις πρώτες σειρές, που σημαίνει ότι χρήστης αυτομάτως συμφωνεί και με όλες τις αλλαγές που μπορεί να γίνουν χωρίς προηγούμενη ενημέρωση.

Οι εφαρμογές δεν εγγυώνται την ασφάλεια. Οι χρήστες του Facebook που χρησιμοποιούν εφαρμογές που προέρχονται από τρίτους, δηλαδή quiz, παιχνίδια κ.α., πρέπει να γνωρίζουν ότι εάν οι προσωπικές τους πληροφορίες διαρρεύσουν μέσα από τα πρωτόκολλα ασφάλειας του Facebook, το Facebook ΔΕΝ φέρει καμία ευθύνη.

1. Αποποιείστε τα πνευματικά σας δικαιώματα. Το Facebook

αναπτύσσεται λόγω της πληρότητας των θέσεων που καταλαμβάνουν οι χρήστες του. Αυτό που πρέπει όμως να γνωρίζουμε είναι ότι ταχυδρομώντας οποιοδήποτε περιεχόμενο δίνουμε στο Facebook την άδεια να το χρησιμοποιήσει με όποιον τρόπο θέλει. Αναλυτικά μέσα στους όρους αναγράφεται το εξής:
«Με την ταχυδρόμηση περιεχομένου από εγγεγραμμένους χρήστες, από οποιαδήποτε περιοχή και μέρος, οι χρήστες χορηγούν αυτόματα και επιτρέπουν στην επιχείρηση Facebook, μια αμετάκλητη, διαρκή, μη αποκλειστέα , μεταβιβάσιμη, πλήρως πληρωμένη, παγκόσμια
πληρωμένη, παγκόσμια άδεια (με το δικαίωμα στο sublicense) να χρησιμοποιήσει, αντιγράψει, αποδώσει δημόσια, επιδείξει δημόσια, να επαναφορμάρει και να μεταφράσει, απόσπασμα (γενικά ή εν μέρει) και να διανείμει το περιεχόμενο χρηστών για οποιοδήποτε σκοπό σχετικά με τον ιστοχώρο ή την προώθησή του, να προετοιμάσεισχετικές παράγωγες εργασίες με τον ιστοχώρο, ή να ενσωματώσει άλλες, και να χορηγήσει και να εγκρίνει sublicenses των ανωτέρω.»Σε απλή γλώσσα, αυτό σημαίνει ότι οι χρήστες δεν ελέγχουν πλέον τα πνευματικά δικαιώματα του υλικού που εναποθέτουν στον ιστοχώρο του Facebook. Για παράδειγμα, εάν φορτώσετε μια φωτογραφία σας στο Facebook, πρέπει να γνωρίζεται με βάση όσα αναγράφονται στους όρους ότι το Facebook μπορεί να δημιουργήσει αντίγραφά της και να τα πουλήσει έναντι πληρωμής ή μη, σε τρίτους χωρίς την άδειά σας ως προωθητική ενέργεια. Εάν κρατάτε κάποια προσωπικά στοιχεία στο Facebook ή προσωπικές σκέψεις, το Facebook μπορεί να τις μετατρέψει σε βιβλίο, να δημιουργήσει αντίγραφα και να τα προωθήσει στην αγορά.

2. Η μυστικότητα δεν είναι εγγυημένη. Πριν δώσετε τα πραγματικά σας στοιχεία από ονοματεπώνυμο, διεύθυνση, ιστορικό, μέχρι και κινητό τηλέφωνο στο Facebook θα πρέπει να γνωρίζετε ότι το Facebook δεν εγγυάται τη μυστικότητα τους. Συγκεκριμένα το Facebook δεν είναι αρμόδιο για την καταστρατήγηση οποιονδήποτε ρυθμίσεων απορρήτου(privacy settings) ή μέτρων ασφαλείας που εμπεριέχονται στον ιστοχώρο. Αυτό σημαίνει ότι εάν ένας hacker κλέψει τα προσωπικά σας δεδομένα μέσα από το Facebook, αυτό δε φέρει καμία ευθύνη ούτε μπορεί να κατηγορηθεί για τα μέτρα ασφαλείας του. Το πιο σημαντικό είναι ότι το ίδιο το Facebook προειδοποιεί τους χρήστες του μέσα από τους Όρους Χρήσης ότι εάν αποκαλύπτουμε προσωπικές πληροφορίες, φωτογραφίες, video , λίστες αγορών, κινητά τηλέφωνα, κ.α., όλα αυτά μπορούν να διατεθούν δημόσια.

3. Είναι τρομερά δύσκολο να διαγράψεις το προφίλ σου στο Facebook.

Ακόμα και αν ο λογαριασμός σου απενεργοποιηθεί, οι πληροφορίες παραμένουν διαθέσιμες στους εξυπηρετητές του Facebook επ' αόριστον, με τη δικαιολογία ότι εάν ο χρήστης αλλάξει γνώμη δε χρειάζεται να ξανακάνει την όλη διαδικασία από την αρχή. Το Facebook σε έχει ήδη βρει!

καταρτίζει συμβάσεις, με τις οποίες αναθέτει στον αντισυμβαλλόμενο και αυτός αναλαμβάνει την υποχρέωση να ασκήσει εξουσίες, που απορρέουν από το περιουσιακό δικαίωμα (συμβάσεις εκμετάλλευσης). 2. Ο δημιουργός του έργου μπορεί να επιτρέπει σε κάποιον άλλον την άσκηση εξουσιών, που απορρέουν περιουσιακό του δικαίωμα (άδειες εκμετάλλευσης).» Όμως στην περίπτωση αυτή το άρθρο 32 του ίδιου νόμου προβλέπει: «1. Η αμοιβή, που οφείλει να καταβάλλει ο αντισυμβαλλόμενος στο δημιουργό για δικαιοπραξίες

που αφορούν τη μεταβίβαση του περιουσιακού δικαιώματος ή εξουσιών από αυτό, την ανάθεση άδειας

εκμετάλλευσης, συμφωνείται υποχρεωτικά σε ορισμένο ποσοστό, το ύψος του οποίου καθορίζεται ελεύθερα μεταξύ των μερών. Βάση για τον υπολογισμό του ποσοστού είναι όλα ανεξαιρέτως τα ακαθάριστα έσοδα ή τα έξοδα ή τα συνδυασμένα ακαθάριστα έσοδα και έξοδα, που πραγματοποιούνται από την δραστηριότητα του αντισυμβαλλόμενου και προέρχονται από την εκμετάλλευση, του έργου. 2. Η υποχρεωτική συμφωνία της αμοιβής σε ποσοστό, που προβλέπεται στην προηγούμενη παράγραφο, εφαρμόζεται σε όλες τις περιπτώσεις, εφόσον δεν υπάρχει ειδικότερη διάταξη στον παρόντα νόμο, και δεν αφορά τα έργα που δημιουργήθηκαν από μισθωτούς σε εκτέλεση σύμβασης εργασίας, τα προγράμματα ηλεκτρονικών υπολογιστών και κάθε είδους διαφήμιση.» Ωστόσο, στην περίπτωση του Facebook πολλοί νέοι τοποθετούν τα προσωπικά τους δεδομένα καθώς και περιεχόμενα σε αυτό χωρίς δεύτερη σκέψη για το ηλεκτρονικό ίχνος που αφήνουν πίσω τους. Με τον τρόπο όμως αυτό δίνουν τη δυνατότητα στο Facebook να τα χρησιμοποιήσει με οποιοδήποτε τρόπο αυτό θέλει. Έτσι όμως, παραβιάζονται ευθέως οι παραπάνω διατάξεις του Ν. 2121/1993. Για το λόγο αυτό οι νέοι πρέπει να μάθουν να διαβάζουν πρώτα τους όρους εγγραφής στους οποίους συμφωνούν και να είναι πιο προσεκτικοί με τις πληροφορίες και το περιεχόμενο που εναποθέτουν στο Διαδίκτυο, καθόσον είναι άγνωστος ο τρόπος με τον οποίο αυτό θα διακινηθεί και θα εκμεταλλευτεί στον κυβερνοχώρο. Για παράδειγμα, το κόστος στο μέλλον ενός νέου ατόμου μπορεί να είναι πολύ υψηλό εάν κάτι ανεπιθύμητο βρεθεί από έναν εργοδότη, ο οποίος χρησιμοποιεί το Διαδίκτυο ως εργαλείο για να εξετάζει τους πιθανούς υπαλλήλους του. Και αυτό δεν αποτελεί το μοναδικό παράδειγμα. Οι κίνδυνοι από την εκμετάλλευση ενός περιεχομένου ή και στοιχείων προσωπικών δεδομένων στο χώρο του Διαδικτύου είναι πολλοί, γι' αυτό πρέπει να υπάρχει ενημέρωση και επαρκής γνώση των όρων στους οποίους οι νέοι προσχωρούν, προκειμένου να χρησιμοποιήσουν κάποια ιστοσελίδα ή δυνατότητα του Διαδικτύου. **Ο κ. Αντώνης Παπαντωνίου, Προϊστάμενος του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος Δ/σης Ασφάλειας Θεσσαλονίκης**, υπογραμμίζει μεταξύ άλλων: «Το Facebook είναι ένας εικονικός χώρος (όπως και πολλοί άλλοι) όπου οποιοσδήποτε χρήστες του διαδικτύου μπορεί να φτιάξει το ηλεκτρονικό του προφίλ και να γνωρίσει άλλους χρήστες του διαδικτύου, μοιράζοντας μαζί τους κοινά ενδιαφέρονται κάνοντας ψηφιακές συζητήσεις, ανταλλάσσοντας απόψεις, χόμπι και οτιδήποτε άλλο μπορεί να προσφέρει η εικονική πραγματικότητα. Το Facebook έχει γίνει πολύ δημοφιλής ιστοχώρος, ιδιαίτερα στο χώρο των εφήβων χρηστών του διαδικτύου.

Απαραίτητη όμως προϋπόθεση είναι ο χρήστης να κάνει «εγγραφή» στην ιστοσελίδα ώστε να γίνει δεκτός στην κοινότητα. Η διαδικασία αυτή αν και είναι εύκολη και φαινομενικά ακίνδυνη, κρύβει αρκετούς κινδύνους καθώς τα προσωπικά στοιχεία και τυχόν φωτογραφίες που θα δώσει κάποιος κατά την εγγραφή του, είναι πλέον προσβάσιμα τόσο από τους διαχειριστές της ιστοσελίδας, όσο και από όλα τα άλλα μέλη της διαδικτυακής αυτής κοινότητας. Δεν είναι λίγες οι περιπτώσεις όπου οι νέοι δίνουν τα πραγματικά τους στοιχεία (ονοματεπώνυμο, διεύθυνση κατοικίας,

τηλέφωνα επικοινωνίας κλπ).
Από καταγγελίες που έχει δεχθεί κατά καιρούς η υπηρεσία μας, προσωπικά στοιχεία ατόμων καθώς και φωτογραφίες αυτών (αυθεντικές ή παραποιημένες) έχουν αναρτηθεί σε άλλες ιστοσελίδες συνοδευόμενα από συκοφαντικά σχόλια ή σχόλια με ερωτικό περιεχόμενο. Τα στοιχεία αυτά τα είχαν οι ίδιοι δημοσιεύσει σε ιστοσελίδες κοινωνικής δικτύωσης χωρίς να μπορούν να φανταστούν μια τέτοιου είδους χρήση τους από άλλους κακόβουλος χρήστες του διαδικτύου.
Για το λόγο αυτό θα πρέπει όλοι μας, αλλά ειδικότερα οι νέοι, να έχουμε υπόψη μας ότι η δημοσίευση των προσωπικών μας στοιχείων σε διάφορες ιστοσελίδες του διαδικτύου ενδεχομένως να κρύβει κινδύνους που μπορεί να θίξουν την τιμή και την προσωπικότητα ενός ατόμου και για το λόγο αυτό θα πρέπει να το σκεφτόμαστε δύο φορές πριν «ανεβάσουμε» τα προσωπικά μας στοιχεία.
Η Υπηρεσία μας είναι δίπλα και στηρίζει πρωτοβουλίες οργανώσεων όπως οι N.E.O.I. οι οποίες ενημερώνουν τους χρήστες του διαδικτύου για τις παγίδες που κρύβει αυτό».
Κίνδυνος απολύσεων λόγω χρήσης του Facebook
Υπάλληλος ελβετικής εταιρείας απολύθηκε καθώς σέρφαρε στο Facebook ενώ είχε δηλώσει άρρωστη. Μια υπάλληλος ελβετικής ασφαλιστικής εταιρίας απολύθηκε από την εργασία της γιατί «σέρφαρε» στη δημοφιλή σελίδα Facebook του διαδικτύου, ενώ είχε δηλώσει ότι ήταν ασθενής, ανακοίνωσε ο εργοδότης της.
Η γυναίκα δήλωσε ότι δεν μπορεί να εργαστεί μπροστά στον υπολογιστή γιατί πρέπει να αναπαυτεί και να μείνει κλινήρης στο σκοτάδι, αλλά εντοπίστηκε να «σερφάρει» στο Facebook, γεγονός που όπως ανακοίνωσε η ασφαλιστική εταιρία Nationale Suisse κατέστρεψε την αξιοπιστία της υπαλλήλου απέναντι στην εταιρία.
«Πρόκειται για κατάχρηση εμπιστοσύνης, καθώς η δραστηριότητα που ανέπτυσσε στο Facebook, οδήγησε στην καταγγελία της συμβάσεως εργασίας», αναφέρεται στην ανακοίνωση της εταιρίας.
Η γυναίκα δήλωσε στην εφημερίδα 20 Minuten ότι «σέρφαρε» στο Facebook από το κρεβάτι της χρησιμοποιώντας το iPhone της και κατηγορεί τους εργοδότες της ότι κατασκόπευαν εκείνη και άλλους εργαζομένους στέλνοντας μυστηριώδη φιλικά μηνύματα στην προσωπική της σελίδα για να την αναγκάζουν να δραστηριοποιείται στο διαδίκτυο.
Η ελβετική ασφαλιστική εταιρία απέρριψε τις καταγγελίες της κατασκοπείας και ανακοίνωσε ότι η δραστηριότητα της υπαλλήλου στο Facebook εντοπίστηκε από συνάδελφό της το Νοέμβριο, πριν η δημοφιλής κοινωνική σελίδα του διαδικτύου αρχίσει να παρακολουθείται από την εταιρεία.

Facebook και κατάθλιψη
Ένα ανησυχητικό στοιχείο που προέκυψε από συνεντεύξεις είναι το αίσθημα κενού, που συνεπάγεται η πολύωρη χρήση του facebook, των 'chat rooms' και των άλλων μέσων κοινωνικής δικτύωσης.

Σχέσεις επιφανειακές, φρενήρεις, στιγμιαίες δημιουργούνται, μεταλλάσσονται και διαγράφονται με ένα κλικ.

Νεαρά άτομα που εφευρίσκουν πολλαπλά προσωπεία, ανάλογα με την πλευρά του εαυτού, που θέλουν να παρουσιάσουν. Χρήστες που καπηλεύονται και οικειοποιούνται προφίλ άλλων ατόμων. Έκφραση κάθε συναισθήματος, παρόρμησης ή ενστίκτου χωρίς κανένα πρόσχημα. Επικοινωνία στην οποία, ακόμα και η χρήση

κάμερας, αποκρύπτει τη γλώσσα του σώματος, αποδυναμώνοντας την αποκωδικοποίηση των μηνυμάτων.

Πλευρές της προσωπικότητας, που αναδεικνύονται αλόγιστα, χαρακτηριστικά που δραματοποιούνται για να εντυπωσιάσουν. Χρήστες άτολμοι στην προσωπική τους ζωή, με περίπλοκες οικογενειακές βιογραφίες, απαξιωμένοι από το εκπαιδευτικό σύστημα, αναδομούν την αυτοεκτίμησή τους μέσα από συγκρίσεις (π.χ. compare hotness) και διαγωνισμούς του Facebook, εισπράττουν φιλοφρονήσεις για την απόκρυφη φωτογραφία που «ανέβασαν».

Γυναικεία σαγηνευτικά και εν πολλοίς ψεύτικα προφίλ, που προκαλούν ρίγη σε χιλιάδες άγνωστους θαυμαστές, εικονικά κεράσματα και δώρα, υπενθύμιση γενεθλίων και σημαντικών στιγμών και έξαφνα ο πολύωρος χρήστης βυθίζεται σε μια ουτοπία κοινωνικότητας, γίνεται το επίκεντρο της προσοχής σε άτομα που υπό άλλες συνθήκες δεν θα θυσίαζαν γι' αυτόν ούτε λεπτό από το χρόνο τους.

Μια ιδιότυπη ψυχοθεραπεία χωρίς κανόνες και όρια. Οι δεξιότητες που πρέπει να καλλιεργηθούν για μια επιτυχημένη προσωπική κοινωνική προσαρμογή, τώρα αντικαθίστανται από άλλες που εγγυώνται ότι η εικονική προσωπικότητα και τα διαδικτυακά επιτεύγματα θα γίνονται διαρκώς αποδεκτά. Η πραγματική ζωή φαντάζει ανιαρή, αργή, πληκτική, ανούσια. Οι σχέσεις, με τα τυπικά και τους κανόνες που επιβάλει η κοινωνία, απαράδεκτες . Το αίσθημα κενού καθώς ο χρήστης επαναφέρεται στην πραγματικότητα, η νέα γενιά που βίωσε την παγίωση του διαδικτύου μετά το 1995, που ανατράφηκε με online παιχνίδια και internet καφέ, που μέσα από το κινητό μπορεί να συνεχίσει απρόσκοπτα ότι άρχισε στον υπολογιστή, παρατείνοντας ακόμα περισσότερο τις ώρες χρήσης, έχει πρόβλημα συνεννόησης με τις υπόλοιπες γενιές, που δεν κατανοούν την ελκυστικότητα του ιντερνέτ.
Η επικοινωνία και οι σχέσεις στην πραγματική ζωή απαιτούν διαπραγμάτευση, ρίσκο, υπομονή, επένδυση χρόνου και συναισθήματος. Η έκβασή τους πολλές φορές αμφίβολη. Αυτός που τις επιχειρεί δεν δέχεται άμεση ενίσχυση, όπως συμβαίνει στο διαδίκτυο, ειδικά σε μια κοινωνία που η συλλογικότητα φθίνει και ο ατομισμός ανακηρύσσεται σε πρώτιστη αξία.
Οι σημερινοί νέοι, που μεγαλώνουν γνωρίζοντας άριστα την ηδονή του 'social networking', που χρησιμοποιούν το facebook περισσότερο από πέντε ώρες την ημέρα, αποδίδουν στις πραγματικές τους ταυτότητες λιγότερη αξία σε σύγκριση με τις διαδικτυακές και δεν μπορούν να λειτουργήσουν αποτελεσματικά στον αληθινό κόσμο. Νιώθουν κατάθλιψη για την ανικανότητα αυτή, αδυνατούν να αντλήσουν ευχαρίστηση από μη ακραίες καταστάσεις, όπως αυτές των ηλεκτρονικών παιχνιδιών. Για το λόγο αυτό τις επιζητούν και στην πραγματική ζωή, με αποτέλεσμα πολλές φορές να φέρονται αντικοινωνικά. Βιώνουν στερητικά σύνδρομα, όταν δεν έχουν πρόσβαση και εξαρτούν την αυτοεκτίμησή τους από ένα πληκτρολόγιο ή joystick. Ο πολύωρος χρήστης αποδίδει μεγαλύτερη σημασία σε μια κακή βαθμολογία στα ratings του facebook, παρά σε μια αποδοκιμασία του δασκάλου ή των γονιών του. Πραγματικές σχέσεις καταστράφηκαν όταν ο ένας από τους δύο συντρόφους ανακάλυψε ότι ο άλλος έκανε flirt στο facebook ή διατηρούσε ένα πολύ επιτυχημένο προφίλ. Η φιλία και η επικοινωνία επανανοηματοδοτείται: Ο «άλλος», ο συνομιλητής σε ένα chat room δεν είναι ένα αμιγώς πραγματικό πρόσωπο, αλλά ένα προσωπείο

ένα κράμα από αληθινές ιδιότητες και φαντασιακές προβολές. Οι αισθητηριακές αναπαραστάσεις μηδαμινές.
Ο χρήστης μιλά σε ένα πρόσωπο που ο ίδιος κατασκευάζει. Προβάλλει επάνω του τις επιθυμίες του, τις ελλείψεις του, τις προσδοκίες του και τις φαντασιώσεις του.

Ο «άλλος» ανάγεται σε μορφή ιδεατή.

Η απογοήτευση είναι το κυρίαρχο χαρακτηριστικό, όσων αποφασίζουν να συναντηθούν στην πραγματική ζωή. Στο Facebook ο κόσμος είναι αταξικός. Ο πλούτος, το φύλο, η ηλικία, η καταγωγή, η εθνικότητα, το παρελθόν, τα επιτεύγματα δεν έχουν καμιά σημασία. Εξάλλου, καθένας μπορεί να προσποιηθεί οτιδήποτε.
Οι περισσότεροι νέοι εκφράζουν αποτροπιασμό και θλίψη, όταν επιχειρούν να μεταφέρουν αυτή την εμπειρία στην πραγματική ζωή. Βυθίζονται έτσι ακόμα περισσότερο στην επίπλαστη κατάσταση των διαδικτυακών κοινοτήτων. Και είναι αυτή η αναντιστοιχία ανάμεσα στην ζωή και την εικονική πραγματικότητα που τελικά οδηγεί στην κατάθλιψη.

Κίνδυνοι στα σχολεία: Facebook και μαθητές
Οι κίνδυνοι στο Facebook και η χρήση των social networks είναι από τα μεγαλύτερα θέματα συζήτησης των ημερών. Τα δίκτυα κοινωνικής δικτύωσης (social network) γοητεύουν τους μαθητές, που βρίσκουν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας. Σε έρευνα που διεξήγαγαν για τη χρήση του

Facebook από μαθητές διαπιστώθηκαν τα εξής: Τα κορίτσια καταλαμβάνουν ακραίες θέσεις, δηλαδή είτε χρησιμοποιούν το

Facebook πολλές ώρες ή είναι περιστασιακοί χρήστες, Τα αγόρια εμφανίζονται πιο ευνοϊκά διακείμενα απέναντι στην κοινωνική δικτύωση από ότι τα κορίτσια και είναι περισσότερο εξαρτημένα από τη χρήση του Facebook.
Οι πολύωροι χρήστες του Facebook έχουν συνήθως γονείς που είναι απόφοιτοι της Τριτοβάθμιας Εκπαίδευσης. Όσο υψηλότερο είναι το επίπεδο γνώσεων των γονέων σχετικά με τον Η/Υ, τόσο περισσότερο ασχολούνται τα παιδιά τους με το διαδίκτυο και την κοινωνική δικτύωση μέσω Η/Υ.
Οι πολύωροι χρήστες του Facebook έχουν χαμηλή συμμετοχή σε δημιουργικές δραστηριότητες κατά τον ελεύθερο χρόνο τους.
Οι περιστασιακοί χρήστες του Facebook στην πλειοψηφία τους ασχολούνται με τους φίλους τους, ενώ όσοι επενδύουν πολύ χρόνο είναι κατά κύριο λόγο μοναχικοί χρήστες.
Πολλοί θεώρησαν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας, που θα αντικαταστήσει το email και τις πιο συμβατικές μορφές διάδρασης. Κανόνιζαν τα ραντεβού τους μέσω του Facebook αντί να τηλεφωνήσουν, συζητούσαν γι' αυτό με τους φίλους τους και χρησιμοποιούσαν την ηλεκτρονική ιδιόλεκτο.
Πολλοί χρήστες δήλωσαν ότι αυτό που τους συναρπάζει στο Facebook είναι ότι γνωρίζουν άτομα που μοιράζονται τα ίδια ενδιαφέροντα, ότι έχουν πρόσβαση σε πληροφορίες που τους ενδιαφέρουν, ακόμη και ότι συγκροτούν ομάδες μελέτης για τις εξετάσεις.
Η ευχαρίστηση που προέρχεται από την ενασχόληση με το Facebook και η

φυγή από το διάβασμα είναι η βασικότεροι λόγοι ενασχόλησης με αυτό (στους μαθητές Λυκείου). Το Facebook δεν είναι πια εργαλείο, αλλά εναλλακτικός τρόπος ζωής. Οι περισσότεροι δήλωσαν ότι μέσω της εφαρμογής αυτής κατάφεραν να επανασυνδεθούν με άτομα ή φίλους που είχαν χάσει εδώ και καιρό.
Οι περισσότεροι χρήστες έχουν κουραστεί πλέον με το πλήθος των

εφαρμογών του Facebook, με τις άπειρες προσκλήσεις σε quiz και ch χαμηλού επιπέδου. Το κυριότερο χαρακτηριστικό του Facebook, που τους προσέλκυσε εξαρχής, ήταν η απλότητα των λειτουργιών του, η δυνατότητα επιλογής των εφαρμογών με τις οποίες θα πλαισίωναν το προφίλ τους

Αρκετοί χρήστες είχαν κουραστεί από το «φακέλωμα» μέσω Facebook, μέσω του οποίου ο καθένας γνώριζε και μετέδιδε ποια η ψυχική διάθεση του χρήστη, τι έκανε όλες τις χρονικές στιγμές κλπ. Οι περισσότεροι από αυτούς πιστεύουν ότι η μόδα του Facebook θα περάσει και θα αντικατασταθεί με κάτι πολύ πιο ενδιαφέρον, επειδή ξεπέρασε το μέτρο. Το διαδίκτυο έχει κανόνες αυτορρύθμισης.
Πολλοί άνοιξαν λογαριασμό στο Facebook, επειδή είναι μόδα.
Οι περισσότεροι κατηγορούν το Facebook ότι προάγει τις επιφανειακές αόριστες σχέσεις και ότι δεν μπορούν να βρουν πραγματική στήριξη μέσω αυτού. Παρόλα αυτά, αναγνώρισαν ότι αποτελεί υποκατάστατο για όσους δεν τα καταφέρνουν στις πραγματικές σχέσεις ή έχουν περιορισμένο χρόνο γι' αυτές.
Οι χρήστες με μεγαλύτερη εξάρτηση από το Facebook, παρουσίαζαν την ίδια νοσηρή σχέση και με τα ηλεκτρονικά παιχνίδια και τον υπολογιστή γενικότερα.
Οι περισσότεροι χρήστες δεν κατάλαβαν την εξάρτηση από το Facebook μέχρι που κατέληξαν να αναλώνουν πολλές ώρες ασχολούμενοι με τις εφαρμογές του και σκεφτόταν γι' αυτό ακόμη κι όταν έκλειναν τον υπολογιστή.
Το Facebook παρέχει το προσωπείο της αυτοεκτίμησης. Πολλοί αρθρώνουν συναισθήματα μέσα από αυτό, που δεν θα τολμούσαν να τα πουν στην πραγματική ζωή. Το ένστικτο και το συναίσθημα απελευθερώνεται. Αρκετοί χρήστες διατηρούσαν παραπάνω από δύο λογαριασμούς στο Facebook με διαφορετικά χαρακτηριστικά κάθε φορά. Πολλαπλές και σχιζοειδείς προσωπικότητες.
Το γλωσσικό επίπεδο των χρηστών του Facebook πολλές φορές κατρακυλάει σε ύβρεις και χυδαιολογίες, ενώ η ελληνική ορθογραφία παραχαράσσεται. Η γλώσσα είναι ένα συνονθύλευμα αγγλικών συντμήσεων και ελληνικών. Συχνή είναι η χρήση emoticons που όμως γίνονται δύσκολα στην αποκρυπτογράφησή τους και δυσχεραίνουν τη φόρτωση της σελίδας.
Το Facebook αποτελεί μέσο επικοινωνίας, ειδικά για νέους επαρχιακών πόλεων, που δεν έχουν πολλές ευκαιρίες να γνωρίσουν όσους θα επιθυμούσαν. Παράλληλα προσφέρει τη δυνατότητα είτε για ιδιωτική συνομιλία είτε για μαζική συζήτηση.
Σε χρήστες μικρότερης ηλικίας αναπτύσσεται ανταγωνισμός για το ποιος θα προσελκύσει περισσότερους φίλους, κυρίως του αντιθέτου φύλου.
Οι γυναίκες χρήστες προβάλλουν τις περισσότερες φορές ένα μυστηριώδη εαυτό, που περιμένει να ανακαλυφθεί από κάποιο χρήστη με έξοχα προσόντα, γρήγορο στη γραφή και με καλές ατάκες. Οι φωτογραφίες που τοποθετούν στο προφίλ τους είναι προκλητικές μερικές φορές ή παρμένες από τον κόσμο των

κινουμένων σχεδίων. Οι άντρες χρήστες συνήθως επαίρονται για τα σωματικά τους προσόντα και για τον 'τσαμπουκά' που μπορούν να επιδείξουν.
Οι περισσότεροι χρήστες δεν ενοχλούνται που το Facebook πολλές φορές παίρνει πολιτική διάσταση ερήμην τους.

Βλασφημία και καθύβριση θρησκευμάτων, μέσω του Facebook

Από τη Δίωξη Ηλεκτρονικού Εγκλήματος σχηματίστηκε δικογραφία αυτόφωρης διαδικασίας, σε βάρος 27χρονου ημεδαπού, ο οποίος κατηγορείται για κακόβουλη βλασφημία και καθύβριση θρησκευμάτων, μέσω της γνωστής σελίδας κοινωνικής δικτύωσης Facebook . Πιο αναλυτικά, η Δίωξη Ηλεκτρονικού Εγκλήματος εντόπισε πρόσφατα στη γνωστή ιστοσελίδα κοινωνικής δικτύωσης Facebook, σελίδα με στοιχεία, η οποία περιείχε βλασφημίες και ύβρεις κατά του Γέροντα Παϊσίου και του Ορθόδοξου Χριστιανισμού. Παράλληλα για το υβριστικό και βλάσφημο περιεχόμενο της συγκεκριμένης σελίδας, η Δίωξη Ηλεκτρονικού Εγκλήματος έγινε αποδέκτης χιλιάδων ηλεκτρονικών καταγγελιών, που προέρχονταν από κατοίκους διάφορων χωρών σε όλο τον κόσμο. Από την αστυνομική ψηφιακή έρευνα, που πραγματοποιήθηκε στο πλαίσιο διενέργειας προκαταρκτικής εξέτασης, διακριβώθηκαν τα αρχεία καταγραφής (logfiles) και τα ηλεκτρονικά ίχνη του διαχειριστή - χρήστη της επίμαχης σελίδας. Στη συνέχεια, την Παρασκευή (21-09-2012) το πρωί, κλιμάκιο εξειδικευμένων Αξιωματικών της Δίωξης Ηλεκτρονικού Εγκλήματος πραγματοποίησε νομότυπη έρευνα, παρουσία Εισαγγελικού λειτουργού, στο σπίτι του 27χρονου στα Ψαχνά Ευβοίας.

Κατά τη διάρκεια της έρευνας βρέθηκε και κατασχέθηκε ένας φορητός υπολογιστής (laptop). Από την επιτόπια αυτοψία στον συγκεκριμένο ηλεκτρονικό υπολογιστή διαπιστώθηκε ότι διαχειριστής της επίμαχης σελίδας ήταν ο 27χρονος, ο οποίος συνελήφθη και με τη δικογραφία που σχηματίστηκε σε βάρος του οδηγήθηκε στην Εισαγγελία Πρωτοδικών Αθηνών.

παράδειγμα

Νέος επικίνδυνος ιός στο Facebook

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, ενημερώνει τους χρήστες του διαδικτύου, σχετικά με την κυκλοφορία ενός νέου ιού, ο οποίος εμφανίσθηκε στο διαδίκτυο στις 10/5/2014, ενώ διαδίδεται μέσα από διάφορα βίντεο τρόμου, που προσπαθούν οι χρήστες του διαδικτύου να «ανοίξουν» και τα οποία προσβάλουν τον ηλεκτρονικό υπολογιστή με κακόβουλο λογισμικό. Ειδικότερα, μόλις εγκατασταθεί το κακόβουλο αυτό λογισμικό αποκτά τη δυνατότητα να εκτελεί διάφορες παράνομες ενέργειες, εν αγνοία του χρήστη, όπως απενεργοποίηση ρυθμίσεων ασφαλείας του συστήματος και πιο συγκεκριμένα το firewall, έτσι ώστε να ανοίξει κερκόπορτες (backdoors) για άλλα μολυσμένα προγράμματα.

Επίσης, παρεμβαίνει στον φυλλομετρητή (browser) αλλά και στην απόδοση του ίδιου του υπολογιστή, αλλάζοντας την αρχική σελίδα και την προεπιλεγμένη μηχανή αναζήτησης (του φυλλομετρητή).

Παράλληλα, αρχίζουν να εμφανίζονται ανεπιθύμητα διαφημίστηκα banners, σελίδες με συνδρομητικές υπηρεσίες μηνυμάτων και κακόβουλα αρχεία για κατέβασμα. Τέλος υπάρχει η δυνατότητα υποκλοπής κωδικών και άλλων κακόβουλων ενεργειών (όπως αποστολή spam emails κ.λπ.) Σημειώνεται ότι στη ροή ενημερώσεων του facebook εμφανίζονται αναρτήσεις οι οποίες φαίνονται σαν "βίντεο" με περίεργο - σοκαριστικό περιεχόμενο, προτρέποντας τους χρήστες να πατήσουν στην ανάρτηση προκειμένου να δουν το "βίντεο".

Οι κακόβουλες αναρτήσεις εμφανίζονται με διάφορους τίτλους όπως : Vin Diesel HasDied While Filming a Deadly Scene From Fast and Furious 7, You Won't Believe What This Pregnant Girl Does, [SCHOCK] Schlimmster Motorrad Unfall Der Welt (Σόκ !Το χειρότερο ατύχημα με μοτοσικλέτα στο κόσμο), Girl Killed herself live On Cam Just After Dad Seen Her While Doing This on cam!, με πιο διαδεδομένους τους παρακάτω τίτλους : "Βίντεο" από επίθεση φαντάσματος (Alleged footage of an "actual" ghost attack). "Βίντεο" που δείχνει το Aswang, ένα μυθικό τέρας από τις Φιλιππίνες (a video featuring the Aswang that is described as "a mythical shape-shifting were-dog/vampire/terrifying thing from the Philippines). "Βίντεο" με γοργόνες (a video of Mermaids claiming they are back!). "Βίντεο" με ένα μεγάλο, λευκό καρχαρία να επιτίθεται σε καπετάνιο πλοίου (Video of a huge great white shark tearing apart a sea captain).

Όταν κάποιος χρήστης πατήσει σε αυτές τις αναρτήσεις συνήθως του ζητείται πρώτα να κοινοποιήσει την ανάρτηση στον «τοίχο» του, για να ξεκλειδώσει το "βίντεο" (συμμετέχοντας και ο ίδιος με αυτόν τον τρόπο στη διάδοση των κακόβουλων αναρτήσεων).

Στη συνέχεια εμφανίζεται μήνυμα ότι πρέπει να κατεβάσει ή να αναβαθμίσει το video player του φυλλομετρητή (browser), προκειμένου να μπορέσει να δει το "βίντεο".

Εάν ο χρήστης προβεί σε αυτή την ενέργεια τότε εγκαθίσταται το αντίστοιχο κακόβουλο αρχείο, όπως αναφέρεται πιο κάτω στις φωτογραφίες.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η τεχνολογία συνέχεια προοδεύει και ο τρόπος που εμφανίζονται τα ηλεκτρονικά εγκλήματα , δυσκολεύει τη διεύρυνση εγκλημάτων , εξαιτίας της έλλειψης του συστήματος που υπάρχει.

Συνήθως, εκείνος που διαπράττει ένα τέτοιο είδους έγκλημα , έχει σκοπό κάποιο οικονομικό όφελος, παραβιάζοντας τον ποινικό κώδικα. Επίσης, παιδιά μικρής ηλικίας πέφτουν θύματα Ηλεκτρονικού Εγκλήματος.

Για την αντιμετώπιση αυτού του φαινομένου πρέπει να υπάρχει σωστή ενημέρωση και να ληφθούν μέτρα από την υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος .

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]www.go-online.gr/e-business/specials/article/html?article_id_370.

[2] www.it.security.gr/ hacker.html.

[3] www.it.security.gr/ cracking.html.

[4] Www. computer.howstuffworks.com/ phishing.html.

[5] www.pharming-fishing.gr.

[6] www.itsecurity.gr.

[7] www.en.wikipedia.org/wiki/Domain_name.gr. .

[8] www.fbi.gov.

[9]http://www.newsbeast.gr/technology/arthro/612029/oi-apeiles-kai-oi-epiptoseis-tou-ilektronikou-eglimatos-sti-hrisi-tou-diadiktuou-/.

[10] Ζάννη Α., «Το διαδικτυακό έγκλημα», Εκδόσεις Α. Σάκκουλα, Αθήνα-Κομοτηνή 2005.

[11] Καρακώστας Ι., «Δίκαιο & Internet. Νομικά ζητήματα στο Διαδίκτυο», Εκδόσεις Α. Σακούλα, Αθήνα 2003.

[12] www. astynomia. gr

[13] http://ipeirotika.gr/greece/item/4347-prosoxi-plasto-e-mail-iposxetai-epistrofi-forou

[14] https://electroniccrime.wordpress

[15] http://www.cyberethics.info/cyethics1/ index

[16] http://el.vessoft.com/software/windows/download/avast

[17] Πτυχιακή Σερέτης Δημήτριος, διπλωματική εργασία –Nemertes

[18] Σημειώσεις Κ. Αναγνωστάκη, μάθημα ηλεκτρονικό εμπόριο.

[19] Πτυχιακή Στούρη Βασιλική, <<έγκλημα στο διαδίκτυο>> Πανεπιστήμιο Πειραιώς , διπλωματική εργασία.

[20] Πτυχιακή Λιανού Κωνσταντίνα, <<έγκλημα και διαδίκτυο>> Εθνικό Μετσόβιο Πολυτεχνείο, διπλωματική εργασία.