Πανεπιστήμιο Πειραιώς
Π.Μ.Σ. Διδακτική της Τεχνολογίας και Ψηφιακών Συστημάτων

Διπλωματική Εργασία

Εγκλήματα στο Διαδίκτυο:
Εναλλακτικοί Τρόποι Εκδήλωσης, Τρόποι Αντιμετώπισης και Διερεύνησής των

Στούρη Βασιλική,
Κατεύθυνση: Δικτυοκεντρικά Συστήματα
ΜΕ/08104

Επιβλέπων Καθηγητής:
Λαμπρινουδάκης Κ.

Πειραιάς
Ιούλιος 2010

Περιεχόμενα

Εισαγωγή

Το πρόβλημα των ηλεκτρονικών εγκλημάτων εμφανίστηκε στη δεκαετία του 1970 στις τεχνολογικά ανεπτυγμένες χώρες. Λίγο αργότερα επεκτάθηκε στις ανεπτυγμένες και αναπτυσσόμενες χώρες. Σήμερα τα «εγκλήματα τελούμενα με υπολογιστή» αυξάνονται και γενικεύονται συνεχώς. Στις νέες μορφές εγκληματικότητας οι ηλεκτρονικοί υπολογιστές (Η/Υ) μπορούν:
• Να χρησιμοποιηθούν οι ίδιοι για να τελεστεί 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 κατέστη επιτακτική η ανάγκη θεσμοθέτησης νόμων ως προς την νόμιμη λειτουργία των υπολογιστών και του Διαδικτύου. Οι νομικοί αυτοί κανόνες, οι δικαστικές αποφάσεις που σχετίζονται με υποθέσεις σχετικές με την παραβατική συμπεριφορά στον τομέα της Πληροφορικής, και η ανάλογη θεωρία που αναπτύσσεται, αποτελούν ένα νέο είδος Δικαίου, το Δίκαιο της Πληροφορικής (Law of Informatics).
Ένα βασικό πρόβλημα που καλείται να διευθετήσει το Δίκαιο της Πληροφορικής είναι η προστασία της πνευματικής ιδιοκτησίας των προϊόντων λογισμικού, των δημιουργών καθώς και η παράνομη αντιγραφή και χρήση του λογισμικού. Στα περισσότερα κράτη φυσικά υπάρχουν αρμόδιοι φορείς που απονέμουν διπλώματα ευρεσιτεχνίας στους παραγωγούς, ενώ έχουν θεσπιστεί αυστηρές διατάξεις για την προστασία της πνευματικής ιδιοκτησίας. Οι υφιστάμενες διατάξεις σχετικά με την κυκλοφορία των προϊόντων της Πληροφορικής, υπάγονται στο «ενοχικό δίκαιο» όπου καλύπτονται δύο βασικές κατηγορίες συμβάσεων:
1) η σύμβαση πώλησης, εγκατάστασης και συντήρησης του υλικού, και
2) η σύμβαση προμήθειας άδειας χρήσης και τεχνικής υποστήριξης.

Τη δεκαετία του 1980 το ηλεκτρονικό έγκλημα διαδόθηκε με μεγάλη ταχύτητα. Αυτό είχε ως αποτέλεσμα να αρχίσουν οι πρώτες εμπεριστατωμένες νομικές και εγκληματολογικές προσεγγίσεις ως προς αυτή την νέα μορφή εγκληματικότητας. Ο όρος «computer crime» χρησιμοποιείται για να υποδηλώσει την παράνομη κατοχή δεδομένων που είναι αποθηκευμένα σε υπολογιστή. Κάθε εγκληματική συμπεριφορά, στην οποία ο υπολογιστής είναι εργαλείο ή σκοπός της πράξης αποτελεί εγκληματικότητα διαμέσου των υπολογιστών. Για την νομική κάλυψη του ηλεκτρονικού εγκλήματος προτάθηκαν αρκετοί ορισμοί για το τι είναι έγκλημα συσχετιζόμενο με την χρήση των Η/Υ. Ο Parker (1976) διακρίνει τρεις τύπους ηλεκτρονικού εγκλήματος:
• Την κατάχρηση υπολογιστών (computer abuse) που αναφέρεται σε κάθε πράξη που σχετίζεται με τους υπολογιστές και μέσω της οποίας ο δράστης ωφελήθηκε ή θα μπορούσε να ωφεληθεί και το θύμα ζημιώθηκε ή θα μπορούσε να ζημιωθεί.
• Το έγκλημα διαμέσου των υπολογιστών (computer crime), δηλαδή κάθε παράνομη κατάχρηση του υπολογιστή μέσω της άμεσης χρήσης του.
• Το έγκλημα σχετιζόμενο με τους υπολογιστές (computer related crime), δηλαδή κάθε πράξη που για να λάβει χώρα είναι αναγκαία η χρήση πληροφορικής τεχνολογίας.
Οι κυριότεροι λόγοι ανάπτυξης της εγκληματολογικής συμπεριφοράς θεωρούνται οι ακόλουθοι:
• Η ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου (e-Commerce).
• Η ευκολία των συναλλαγών μέσω πλαστικού χρήματος.

• Η ευχέρεια πραγματοποίησης τραπεζικών ή συναλλαγματικών πράξεων από απόσταση.
• Η ευκολία παρουσίασης νέων προϊόντων χωρίς την προηγούμενη δοκιμή τους για αποκλεισμό ή μείωση περιθωρίου λάθους.
• Η παγκοσμιοποίηση της επικοινωνίας και της πληροφορίας.
• Οι δυνατότητες διάπραξης του εγκλήματος από απόσταση και χωρίς να εκτίθεται σε κίνδυνο ο δράστης.
• Η δυσχέρεια των αστυνομικών αρχών για ανακάλυψη ή αποκάλυψη του εγκλήματος μετά την παρέλευση κάποιου χρόνου.
• Η απειρία των διωκτικών αρχών σε νέες μορφές εγκληματικότητας.
• Το ανύπαρκτο νομοθετικό πλαίσιο (ιδιαίτερα σε παγκόσμιο επίπεδο).

Ο **Wasik** (1991) διατυπώνει τρία διαφορετικά προβλήματα που σχετίζονται με τα ηλεκτρονικά εγκλήματα:
• Το πρώτο πρόβλημα αναφέρεται στο ερώτημα αν πραγματικά υπάρχει το ηλεκτρονικό έγκλημα, θεωρώντας ως εξωπραγματική τη θέση ότι «το ηλεκτρονικό έγκλημα είναι πλάσμα της φαντασίας».
• Το δεύτερο πρόβλημα αναφέρεται στο ερώτημα αν το ποινικό δίκαιο (ως έχει) μπορεί να θέσει το ηλεκτρονικό έγκλημα κάτω από κοινωνικό έλεγχο, κάτι που δεν είναι δυνατόν λόγω της δημιουργίας νέων κοινωνικών συνθηκών.
• Το τρίτο πρόβλημα αναφέρεται στον ορισμό του εύρους του ηλεκτρονικού εγκλήματος και στο τι είναι λογικό και αναγκαίο να περιλαμβάνεται στο εύρος αυτό. Προτείνεται η εισαγωγή της έννοιας «κατάχρηση υπολογιστή» (computer abuse) η οποία ορίζεται ως κάθε ανήθικη ή χωρίς εξουσιοδότηση συμπεριφορά σε σχέση με τη χρήση υπολογιστών, προγραμμάτων, ή δεδομένων. Η έννοια αυτή συνιστά ένα πλαίσιο συνολικού διαλόγου στον οποίο κατατίθεται κάθε προβληματισμός για οποιαδήποτε συμπεριφορά θα μπορούσε να ορισθεί ως ηλεκτρονικό έγκλημα. Η συμπεριφορά αυτή θα εισάγεται για διάλογο με την «προδικαϊκή» μορφή της κατάχρησης, και στη συνέχεια θα μελετάται ποιες από τις καταχρήσεις του υπολογιστή μπορούν να ορισθούν σαν εγκληματικές συμπεριφορές και ποιες θα παραμένουν στην κατάσταση της απλής κατάχρησης. Η πρόταση είναι ιδιαίτερα χρήσιμη αφού απομακρύνει χωρίς και να αποσυνδέει το ηλεκτρονικό έγκλημα ως πραγματικότητα από τον ορισμό του. Ωστόσο, το μεγάλο πρόβλημα είναι οι συνεχείς και ριζικές αλλαγές στην Πληροφορική και στις εξ αυτών προερχόμενες και διευρυμένες εγκληματικές συμπεριφορές που δεν μπορούν να καλυφθούν από τις υπάρχουσες προσεγγίσεις και ορισμούς του ηλεκτρονικού εγκλήματος.
Το 1986 ο Οργανισμός Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ανέθεσε σε μία ομάδα ειδικών να μελετήσει τις νέες εκφάνσεις του ηλεκτρονικού εγκλήματος, να επεξεργαστεί τα νέα δεδομένα, και να καθορίσει εκ νέου την υπόσταση του εγκλήματος. Η συγκεκριμένη μελέτη οριοθετεί «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, διότι δεν είναι εξειδικευμένος, ώστε να ξεπεραστεί σύντομα από τις συνεχείς και ριζικές αλλαγές της Πληροφορικής, ούτε τόσο γενικός ώστε να έχει περιορισμένη χρησιμότητα.

Σκοπός της εργασίας

Η εργασία έχει σκοπό την διερεύνηση ηλεκτρονικών εγκλημάτων, πώς δηλαδή αυτά εκδηλώνονται και πώς αντιμετωπίζονται σε νομικό και τεχνικό επίπεδο.
Συγκεκριμένα παρουσιάζονται διάφορες μορφές ηλεκτρονικών εγκλημάτων σε όλο τον κόσμο, κάποια πρόσφατα παραδείγματα, η αντιμετώπισή τους από τις αρχές και τεχνικά μέτρα τα οποία λαμβάνονται.
Τέλος παρουσιάζονται κάποιες βέλτιστες πρακτικές οι οποίες θα πρέπει να εφαρμόζονται από όλους μας προς αποφυγή παραπλάνησης.
Δίνεται έμφαση στην παιδική ηλικία, διότι τα παιδιά σήμερα έχουν επαφή με το διαδίκτυο από πολύ μικρή ηλικία με αποτέλεσμα να μην κάνουν σωστή χρήση του διαδικτύου και να πέφτουν συχνά θύματα ηλεκτρονικών εγκλημάτων.

1. Ηλεκτρονικά εγκλήματα

Για να οριστεί μια δραστηριότητα ως έγκλημα θα πρέπει με τη συγκεκριμένη δραστηριότητα να προσβάλλεται κάποιο αγαθό που προστατεύεται από τον νόμο (έννομο αγαθό).

Στη γενική έννοια των εννόμων αγαθών διακρίνουμε δύο διαστάσεις:
Α. Την οντολογική διάσταση που αναφέρεται στον καθεαυτό ορισμό του αγαθού, και
Β. Την αξιολογική διάσταση που αναφέρεται στην αξία που αποδίδεται από το δίκαιο και την έννομη τάξη στο συγκεκριμένο αγαθό. Είναι κοινή διαπίστωση ότι το αγαθό που προσβάλλεται από το ηλεκτρονικό έγκλημα δεν έχει ακόμα καθοριστεί με ακρίβεια. Υπάρχουν δύο διαφορετικές προσεγγίσεις καθορισμού του ηλεκτρονικού εγκλήματος.
Σύμφωνα με την πρώτη προσέγγιση, ως προσβαλλόμενο από το ηλεκτρονικό έγκλημα έννομο αγαθό μπορεί να οριστεί η μικρότερη μονάδα της γνώσης, υπό τον όρο ότι είναι κοινωνική, δηλαδή μεταβιβάσιμη χωρίς ουσιαστική αλλοίωση, έννοια η οποία και συναρτάται άμεσα με την έννοια της Πληροφορικής.
Το δικαίωμα στην πληροφορία αποτελεί μια υποκειμενική αξίωση με δύο πλευρές:
α) το δικαίωμα απόκτησης πληροφοριών από γενικά προσιτές πηγές, και
β) το δικαίωμα διάθεσης της πληροφορίας.
Οι δύο αυτές πλευρές αποτελούν το περιεχόμενο ενός ατομικού δικαιώματος που αποτελεί τη λειτουργική βάση μιας φιλελεύθερης δημοκρατίας.
Σύμφωνα με τη δεύτερη προσέγγιση, το προστατευόμενο αγαθό από το ηλεκτρονικό έγκλημα συναντάται στο επίπεδο των δεδομένων (data), τα οποία και αποτελούν την πρώτη ύλη για τη σύνθεση της πληροφορίας.
Οι έννοιες «πληροφορία» και «δεδομένα» είναι δύσκολο να αποδοθούν με ακρίβεια. Το Συμβούλιο της Ευρώπης θεωρεί τα δεδομένα ως μια τυπική αναπαράσταση εννοιών, γεγονότων ή οδηγιών και τις «πληροφορίες» ως το νόημα που έχουν τα δεδομένα για τους ανθρώπους.
Τα ηλεκτρονικά εγκλήματα ανακαλύπτονται και στοιχειοθετούνται δύσκολα. Επιπλέον, είναι δύσκολο να προσδιοριστεί η νομισματική αξία επάνω στην απώλεια της πνευματικής ιδιοκτησίας, για την οποία η πραγματική αξία πιθανόν να μην είναι γνωστή για αρκετό καιρό.
Στις επιχειρήσεις, τα ηλεκτρονικά εγκλήματα διαπράττονται κυρίως από υπαλλήλους αποκλειστικής απασχόλησης και σπάνια από παράνομους εισβολείς στους

υπολογιστές των επιχειρήσεων. Ο αυξανόμενος ρυθμός πρόσβασης χρηστών στο Διαδίκτυο συμβαδίζει με την αυξανόμενη εγκληματική συμπεριφορά της κλοπής.
Σήμερα το πλέον διαδεδομένο ηλεκτρονικό έγκλημα είναι η κλοπή συγκεκριμένων πληροφοριών που αφορούν σχέδια νέων προϊόντων, έρευνες αγοράς, καταλόγους πελατών με αγοραστική δύναμη κτλ.
Η κλοπή (ιδιαίτερα της πνευματικής ιδιοκτησίας) δεν γίνεται εύκολα αντιληπτή ως λάθος, και επομένως ψυχολογικά είναι πιο εύκολο να διαπραχθεί.
Γενικά, τα θύματα (λ.χ., οι επιχειρήσεις) ανακαλύπτουν κλοπές με τους εξής τρόπους:
1) με το λογιστικό έλεγχο ιχνών που δείχνουν πρόσβαση σε πληροφορίες για τις οποίες ο χρήστης δεν είχε τη νόμιμη πρόσβαση,
2) με τη βοήθεια ενός πληροφοριοδότη που ενημέρωσε την επιχείρηση για την κλοπή,
3) με την προβολή εξωτερικών πληροφοριών όπως οι ενέργειες ή τα προϊόντα ενός ανταγωνιστή που φανέρωσαν την κλοπή.

1.1. Κατηγορίες ηλεκτρονικών εγκλημάτων

Η έκθεση του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ταξινομεί το ηλεκτρονικό έγκλημα σε πέντε κατηγορίες.
• Η πρώτη κατηγορία αναφέρεται στη μη επιτρεπόμενη αντιγραφή ή χρήση προϊόντων λογισμικού και την εξ αυτής παραβίαση των αποκλειστικών δικαιωμάτων του δημιουργού
ή νομίμου κατόχου προϊόντων λογισμικού, κυρίως προγραμμάτων. Η παραβατική αυτή συμπεριφορά είναι γνωστή ως «πειρατεία στο software» και παραβιάζει τους θεσμοθετημένους κανόνες περί πνευματικής ιδιοκτησίας.
• Η δεύτερη κατηγορία αναφέρεται στην χωρίς εξουσιοδότηση εισαγωγή δεδομένων, στο υπολογιστικό σύστημα ή στην μετατροπή τους καθώς και στην καταστροφή δεδομένων, τα οποία είναι αποθηκευμένα σε προϊόντα λογισμικού που είναι εγκαταστημένα στο υπολογιστικό σύστημα.
• Η τρίτη κατηγορία αναφέρεται στην αλλοίωση ή μείωση της αξιοπιστίας δεδομένων ενός υπολογιστικού συστήματος.
• Η τέταρτη κατηγορία αναφέρεται στη παρεμπόδιση της λειτουργίας πληροφοριακών ή τηλεπικοινωνιακών συστημάτων.
• Η πέμπτη κατηγορία αναφέρεται στη χωρίς άδεια εισβολή σε πληροφοριακά συστήματα και αφαίρεση στοιχείων. Όλες οι κατηγορίες, εκτός της πρώτης, αφορούν συμπεριφορές που έχουν ως κοινό σκοπό, την εκ προθέσεως τέλεση εγκλήματος.
Ο **Sieber** (1997) με κριτήριο το προστατευόμενο αγαθό που προσβάλλεται ή απειλείται, κατηγοριοποίησε το ηλεκτρονικό έγκλημα σε τρεις άλλες κατηγορίες:
• Η πρώτη κατηγορία περιλαμβάνει τα ηλεκτρονικά οικονομικά εγκλήματα όπως η απάτη, η πλαστογραφία, η ηλεκτρονική κατασκοπεία, το ηλεκτρονικό σαμποτάζ.
• Η δεύτερη κατηγορία περιλαμβάνει τα ηλεκτρονικά εγκλήματα κατά των ατομικών δικαιωμάτων.
• Η τρίτη κατηγορία περιλαμβάνει τα υπερατομικά ηλεκτρονικά εγκλήματα, όπως τα εγκλήματα κατά της Εθνικής Ασφάλειας, του ελέγχου, της διασυνοριακής ροής πληροφοριών, της δημοκρατικής νομιμότητας, της ακεραιότητας των κοινωνικών διαδικασιών που στηρίζονται σε επεξεργασίες με Η/Υ, της ακεραιότητας δικτύων επικοινωνιών κ.α.

1.2. Διαδεδομένα ηλεκτρονικά εγκλήματα

Τα πιο διαδεδομένα ηλεκτρονικά εγκλήματα είναι, το ηλεκτρονικό οικονομικό έγκλημα, η απάτη στις τηλεπικοινωνίες, η απάτη με Η/Υ, η αφαίρεση ή τροποποίηση δεδομένων, ο Δούρειος Ίππος, η μέθοδος της σαλαμοποίησης, το superzapping, η ηλεκτρονική κατασκοπεία, η παραβίαση της ιδιωτικής ζωής, οι λογικές βόμβες, η διάδοση ιών.

• Το ηλεκτρονικό οικονομικό έγκλημα κατέχει πρωτεύουσα θέση στο χώρο των διαπιστωθέντων ηλεκτρονικών εγκλημάτων και ενδιαφέρει τους περισσότερους ερευνητές. Αυτό συμβαίνει διότι η διαπίστωση του ηλεκτρονικού οικονομικού εγκλήματος είναι μία εύκολη διαδικασία που συνήθως γίνεται αντιληπτή σε μικρό χρονικό διάστημα και τα οικονομικά μεγέθη της απάτης αποτιμούνται με μεγάλη ακρίβεια. Τα ηλεκτρονικά οικονομικά εγκλήματα κατατάσσονται σε διάφορες κατηγορίες, όπως σε απάτες που τελούνται σε βάρος ενός συστήματος επεξεργασίας δεδομένων, ηλεκτρονική κατασκοπεία, κλοπή προγραμμάτων και πειρατεία λογισμικού, σαμποτάζ σε βάρος του υπολογιστικού συστήματος, πρόσβαση στο υπολογιστικό σύστημα χωρίς την αναγκαία προς τούτο εξουσιοδότηση και απάτη σε βάρος επιχειρήσεων και ιδιωτών σε εθνική κλίμακα μέσω του Διαδικτύου.

• Η απάτη στις Τηλεπικοινωνίες ξεκίνησε στις αρχές της δεκαετίας του 1960 από την Αμερική. Το αυτοματοποιημένο πλέον τηλεφωνικό δίκτυο άρχισε να χρησιμοποιεί ήχους για την μεταφορά εντολών. Αυτός ο ήχος είναι ένα σήμα στον τοπικό κατανεμητή, μια εντολή που κατευθύνει την κλήση σε ένα συγκεκριμένο τόπο. Πληκτρολογώντας επτά, δέκα ή δεκαπέντε διαδοχικά νούμερα, στέλνοντας δηλαδή αντίστοιχους ήχους η κλήση μας κατευθύνεται σε ένα συγκεκριμένο τηλέφωνο. Όταν κλείσει το τηλέφωνο, αποστέλλεται ένας διαφορετικός ήχος, ένα σήμα στον κατανεμητή ότι η γραμμή απελευθερώθηκε και ότι πρέπει να σταματήσει τη χρέωση. Αναπαράγοντας όμως το συγκεκριμένο ήχο, κάποιοι χρήστες στην Αμερική ανακάλυψαν ότι ναι μεν ο κατανεμητής θεωρούσε ότι το τηλέφωνο έκλεισε και σταματούσε τη χρέωση, η γραμμή ωστόσο παρέμενε ανοικτή. Έτσι λοιπόν θα μπορούσαν να τηλεφωνούν στην άλλη άκρη του κόσμου, αρκεί να σφυρίξουν τον συγκεκριμένο ήχο των 2600 Hz και να μιλούν με τις ώρες χωρίς να πληρώνουν.

• Η απάτη με Η/Υ σε βάρος του κατόχου ή του νόμιμου χρήστη ενός συστήματος επεξεργασίας δεδομένων, περιλαμβάνει την μετατροπή δεδομένων που βρίσκονται αποθηκευμένα στον υπολογιστή σε βάσεις δεδομένων, είτε σε προγράμματα και μηχανογραφικές εφαρμογές, με σκοπό τον προσπορισμό οικονομικού οφέλους. Ειδικότερα, το έγκλημα της απάτης σε βάρος ενός υπολογιστή τελείται με την κλοπή, διαγραφή, αλλοίωση ή προσθήκη δεδομένων ή πληροφοριών, με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο κέρδος.

Οι παραβάτες των δεδομένων δραστηριοποιούνται κυρίως σε δύο ειδών απάτες. Σε αυτές που ο υπολογιστής έχει ρόλο βοηθητικό και σε αυτές που έχει κύριο ρόλο.

Α) Ο βοηθητικός ρόλος των υπολογιστών αφορά κυρίως απάτες με πλαστογραφήσεις εγγράφων, όπως δελτία αστυνομικών ταυτοτήτων, πτυχία διαφόρων σχολών, δελτία Προπό Τζόκερ και Λόττο, όπου παραποιούνται ορισμένοι αριθμοί και βιβλιάρια τραπεζών για απ' ευθείας ανάληψη χρημάτων.

Β) Αποκλειστική χρήση των υπολογιστών σε απάτες έχουμε στις περιπτώσεις κατάρτισης πλαστών χαρτονομισμάτων, στην κατάρτιση πλαστών πιστωτικών καρτών, στη χρήση κεντρικών συστημάτων ηλεκτρονικών υπολογιστών από τους hackers και σε κατάρτιση

πλαστών επιταγών με τη χρησιμοποίηση του σαρωτή (scanner). Συγκεκριμένα, έχουν επισημανθεί οι ακόλουθοι βασικοί τρόποι πλαστογράφησης.

• Ο ηλεκτρονικός πλαστογράφος με σύστημα υπολογισμού εισχωρεί στο μαγνητικό πεδίο αναγνώρισης μιας πιστωτικής κάρτας (μαύρη ταινία) και σβήνει τα πραγματικά στοιχεία κατόχου και αναγράφει άλλα πλασματικά, οπότε η κάρτα χρεώνει σε άλλο όνομα από αυτό που αναγράφεται στην κάρτα.
• Ο ηλεκτρονικός πλαστογράφος καταρτίζει από την αρχή πιστωτικές κάρτες.
• Έναν άλλο τρόπο πλαστογράφησης του πλαστικού χρήματος συνιστά το γεγονός, ότι με μηχανικά μέσα αποσπούν τους αριθμούς μιας πιστωτικής κάρτας ενός πελάτη από οποιοδήποτε μέρος του κόσμου, καταρτίζουν μια νέα κάρτα λευκή, την οποία δίνουν σε
συνεργαζόμενα καταστήματα, και μέσω των ειδικών συσκευών χρέωσης καρτών, χρεώνουν όποιο ποσό θέλουν ερήμην του κατόχου του αριθμού.
• Με τη χρησιμοποίηση απ' ευθείας κλεμμένης ή απολεσθείσας πιστωτικής κάρτας για αγορές μέσω του Διαδικτύου, μικρής αξίας που δεν χρειάζεται έγκριση.
Ως προς την παραχάραξη χαρτονομισμάτων κυριαρχούν δύο τρόποι:
α) Ο τρόπος του Offset, όπου ο παραχαράκτης τυπώνει τα χαρτονομίσματα σε έγχρωμα τυπογραφικά μηχανήματα (καλούπια).
β) Ο τρόπος του Inkjet, όπου ο παραχαράκτης εκτυπώνει χαρτονομίσματα στον υπολογιστή
με τη βοήθεια του scanner.
• Η αφαίρεση-τροποποίηση δεδομένων διαπράττεται με τη διαγραφή ή τροποποίηση των δεδομένων που είναι καταχωρημένα σε έναν Η/Υ από άτομα που δεν έχουν την ανάλογη εξουσιοδότηση από τον ιδιοκτήτη των δεδομένων. Το αδίκημα χαρακτηρίζεται από τον τρόπο διάπραξης (modus operanti) και διαπράττεται από δράστες που έχουν πρόσβαση στον υπολογιστή, αλλά δεν έχουν εξουσιοδότηση να προβούν στις παραπάνω ενέργειες ή έχουν δικαίωμα πρόσβασης στο χώρο όπου είναι εγκαταστημένος ο υπολογιστής, χωρίς δικαίωμα χρήσης αυτού, υποκλέπτοντας με διάφορους τρόπους την κωδικοποιημένη είσοδο του συστήματος. Το αδίκημα μπορεί να διαπραχθεί και από απόσταση αν ο υπολογιστής επιτρέπει την πρόσβαση και ο δράστης διαθέτει τον απαραίτητο εξοπλισμό, με αποτέλεσμα να διασπά την ηλεκτρονική ασφάλεια του.
• Ο Δούρειος Ίππος διαπράττεται με την παράνομη προσθήκη εντολών σε προγράμματα Η/Υ που έχουν δημιουργηθεί για τη διεκπεραίωση συγκεκριμένων εργασιών. Τα προγράμματα αυτά οφείλουν την ονομασία τους στο γνωστό «Δούρειο Ίππο», καθώς ενώ φαινομενικά εκτελούν μόνο την εργασία για την οποία έχουν δημιουργηθεί, στην πραγματικότητα μαζί με αυτή ο παράνομα προστεθείς κώδικας εκτελεί ανεπιθύμητες ή ζημιογόνες λειτουργίες. Για παράδειγμα, ο υπάλληλος μιας τράπεζας που εργάζεται στο μηχανογραφικό της τμήμα εισάγει τον απαραίτητο κώδικα σε ένα πρόγραμμα διαχείρισης των αναλήψεων των πελατών και δίνει εντολές και οδηγίες στο υπολογιστικό σύστημα να μην καταχωρήσει τις αναλήψεις από συγκεκριμένους λογαριασμούς, ενώ στην οθόνη του τερματικού που υπάρχει στο ταμείο, να δείχνει ότι η συναλλαγή έγινε κανονικά.
• Η μέθοδος Σαλαμοποίησης διαπράττεται με την τροποποίηση προγραμμάτων που είναι εγκαταστημένα στον υπολογιστή με την προσθήκη του απαραίτητου κώδικα λογισμικού, ώστε διάφορα μικροποσά αφαιρούνται από λογαριασμούς, ή κατά τη διαδικασία των συναλλαγών να καταχωρούνται σε άλλον προκαθορισμένο λογαριασμό. Λαμβάνοντας όλες τις προφυλάξεις, όπως η στρογγυλοποίηση των χρηματικών ποσών να γίνονται κατά τέτοιο τρόπο, ώστε να μη γίνεται εύκολα αντιληπτή. Τα θύματα συνήθως δεν αντιλαμβάνονται την εγκληματική πράξη λόγω του ασήμαντου του ποσού.

• Το Superzapping διαπράττεται με τη χρησιμοποίηση του ειδικού προγράμματος αποκατάστασης ενός υπολογιστή που έχει «καταρρεύσει» και δεν λειτουργεί. Το πρόγραμμα αυτό το έχουν στη διάθεσή τους ο διαχειριστής του συστήματος ή εξουσιοδοτημένα άτομα και σε περίπτωση μη λειτουργίας του, το χρησιμοποιεί για να παρακάμψει τα συστήματα ασφαλείας και να μπορεί να μπει σε όλα τα προγράμματα. Αν λοιπόν αυτό το πρόγραμμα πέσει στα χέρια άλλου είναι δυνατόν να μετατραπεί σε εργαλείο τέλεσης εγκληματικών πράξεων με Η/Υ.
• Η ηλεκτρονική κατασκοπεία διαπράττεται με τη χρησιμοποίηση Η/Υ ή τερματικών για να συνδεθούν σε υπολογιστή και αφού «σπάσουν» τους κωδικούς ασφάλειας, γίνονται γνώστες πληροφοριών ζωτικού ενδιαφέροντος για λόγους κατασκοπείας μεταξύ κρατών, για να παρακολουθήσουν πολιτικούς αντιπάλους, καθεστωτικούς αντιφρονούντες, βιομηχανικές δραστηριότητες. Η ηλεκτρονική κατασκοπεία σχετίζεται περισσότερο με τον ανταγωνισμό των επιχειρήσεων και αποτελεί την ιδιαίτερα συνηθισμένη μορφή ηλεκτρονικού οικονομικού εγκλήματος. Φυσικοί αυτουργοί της ηλεκτρονικής κατασκοπείας μπορεί να είναι υπάλληλοι της επιχείρησης ή του οργανισμού που χρηματίζονται, ή δίνουν στοιχεία στον ανταγωνιστή της επιχείρησης, ή συνδέουν τα υπολογιστικά συστήματα του χρηματοδότη τους με το υπολογιστικό σύστημα της επιχείρησης ή του οργανισμού που εργάζονται. Τις τελευταίες δεκαετίες, με την ταχύτατη ανάπτυξη της τεχνολογίας μπορεί να γίνει ηλεκτρονική κατασκοπεία σε βάρος υπολογιστικών συστημάτων από απόσταση μέσω των ηλεκτρονικών πεδίων και της ακτινοβολίας που εκπέμπουν τα τερματικά των υπολογιστών (ακτινοβολία Van Eck).

Η παραβίαση της ιδιωτικής ζωής (των δεδομένων προσωπικού χαρακτήρα) διαπράττεται από οποιονδήποτε που με την χρησιμοποίηση των σύγχρονων υπολογιστών γίνεται γνώστης προσωπικών πληροφοριών. Η ιδιωτική και προσωπική ζωή των ανθρώπων αναγνωρίζεται ως ένα από τα θεμελιώδη αγαθά της ανθρώπινης ύπαρξης, στενά συνυφασμένο με την προσωπικότητα και την ανθρώπινη αξιοπρέπεια. Το Ελληνικό Σύνταγμα του 1975 στο άρθρο του 9, παράγραφος 1, θεωρεί το δικαίωμα της ιδιωτικής και οικογενειακής ζωής ως προστατευόμενο αγαθό και απαραβίαστο. Για την προστασία της συγκεκριμένης θεμελιακής αξίας θεσπίστηκαν ισχυροί κανόνες δικαίου. Ωστόσο, η προστασία των πολιτών από την παράνομη δημοσιοποίηση των προσωπικών στοιχείων τους εξακολουθεί να συνιστά μία δύσκολη υπόθεση. Λίστες με ευαίσθητα προσωπικά στοιχεία, με συνδυασμένες πληροφορίες, πωλούνται από δημόσιες υπηρεσίες, κρατικούς φορείς, ιδιωτικά νοσηλευτήρια, μαιευτήρια, πιστωτικά ιδρύματα, επιμελητήρια, μητροπόλεις και εταιρείες. Επίσημα ή μέσω υπαλλήλων που αμείβονται αδρά, τα προσωπικά δεδομένα, αλλάζουν χέρια, κυκλοφορούν λαθραία τις περισσότερες φορές στην αγορά. Συνήθως υπεύθυνοι για τις διαρροές ευαίσθητων πληροφοριών είναι ορισμένοι υπάλληλοι που έχουν πρόσβαση στα αρχεία και τα πωλούν έναντι χρημάτων. Οι τεράστιες δυνατότητες των Η/Υ και των Επικοινωνιών, η δυνατότητα ηλεκτρονικής αποθήκευσης τεραστίου όγκου πληροφοριών, η ταχύτητα επεξεργασίας πληροφοριών, καθιστούν εφικτή τη συγκέντρωση πληροφοριών σχετικών με την προσωπική ζωή των πολιτών, τις οικονομικές δραστηριότητες και τα πλάνα ανάπτυξης των επιχειρήσεων ή απόρρητων πληροφοριών κρατικών υπηρεσιών. Η χρήση συστημάτων όπως ο «Ενιαίος Κωδικός Αριθμός Μητρώου» (ΕΚΑΜ) παρέχουν τη δυνατότητα συσχέτισης στοιχείων και μπορεί να επιφέρουν κινδύνους παραβίασης της ιδιωτικής ζωής του ατόμου και λήψης αποφάσεων σχετικά με το άτομο αυτό μέσα από την απρόσωπη εικόνα, την οποία είναι δυνατόν να συνθέσουν τα αποτελέσματα αυτόματης επεξεργασίας στοιχείων. Ο Ενιαίος Κωδικός Αριθμός Μητρώου συνοδεύει πλέον κάθε έλληνα πολίτη και περιλαμβάνει: το δελτίο

ταυτότητας, τις ληξιαρχικές πράξεις, το εκλογικό βιβλιάριο και τον αριθμό εκλογικού καταλόγου, το διαβατήριο, το ασφαλιστικό βιβλιάριο, το φορολογικό μητρώο, την άδεια οδηγού, το μητρώο αρρένων, το δημοτολόγιο, το προξενικό μητρώο, το ποινικό μητρώο κλπ. Στις υπηρεσίες του υπουργείου Εσωτερικών εκτιμάται ότι σε σύντομο χρονικό διάστημα η έκδοση των νέων προσωρινών δελτίων ταυτότητας και η εγγραφή των νεογέννητων στα ληξιαρχεία, στα δημοτολόγια κλπ. θα πραγματοποιείται με βάση τον ΕΚΑΜ. Επίσης, η χρήση του πλαστικού χρήματος για τις οικονομικές συναλλαγές μπορεί να παράσχει πληροφορίες σχετικές με την προσωπική ζωή, τις κινήσεις και τις συνήθειες του πολίτη στο βαθμό που αυτές αντανακλώνται στις συναλλαγές του.

Τραπεζικές συναλλαγές (λ.χ. η ηλεκτρονική μεταφορά κεφαλαίων) είναι πάντα ευάλωτες σε ηλεκτρονικές επιθέσεις παρά τα αυστηρά μέτρα ασφάλειας. Η μεγάλη συγκέντρωση ζωτικών πληροφοριών στον ίδιο χώρο ενέχει τον κίνδυνο εγκληματικών προσβολών. Φανταστείτε τι θα συμβεί αν ηλεκτρονικοί εισβολείς επιτεθούν σε ένα σύστημα, στο οποίο είναι καταχωρημένες πληροφορίες ύψιστης κρατικής ασφάλειας και τις καταστρέψουν ή προβούν σε τροποποίησή τους ή τις αντιγράψουν και τις διοχετεύσουν σε εχθρικές υπηρεσίες!

• Η εισβολή των ιών στους Η/Υ είναι οι λεγόμενες λογικές βόμβες που ανήκουν στην κατηγορία των βλαπτικών προγραμμάτων (ιομορφές-viruses) και είναι γραμμένες με τέτοιο τρόπο, ώστε να προκαλούν κάποιου είδους ζημιά στα αρχεία ενός υπολογιστή. Οι συγκεκριμένοι ιοί συνδέονται με άλλα προγράμματα και είναι προγραμματισμένοι να δράσουν, όταν οι χρήστες λειτουργήσουν αυτά τα προγράμματα. Ο ιός μπορεί να πολλαπλασιάζει τον εαυτό του και να προσκολλάται σε όλα τα προγράμματα που ήδη βρίσκονται στο σκληρό δίσκο. Η επίδραση των ιών στο δίσκο ή στη μνήμη του υπολογιστή είναι καταστροφική και χάνονται τα δεδομένα που έχουν αποθηκευτεί ή τα εγκαταστημένα προγράμματα, οπότε ο υπολογιστής ή γίνεται αδρανής ή φέρνει λάθος αποτελέσματα. Ο πιο απλός τρόπος διάδοσης των ιών είναι η ανταλλαγή δισκετών μεταξύ των χρηστών, χωρίς να προηγηθεί έλεγχός τους, είτε μέσω Διαδικτύου με την αποστολή email. Επίσης, οι ιοί μπορούν να διαδοθούν από παράνομο λογισμικό ή από παράνομα αντίγραφα παιχνιδιών. Διάσημοι ιοί που έχουν εμφανιστεί μέχρι σήμερα είναι οι Melissa, Chernobyl, Bubbleboy, Laroux, Ethan, Market, Pretty Park, Harry, Explore Zip κ.α. Αναμφίβολα, οι ιοί που εκμεταλλεύονται τις δυνατότητες του Διαδικτύου θα κυριαρχήσουν μέσα στα επόμενα χρόνια.

Ας μην ξεχνάμε ότι τα νέα οπλικά συστήματα βασίζονται σε ηλεκτρονικά μέσα. Η διατάραξη της σωστής λειτουργίας των οπλικών συστημάτων αποτελεί συνήθως στόχο εχθρικών πράξεων. Οι υπολογιστές αναμφίβολα μπορούν να χρησιμοποιηθούν για πολεμικούς σκοπούς. Για παράδειγμα, το 1999 στην πολεμική αντιπαράθεση των Νατοϊκών Δυνάμεων εναντίον της Γιουγκοσλαβίας χρησιμοποιήθηκαν «έξυπνες βόμβες». Συνεπώς τα σύγχρονα όπλα θα αποτελούνται από:

• **Καταστρεπτικό λογισμικό**: Ιοί ή προγράμματα «εμφυτευμένα» σε επεξεργαστές, τα οποία βρίσκονται σε σύγχρονα οπλικά συστήματα, θα μπορούν κάποια δεδομένη στιγμή να εκτελούν εντολές αντίθετες με τις εντολές του χειριστή. Αυτοί οι υπολογιστικοί ιοί είτε θα μπορούν να εμφυτεύονται με κάποιον εξωγενή παράγοντα (π.χ. από κάποιον κατάσκοπο) είτε θα είναι ενσωματωμένοι από τον κατασκευαστή τους στο υλικό, δίνοντας το δικαίωμα σε αυτόν να αχρηστεύει τα οπλικά συστήματα που έχει πουλήσει με το πάτημα ενός κουμπιού. Η προσωρινή συμμαχία του κατασκευαστή της πλειονότητας των οπλικών συστημάτων μιας χώρας με τον αντίπαλο θα είναι ικανή για τη χωρίς όρους παράδοση.

• **Ηλεκτρονικές παρεμβολές:** Οι ηλεκτρονικές παρεμβολές χρησιμοποιούνται σε πολεμικές επιχειρήσεις για αχρήστευση ή αλλοίωση των επικοινωνιών.

• **Όπλα ηλεκτρομαγνητικών παλμών:** Τέτοια όπλα εξουδετερώνουν τον ηλεκτρονικό εξοπλισμό του αντιπάλου. Ήδη έχουν αναπτυχθεί όπλα αυτού του είδους σε μέγεθος χαρτοφύλακα. Χρησιμοποιούνται και για την εξουδετέρωση αεροπλάνων, ελικοπτέρων, κατευθυνόμενων πυραύλων κ.α.
• **Καταστρεπτικά μικρόβια:** Μεταλλαγμένα μικρόβια θα μπορούν να «τρώνε» επιλεκτικά τα ηλεκτρονικά στοιχεία.
• **Μεταμόρφωση (morphing)** σε βίντεο: Με την τεχνική της μεταμόρφωσης μπορεί να εμφανιστεί ένα βίντεο με ένα οποιοδήποτε πρόσωπο να λέει οτιδήποτε. Αυτή η τεχνική θα παίξει ρόλο στον ψυχολογικό πανικό του στρατού και του λαού.
Ας επανέλθουμε στους ιούς και στην ταξινόμησή τους σε δύο κατηγορίες:
• **Στα σκουλήκια**. Το σκουλήκι είναι ένα πρόγραμμα που παράγει αντίγραφα του εαυτού του χωρίς να μολύνει άλλα προγράμματα στον υπολογιστή. Διαδίδεται αστραπιαία μέσω του ηλεκτρονικού ταχυδρομείου γιατί είναι προγραμματισμένο να αποστέλλεται σε πολλές ή όλες τις διευθύνσεις email, που βρίσκονται αποθηκευμένες στην ηλεκτρονική ατζέντα του χρήστη.
• Ο **Δούρειος Ίππος** είναι ένα πρόγραμμα που κρύβεται μέσα σε ένα άλλο μέχρι τη στιγμή που είναι προγραμματισμένο να δράσει στον υπολογιστή.

1.3. Hacking

Η παράνομη σύνδεση ενός ατόμου σε κάποιον υπολογιστή αποδίδει την έννοια του hacking ή cracking. Η συγκεκριμένη πράξη αποδίδεται σε άτομα με υψηλές γνώσεις στον τομέα των υπολογιστών και επικοινωνιών, οι γνωστοί hackers που εισχωρούν στο σύστημα μέσω δικτύου και καταφέρνουν να παραβιάσουν τα συστήματα ασφαλείας. Ο όρος hacking ορίζεται ως μια εκλεκτή τέχνη ασκούμενη από μικρές ομάδες από εξαιρετικά χαρισματικά άτομα (Steele, 1983). Το hacking στην αρχική του μορφή ήταν μια πνευματική πρόκληση. Το κύριο ενδιαφέρον των περισσοτέρων hackers είναι η κατανόηση των εσωτερικών μηχανισμών ενός συστήματος. Ωστόσο, η εμπορευματοποίηση του λογισμικού ευθύνεται έμμεσα για την εμφάνιση του hacking στην εγκληματική του μορφή.
Είναι γεγονός ότι πολλοί οργανισμοί κατέχουν τα δικαιώματα συλλογής, διατήρησης, και χρήσης πληροφοριών που είναι σε ψηφιακή μορφή. Η συγκέντρωση πληροφοριών σε ισχυρούς υπολογιστές αυξάνει σημαντικά την επιρροή τους ως προς τη διακίνηση των πληροφοριών. Φυσικό επακόλουθο είναι η αντίδραση των hackers που διεκδικούν επίσης ιδιαίτερα δικαιώματα, όσον αφορά την πρόσβαση και την κατοχή πληροφοριών.
Οι hackers ακόμη και όταν διεισδύουν σε υπολογιστές το θεωρούν ως μια διαδικασία κατάκτησης της γνώσης και δεν πειράζουν ούτε τροποποιούν τίποτε. Γι' αυτό συνήθως αντιπαθούν τους crackers, τους οποίους θεωρούν ως αδαείς προγραμματιστές (με μεγάλη όμως υπομονή) που δεν έχουν να κάνουν τίποτε καλύτερο, από το να διεισδύουν σε υπολογιστικά συστήματα, αφήνοντας εμφανή ίχνη πίσω τους, ίχνη που πολλές φορές είναι καταστροφικά για τα συστήματα. Τα συγκεκριμένα άτομα μπορούν να χωριστούν σε τέσσερις βασικές κατηγορίες:
• Οι εγκληματίες που εκμεταλλεύονται τις αδυναμίες των συστημάτων και διεισδύουν κυρίως σε τραπεζικά συστήματα κάνοντας «ηλεκτρονικές ληστείες». Η ουσιώδης διαφορά τους με τις άλλες κατηγορίες είναι ότι δεν χρησιμοποιούν τις απλοποιημένες μεθόδους και τα μέσα που χρησιμοποιούν οι ερασιτέχνες και που είναι έως ένα βαθμό αντιμετωπίσιμες.

• Οι ειδικοί που είναι ενημερωμένοι σε θέματα Η/Υ, σε επικοινωνίες δεδομένων και τηλεπικοινωνίες. Μπορούν να μπουν σε ένα σύστημα με ερευνητικές μεθόδους. Αρκούνται στο σπάσιμο του συστήματος και μετά αποσύρονται.
• Οι βάνδαλοι που είναι η μειοψηφία. Συνήθως μπαίνουν σε δίκτυα ή υπολογιστές και αφήνουν μηνύματα ή διαγράφουν αρχεία. Αν και ξεκινούν από παιχνίδια συνήθως καταλήγουν σε καταστροφές ή απόκτηση απορρήτων στοιχείων, που τα χρησιμοποιούν για να προξενήσουν ζημιές.
• Οι swappers είναι η πλειοψηφία και αποτελούνται από άτομα νεαρής ηλικίας που δρουν ακόμη με τη νοοτροπία του παιχνιδιού. Γνωρίζουν συνήθως αρκετά γύρω από τους υπολογιστές. Δεν θεωρούν τους εαυτούς τους κλέφτες, αλλά σαν έξυπνους που ξεπερνούν τις στημένες δυσκολίες. Είναι πιο επικίνδυνοι από τους ειδικούς, γιατί χρειάζονται πολύ λιγότερα κίνητρα για να περάσουν από την ακίνδυνη στην καταστρεπτική επέμβαση.

Μερικές φορές το hacking περιλαμβάνει πράξεις εκδίκησης, συνήθως από έναν δυσαρεστημένο υπάλληλο εναντίον ενός προηγούμενου εργοδότη. Για άλλους το hacking αντιπροσωπεύει έναν τρόπο ζωής που στηρίζεται πάνω στην κοινωνική ανεπάρκεια, ανάμεσα σε διάφορα διανοητικώς ικανά άτομα το επονομαζόμενο σύνδρομο των computer nerd που επηρεάζει κυρίως τους αρσενικούς εφήβους, μεταξύ των ηλικιών 14 και 16. Αυτά τα άτομα είναι συνήθως αυτοδίδακτα, απολαμβάνουν διανοητικά παιχνίδια, και δεν είναι σεξουαλικά ενεργά. Μάλιστα μια περίπτωση ψύχωσης με τον υπολογιστή έχει ήδη αναφερθεί στην Κοπεγχάγη της Δανίας. Προφανώς, ο αναφερόμενος νεαρός γοητεύτηκε από τον υπολογιστή του τόσο πολύ ώστε του ήταν αδύνατο να ξεχωρίσει τον πραγματικό κόσμο από τα υπολογιστικά προγράμματα και μιλούσε σε γλώσσα προγραμματισμού όταν εκτελούσε συνηθισμένες καθημερινές δουλειές. Οι περισσότεροι hackers χρησιμοποιούν μόνο ένα μικρό σύνολο εξαρτημάτων. Ένα μόντεμ, έναν προσωπικό υπολογιστή και διάφορα λογισμικά επικοινωνίας. Όταν το μόντεμ του hacker έχει συνδεθεί με το μόντεμ της μηχανής-στόχου, και οι δύο συσκευές θα μετατρέψουν τα αναλογικά τηλεφωνικά σήματα πίσω σε ψηφιακά και θα επιτρέψουν στην επικοινωνία να προχωρήσει. Γενικά το λογισμικό επικοινωνιών που χρησιμοποιεί ο hacker προβάλλει υψηλής ποιότητας εξομοίωση σε μια μεγάλη κλίμακα δημοφιλών τύπων τερματικών και μερικές φορές τέτοια πακέτα έχουν έναν αριθμό ενσωματωμένων χαρακτηριστικών που βοηθούν τον hacker. Σύμφωνα με έρευνα του National Council on Crime and Delinquency (NCCD) των ΗΠΑ, η ηλικία των hackers κυμαίνεται μεταξύ 20 και 50 ετών με μεγαλύτερη έξαρση στην ηλικία των 22 ετών.

Οι περισσότεροι από αυτούς (75%) είχαν κολεγιακή μόρφωση. Το 60% ενήργησε όχι προμελετημένα αλλά λόγω ευκαιριακών παραγόντων, ενώ υπήρξε ένα μικρό ποσοστό που εντόπισε κάποια αδυναμία του συστήματος και μετά από αρκετό διάστημα και προβληματισμό δεν μπόρεσε να αντισταθεί στον πειρασμό. Το 50% δεν προβληματίστηκε καθόλου για τις συνέπειες των ενεργειών τους, ενώ οι υπόλοιποι το σκέφτηκαν, αλλά αποφάσισαν να ρισκάρουν.

Αξίζει να σημειωθεί ότι στην Ελλάδα έχει δημιουργηθεί ομάδα hackers με την ονομασία «Δικτυακή Πάλη-Νοέμβρης 1998», η οποία έχει πολιτική χροιά. Το 1996 συστάθηκε η Ειδική Ομάδα Αντιμετώπισης του Ηλεκτρονικού Εγκλήματος που λειτουργεί στη Διεύθυνση Ασφάλειας Αττικής και στο Τμήμα Οικονομικών Εγκλημάτων. Τα μέλη της συγκεκριμένης ομάδας είναι άριστα εκπαιδευμένα και παρακολουθούν σε τακτά χρονικά διαστήματα ειδικά σεμινάρια. Το συγκεκριμένο τμήμα οργανώνεται και εξελίσσεται σύμφωνα με το πρότυπο του Βρετανικού «Computer Crime Unit» και των τμημάτων «Cyber Crime». Οι αστυνομικοί του

Κυβερνοχώρου αναζητούν και εντοπίζουν τα ίχνη που αφήνουν οι εν δυνάμει ηλεκτρονικοί εγκληματίες χρήστες. Συγκεκριμένα, παρακολουθούν το Διαδίκτυο, εντοπίζουν ύποπτες κινήσεις, ανιχνεύουν τα ίχνη των δραστών, γίνονται αόρατοι για να παρακολουθούν συνομιλίες στο Διαδίκτυο και σε chat rooms, όπου υπάρχουν βάσιμες υποψίες πως γίνονται παράνομες συναλλαγές και συνεννοήσεις, συνδυάζουν τις πληροφορίες, στοιχειοθετούν κατηγορίες και φτάνουν στους ενόχους.

1.4. Πορνογραφία

Τα παιδιά σε όλον τον κόσμο είναι αθώα, ευάλωτα και δε μπορούν να επιβιώσουν μόνα τους. Είναι, επίσης, περίεργα, ενεργητικά και ελπίζουν. Ο χρόνος τους θα πρέπει να είναι γεμάτος χαρά και ειρήνη, παιχνίδι, μάθηση και ανάπτυξη. Το μέλλον τους θα πρέπει να κτίζεται μέσα σε πνεύμα αρμονίας και συνεργασίας. Η ζωή τους θα ωριμάσει, καθώς θα διευρύνονται οι προοπτικές τους και θα κερδίσουν εμπειρίες.

1.4.1. Ορισμός του πορνογραφικού υλικού ανηλίκων και η νομική αντιμετώπιση των δραστών κατά το ελληνικό δίκαιο

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

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

1.4.2. Οι διαστάσεις του εγκλήματος σε διεθνές και ελληνικό επίπεδο

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

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

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

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

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

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

Έχει χαρακτηριστεί «παράδοξο» το πώς μια από τις μεγαλύτερες επιτεύξεις του περασμένου αιώνα, το ίντερνετ, από δημοκρατικό «forum ελεύθερης ανταλλαγής απόψεων» κατέστη φορέας σεξουαλικής κακοποίησης παιδιών και παιδοφιλίας Είναι, όμως, αναγκαία η επισήμανση ότι η δημιουργία του ίντερνετ δε συνιστά σε καμία περίπτωση το μόνο λόγο της ύπαρξης του φαινομένου της παιδικής πορνογραφίας.

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

1.4.3. Το προφίλ του δράστη της παιδικής πορνογραφίας στο διαδίκτυο

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

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

Αξιοσημείωτο είναι, επιπρόσθετα, το γεγονός ότι οι επιτήδειοι του είδους κάνουν χρήση παραπλανητικών κειμένων ή φωτογραφιών, ώστε να προσελκύσουν τους χρήστες του διαδικτύου στις ιστοσελίδες τους. Συνήθως, εμφανίζονται χαμογελαστά παιδιά να παίζουν ξέγνοιαστα, να επιδίδονται σε ερωτικές περιπτύξεις ή ακόμη και να ποζάρουν με νάζι, όπου, πατώντας απλώς ένα πλήκτρο, ο χρήστης μεταφέρεται στα «άδυτα» της ιστοσελίδας. Να σημειωθεί ακόμη πως αρκετοί από τους δημιουργούς των υπό αναφορά ιστοσελίδων χωρίζουν τα παιδιά ανά κατηγορίες και πιο συγκεκριμένα, ανάλογα με την ηλικία τους ή το πόσο αποκαλυπτικές είναι οι πόζες και ερωτικές τους περιπτύξεις, με συνακόλουθη αύξηση του χρηματικού ποσού που πρέπει να καταβάλει ο χρήστης, ώστε να αποκτήσει πρόσβαση. Επιπρόσθετα, μέσω των chat rooms, ορισμένοι παιδεραστές ξεκινούν τη συνομιλία με τα υποψήφια θύματά τους, με στόχο τη δημιουργία ενός κλίματος εμπιστοσύνης και την πιο άνετη επικοινωνία. Ο ανωτέρω στόχος επιτυγχάνεται με αργούς ρυθμούς είτε μέσω της

αποστολής φωτογραφιών παιδικής πορνογραφίας είτε με φράσεις όπως: «*είναι κάτι το φυσιολογικό*», «*είναι κάτι το ωραίο*», ή «*δεν θα ήθελες κι εσύ να δεις το ωραίο γυμνό σου κορμάκι στο διαδίκτυο, όπως κάνουν και άλλα παιδιά;*».

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

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

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

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

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

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

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

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

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

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

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

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

1.4.4. Καταληκτική παρατήρηση

Από τα παραπάνω συνάγεται το συμπέρασμα ότι δεν υφίσταται ομοιογένεια ως προς το προφίλ του ατόμου που διαπράττει το έγκλημα της πορνογραφίας ανηλίκων στο διαδίκτυο. Το μόνο που μπορεί κανείς να επισημάνει με ασφάλεια είναι ότι κατά κύριο λόγο αποτελούν άντρες. Η ανομοιογένειά τους οφείλεται – σωρευτικά με άλλους παράγοντες – στη διαφορά των κινήτρων τους. Προκύπτει, πάντως, ότι δεν χαρακτηρίζεται το σύνολό τους από σεξουαλικές διαταραχές, (π.χ. παιδοφιλία).

2. Παραδείγματα που έχουν σχέση με το έγκλημα στον κυβερνοχώρο

Είναι γνωστό ότι η χώρα μας κατατάσσεται στις τελευταίες χώρες, στη λίστα με τους χρήστες ίντερνετ, πράγμα το οποίο φυσικά σημαίνει, ότι και οι γνώσεις μας γύρω από το θέμα, είναι εκ των πραγμάτων περιορισμένες.

· Ένα πρόβλημα περί εκβιασμών μέσω blog στο Ιντερνετ.
Λόγω των καταγγελιών για τη διάπραξη και κακουργήματος, όπως ο εκβιασμός, έχει αρθεί το απόρρητο και έτσι οι αξιωματικοί της Δίωξης Ηλεκτρονικού Εγκλήματος στο πλαίσιο ερευνών του 5ου τακτικού ανακριτή έχει φτάσει στα ηλεκτρονικά ίχνη των πέντε διαχειριστών. Τη μήνυση, για εκβίαση σε βαθμό κακουργήματος και συκοφαντική δυσφήμηση σε βαθμό πλημμελήματος, είχε υποβάλλει ο δημοσιογράφος που δέχθηκε τον εκβιασμό πριν από ένα χρόνο.

· Ένας 20χρονος σώθηκε από αυτοκτονία με προτροπή μέσα από το Ιντερνετ.
20χρονος σώθηκε την τελευταία στιγμή από αστυνομικούς της δίωξης ηλεκτρονικού εγκλήματος γατί είχε εκφράσει την πρόθεσή του μέσω Ίντερνετ συζητώντας σε τσατ ρουμ να αυτοκτονήσει. Οι αστυνομικοί εντόπισαν τα ηλεκτρονικά του ίχνη και κατάφεραν να βρουν και τη διεύθυνση του σπιτιού του με αποτέλεσμα και με τη βοήθεια ψυχολόγου από μη κυβερνητική οργάνωση της Εκκλησίας της Ελλάδος να τον στηρίξουν ψυχολογικά για να μην προχωρήσει σε αυτή την ενέργεια. Τα τελευταία 2 χρόνια η υπηρεσία δίωξης ηλεκτρονικού εγκλήματος έχει διασώσει 8 ενήλικους και ανήλικους που ήθελαν να αυτοκτονήσουν.

· Ο «φίλος» έστελνε ύπουλα Sms για να τους χωρίσει!
Είναι ο ανθρώπινος ψυχισμός φτιαγμένος έτσι, με σκοπό να έχει την τάση να εμπιστεύεται περισσότερο τους τρίτους, παρά αυτούς που αγαπά! Λίγο έλειψε να φτάσει στο χωρισμό ένα ζευγάρι που πέρασε τρεις μήνες απίστευτης έντασης, ώσπου να ανακαλύψει τις ύπουλες προθέσεις ενός «φίλου» που, με τη βοήθεια της τεχνολογίας ! Μια υπόθεση, που, είχε ευτυχή κατάληξη για τους πρωταγωνιστές της, έναν 32χρονο πολιτικό μηχανικό και μια 28χρονη στέλεχος μεγάλης εταιρείας πληροφορικής. Λίγο έλειψε, όμως, να τινάξει στον αέρα ένα γάμο με διάρκεια μόλις ενάμιση χρόνου, που είχε και έχει όλες τις προοπτικές να πετύχει! Και οι δύο πέρασαν μια κόλαση ώσπου να μάθουν την αλήθεια. Όλα ξεκίνησαν λίγο μετά την πρώτη επέτειο γάμου του ζευγαριού. Πρώτος ο σύζυγος άρχισε να δέχεται ανώνυμα SMS στο κινητό του από κάποια γυναίκα που δεν αποκάλυπτε την ταυτότητά της και ισχυριζόταν ότι είναι ερωτευμένη μαζί του. Ο άνθρωπος δεν έδωσε σημασία. Λίγες μέρες μετά, SMS άρχισε να παίρνει και η σύζυγος, από μια άγνωστη της συνάδελφο του άντρα της που ήθελε το καλό τους και της συνιστούσε να προσέχει. Αργότερα, τα μηνύματα έγιναν πιο συγκεκριμένα: «Έχει σχέσεις με τη γραμματέα του», «Κλείνονται συνεχώς στο γραφείο του» και άλλα παρόμοια! Η 28χρονη άρχισε να πείθεται όταν αναζήτησε επανειλημμένα στο γραφείο τον σύζυγό της και η «ύποπτη» γραμματέας δεν τη συνέδεσε με την πρόφαση ότι είχε σύσκεψη και όταν, μια δυο φορές το κινητό του ήταν κλειστό! Η θύελλα ξέσπασε ένα ξημέρωμα, όταν ξαφνικά χτύπησε μήνυμα στο κινητό του 32χρονου. Εκείνος κοιμόταν, αλλά η σύζυγος αγρυπνούσε. Άνοιξε το SMS και διάβασε έκπληκτη: «Σε λατρεύω. Δεν μπορώ χωρίς εσένα»! Έξαλλη από οργή τον ξύπνησε και το τι ακολούθησε δεν περιγράφεται! Μάταια ο δυστυχής άνδρας διαμαρτυρόταν ότι δεν συμβαίνει κάτι. Η 28χρονη του

ανακοίνωσε ότι χωρίζουν κι έφυγε για το πατρικό της! Πληγωμένος αλλά ψύχραιμος ο πολιτικός μηχανικός ζήτησε τη βοήθεια της Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας για να βρει ποιος έστειλε το μοιραίο SMS. Ως αποστολέας εμφανιζόταν ένας περίπλοκος αριθμός. Οι έμπειροι αστυνομικοί κατάλαβαν ότι το μήνυμα είχε σταλεί μέσω δορυφορικού Ιντερνετ. Ωστόσο, είχε αφήσει τα ψηφιακά του ίχνη και δεν άργησαν να τα εντοπίσουν, στον Ινδικό ωκεανό! Όπως αποδείχθηκε, αποστολέας ήταν ένας 35χρονος φίλος του ζευγαριού, που ήταν ερωτευμένος με την κυρία και είχε αποφασίσει να τους χωρίσει!

Ροζ επίθεση χάκερ σε youtube και iTunes

Επίθεση δέχτηκαν σελίδες του ιστότοπου youtube όπου παρουσιάζονταν παράθυρα τα οποία πήγαιναν τον χρήστη σε πορνογραφικές σελίδες ενώ παράπονα έκαναν άνθρωποι με λογαριασμούς του iTunes οι οποίοι κάνουν λόγο για παράνομες αγορές στο όνομά τους.

Αναλυτικότερα, διαμαρτυρίες έχουν καταγραφεί από χρήστες οι οποίοι ισχυρίζονται πως στο λογαριασμό τους στο iTunes πραγματοποιήθηκαν αγορές εφαρμογών εκατοντάδων δολαρίων εν αγνοία τους. Το μεγαλύτερο μέρος των συναλλαγών αφορά διαδικτυακά βιβλία.
Η αμερικανική εταιρία από την πλευρά της δεν έχει κάνει κάποιο σχόλιο σε ερώτηση πάνω στο συγκεκριμένο θέμα που έθεσε η ιστοσελίδα Cnet.
Την Κυριακή (4/7/2010) το youtube δέχτηκε επίθεση από χάκερς με παράθυρα να εμφανίζονται κατά τη διάρκεια ενός βίντεο τα οποία οδηγούσαν σε ροζ sites. Αυτά τα παράθυρα εμφανίζονταν κατά κύριο λόγο σε βίντεο του ανήλικου τραγουδιστή Τζάστιν Μπίμπερ.
Λίγες ώρες μετά την επίθεση εργαζόμενοι στη Google έκλεισαν την τρύπα ασφαλείας.

Η πρώτη μεγάλη απάτη στον ελληνικό κυβερνοχώρο

Το πρώτο ηλεκτρονικό «ριχτάδικο» αποκάλυψε πριν από περίπου έναν μήνα η Δίωξη Ηλεκτρονικού Εγκλήματος. Το διαδικτυακό κατάστημα Megamarket.gr, το οποίο πωλούσε κυρίως ηλεκτρικά και ηλεκτρονικά είδη αλλά και διάφορα άλλα προϊόντα, αφού συγκέντρωσε τις προκαταβολές των πελατών του «εξαφανίστηκε» από την ηλεκτρονική του διεύθυνση. Σύμφωνα με πηγές της Δίωξης Ηλεκτρονικού Εγκλήματος υπάρχει σωρεία καταγγελιών, οι οποίες μαζί με τις μηνύσεις ξεπερνούν τις 1.000. Οι ίδιες πηγές μάλιστα αναφέρουν ότι το Megamarket. gr πριν καταργήσει την ηλεκτρονική του διεύθυνση είχε συγκεντρώσει γύρω στα 500.000 ευρώ και

θύματα της απάτης δεν είναι μόνο οι πελάτες αλλά και οι προμηθευτές του.

Οι καταγγελίες.
Οι ψηφιακές αγορές σύμφωνα με τους ειδικούς κρύβουν παρόμοιους κινδύνους με εκείνες που κάνουν οι καταναλωτές στην πραγματικότητα, χωρίς αυτό να σημαίνει ότι δεν πρέπει να είναι προσεκτικοί. Όπως υποστήριζε παλαιότερη έρευνα του Δικτύου των Ευρωπαϊκών Κέντρων Καταναλωτή το κυριότερο πρόβλημα που αντιμετωπίζουν οι on-line καταναλωτές αφορά την παράδοση των προϊόντων. Ειδικά στην Ελλάδα, το 49% των συμμετεχόντων είχε καταγγείλει ότι δεν παρέλαβε ποτέ αυτά που αγόρασε και το 22% πώς ήταν προϊόντα ελαττωματικά ή με διαφορετικές προδιαγραφές απ' αυτές που επιθυμούσε. Πάντως στην πιο πρόσφατη έρευνα του Παρατηρητηρίου της Κοινωνίας της Πληροφορίας το 93% δήλωσε πώς δεν υπήρξε κανένα πρόβλημα στις ψηφιακές αγορές του.

3. Δίωξη ηλεκτρονικού εγκλήματος

Οι πρώτες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, ιδρύθηκαν στις Ηνωμένες Πολιτείες της Αμερικής, καθότι από εκεί ξεκίνησε το hacking, στα μέσα της δεκαετίας του '70 και αναπτύχθηκε τόσο η τεχνολογία των ηλεκτρονικών υπολογιστών όσο και το Διαδίκτυο. Σήμερα, στις Η.Π.Α. λειτουργούν υπηρεσίες αντιμετώπισης και δίωξης του ηλεκτρονικού εγκλήματος σε κάθε πολιτεία, οι οποίες έχουν τοπική αρμοδιότητα. Οι απειλές, όμως, που προβάλλουν από το οργανωμένο έγκλημα, μέσω του κυβερνοχώρου, οδήγησαν στη σύσταση της US-CERT170 (United States Computer Emergency Readness Team) μιας εθνικής υπηρεσίας που φέρει την κύρια ευθύνη για την ασφάλεια των Η.Π.Α. από επιθέσεις που μπορεί να προκύψουν από τον κυβερνοχώρο. Η US-CERT αποτελεί το επιχειρησιακό κομμάτι της NCSD (National Cyber Security Division), η οποία με τη σειρά της υπάγεται στο Υπουργείο Εσωτερικών. Οι κύριες αρμοδιότητες της US-CERT είναι:
• Η ανάλυση των πιθανών διαδικτυακών απειλών και ευπαθειών και η καταβολή προσπαθειών για τον περιορισμό τους.
• Η ενημέρωση των συναρμόδιων υπηρεσιών για πιθανές δικτυακές απειλές.
• Ο συντονισμός των ενεργειών αντιμετώπισης συμβάντων σχετικών με το Διαδίκτυο.

Σε επίπεδο εξέτασης ψηφιακών τεκμηρίων, το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau Of Investigations – FBI) 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 πάσης 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.ά.
Στην Αγγλία έχει ιδρυθεί Μονάδα Ηλεκτρονικού Εγκλήματος στη 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 στη Royal Canadian Mounted Police.
Στην Αυστραλία έχει συσταθεί το Australian High Tech Crime Centre176 υπαγόμενο στην Ομοσπονδιακή Αστυνομία. Σκοπός του είναι ο συντονισμός των εθνικών προσπαθειών για την πάταξη του ηλεκτρονικού εγκλήματος, καθότι αναγνωρίζει ότι,

η αντιμετώπισή του δυσχεραίνεται από πλήθος εμποδίων νομικών και μη. Για το σκοπό αυτό συνεργάζεται και με άλλες υπηρεσίες στον κόσμο, με τις οποίες μπορεί από κοινού να ερευνήσουν υποθέσεις παράνομης δραστηριότητας στο Διαδίκτυο και να ανταλλάξουν τεχνογνωσία.

- *Δίωξη ηλεκτρονικού εγκλήματος του internet από την καλύτερη υπηρεσία του κόσμου και μορφές ηλεκτρονικού εγκλήματος.*

Όλοι μας και ιδιαίτερα εκείνοι που χρησιμοποιούν το Internet γνωρίζουμε την ραγδαία εξέλιξη της τεχνολογίας, την ανάπτυξη της πληροφορικής και την ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της 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».

- *Δίωξη ηλεκτρονικού εγκλήματος στην Ελλάδα*

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

Ιανουάριος 2006
Ένας 35χρονος κατηγορείται ότι σε συνεργασία με ουκρανικά κυκλώματα εφάρμοζε την απάτη του ψαρέματος (phishing), στο Διαδίκτυο. Έστελνε παραπλανητικά e-mail και μάζευε στοιχεία, με τα οποία διεκπεραίωναν ηλεκτρονικές συναλλαγές πελάτες ελληνικών τραπεζών, μεταξύ αυτών και της Εθνικής. Ένας 67χρονος συνταξιούχος στρατιωτικός και ένας 50χρονος Νιγηριανός, κάτοικος Κύπρου, είχαν στήσει Λοταρία μέσω ιστοσελίδας και e-mails, που υποσχόταν μυθικά ποσά με την προϋπόθεση ότι, οι νικητές θα πλήρωναν τους φόρους. Μέχρι να συλληφθούν είχαν αποσπάσει από ανυποψίαστους χρήστες πάνω από 3,5 εκατομμύρια ευρώ.

Οκτώβριος 2005
Σύλληψη ενός 40χρονου Δανού, ο οποίος έστελνε ηλεκτρονικά μηνύματα, υφάρπαζε προσωπικά δεδομένα και στη συνέχεια αποσπούσε μεγάλα χρηματικά ποσά από τραπεζικούς λογαριασμούς.

Ιούλιος 2005
Εξιχνιάζεται η πρώτη υπόθεση παράνομης κατασκευής όπλων, που διακινούνταν μέσω Διαδικτύου. Οι πωλήσεις γίνονταν μέσω ιστοσελίδας γνωστής εταιρίας δημοπρασιών και τα όπλα, πιστά αντίγραφα των αυθεντικών, παραδίδονταν στους ενδιαφερόμενους μέσω εταιρίας ταχυμεταφορών.

Σεπτέμβριος 2004
Ένας 27χρονος ομολογεί, ότι έβγαζε κρυφά φωτογραφίες μικρών παιδιών, που εντόπιζε στα αποδυτήρια παιδικών κατασκηνώσεων, ποδοσφαιρικών ομάδων και διαφόρων σχολείων, τις οποίες, στη συνέχεια, διακινούσε σε ξένες ιστοσελίδες αντί

αμοιβής. Τον ίδιο μήνα συνελήφθησαν δύο 32χρονοι, οι οποίοι διείσδυσαν στα υπολογιστικά προγράμματα ελληνικής τράπεζας και μετέφεραν χρήματα στους δικούς τους λογαριασμούς. Η αντιμετώπιση των υποθέσεων ηλεκτρονικού εγκλήματος από την Ελληνική Αστυνομία, ουσιαστικά, αρχίζει με την ίδρυση του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος το 2004. Έως τότε, οι υποθέσεις που σχετίζονταν καθ' οποιονδήποτε τρόπο με ηλεκτρονικούς υπολογιστές αντιμετωπίζονταν από το Τμήμα Δίωξης Οικονομικού Εγκλήματος.

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

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

Οι υπηρεσίες αυτές, αν και βρίσκονται στο αρχικό στάδιο σύστασης και λειτουργίας και στερούνται τόσο του απαραίτητου εξοπλισμού (υλικού και λογισμικού) όσο και εξειδικευμένου προσωπικού, έχουν να επιδείξουν σημαντικό έργο στην καταπολέμηση του ηλεκτρονικού εγκλήματος.

Η πρώτη υπόθεση που απασχόλησε το εργαστήριο ήταν το 1995. από εκεί και έπειτα, οι υποθέσεις πολλαπλασιάστηκαν με γεωμετρικούς ρυθμούς, όπως φαίνεται και από το παραπάνω γράφημα. Σήμερα, το εργαστήριο διαθέτει εξειδικευμένο προσωπικό και τεχνικά μέσα για τη διεκπεραίωση απαιτητικών εργασιών.

Το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος είναι στη χώρα μας μια πολύ σημαντική και καλά δομημένη υπηρεσία. Από την αρχή της ίδρυσης και λειτουργίας του έως σήμερα έχει καταφέρει να αποτρέψει και να εξιχνιάσει πλειάδα ηλεκτρονικών παραβάσεων ιδιαίτερα σοβαρών και επικίνδυνων για την ασφάλεια μας στο διαδίκτυο. Είναι με λίγα λόγια ο φορέας εκείνος που οφείλει κάποιος να αποτανθεί όταν γίνεται δέκτης μιας συμπεριφοράς στο διαδίκτυο που εντάσσεται στα πλαίσια της παραβατικότητας.

Στο Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος καταγγέλλονται πράξεις όπως η παιδική πορνογραφία και κακοποίηση των παιδιών, η διακίνηση παράνομου - πειρατικού λογισμικού, οι απάτες μέσω διαδικτύου,οι απάτες μέσω πιστωτικών καρτών και το Cracking (ψηφιακοί βανδαλισμοί-Deface και άλλα). Επιπλέον η διακίνηση ναρκωτικών, η εκβίαση μέσω του ιντερνετ και τέλος η συκοφαντική δυσφήμηση και η παραβίαση προσωπικών δεδομένων μέσω του διαδικτύου.

Θεσμοφύλακες της ασφάλειας της χρήσης του διαδικτύου και προαγωγοί της ασφαλούς χρήσης, οι άνθρωποι που πλαισιώνουν την υπηρεσία αυτή έχουν ανώτερες γνώσεις πάνω στο internet και στην ασφάλεια.

4. Μέτρα Ασφάλειας ενάντια στο Ηλεκτρονικό έγκλημα σε Νομικό επίπεδο

4.1. Νομική Διάσταση

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 23.11.2001.
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.

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:

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.
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.

4.2. Προστασία των Domain Names

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

4.3. Παράνομη Διείσδυση σε Δεδομένα

Η χωρίς δικαίωμα διείσδυση – πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του Ποινικού κώδικα.
Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. 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, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων.
2. Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.

3. Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173-CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεσης μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών.

4.4. Προστασία των δεδομένων από ιούς

Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ.
Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

4.5. Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Προσωπικά δεδομένα είναι , σύμφωνα με τον *Νόμο 2472/1997* και την *Οδηγία 95/46/ΕΚ* κάθε πληροφορία που αναφέρεται στο πρόσωπό του κάθε ατόμου, π.χ. το όνομα και το επάγγελμά του ατόμου, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, 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 οι τυχόν ποινικές του διώξεις και καταδίκες.
Για την επεξεργασία και συλλογή προσωπικών δεδομένων είναι απαραίτητη άδεια από την Αρχή Προστασίας Προσωπικών Δεδομένων. Οι οδηγίες για την χορήγηση άδειας επεξεργασίας αναλύονται στην *Κανονιστική Πράξη 1/1999 ΑΠΠΔ* σχετικά με την ενημέρωση υποκειμένου των δεδομένων *κατ' άρθρο 11 Ν. 2472/1997* και στην *Απόφαση 408.1998 ΑΠΠΔ* σχετικά με την ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου.
Η συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί έναν από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική σφαίρα και στην ιδιωτική ζωή του ατόμου. Κάθε δραστηριότητα του σύγχρονου ανθρώπου γίνεται καθημερινά αντικείμενο επεξεργασίας και ανάλυσης γεγονός που χρήζει αντιμετώπισης και νομική κατοχύρωσης.
Στην Ελλάδα και την Ευρώπη ισχύουν πολλά νομοθετήματα που προστατεύουν τους πολίτες από την επεξεργασία προσωπικών δεδομένων σε διάφορους τομείς. Έτσι έχουμε:
Τον *Νόμο 2774.1999*, 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 της 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 η "Αρχή Διασφάλισης Απορρήτου" *(Νόμος 3115.2003*) και στην Ευρώπη "Ο Ευρωπαίος Επόπτης Προσωπικών Δεδομένων" *(Απόφαση 1247.2002.ΕΚ*) είτε ρυθμίζουν την διαβίβαση προσωπικών δεδομένων από την Κοινότητα σε άλλες χώρες *(Απόφαση 2003.490, Απόφαση του Συμβουλίου 2004/644/ΕΚ*).
Η συγκέντρωση και επεξεργασία ηλεκτρονικών δεδομένων αντιμετωπίστηκε από πολύ νωρίς ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική και προσωπική σφαίρα. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση υπάρχει νομοθεσία που ρυθμίζει τα σχετικά με την επεξεργασίας δεδομένων όπως η Οδηγία 2002/58 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και η Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού.

5. Τεχνικά μέτρα αντιμετώπισης Ηλεκτρονικών Εγκλημάτων

Για την αντιμετώπιση των ηλεκτρονικών εγκλημάτων επινοήθηκαν μια σειρά από μέθοδοι 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 έναν γνήσιο κωδικό πρόσβασης. Ένα φίλτρο προστασίας δρα κυρίως ως ένα εξελιγμένο ηλεκτρονικό σύστημα.

- Η **ταυτοποίηση του χρήστη (identification)** 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 είσοδός του στον Η/Υ. Συνήθως απαιτείται ο χρήστης να συμπληρώνει το όνομά του και τον κωδικό πρόσβασης (password). Η ταυτοποίηση ή αλλιώς αναγνώριση, έχει ορισθεί ως απαίτηση που ικανοποιεί την ιδιωτικότητα, αφενός μεν της εξωτερικής οντότητας που ζητά να αποκτήσει πρόσβαση σε μία 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 ιδιωτικότητα της αφού επιστρέφονται τα αντίστοιχα δεδομένα ή η 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 κανέναν μη εξουσιοδοτημένο χρήστη η 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 της **αυθεντικοποίησης (authentication)** 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 (passwords). Η αυθεντικοποίηση αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας ενός συστήματος. Ωστόσο, έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας. Έτσι, όταν μια οντότητα αιτείται 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 αυτόν τον τρόπο προστατεύεται και η ιδιωτικότητα της οντότητας, αλλά και τα ευαίσθητα δεδομένα του συστήματος. Ο χρήστης με την μέθοδο αυτή βεβαιώνει στο σύστημα ότι 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 (συνθηματικά) 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 (authorization)** 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 μία οντότητα αποκτά δικαιώματα (π.χ. χρήση, τροποποίηση, προσπέλαση κτλ.) σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος. Σε ένα σύστημα που υπάρχουν πολλοί χρήστες ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους στο σύστημα. Η εξουσιοδότηση, όπως και η αυθεντικοποίηση, αποτελεί κυρίως απαίτηση 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 εξουσιοδοτημένοι 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 μία οντότητα και μετά να της ανατεθούν τα αντίστοιχα δικαιώματα ανάλογα με το ρόλο της στο σύστημα.

- Η μέθοδος της **κρυπτογράφησης (encryption)** στηρίζεται στη χρησιμοποίηση ενός αλγόριθμου, 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 αναγνώσει. Η κρυπτογράφηση θεωρείται ένα ιδιαίτερα σημαντικό εργαλείο που προστατεύει 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 ιχνών και
• Η τακτική επιθεώρηση λογαριασμών μετρητών για μικρές απώλειες, γιατί τα μικρά λογιστικά λάθη στους φακέλους των 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 οποιονδήποτε 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.

Μία 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 παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κ.λπ).

Η ασύμμετρη κρυπτογραφία (ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την 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 ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον 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 δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα

κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή 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 επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.
Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την 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 (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). 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 για 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 να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.

  Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

  Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

  Αποστολέας
  1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί

θα είναι μία 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 ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).

2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

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 την σύνοψη που έχει κρυπτογραφηθεί.

Η έννοιες της κρυπτογράφησης και της ψηφιακής υπογραφής, σχετίζονται όπως θα δούμε και πιο κάτω με αντιμετώπιση απάτης μέσω ηλεκτρονικού ταχυδρομείου ή απάτη τοποθεσιών web το λεγόμενο ηλεκτρονικό ψάρεμα

- Μία άλλη έννοια που αφορά την προστασία από ηλεκτρονικά εγκλήματα είναι η **ιδιωτικότητα**. Όταν κάποιος χρησιμοποιεί μια τυπική εφαρμογή ηλεκτρονικής επεξεργασίας κειμένου, συνήθως δεν σκέπτεται αν κάποιος βρίσκεται κοντά του και παρακολουθεί το κείμενο που παράγεται. Όταν ο ίδιος χρήστης περιηγείται στο Διαδίκτυο, «είναι σα να βρίσκεται στο κέντρο μιας συναυλίας όπου εκατοντάδες άνθρωποι μπορούν να δουν τι κάνει ή και να ακούσουν τι ακριβώς αναφέρει». Οι περισσότεροι χρήστες Η/Υ χρησιμοποιούν το Διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου για επαγγελματικούς και προσωπικούς σκοπούς. Οι υπηρεσίες του ηλεκτρονικού ταχυδρομείου και του Διαδικτύου προσφέρονται από Παρόχους Υπηρεσιών Διαδικτύου (Internet Service Providers), και ειδικά συστήματα που αναφέρονται ως εξυπηρετητές (Servers) διεκπεραιώνουν τις αιτήσεις υπηρεσιών των χρηστών. Οι εξυπηρετητές διατηρούν δεδομένα των χρηστών που τους επισκέπτονται για διάφορους λόγους, όπως καλύτερη και γρηγορότερη παροχή υπηρεσίας την επόμενη φορά που θα ζητηθούν οι ίδιες υπηρεσίες, διευκόλυνση των χρηστών στον τρόπο πρόσβασης στις υπηρεσίες αυτές (διατηρώντας τα στοιχεία αναγνώρισής τους) κ.α. Τα στοιχεία αυτά διατηρούνται αποθηκευμένα για σημαντικό χρονικό διάστημα σε αρχεία καταγραφής (Log Files), τα οποία είναι στη διάθεση του διαχειριστή των συστημάτων αυτών, τόσο για ανάγνωση όσο και για επεξεργασία. Η χρήση

του Διαδικτύου και του ηλεκτρονικού 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 αποτέλεσμα 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 ιδιωτικότητα, ως ένα ζήτημα κοινωνικό και νομικό, έχει απασχολήσει εδώ και καιρό κοινωνικούς επιστήμονες, φιλόσοφους και νομικούς. Με την αξιοποίηση των Η/Υ και τις ολοένα αυξανόμενες δυνατότητες που προσέφεραν τα σύγχρονα πληροφοριακά συστήματα και τα δίκτυα επικοινωνιών, η ιδιωτικότητα των χρηστών άρχισε να κινδυνεύει. Στην πορεία για τη δημιουργία μίας παγκόσμιας κοινωνίας της πληροφορίας και με την ύπαρξη ολοένα και περισσότερων προγραμμάτων ανάπτυξης των δικτύων τηλεπικοινωνιών μεταξύ των κρατών, δημιουργούνται ποικίλοι κίνδυνοι όσον αφορά στη διαφύλαξη της ιδιωτικότητας των χρηστών που χρησιμοποιούν ή θα χρησιμοποιήσουν τα δίκτυα αυτά. Η ιδιωτικότητα, ως βασικό ανθρώπινο δικαίωμα αναγνωρισμένο από τη δήλωση του Οργανισμού Ηνωμένων Εθνών για την προστασία των ανθρωπίνων δικαιωμάτων, αλλά και από πολλές διεθνείς και τοπικές συνθήκες, πρέπει να προστατεύεται σε μια δημοκρατική κοινωνία. Αυτό μπορεί να επιτευχθεί με έναν από τους παρακάτω τρόπους:

• *Θέσπιση νόμων για την ιδιωτικότητα και την προστασία δεδομένων*
• *Εφαρμογή τεχνολογιών ενίσχυσης της ιδιωτικότητας που επιλέγονται και εφαρμόζονται από τους χρήστες*
• *Εκπαίδευση των χρηστών και των επαγγελματιών πληροφορικής σε θέματα ιδιωτικότητας*
• Τήρηση επιχειρησιακών κανονισμών *(κώδικες δεοντολογίας) που αφορούν σε πρακτικές εφαρμογής και υλοποίησης της ιδιωτικότητας*

Ο πρώτος ορισμός της ιδιωτικότητας δόθηκε από τους Warren και Brandeis στο άρθρο τους «Το δικαίωμα στην ιδιωτικότητα» (The Right to Privacy). Οι δύο αυτοί αμερικανοί δικηγόροι όρισαν την ιδιωτικότητα ως «το δικαίωμα του να είναι κανείς μόνος του».
Πιο πρόσφατα ο Alen Westin απέδωσε τον όρο ιδιωτικότητα ως «το δικαίωμα του κάθε ανθρώπου ή ομάδας ατόμων ή οργανισμών, να καθορίζουν από μόνοι τους, πότε, πώς και σε ποιο βαθμό οι προσωπικές τους πληροφορίες θα γίνονται γνωστές σε τρίτους». Ως «ομάδες ατόμων ή οργανισμούς» αναφερόμαστε σε νομικά πρόσωπα.
Η ιδιωτικότητα, ως έννοια, προσεγγίζεται από τρεις πλευρές:
• *Χωρική Ιδιωτικότητα* (Territorial Privacy): Αναφέρεται στην προστασία της ιδιωτικότητας του ατόμου στο φυσικό χώρο που τον περιβάλει π.χ. να μην μπορούν τρίτοι να παρατηρήσουν τις εργασίες που κάνει ένα άτομο στο γραφείο του.
• *Ιδιωτικότητα του ατόμου* (Privacy of the Person): Αναφέρεται στην προστασία του ατόμου από αναίτιες παρεμβάσεις τρίτων σε αυτό, π.χ. φυσική έρευνα χωρίς δικαιολογία, έλεγχο για κατοχή φαρμάκων, ανήθικη και παράνομη έρευνα για την απόκτηση προσωπικών πληροφοριών κλπ.
• *Πληροφοριακή Ιδιωτικότητα* (Informational Privacy): Αναφέρεται στο δικαίωμα του κάθε ατόμου να ελέγχει αν και με ποιο τρόπο τα προσωπικά του δεδομένα συλλέγονται, αποθηκεύονται, επεξεργάζονται και διαμοιράζονται σε τρίτους.
Ο όρος προσωπικά δεδομένα (Personal Data) αφορά σε κάθε πληροφορία που προσδιορίζει την προσωπικότητα ενός ατόμου. Ο όρος προστασία δεδομένων (Data

Protection) αναφέρεται στην προστασία των προσωπικών δεδομένων με σκοπό τη διαφύλαξη της ιδιωτικότητας και αποτελεί μέρος της γενικής έννοιας της ιδιωτικότητας.
Ωστόσο, η ιδιωτικότητα δεν μπορεί να αποτελεί δικαίωμα απόλυτο, για όλες τις περιπτώσεις, μιας και πολλές φορές η προστασία της έρχεται σε αντίθεση με άλλα δικαιώματα ή νόμους. Επίσης είναι γενικά αποδεκτό ότι κανένας δεν μπορεί να είναι αναγνωρίσιμο μέλος σε μια κοινωνία χωρίς να αποκαλύπτει μέρος των προσωπικών του δεδομένων.
Σε μια κοινωνία αρκετά δικτυακή όπως η σημερινή, η ιδιωτικότητα δεν μπορεί να προστατευθεί μόνον από νόμους και κανονισμούς. Τα πληροφοριακά συστήματα που συλλέγουν προσωπικά δεδομένα, θα πρέπει επίσης, να αποτρέπουν την παραβίαση της ιδιωτικότητας Για το λόγο αυτό, οι υπεύθυνοι για την προστασία δεδομένων απαιτούν από τους αναλυτές και προγραμματιστές πληροφοριακών συστημάτων να συμπεριλαμβάνουν την ιδιωτικότητα ως τεχνική απαίτηση που πρέπει να λαμβάνεται υπόψη στο υπό-ανάπτυξη σύστημα και πιο συγκεκριμένα θα πρέπει να λαμβάνεται υπόψη από τη φάση της σχεδίασης του συστήματος αποτελώντας ξεχωριστό κριτήριο που πρέπει να υλοποιηθεί.
Για να επιτευχθεί ο παραπάνω στόχος και να μπορέσει η ιδιωτικότητα από μία γενική έννοια να μετατραπεί σε τεχνική απαίτηση, ορίστηκε μια σειρά από επιμέρους απαιτήσεις, οι απαιτήσεις ιδιωτικότητας (Privacy Requirements) οι οποίες είναι οι ακόλουθες και κάποιες από αυτές αναφέρθηκαν πιο πάνω:
• *αυθεντικοποίηση* (authentication)
• *εξουσιοδότηση* (authorization)
• *αναγνώριση* (identification)
• *προστασία δεδομένων* (Data Protection)
• *ανωνυμία* (Anonymity)
• *ψευδωνυμία* (Pseudonymity)
• *μη-συνδεσιμότητα* (Unlinkability)
• *μη-παρατηρησιμότητα* (Unobservability)

Οι απαιτήσεις αυτές καλύπτουν διάφορες όψεις της ιδιωτικότητας κατά τη χρήση ενός πληροφοριακού συστήματος. Ανάλογα με τον τρόπο προστασίας της ιδιωτικότητας σε ένα πληροφοριακό σύστημα, υλοποιείται μία ή περισσότερες από αυτές.

5.1. Anonymizer

Ο Anonymizer είναι μία υπηρεσία που καταχωρεί http αιτήσεις σε ιστοθέσεις για λογαριασμό των χρηστών του.

Αποτελεί ιστοσελίδα που λειτουργεί ως proxy server για τις αιτήσεις στο Internet, αντιπροσωπεύοντας τους χρήστες του.
Η μόνη IP διεύθυνση που αποκαλύπτεται στους εξυπηρετητές είναι η διεύθυνση του Anonymizer.
Ο Anonymizer παρέχεται από έναν HTTP proxy server που εκτελείται στη θύρα 8080 του server που φιλοξενεί την Anonymizer σελίδα, δηλαδή τη σελίδα με διεύθυνση www.Anonymizer.com
Η υπηρεσία ανωνυμίας είναι απλή στη χρήση και είναι δωρεάν με μια μικρή καθυστέρηση που προκύπτει από την εμφάνιση διαφημίσεων είτε παρακάμπτοντας αυτές τις διαφημίσεις πληρώνοντας μια μικρή συνδρομή.

Χρήση του Anonymizer μπορεί να γίνει με δύο τρόπους. Αν υποτεθεί ότι ο χρήστης θέλει να ανακτήσει τα περιεχόμενα της σελίδας, http://msc.ds.unipi.gr/ τότε μπορεί:

- Να τη ζητήσει μέσω του site του Anonymizer.
- Να δημιουργήσει ένα φωλιασμένο URL:

http://www.Anonymizer.com:8080/http:// http://msc.ds.unipi.gr/

Και στις δύο περιπτώσεις η σελίδα θα ανακτηθεί από τον proxy server του Anonymizer. Έτσι ο browser αφήνει ίχνη μόνο στα log files του Anonymizer.

Ο Anonymizer περιέχει ορισμένα σημεία ευπάθειας:

- Όποιος επιλέγει τον Anonymizer θα πρέπει να εμπιστεύεται τους διαχειριστές αυτής της υπηρεσίας.
- Ο Anonymizer μπορεί να συλλέξει έναν τεράστιο όγκο πληροφοριών που αφορούν ένα χρήστη.
- Ένας τρόπος παραβίασης της ανωνυμίας είναι οι βοηθητικές εφαρμογές οι οποίες παρακάμπτουν τον proxy server και δημιουργούν δικές τους απευθείας συνδέσεις (π.χ. Real Audio).

5.2. Αναγνώριση πλαστών μηνυμάτων ηλεκτρονικού ταχυδρομείου και τακτικών "ψαρέματος"

Δυστυχώς, πολλοί ανυποψίαστοι παραλήπτες πέφτουν θύματα αυτών των τακτικών και χωρίς τη γνώση τους παρέχουν προσωπικά στοιχεία:

- Αριθμός κοινωνικής ασφάλισης.
- Κωδικός πρόσβασης ή PIN.
- Αριθμός τραπεζικού λογαριασμού.
- Αριθμός κάρτας ATM ή πιστωτικής.
- Κωδικός επαλήθευσης πιστωτικής κάρτας ή τιμή επαλήθευσης κάρτας.
- Αριθμός τηλεφώνου και διεύθυνση.

Οι εγκληματίες χρησιμοποιούν αυτές τις πληροφορίες 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 ATM σε όλο τον κόσμο.

5.2.1. Παραδείγματα τακτικών "ψαρέματος"

Ορισμένα παραδείγματα τακτικών ψαρέματος είναι:

- Ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνεται ότι προέρχονται από την τράπεζά σας ή την εταιρεία έκδοσης της πιστωτικής σας κάρτας και σας προειδοποιούν ότι πρέπει να επαληθεύσετε τα στοιχεία του τραπεζικού σας λογαριασμού διαφορετικά θα ακυρωθεί.
- Συνδυασμός απάτης σε πλειστηριασμούς και ψεύτικων τοποθεσιών χρηματικής εγγύησης. Αυτό συμβαίνει όταν υπάρχουν αντικείμενα προς πώληση σε έγκυρη τοποθεσία πλειστηριασμών για να σας προσελκύσει ώστε να κάνετε πληρωμές σε ψεύτικες τοποθεσίες χρηματικής εγγύησης.
- Ψεύτικες ηλεκτρονικές συναλλαγές πωλήσεων, όπου ο εγκληματίας διατίθεται να αγοράσει κάτι από εσάς και ζητάει να σας πληρώσει ένα ποσό αρκετά μεγαλύτερο από την τιμή του προς αγορά αντικειμένου. Σε αντάλλαγμα, ζητούν την αποστολή επιταγής με το ποσό της διαφοράς. Η πληρωμή σε εσάς δεν αποστέλλεται ποτέ, ωστόσο η επιταγή σας εξαργυρώνεται και ο εγκληματίας τσεπώνεται τη διαφορά. Επιπλέον, η επιταγή που στείλατε περιλαμβάνει τον τραπεζικό σας λογαριασμό, τον κωδικό υποκαταστήματος, τη διεύθυνση και τον αριθμό τηλεφώνου.
- Ψεύτικοι φιλανθρωπικοί οργανισμοί μπορεί να σας ζητήσουν χρήματα. Δυστυχώς, πολλοί εγκληματίες εκμεταλλεύονται την καλή σας πρόθεση.

5.2.2. Ένα ψεύτικο μήνυμα ηλεκτρονικού ταχυδρομείου

Δυστυχώς, μπορεί να είναι δύσκολο να καταλάβετε με την πρώτη ματιά αν το μήνυμα θέλει να σας εξαπατήσει. Για παράδειγμα, πολλά ψεύτικα μηνύματα συνδέονται με πραγματικά εταιρικά λογότυπα. Ωστόσο, μπορείτε να αναζητήσετε τα παρακάτω στοιχεία:

- **Αιτήματα για προσωπικά στοιχεία σε μήνυμα ηλεκτρονικού ταχυδρομείου** Οι περισσότερες νόμιμες εταιρείες έχουν ως πολιτική να μην ρωτούν μέσω ηλεκτρονικού ταχυδρομείου τα προσωπικά στοιχεία των πελατών τους. Πρέπει να υποψιαστείτε αν λάβετε μήνυμα που σας ρωτάει τα προσωπικά σας στοιχεία, ακόμα και αν όλα φαίνονται νόμιμα.
- **Φρασεολογία που εκφράζει έκτακτη ανάγκη ή βιασύνη** Η φρασεολογία σε μηνύματα ψαρέματος είναι συνήθως ευγενική και εξυπηρετική. Συνήθως σας προτρέπει να απαντήσετε στο μήνυμα ή να κάνετε κλικ στη

συμπεριλαμβανόμενη σύνδεση. Για μεγαλύτερο αριθμό απαντήσεων, οι εγκληματίες προσπαθούν να καλλιεργήσουν μια αίσθηση ανάγκης και βιασύνης, ώστε οι παραλήπτες να απαντήσουν χωρίς να το πολυσκεφτούν. Συνήθως, τα ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου ΔΕΝ είναι εξατομικευμένα, ενώ τα έγκυρα μηνύματα από την τράπεζά σας ή από την εταιρεία ηλεκτρονικού εμπορίου είναι. Ακολουθεί ένα παράδειγμα πραγματικής τακτικής ψαρέματος:

Αγαπητέ πελάτη μας, υπέπεσε στην αντίληψή μας ότι πρέπει να ενημερώσετε τα στοιχεία του λογαριασμού σας καθώς έχουμε λάβει αναφορές για αδράνεια, απάτες και κλοπή. Αν δεν ενημερώσετε τα στοιχεία σας, ο λογαριασμός θα διαγραφεί. Ακολουθήστε την παρακάτω σύνδεση για να επιβεβαιώσετε τα στοιχεία σας.

- **Ψεύτικες συνδέσεις** Σε μηνύματα που έχουν μορφοποιηθεί με, οι συνδέσεις που σας προτρέπουν να κάνετε κλικ σε όλο ή μέρος μιας εταιρικής επωνυμίας είναι συνήθως "μεταμφιεσμένες", δηλαδή η σύνδεση που βλέπετε δεν σας οδηγεί στη συγκεκριμένη διεύθυνση αλλά κάπου αλλού, συνήθως σε ψεύτικη τοποθεσία Web. Παρατηρήστε σε αυτό το παράδειγμα με το Outlook ότι αν τοποθετήσετε το δείκτη του ποντικιού πάνω στη σύνδεση θα εμφανιστεί η πραγματική διεύθυνση στο πλαίσιο με το κίτρινο φόντο. Η συμβολοσειρά με τους παράξενους αριθμούς δεν έχει την εμφάνιση μιας εταιρικής τοποθεσίας στο Web ή μιας διεύθυνσης URL και αποτελεί ένδειξη που πρέπει να κινήσει τις υποψίες σας.

Μια άλλη συνηθισμένη τακτική που χρησιμοποιούν οι εγκληματίες είναι μια διεύθυνση URL που με την πρώτη ματιά αποτελεί το όνομα γνωστής εταιρείας αλλά μετά από προσεχτική εξέταση μπορείτε να διαπιστώσετε ότι έχει μικρές αλλαγές. Για παράδειγμα, η διεύθυνση www.microsoft.com μπορεί να είναι:

www.micosoft.com

www.verify-microsoft.com

www.mircosoft.com

Η Microsoft έχει κερδίσει πρόσφατα διάφορες δικαστικές αγωγές κατά ατόμων που χρησιμοποιούσαν αυτούς τους τύπους URL για να γελοιοποιήσουν νόμιμες ιδιότητες της Microsoft. Ωστόσο, η πρακτική συνεχίζεται και συχνά προστατεύεται από τα εθνικά σύνορα.

- **Το κυρίως μήνυμα είναι εικόνα** Για να αποφευχθεί ο εντοπισμός τους από τα φίλτρα ανεπιθύμητης αλληλογραφίας, τα ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν εικόνα αντί για κείμενο στο κυρίως μήνυμα. Αν το απεσταλμένο ανεπιθύμητο μήνυμα χρησιμοποιεί πραγματικό κείμενο, το φίλτρο ανεπιθύμητης αλληλογραφίας του Outlook θα μετακινήσει το μήνυμα στο φάκελο **Ανεπιθύμητη αλληλογραφία**. Η εικόνα στο κυρίως μήνυμα είναι συνήθως μια. Αυτό μπορείτε να το καταλάβετε επειδή αν τοποθετήσετε το δείκτη του ποντικιού στο κυρίως μήνυμα, ο δείκτης θα μετατραπεί σε ένα χεράκι.

Άλλοι τύποι εικόνων που περιλαμβάνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να συνδέονται με το διακομιστή του αποστολέα της ανεπιθύμητης αλληλογραφίας και να λειτουργούν ως Web beacon. Όταν ανοίγετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, γίνεται λήψη των εικόνων και οι πληροφορίες διαβιβάζονται στο διακομιστή. Αυτές οι πληροφορίες χρησιμοποιούνται για να επαληθεύσουν ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου είναι έγκυρη ώστε να σας αποσταλεί πάλι ανεπιθύμητη αλληλογραφία. Από προεπιλογή, το Outlook εμποδίζει αυτόματα αυτές τις εξωτερικές εικόνες.

- **Συνημμένα** Πολλές τακτικές ψαρέματος σας ζητούν να ανοίξετε συνημμένα αρχεία που μπορεί να μολύνουν τον υπολογιστή σας με ιούς. Δεν πρέπει να ανοίξετε τα συνημμένα αυτών των ύποπτων μηνυμάτων. Αποθηκεύστε πρώτα τα συνημμένα που θέλετε να δείτε και ανιχνεύστε τα αρχεία με ενήμερο πρόγραμμα αντιμετώπισης ιών πριν το ανοίξετε. Για την προστασία του υπολογιστή σας, το Outlook και το Microsoft Outlook Express εμποδίζουν αυτόματα ορισμένους τύπους συνημμένων αρχείων που μπορεί να μεταδώσουν ιούς.

5.2.3. Τοποθεσίες web που αποτελούν απάτη

Όπως και στην περίπτωση των μηνυμάτων ηλεκτρονικού ταχυδρομείου που προσπαθούν να σας εξαπατήσουν, οι ψεύτικες τοποθεσίες Web περιέχουν έγκριτα γραφικά λογότυπων και συνδέσεις Web. Έτσι δεν μπορείτε να διαπιστώσετε εύκολα ότι πρόκειται για απάτη. Η καλύτερη στρατηγική είναι να αναζητείτε στοιχεία που έχουν οι νόμιμες τοποθεσίες Web:

- **Ασφάλεια SSL** Οι μόνιμες τοποθεσίες Web χρησιμοποιούν Secure Sockets Layer (SSL) ή άλλη τεχνολογία ασφαλείας για να προστατεύσουν τα στοιχεία που καταχωρήσατε όταν ανοίξατε το νέο λογαριασμό και όταν εγγραφήκατε στην τοποθεσία αργότερα. Η ασφάλεια φαίνεται στη γραμμή κατάστασης του προγράμματος περιήγησης στο Web με ένα εικονίδιο κλειδαριάς. Επιπρόσθετα, της διεύθυνσης Web προηγείται η έκφραση https:// αντί για το συνηθισμένο http:// στη γραμμή διευθύνσεων.
- **Ψηφιακό πιστοποιητικό για την τοποθεσία Web** Ένα πρόσθετο πλεονέκτημα της τεχνολογίας SSL είναι ο έλεγχος ταυτότητας, μια διαδικασία αναγνώρισης μιας τοποθεσίας Web. Η τεχνολογία SSL προσφέρει αυτό το πλεονέκτημα χρησιμοποιώντας ένα ψηφιακό πιστοποιητικό, το οποίο η τοποθεσία καταθέτει στο πρόγραμμα περιήγησης κατά τη σύνδεση. Για προβολή του πιστοποιητικού, κάντε διπλό κλικ στο εικονίδιο της κλειδαριάς στην κάτω δεξιά γωνία του προγράμματος περιήγησης και εξετάστε το πεδίο **Εκδόθηκε σε**. Το όνομα που εμφανίζεται στο πιστοποιητικό πρέπει να αντιστοιχεί στην τοποθεσία με την οποία πιστεύετε ότι έχετε συνδεθεί. Για παράδειγμα, αν η τοποθεσία είναι όντως η Wood Grove Bank, τότε το όνομα **Εκδόθηκε σε** πρέπει να αντιστοιχεί στη διεύθυνση URL "woodgrovebank.com." Αν το όνομα είναι διαφορετικό, ίσως η τοποθεσία να είναι ψεύτικη. Πάλι, πρέπει να είστε προσεχτικοί για εκείνες τις μικρές αλλαγές στο όνομα που περιγράψαμε παραπάνω. Αν το πιστοποιητικό έχει λήξει, αν δεν είναι έμπιστο από την αρχή πιστοποίησης ή ακόμα αν το όνομα

δεν αντιστοιχεί στο όνομα που εμφανίζεται στη γραμμή διεύθυνσης, στο Microsoft Internet Explorer εμφανίζεται ένα προειδοποιητικό μήνυμα.

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (μη αποποίηση).

Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί.

Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.

Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης

μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

5.3. Αντιμετώπιση του Hacking

Εάν υποθέσουμε ότι ένας εισβολέας καταφέρει να δει στο τερματικό του απάντηση από τον υπολογιστή στον οποίο προσπαθεί να μπει, πρέπει να πληκτρολογήσει μια αποδεκτή ταυτότητα χρήστη κι ένα συνθηματικό. Συχνά δεν είναι ιδιαίτερα δύσκολο να βρεις έναν αριθμό ταυτότητας χρήστη, αφού πληροφορίες σαν κι αυτή δεν θεωρούνται γενικά εμπιστευτικές. Αυτό μπορεί να γίνει:

- Δοκιμάζοντας τυπικές ταυτότητες χρηστών που μπορεί να υπάρχουν στο σύστημα και δημοσιεύονται στα βιβλία του κατασκευαστή που τα περιγράφουν.
- Ψάχνοντας στα άχρηστα χαρτιά της εγκατάστασης. Οι αριθμοί ταυτότητες των χρηστών συνήθως τυπώνονται στις λίστες των υπολογιστών.
- Με τη μέθοδο των συνεχών δοκιμών. Το σύστημα συχνά δέχεται απεριόριστο αριθμό προσπαθειών, μέχρι να βρεθεί η σωστή ταυτότητα χρήστη, χωρίς να δίνει προειδοποίηση ή να απομονώνει το τερματικό.

Αφού ο εισβολέας καταφέρει να υπογράψει στο σύστημα με την ορθή ταυτότητα χρήστη, χρειάζεται κατόπιν το σωστό συνθηματικό, για να μπει σε αυτό. Οι χρήστες πρέπει να μάθουν να χρησιμοποιούν το συνθηματικό τους ως στοιχείο άκρως εμπιστευτικό. Ως εκ τούτου τα συνθηματικά δεν πρέπει να βρίσκονται εύκολα όπως οι ταυτότητες χρηστών. Όμως, άπαξ και ο εισβολέας μάθει με οποιοδήποτε τρόπο ένα συνθηματικό, μπορεί να το ανακοινώσει μέσω του ηλεκτρονικού πίνακα ανακοινώσεων, κι έτσι να μεταδοθεί αμέσως στους άλλους εισβολείς. Η πιθανότητα να βρεθεί κάποιο συγκεκριμένο συνθηματικό στον πίνακα ανακοινώσεων είναι μικρή. Όμως αν κάποια μονάδα έχει την ατυχία να βρεθεί η πληροφορία της αυτή δημοσιευμένη, τότε είναι σίγουρο ότι θα υποστεί πλήθος εισβολών.

5.3.1. Αποτροπή της εισβολής

Για την προστασία των υπολογιστών, είναι σημαντικό τα εργαλεία των χάκερ να ανιχνεύονται πριν εγκατασταθούν στο σύστημα. Το πρόβλημα είναι ότι επειδή δεν είναι εχθρικός κώδικας με την αυστηρή έννοια του όρου, οι εφαρμογές antivirus δεν μπορούν να τα ανιχνεύουν· για την ανίχνευσή τους απαιτούνται συγκεκριμένες εφαρμογές.

Μία καλή λύση είναι η εγκατάσταση ενός ολοκληρωμένου πακέτου ασφάλειας το οποίο περιλαμβάνει όλα τα αναγκαία εργαλεία για την ανίχνευση και εξουδετέρωση όχι μόνο των ιών, αλλά επίσης και άλλων προερχόμενων από το Internet απειλών. Μία τέτοια λύση είναι το Platinum Internet Security της Panda Software, το οποίο, εκτός από την πλέον προηγμένη τεχνολογία antivirus, ενσωματώνει επίσης πρωτοποριακά συστήματα για την προστασία έναντι των νεότερων απειλών που έχουν παρουσιαστεί λόγω του Internet, όπως το spam, τα προγράμματα dialer, τα προβλήματα ασφάλειας διάφορων εφαρμογών λογισμικού, οι ιοί-φάρσες, οι χάκερ και τα εργαλεία τους.

Στη συνέχεια παρουσιάζονται κάποιες διαδικασίες που μπορούν να υιοθετηθούν, ώστε να δυσκολέψουν τη μη-εξουσιοδοτημένη εισβολή:

- Η δυνατότητα των συνδέσεων μέσω επιλεγόμενης γραμμής πρέπει να περιοριστεί στο ελάχιστο. Αν υπάρχει τέτοια δυνατότητα, θα πρέπει να κρατηθεί έξω από το σύστημα. Δηλαδή θα πρέπει η επιλογή της σύνδεσης με τον υπολογιστή να γίνεται μετά από τηλεφωνική επαφή του χρήστη με τον υπεύθυνο του συστήματος, ώστε να επιβεβαιωθεί το δικαίωμα σύνδεσης. Στη συνέχεια ο χρήστης πρέπει να κληθεί από το σύστημα, ως μία περαιτέρω επιβεβαίωση του ότι η αίτηση σύνδεσης προέρχεται από έναν εξουσιοδοτημένο αριθμό.
- Οι τηλεφωνικοί αριθμοί του συστήματος, οι αριθμοί ταυτότητας χρήστη δικτύου (NUI) και οι διευθύνσεις χρήστη δικτύου (NUA) του PSS πρέπει να φυλάσσονται όσο το δυνατόν σχολαστικότερα.
- Θα πρέπει να εξεταστεί το ενδεχόμενο χρήσης της ειδικής συσκευής η οποία καλεί τον «αιτούντα σύνδεση».
- Οι τυπικοί αριθμοί ταυτότητας χρήστη δικτύου (NUI) δεν πρέπει να χρησιμοποιούνται.
- Μια σειρά από ελέγχους πρέπει να εφαρμόζεται αναφορικά με τα συνθηματικά.

Τα συνθηματικά πρέπει:

- Να έχουν μήκος τουλάχιστον 6 αλφαριθμητικών χαρακτήρων
- Να αλλάζουν τακτικά
- Να μην σχετίζονται καθ' οποιοδήποτε τρόπο με τον χρήστη, ώστε να μην είναι εύκολο να τα μαντέψει κάποιος
- Οι απόπειρες μη εξουσιοδοτημένης προσπέλασης πρέπει να ελέγχονται και να ερευνώνται. Μετά από δύο ανεπιτυχείς απόπειρες, ο χρήστης πρέπει να αποσυνδέεται από το σύστημα και η ταυτότητα του να ακυρώνεται.

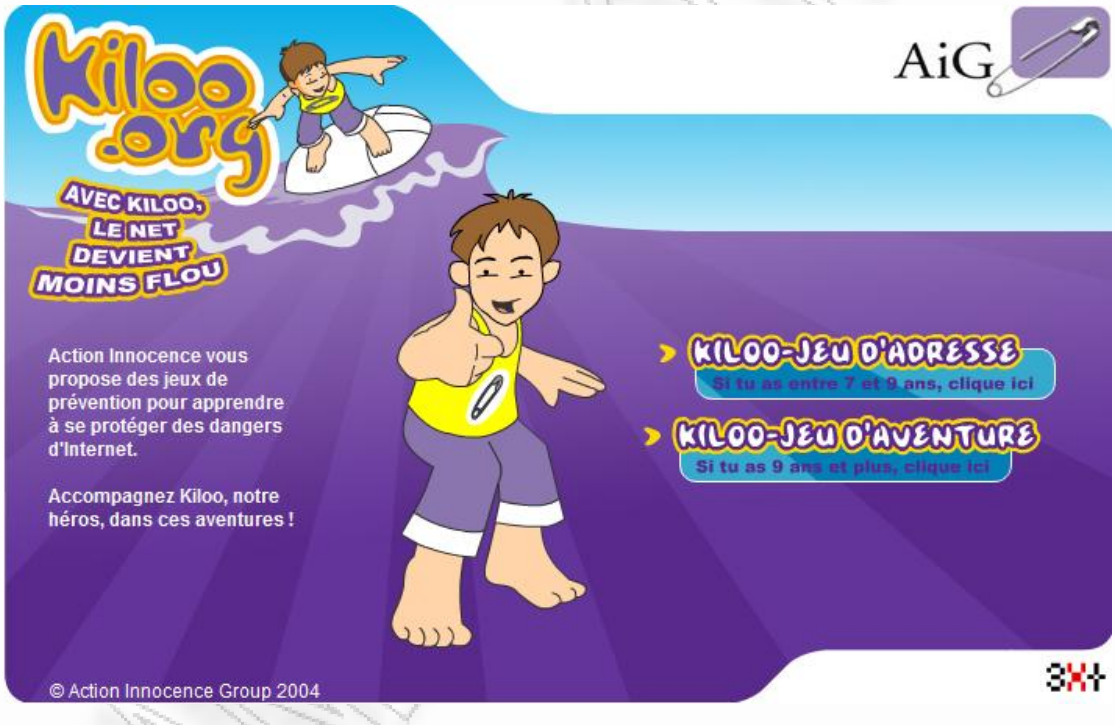
5.4. Προληπτικά τεχνικά μέτρα για την παιδική πορνογραφία

Στα προληπτικά τεχνικά μέσα ανήκουν φίλτρα που είναι ειδικό λογισμικό που εγκαθίσταται στον ηλεκτρονικό υπολογιστή και δεν επιτρέπει την πρόσβαση σε τόπους με πορνογραφικό περιεχόμενο, όπως αυτά που προσφέρονται από την ελβετική οργάνωση Action Innocence.

5.4.1. Η καταπολέμηση της παιδικής πορνογραφίας μέσω internet από την Action Innocence

Στις δραστηριότητες τις συγκεκριμένης οργάνωσης περιλαμβάνονται οι παρακάτω διαδικτυακές πλατφόρμες:

- www.kiloo.org : διαδραστικό παιχνίδι για τα παιδιά και τους επιτρέπει να μάθουν να προστατεύονται από online απειλές, ενώ προστατεύουν τον εαυτό τους.



- www.filtra.info : η ιστοσελίδα στοχεύει στο να παρέχει σαφή και λεπτομερή στοιχεία σχετικά με τις διάφορες λύσεις που προσφέρονται από το φιλτράρισμα λογισμικού γονικού ελέγχου.

Πρόγραμμα AntiPedoFiles

Η Action Innocence λύσεις πληροφορικής, έχει αναπτυχθεί από το 2003 για τις αστυνομικές υπηρεσίες. Τα εργαλεία αυτά βοηθούν την καταπολέμηση του εμπορίου των αρχείων online παιδικής πορνογραφίας.

Το πρόγραμμα χωρίζεται σε διάφορες ενότητες AntiPedoFiles:

1. AntiPedoFiles - Βάση Δεδομένων: ανάπτυξη μιας βάσης δεδομένων δακτυλικών αποτυπωμάτων που αποτελείται από αρχεία που περιέχουν παιδική πορνογραφία με στόχο την ανάπτυξη εργαλείων ανίχνευσης

2. AntiPedofiles - P2P: ανάπτυξη λογισμικού που ειδικεύεται στην ανίχνευση των αρχείων δεδομένων, ενός παιδεραστή σε δίκτυα "Peer-to-Peer (P2P)

3. AntiPedoFiles - WebScan: Ανάπτυξη λογισμικού για την παρακολούθηση των εθνικών δικτύων

Αυτές οι μονάδες παραδίδονται δωρεάν σε ενδιαφερόμενες αστυνομικές υπηρεσίες. Από το 2005, πολλές πολιτικές στην Ευρώπη χρησιμοποιούν τις λύσεις που αναπτύχθηκαν από την Ένωση για να επιτύχει αποτελέσματα. Το 2006, η Action Innocence ξεκίνησε μια στενή συνεργασία με την Ελβετική Ομοσπονδιακή Αστυνομία, ιδίως με την έκθεση (Τμήμα συντονισμό της καταπολέμησης της εγκληματικότητας στο Διαδίκτυο). Αυτή η από κοινού εργασία επιτρέπει την Ένωση να ανταποκριθεί καλύτερα στην αστυνομία.

5.5. Αστυνομία για καταγγελίες Διαδικτυακής παρενόχλησης και βίας στα παιδιά της Μεγάλης Βρετανίας

Μια διαδικτυακή αστυνομία ιδρύθηκε και λειτουργεί στη Μεγάλη Βρετανία με σκοπό την πάταξη και την αντιμετώπιση της διαδικτυακής βίας και της κακοποίησης ιδιαίτερα σε παιδιά - χρήστες. Ανησυχητικά είναι τα νούμερα, καθώς η αστυνομία απαντά σε περισσότερες από 100 κλήσεις κάθε μήνα από παιδιά που χρησιμοποιούν το διαδίκτυο και καταγγέλλουν σεξουαλική παρενόχληση ή βία.

Οι ειδικοί υπάλληλοι της υπηρεσίας Ceop, του κέντρου Home Office-funded Child Exploitation and Online Protection , λαμβάνουν περίπου 4 κλήσεις καθημερινά από παιδιά που πρόκειται να συναντήσουν κάποιον περίεργο χαρακτήρα που γνώρισαν μέσω του ιντερνετ. Κάποια από τα παιδιά ειδοποιούν ακόμη και αφού έχουν υποστεί κακοποίηση και χρειάζονται ιατρική βοήθεια. Το σήμα κινδύνου μεταδίδεται με το πάτημα ενός κουμπιού (σε κάποιο Link της σελίδας), το οποίο αυτόματα ενημερώνει μια ομάδα ειδικών αστυνομικών που είναι εκπαιδευμένοι στο να χειρίζονται τη διαδικτυακή κακοποίηση. Ανησυχίες εκφράζονται για το ότι ο αριθμός των ειδοποιήσεων δεν αντιστοιχεί στα πραγματικά κρούσματα γιατί πολλά sites κοινωνικοποίησης έχουν αρνηθεί να αναρτήσουν το σύνδεσμο στην υπηρεσία. Φαίνεται πως ο κόσμος στη Μεγάλη Βρετανία, αφού έχει τα μέσα να καταγγείλει την παιδική διαδικτυακή βία και παρενόχληση, ευαισθητοποιήθηκε και το κάνει.

5.6. Κατασταλτικά τεχνικά μέτρα για την παιδική πορνογραφία

Τα κατασταλτικά τεχνικά μέσα διακρίνονται σε αυτά που χρησιμοποιούν ειδικό λογισμικό για να εντοπίζουν δικτυακούς τόπους με παιδοφιλικό περιεχόμενο όπως το πρόγραμμα CETS που δημιούργησε η Microsoft και επιτρέπει στις αστυνομικές αρχές να εντοπίζουν απόπειρες εισόδου σε πορνογραφικές ιστοσελίδες, ή το AntiPedoFiles που απευθύνεται επίσης στις αστυνομικές αρχές ως εργαλείο έρευνας και το LogP2P που δρα ιδίως στα μοντέλα δικτύωσης Peer-to-Peer. Ένα τέτοιο εργαλείο που προσφέρει δυνατότητα συνεργασίας ανάμεσα σε πολλά κράτη είναι αυτό που δημιούργησε η Οικουμενική Εικονική Ομάδα Δράσης (VGT).
Η Οικουμενική Εικονική Ομάδα Δράσης (Virtual Global Task Force: VGT) είναι ένας διεθνής συνεταιρισμός αρχών εφαρμογής του νόμου που δημιουργήθηκε για την διαδικτυακή καταπολέμηση αρχικά της παιδικής κακοποίησης, αλλά μπορεί να τύχει εφαρμογής και σε άλλες εγκληματικές συμπεριφορές που χρησιμοποιούν το Διαδίκτυο. Η Ομάδα αυτή αποτελείται από το Κέντρο Εγκλημάτων Υψηλής Τεχνολογίας της Αυστραλίας, το Βρετανικό Κέντρο για την παιδική εκμετάλλευση και διαδικτυακή προστασία (Child Exploitation and Online Protection Centre: CEOP), τη Βασιλική Καναδική Έφιππη Αστυνομία, την υπηρεσία μετανάστευσης και τελωνείων των ΗΠΑ, ιταλικές και γαλλικές αστυνομικές αρχές, καθώς και τις Europol και Interpol.
Η Ομάδα αυτή έχει θέσει σε εφαρμογή ένα σύστημα απλής εφαρμογής που λειτουργεί σε 24ωρη βάση επτά ημέρες την εβδομάδα και επιτρέπει στα παιδιά που αντιλαμβάνονται κίνδυνο να τον αναφέρουν οποιαδήποτε ώρα της ημέρας ή της νύχτας με την πίεση ενός εικονιδίου, ώστε να επιληφθούν άμεσα οι αστυνομικές αρχές. Με το σύστημα αυτό τίθεται σε εφαρμογή η δυνατότητα συνεργασίας και ταυτόχρονης δράσης σε περισσότερα κράτη κάτι που είναι αναγκαίο για την αντιμετώπιση αυτού του είδους της εγκληματικότητας.

5.6.1. Το CETS

Το (CETS) είναι ένα μοναδικό εργαλείο λογισμικού που αναπτύχθηκε από την καναδική αστυνομία, τους διεθνείς αξιωματούχους επιβολής του νόμου, και τη Microsoft για να βοηθήσει στην online μάχη εκμετάλλευσης των παιδιών. Προφέρει "μηχανισμούς υποβολής προσφυγών," αυτό το εργαλείο βοηθά τους υπαλλήλους επιβολής του νόμου να συνεργάζονται και να ανταλλάσσουν πληροφορίες με άλλες αστυνομικές υπηρεσίες που βασίζονται στις νομικές συμφωνίες στη θέση του. Όταν οι υπάλληλοι επιβολής του νόμου στράφηκαν προς τη Microsoft για να βοηθήσει στην επίλυση μια σημαντική πρόκληση που αντιμετώπισαν, η CETS δημιουργήθηκε για να αυξηθεί η αποτελεσματικότητα των ερευνών και των ομάδων, παρέχοντάς τους με λογισμικό για την αποθήκευση, αναζήτηση, το μερίδιο της, και την ανάλυση μεγάλου όγκου των αποδεικτικών στοιχείων και να ταιριάξει περιπτώσεις σε όλη την αστυνομία.
Το CETS έχει ήδη διαδραματίσει ρόλο σε αρκετές έρευνες στο σύνολο των γεωγραφικών συνόρων, η δημιουργία δεσμών, οι οποίοι βοήθησαν τη σύλληψη δραστών σε απευθείας σύνδεση και, πιο σημαντικό, να οδηγήσει στη διάσωση των παιδιών στις χώρες σε όλο τον κόσμο.
Βασικά πλεονεκτήματα
Το CETS προσφέρει την επιβολή του νόμου, ισχυρή συνεργασία και ανάλυση.

• **Συνεργασία.** Οργανισμοί μπορούν να διασπάσουν τα σύνορα μέσω της συνεργασίας και ανταλλαγής πληροφοριών. Χρήση τυποποιημένων Web-based τεχνολογίων, υπηρεσίες επιβολής του νόμου μπορούν να συνεργάζονται με έρευνες για την εκμετάλλευση των παιδιών με βάση τις νομικές συμφωνίες που στη θέση του, με ενισχυμένη ασφάλεια, οι τεχνολογίες. Από τεχνική σκοπιά, το CETS βασίζεται σε Extensible Markup Language (XML), έτσι ώστε οι ερευνητές να μπορούν να παράγουν τόσο και να λαμβάνουν πληροφορίες από σχεδόν οποιοδήποτε ηλεκτρονικό σύστημα που περιέχει σχετικά δεδομένα, ανεξαρτήτως του υλικού ή του λογισμικού.

•**Ανάλυση.** Οργανισμοί μπορούν να χρησιμοποιήσουν ισχυρά εργαλεία πληροφορικής για την καταπολέμηση του εγκλήματος πληροφορικής. Το CETS περιέχει ισχυρά χαρακτηριστικά για να επιτρέψει ανακριτές για εύκολη εισαγωγή, οργάνωση, ανάλυση, ανταλλαγή και αναζήτηση πληροφοριών από το σημείο εντοπισμού του δικαιώματος μέσω του προπαρασκευαστικού σταδίου.

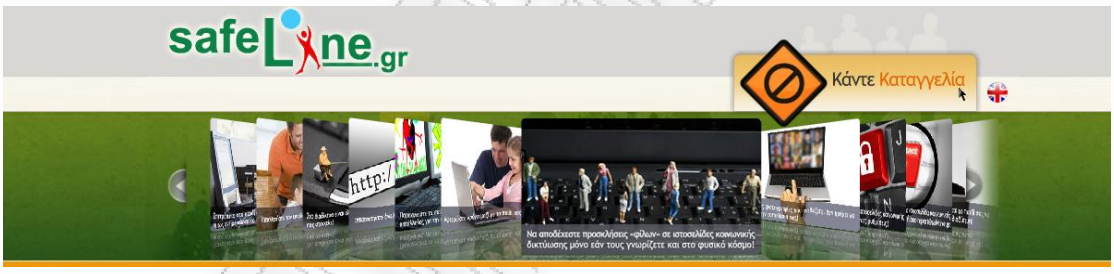
5.7. Μέτρα για Ασφαλές Διαδίκτυο από το Ευρωπαϊκό Κοινοβούλιο

Σύμφωνα με ένα δελτίο τύπου που εξέδωσε το Ευρωπαϊκό Κοινοβούλιο, σημαντικές ενέργειες ετοιμάζονται από οργανωμένους κρατικούς φορείς για ένα ασφαλές διαδίκτυο. Το ευρωπαϊκό Κοινοβούλιο σε συνεργασία με το Υπουργικό Συμβούλιο ετοιμάζεται να παρουσιάσει και να καταθέσει ένα σχέδιο δράσης με την ονομασία " **safer internet plus**". Σύμφωνα με το άρθρο φαίνεται πως μεγάλο ποσοστό των παιδιών μεταξύ 11 και 15 ετών περνούν τουλάχιστον 3 ώρες (!!!!!) ημερησίως μπροστά τον υπολογιστή τους. Το γεγονός αυτό σε συνδυασμό με την περιέργεια και την έλλειψη σωστής πληροφόρησης είναι επόμενο να τα καθιστά ευάλωτα σε κινδύνους. Τέτοιο κίνδυνοι είναι η πλοήγηση σε ακατάλληλα για ανηλίκους sites, sites με περιεχόμενο βίαιο ή πολλές φορές διακίνηση ακατάλληλου υλικού μα ακόμα και παρενόχληση από επικίνδυνους ενήλικες με καθόλου αγνές προθέσεις.
Το σχέδιο δράσης αυτό προσπαθώντας να δώσει στα παιδιά ένα ασφαλές ιντερνετ θα καταπολεμήσει το παράνομο περιεχόμενο προάγοντας ένα ασφαλές περιβάλλον, θα ενισχύσει τη δημόσια πληροφόρηση και θα εγκαταστήσει μια "βάση γνώσης" όπως χαρακτηριστικά την ονομάζει για ανακριτικούς σκοπούς.
Η επιτροπή επίσης πρότεινε τη δημιουργία μιας δωρεάν πανευρωπαϊκής γραμμής βοηθείας και τον χαρακτηρισμό "child safe" για εκείνους τους ιστότοπους που θα πληρούν τις προϋποθέσεις της και θα αποτελούν ασφαλή περιβάλλοντα πλοήγησης για τα παιδιά. Μια άλλη πρόταση που τέθηκε υπό συζήτηση είναι η δημιουργία ιστότοπων με την προέκταση "kid.eu" για εκείνα που είναι ασφαλή και ακίνδυνα για τα παιδιά.
Τέλος ένας πιο μακροπρόθεσμος στόχος της επιτροπής είναι η καθιέρωση μιας Πανευρωπαϊκής βάσης δεδομένων, στην οποία θα έχει πρόσβαση η Europol και η οποία θα συλλέγει φωτογραφίες σεξουαλικής κακοποίησης όπως επίσης και θα ανιχνεύει την εκμετάλλευση των παιδιών**.** Η προσπάθεια αυτή φαίνεται να έχει διττό όφελος για την κοινωνία. Αφενός οι επίσημοι φορείς αναγνωρίζουν την έκταση του προβλήματος και αφετέρου έχουν ήδη σκεφτεί και προτείνει μέτρα για την καταπολέμησή του. Αρκεί να εφαρμοστούν γρήγορα και σωστά προς όφελος των νεαρών πολιτών.

6. Τεχνικά μέτρα κατά του ηλεκτρονικού εγκλήματος στην Ελλάδα

Αξίζει να αναφερθεί μια αξιόλογη προσπάθεια που υλοποίησε η βρετανική μη κυβερνητική οργάνωση Internet Watch Foundation (IWF), η οποία δημιούργησε ένα είδος ανοικτής διαδικτυακής γραμμής επειγουσών κλήσεων (hotline) για καταγγελίες περιπτώσεων παιδικής πορνογραφίας οπουδήποτε στον κόσμο.
Στην Ελλάδα το 2007 το Υπουργείο Οικονομικών δημιούργησε την Ομάδα Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness and Response to Threats: DART) με στόχο την ενημέρωση των πολιτών, την πρόληψη αλλά και την αντιμετώπιση κινδύνων που σχετίζονται με τις νέες τεχνολογίες πληροφορικής και ηλεκτρονικών επικοινωνιών. Η ιστοσελίδα της Ομάδας επιτρέπει επίσης και την δικτυακή καταγγελία μέσω μιας ανοικτής γραμμής, της Safeline, που παίζει τον ρόλο του μεσολαβητή μεταξύ των πολιτών και των αστυνομικών αρχών.
Η καταγγελία που μπορεί να γίνει και ανώνυμα μπορεί να αφορά οποιοδήποτε ηλεκτρονικό έγκλημα και διευκολύνει σε περιπτώσεις αυτεπάγγελτης δίωξης για την άμεση κινητοποίηση των αρχών. Επίσης, επιτρέπει σε άτομα που δεν μπορούν να έχουν εύκολα πρόσβαση σε αρχές, είτε λόγω ηλικίας, είτε λόγω του τόπου στον οποίο βρίσκονται, είτε επειδή φοβούνται, να καταγγείλουν πράξεις, που υπό άλλες προϋποθέσεις δεν θα το έκαναν.

6.1. Safeline.gr

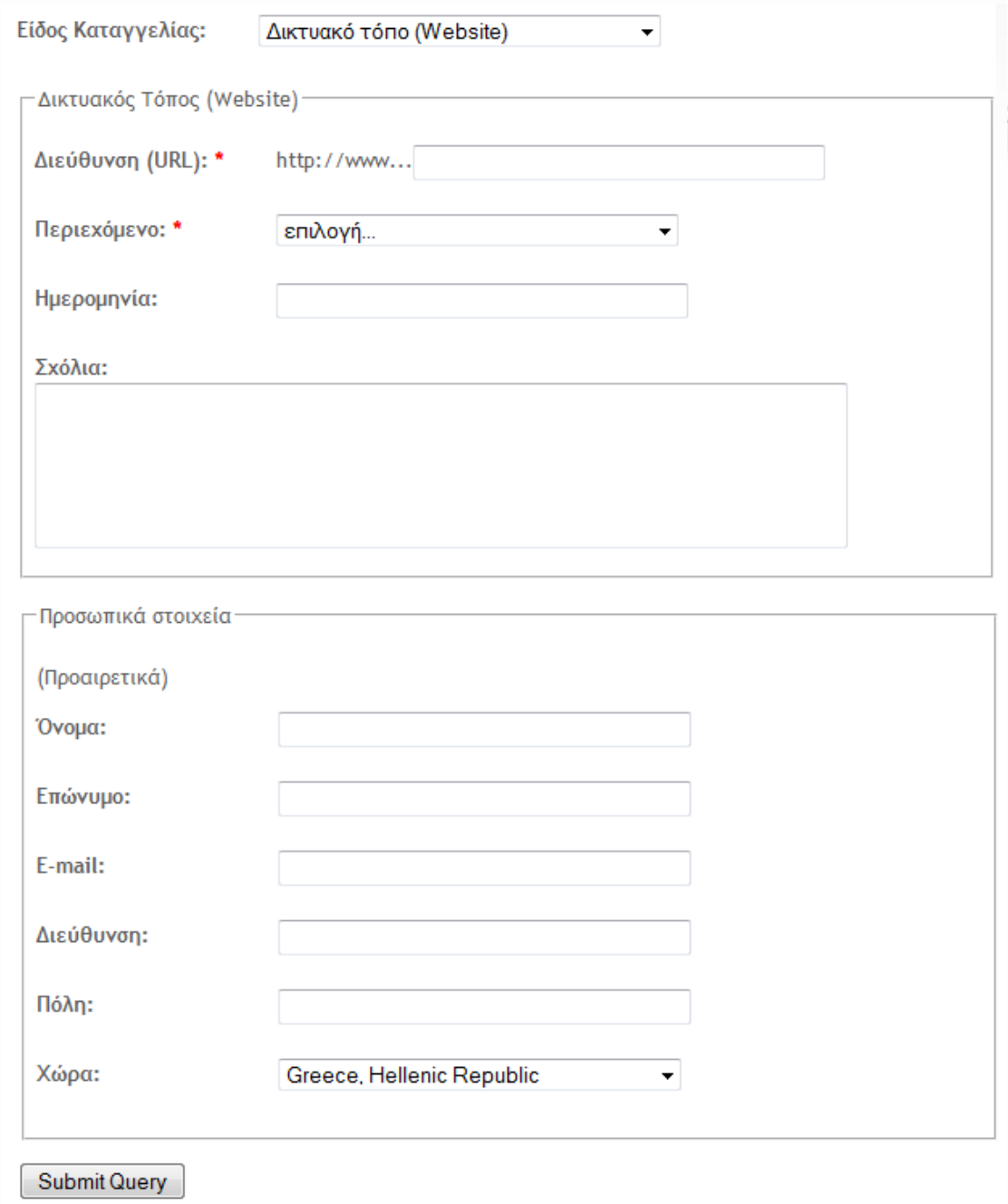


Η SafeLine δέχεται καταγγελίες για περιεχόμενο που εντοπίζετε στο Διαδίκτυο και περιέχει:

- ✓ εικόνες κακοποίησης παιδιών σε οποιοδήποτε σημείο του κόσμου
- ✓ ρατσιστικό και ξενοφοβικό υλικό που παραβαίνει την ελληνική νομοθεσία
- ✓ οτιδήποτε άλλο θεωρείτε ότι είναι παράνομο.

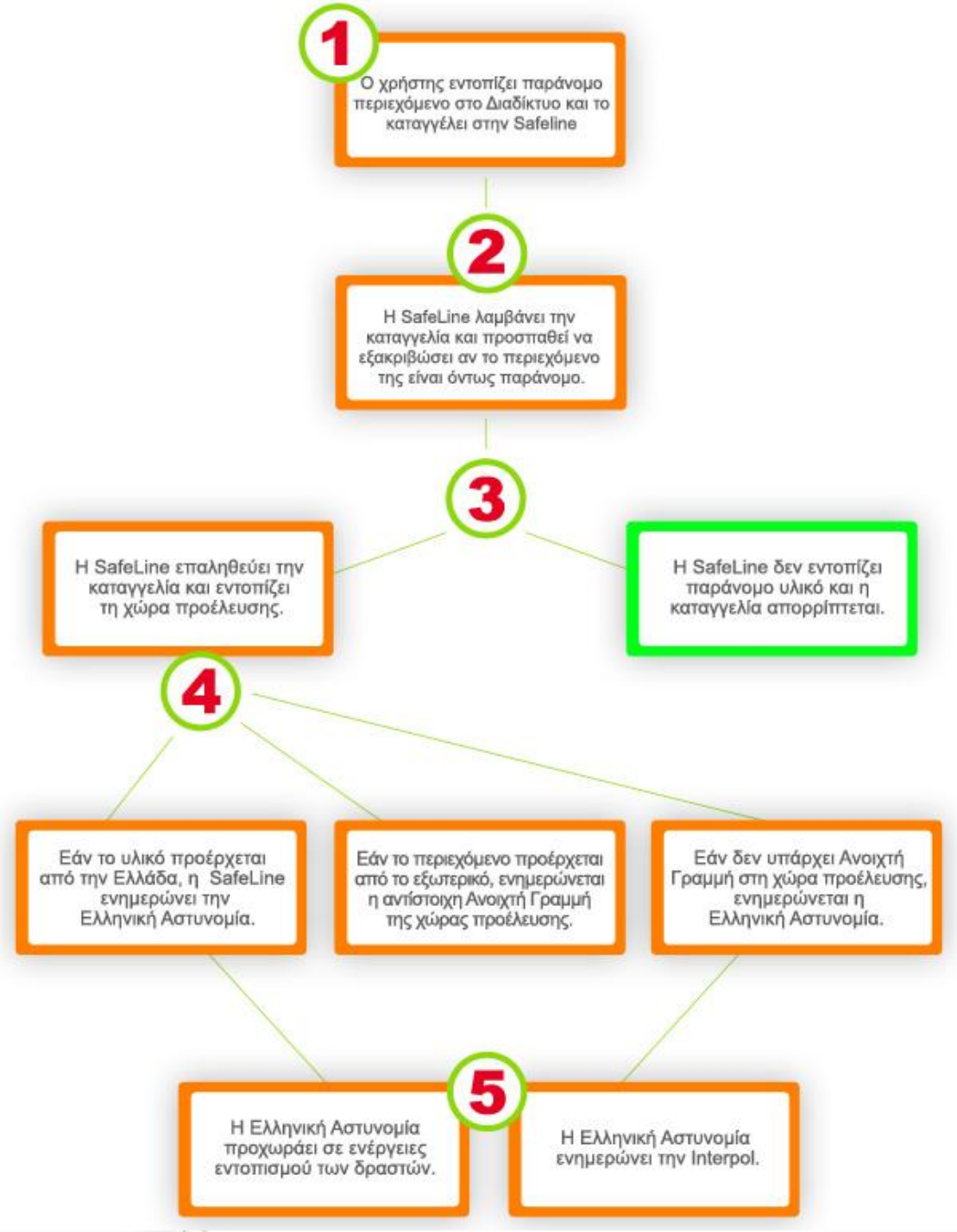
Συνεργάζεται με τους Φορείς Παροχής Υπηρεσιών Διαδικτύου, το Ακαδημαϊκό Δίκτυο ΕΔΕΤ και το Σχολικό Δίκτυο, Ερευνητικά και Πολιτιστικά Ιδρύματα, Ενώσεις Καταναλωτών και την Ελληνική Αστυνομία για τον περιορισμό της ροής του παράνομου περιεχομένου στο Διαδίκτυο.
Η SafeLine υποστηρίζεται από το Safer Internet Programme της Ευρωπαϊκής Ένωσης και υλοποιείται από τους οργανισμούς ΙΤΕ-ΙΠ Ίδρυμα Τεχνολογίας και Έρευνας, Ινστιτούτο Πληροφορικής και SAFENET Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Ίντερνετ.

Μέσω της Safeline, μπορεί κανείς να κάνει καταγγελία για ηλεκτρονικά εγκλήματα συμπληρώνοντας την παρακάτω φόρμα.



Καταγγελίες- Επεξεργασία καταγγελιών

Λαμβάνοντας μια καταγγελία, η SafeLine ακολουθεί μία προκαθορισμένη διαδικασία, όπως περιγράφεται στο παρακάτω διάγραμμα:



Συνεργασία με την Ελληνική Αστυνομία

Η SafeLine συνεργάζεται άμεσα με την Ελληνική Αστυνομία προωθώντας σε αυτήν τις καταγγελίες των οποίων το περιεχόμενο είναι εξακριβωμένα παράνομο. Πανελλαδικά υπάρχουν δύο εξειδικευμένες ομάδες της Ελληνικής Αστυνομίας που

ασχολούνται με εγκληματικές δραστηριότητες στο Διαδίκτυο, η Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος στην Αθήνα που λειτουργεί από το 2004 και η Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος στη Θεσσαλονίκη που λειτουργεί από το 2006.

7. Ο εντοπισμός του ηλεκτρονικού εγκληματία στο διαδίκτυο

7.1. Αρχεία καταγραφής (log files)

Τα αρχεία καταγραφής διαδραματίζουν σημαντικό ρόλο, καθώς σε αυτά αποθηκεύονται πληροφορίες, που αφορούν τη λειτουργία του συστήματος. Στα λειτουργικά συστήματα της οικογένειας Windows, υπάρχουν τρία βασικά είδη αρχείων καταγραφής: Application log, System log και Security log.162
Ο εντοπισμός όλων των πληροφοριών, που αποθηκεύονται τα αρχεία καταγραφής, μπορεί να πραγματοποιηθεί μέσω της κονσόλας διαχείρισης των Windows.
Η χρησιμότητα των αρχείων καταγραφής των Windows μεγιστοποιείται, όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές ομάδων (group policies). Τα security logs είναι κενά, εάν δεν έχει οριστεί συγκεκριμένη πολιτική ασφάλειας για μια ομάδα χρηστών. Η ευθύνη ορισμού πολιτικών ασφάλειας ανήκει στον διαχειριστή και υπεύθυνο ασφαλείας ενός συστήματος.
Από τα αρχεία καταγραφής, ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί να διαπιστώσει εάν χρησιμοποιήθηκε συγκεκριμένη εφαρμογή από έναν χρήστη, εάν κάποιος μη εξουσιοδοτημένος χρήστης απέκτησε πρόσβαση στο σύστημα, εάν χρησιμοποιήθηκε κάποια περιφερειακή συσκευή και πλήθος άλλων σημαντικών πληροφοριών.
Εκτός από το λειτουργικό σύστημα, αρχεία καταγραφής δημιουργούνται και από άλλες εφαρμογές. Το firewall, ως βασικό εργαλείο, που ελέγχει την κίνηση από και προς ένα προστατευόμενο δίκτυο ή υπολογιστή, αποθηκεύει σημαντικές πληροφορίες στα αρχεία καταγραφής του. Οι πληροφορίες των αρχείων αυτών, αποτελούν σημαντικό προανακριτικό αλλά και αποδεικτικό υλικό, σε περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε δίκτυα.

7.2. Εντοπισμός ονόματος χώρου και διεύθυνσης IP

Ο εντοπισμός της διεύθυνσης IP, αποτελεί βασική ενέργεια των διωκτικών αρχών για την εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο. Στις επιθέσεις αυτές οι εισβολείς χρησιμοποιούν πλαστές διευθύνσεις IP, προκειμένου να παραπλανήσουν τις διωκτικές αρχές. Κάθε διεύθυνση στο Διαδίκτυο έχει έναν αντίστοιχο αριθμό IP. Το σύστημα, που έχει αναλάβει τη διατήρηση των αντιστοιχιών μεταξύ μιας ηλεκτρονικής διεύθυνσης και του αντίστοιχου IP, είναι το DNS (Domain Name System).
Κατά την εκδήλωση μιας επίθεσης, ο επιτιθέμενος πλαστογραφεί τη διεύθυνσή του για να φαίνεται ότι είναι νόμιμος χρήστης, δεν πλαστογραφεί όμως (ή δεν μπορεί να πλαστογραφήσει) τον αντίστοιχο αριθμό IP. Συνήθως, συσκευές, όπως τα firewalls, έχουν τη δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα

να επιτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη. Εφόσον το firewall δεν έχει ρυθμιστεί κατάλληλα, ο ερευνητής θα κληθεί να ελέγξει τις διευθύνσεις όλων όσοι απέκτησαν πρόσβαση, προκειμένου να εξακριβώσει από ποιον προήλθε η κακόβουλη επίθεση. Η εργασία αυτή μπορεί να διεκπεραιωθεί με διάφορα εργαλεία λογισμικού, τα οποία ελέγχουν αν οι ηλεκτρονικές διευθύνσεις, αναλογούν σε σωστούς αριθμούς IP.
Επίσης, υπάρχουν και δικτυακοί τόποι που επιτελούν on-line την εργασία αυτή. Για παράδειγμα στο www.dnsreport.com μπορεί να δοθεί μια ηλεκτρονική διεύθυνση ή διεύθυνση ηλεκτρονικού ταχυδρομείου και να ληφθούν διάφορες πληροφορίες για αυτή, όπως το IP, ο server κ.ά.

8. Παραδείγματα αντιμετώπισης ηλεκτρονικών εγκλημάτων

- *Αποκλείστηκαν από το Facebook και το MySpace άτομα που έχουν καταδικαστεί για σεξουαλικά εγκλήματα*

Περίπου 3.500 άτομα, τα οποία έχουν καταδικαστεί για σεξουαλικά εγκλήματα στην πολιτεία της Νέας Υόρκης, "εξοστράκισαν" από τις ιστοσελίδες κοινωνικής δικτύωσης Facebook και MySpace ανακοίνωσε την Τρίτη ο υπουργός Δικαιοσύνης της πολιτείας Άντριου Κουόμο. Κατά τη διάρκεια συνέντευξης Τύπου, ο κ. Κουόμο χαιρέτισε την απόφαση των δύο ιστοσελίδων να εφαρμόσουν το νόμο "e-STOP", με τον οποίο τα 3.500 άτομα αποκλείστηκαν από τις δημοφιλείς ιστοσελίδες. Ο νόμος υιοθετήθηκε στην πολιτεία της Νέας Υόρκης το προηγούμενο έτος για την καταπολέμηση των διαδικτυακών σεξουαλικών εγκλημάτων. "Το Facebook και το MySpace εφάρμοσαν αποτελεσματικά το e-STOP για να βοηθήσουν να γίνει πιο ασφαλές το διαδίκτυο και έχει έρθει ο καιρός ώστε όλες οι ιστοσελίδες κοινωνικής δικτύωσης να διασφαλίσουν ότι δε θα υπάρξουν άλλα θύματα", δήλωσε ο υπουργός Δικαιοσύνης της Νέας Υόρκης.

- *Εξαρθρώθηκε το μεγαλύτερο κύκλωμα hacker*

Ένα από τα μεγαλύτερα δίκτυα hacker εξάρθρωσαν την Τετάρτη (3/3/2010) οι ισπανικές αρχές, που είχαν καταφέρει να μολύνουν με ιούς 13 εκατομμύρια ηλεκτρονικούς υπολογιστές και να υποκλέψουν προσωπικά και τραπεζικά δεδομένα από χρήστες 190 χωρών σε όλον τον κόσμο.
Σύμφωνα με την ισπανική αστυνομία, οι ύποπτοι που έφεραν το όνομα Mariposa, ή στα ελληνικά Πεταλούδα, είναι ηλικίας 25 ως 31 ετών και το εντυπωσιακό είναι ότι δεν είχαν και ιδιαίτερες γνώσεις πάνω στους υπολογιστές, αλλά αγόραζαν τα προγράμματα που χρησιμοποιούσαν από τη μαύρη αγορά.
Η ομάδα αυτή κέρδιζε εκατομμύρια, μισθώνοντας τμήματα του δικτύου τους σε εγκληματίες του Internet και πουλώντας κώδικες πρόσβασης, usernames, πληροφορίες από διαπιστευτήρια τραπεζών και πιστωτικές κάρτες για παράνομες οικονομικές συναλλαγές.
Η εξάπλωση του ιού από το δίκτυο Mariposa ξεκίνησε τον Μάιο του 2009 και σταδιακά μόλυνε ηλεκτρονικούς υπολογιστές στις μισές από τις 1.000 κορυφαίες εταιρείες παγκοσμίως καθώς και περισσότερες από 40 τράπεζες.

Μάλιστα ένας από τους υπόπτους είχε αποθηκεύσει στον ηλεκτρονικό υπολογιστή του προσωπικά δεδομένα από περισσότερους από 800.000 χρήστες.
Τον Δεκέμβριο, η ισπανική αστυνομία, το FBI και μερικές εταιρείες για την ασφάλεια στον κυβερνοχώρο κατάφεραν να εξαρθρώσουν το δίκτυο αλλά οι ύποπτοι ανέκτησαν τον έλεγχο σε μερικούς από τους μολυσμένους υπολογιστές και αντεπιτέθηκαν, σύμφωνα με την αστυνομία.
Οι τρεις hackers συνελήφθησαν και αφέθηκαν ελεύθεροι αφού τους απαγγέλθηκαν κατηγορίες.

- Πάτρα : 40χρονος σωματέμπορος μέσω facebook

Έναν 40χρονο τεχνικό ραδιοφώνου, αρθρογράφο και διανομέα τοπικής εφημερίδας στην Πάτρα, συνέλαβε την Πέμπτη (10/06/2010) κλιμάκιο της Δίωξης Ηλεκτρονικού Εγκλήματος Αττικής, που μετέβη στην αχαϊκή πρωτεύουσα, με την κατηγορία της σωματεμπορίας και πορνογραφίας ανηλίκων μέσω διαδικτύου.

Όπως έγινε γνωστό από την αστυνομία, ο κατηγορούμενος διατηρούσε σελίδα στο facebook, μέσω της οποίας έκανε επαφές με ανηλίκους 13 έως 16 ετών, υποσχόμενος μασάζ και διασκεδάσεις, με αποτέλεσμα να προσελκύει παιδιά.
Στη συνέχεια, αναρτούσε στο διαδίκτυο φωτογραφίες τους σε προκλητικές και ερωτικές στάσεις.
Η υπόθεση αποκαλύφθηκε μετά από πληροφορίες και αφού έγινε ψηφιακή έρευνα, από την οποία προέκυψαν τα ηλεκτρονικά ίχνη του 40χρονου και διαπιστώθηκε η διακίνηση υλικού παιδικής πορνογραφίας.
Ο 40χρονος συνελήφθη στο σπίτι του 16χρονου με τον οποίο συζούσε, παρουσία εισαγγελέα, ενώ βρέθηκαν και κατασχέθηκαν ένας φορητός ηλεκτρονικός υπολογιστής, δυο σκληροί δίσκοι ηλεκτρονικού υπολογιστή, έξι ψηφιακοί δίσκοι dvd, ένα σπαθί και ένα ξιφίδιο.

9. Πρακτικές συμβουλές για προστασία από ηλεκτρονικά εγκλήματα

- ***Για παιδιά 11-13 ετών***

Τα παιδιά ηλικίας 11- 13 ετών έχουν εξοικειωθεί με την τεχνολογία και αναπτύσσουν δικά τους συστήματα αξιών που πολλές φορές διαφέρουν από εκείνα των γονιών τους. Η κριτική τους σκέψη δεν έχει φτάσει στα ανώτερα επίπεδα και έτσι πολλές φορές αποδέχονται τη συμμετοχή σε παιχνίδια χωρίς πολύ σκέψη. Είναι εκτιθεμένα σε online κινδύνους και πολλές φορές δίνουν προσωπικά τους δεδομένα σε αγνώστους. Η ηλικία αυτή χαρακτηρίζεται από έντονη ανάπτυξη της σεξουαλικότητας και έτσι πολλές φορές , ειδικά τα αγόρια πλοηγούνται σε ακατάλληλα sites και δημιουργούν « σχέσεις» online.

ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ

• Φτιάξτε έναν κανονισμό στο σπίτι με κανόνες χρήσης του ιντερνετ. Βάλτε και τα παιδιά να συμμετέχουν στη διαδικασία ώστε να είναι οι κανόνες κοινά αποδεκτοί.

• Διατηρήστε τους υπολογιστές σε περιβάλλον που μπορείτε να τους ελέγχετε εύκολα

• Ζητήστε από τα παιδιά να σας ενημερώνουν κάθε φορά που σκοπεύουν να αλληλεπιδράσουν με κάποιον στο internet

• Συζητήστε με τα παιδιά σας για τους φίλους που απέκτησαν από το διαδίκτυο ή τις δραστηριότητές τους ακριβώς όπως θα κάνατε για έναν φίλο ή δραστηριότητα που κάνουν κάθε μέρα.

• Ενισχύστε τα να σας μιλούν και να σας συμβουλεύονται όταν κάτι που συναντούν στο διαδίκτυο τα κάνει να μην νιώθουν άνετα. Θα πρέπει να είστε έτοιμοι να ακούσετε ότι έχουν να σας που με ψυχραιμία γιατί μόνο έτσι θα κερδίσετε την εμπιστοσύνη τους.

• Μιλήστε τους και διαπαιδαγωγήστε τα σωστά σεξουαλικά γιατί είναι πολύ εύκολο

να βρεθούν αντιμέτωπα με ακατάλληλο υλικό

• Εκπαιδεύστε τα παιδιά να μη δίνουν ποτέ προσωπικά δεδομένα στο διαδίκτυο χωρίς την άδεια σας, να μη συμπληρώνουν αιτήσεις για προσωπικά προφίλ και να μην παίρνουν μέρος σε Online διαγωνισμούς χωρίς να το γνωρίζετε.

• Επιμείνετε στο να έχετε πρόσβαση στο e-mail των παιδιών σας και στους λογαριασμούς instant messaging

• Ενημερώστε τα παιδιά για την online συμπεριφορά. Τα sharing αρχεία μουσικής, ταινιών κ.τ.λ. μπορεί να υπόκεινται σε παράβαση πνευματικών δικαιωμάτων

• Μιλήστε τους για την αρχές ηθικής. Δε θα πρέπει να χρησιμοποιούν το ιντερνετ για να μεταδίδουν φήμες ή να απειλούν άλλους

• Επιτρέψτε τους τη χρήση ελεγχόμενων chat room που είναι κατάλληλα για την ηλικία τους.

- ***Για παιδιά 14-17 ετών***

Τα παιδιά αυτής της ηλικίας είναι ανοιχτά σε νέες ιδέες αλλά δεν έχουν την εμπειρία που χρειάζονται για να μπορούν κριτικά να τις κατατάσσουν.
Η ενασχόλησή τους με το διαδίκτυο έγκειται στο να κατεβάζουν μουσική και ταινίες, να στέλνουν e-mail, να παίζουν παιχνίδια online. Τα παιδιά σε αυτή την ηλικία είναι ιδιαίτερα επιδέξια στη χρήση μηχανών αναζήτησης στο internet και στη χρήση του chat. Ιδιαίτερα τα αγόρια σπρώχνουν τα όρια και πολλές φορές εμπλέκονται σε τζόγο ή ακατάλληλα sites.
Τα παιδιά 14 – 17 ετών έχουν περισσότερο ανεπτυγμένη κριτική σκέψη σε ότι αφορά τις δραστηριότητές τους. Είναι πιο ευάλωτα στο να δεχτούν σεξουαλικώς ακατάλληλα σχόλια στο διαδίκτυο και μεγαλύτερο όγκο ακαταλλήλου υλικού. Δημιουργούν εύκολα σχέσεις στο internet και είναι πολύ πιθανό να τολμήσουν να ζητήσουν και συνάντηση με το άτομο που συνομιλούν μέσω του διαδικτύου. Είναι εύκολα θύματα σε όσους πουλούν αντικείμενα στο ιντερνετ και είναι πιο πιθανό να χρησιμοποιήσουν πιστωτικές κάρτες για τις αγορές τους. Τέλος τα παιδιά αυτής της ηλικίας πειραματίζονται με την ανεύρεση ακατάλληλων sites και τον online τζόγο.

• Εκπαιδεύστε **τα παιδιά** να μη δίνουν ποτέ προσωπικά δεδομένα στο **διαδίκτυο,** να μη συμπληρώνουν αιτήσεις για προσωπικά προφίλ και να μην παίρνουν μέρος σε Online διαγωνισμούς χωρίς να το γνωρίζετε.
• Επιμείνετε στο να παραμένουν σε δημόσια chat rooms
• Ελέγχετε ποια chat rooms ή message boards επισκέπτονται
• Ενημερώστε τα **παιδιά** για την online συμπεριφορά. Τα sharing αρχεία μουσικής, ταινιών κ.τ.λ. μπορεί να υπόκεινται σε παράβαση πνευματικών δικαιωμάτων
• Βοηθήστε **τα παιδιά** να προστατευτούν από spam. Καθοδηγήστε τα να μη δίνουν το e-mail address τους, να μην απαντούν σε junk e-mails και να χρησιμοποιούν e-mail filters.
• Συζητήστε μαζί τους το τζόγο και τα πιθανά ρίσκα του
• Βεβαιωθείτε ότι ξέρετε τις οικονομικές τους συναλλαγές στο διαδίκτυο και ότι είναι ασφαλείς.

- ***Συμβουλές για τους γονείς***

• Κρατήστε τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το Διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον Κυβερνοχώρο και μάθετε από αυτά.
• Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους.
• Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms (δωμάτια συνομιλίας), χωρίς την επίβλεψη σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του Διαδικτύου χωρίς να είστε και εσείς μαζί.
• Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.
• Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου.
• Συζητήστε με τα παιδιά σας για την ασφάλεια του Διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του Διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.
• Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο.

- ***Ασφαλής χρήση του κινητού τηλεφώνου***

✓Να είστε ιδιαίτερα προσεκτικοί όταν δίνετε σε κάποιον τον αριθμό του κινητού σας τηλεφώνου. Υπάρχει κίνδυνος να αρχίσετε να λαμβάνετε ανεπιθύμητες κλήσεις και μηνύματα.

✓Πάντα να έχετε το κινητό σας υπό την επίβλεψή σας. Αποφύγετε να το δανείζετε σε τρίτους παρά μόνο αν είναι απολύτως αναγκαίο και όταν είστε και εσείς παρόντες.

✓Αποφύγετε να συναντήσετε κάποιον που γνωρίσατε μέσω του κινητού σας τηλεφώνου.

✓Χρησιμοποιείτε το κινητό σας τηλέφωνο μόνο για να επικοινωνήσετε με κάποιον όταν είναι ανάγκη και όχι για να στέλνετε ενοχλητικά μηνύματα. Πώς θα νιώθατε αν λαμβάνατε εσείς ενοχλητικά μηνύματα στο δικό σας κινητό τηλέφωνο;

✓Όταν λαμβάνετε στο κινητό σας τηλέφωνο μηνύματα ή εικονομηνύματα από αγνώστους, διαγράψτε τα χωρίς να απαντήσετε σε αυτά.

✓Για να τραβήξετε φωτογραφίες άλλων ανθρώπων πρέπει πρώτα να πάρετε την άδειά τους. Προσέξτε γιατί αν ανεβάσετε φωτογραφίες στο Διαδίκτυο μπορεί να μείνουν εκεί για πάντα και πιθανώς να χρησιμοποιηθούν με τρόπο διαφορετικό από αυτόν που εσείς αρχικά σκοπεύατε.

- ***Ασφαλής χρήση των συστημάτων ιστοσελίδων κοινωνικής δικτύωσης***

✓Δε θα πρέπει να δίνετε σε κανέναν τον κωδικό πρόσβασης στο εικονικό προφίλ σας. Όποιος αποκτά πρόσβαση στο προφίλ σας μπορεί να διαχειριστεί πλήρως τα δεδομένα που εμφανίζονται σε αυτό.

✓Μην ανεβάζετε στο προφίλ σας φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκεστε (ειδικότερα αν πρόκειται για το σπίτι σας, το σχολείο ή μέρη που συχνάζετε). Έτσι θα μειώσετε τις πιθανότητες εντοπισμού σας στο φυσικό κόσμο.

✓Αν δεχθείτε ένα προσβλητικό ή ανεπιθύμητο μήνυμα, αναφέρετέ το στην ενσωματωμένη μέθοδο καταγγελιών της ιστοσελίδας κοινωνικής δικτύωσης που χρησιμοποιείτε ή καταγγείλετε το στη SafeLine. Συνήθως αναφέρεται με τη λέξη «report».

✓Να έχετε πάντα υπόψιν σας ότι οι πληροφορίες που δημοσιεύετε στις ιστοσελίδες κοινωνικής δικτύωσης είναι ευρέως προσπελάσιμες, επομένως, καλό θαήταν να μην παρέχετε στοιχεία και φωτογραφίες που θα σας έφερναν σε δύσκολη θέση. Ακόμα και όταν διαγράψετε το προφίλ σας πολλές πληροφορίες δεν αφαιρούνται και ενδέχεται επίσης να τις συναντήσετε και αλλού στο Διαδίκτυο.

✓Να γνωρίζετε ότι από τη στιγμή που προσθέτετε στη λίστα των φίλων σας κάποιο άτομο (αποδοχή friend request), αυτό αποκτά πρόσβαση στα προσωπικά δεδομένα που εμφανίζονται στο προφίλ σας, μεταξύ των οποίων οι φωτογραφίες και τα στοιχεία επικοινωνίας σας.

✓Από τη στιγμή που δημιουργείτε το εικονικό σας προφίλ θα πρέπει να πάτε στο μενού των ρυθμίσεων για τη διαχείριση των προσωπικών σας δεδομένων (συνηθέστερα θα το βρείτε στα αγγλικά ως privacy settings) και να αλλάξετε τις προεπιλεγμένες ρυθμίσεις.

- ***Ασφαλής χρήση παιχνιδιών εικονικής πραγματικότητας***

✓Οι γονείς πρέπει να εξοικειώνονται με τα παιχνίδια εικονικής πραγματικότητας (δηλ. υπηρεσίες και προϊόντα που προσφέρονται από τα παιχνίδια εικονικής πραγματικότητας) και να γνωρίζουν πώς τα παιδιά ξοδεύουν το χρόνο τους online.

✓Ενεργοποιήστε το λογαριασμό του παιδιού σας στο επιλεγμένο παιχνίδι εικονικής πραγματικότητας χρησιμοποιώντας το δικό σας email.

✓Ελέγξτε εάν ο εικονικός κόσμος που χρησιμοποιείται από τα παιδιά σας έχει γονικό έλεγχο ή οποιοδήποτε εργαλείο που φιλτράρει Διαδικτύου, και σιγουρευτείτε ότι τέτοια εργαλεία ενεργοποιούνται.

✓Συνήθως η ηλικία ελέγχεται κατά την αγορά των προϊόντων. Δεν υπάρχει προς το παρόν σύστημα για να εγγυηθεί την επαλήθευση ηλικίας.

✓Υπάρχουν εργαλεία που εμποδίζουν τη πρόσβαση σε ανεπιθύμητους ιστοχώρους. Καλό είναι να χρησιμοποιούνται.

✓Συνήθως απαιτείται γονική συγκατάθεση για την επεξεργασία να επεξεργαστεί τα ευαίσθητα προσωπικών δεδομένων στοιχείων, για πρόσβαση σε δωμάτια συνομιλίας (chat rooms), για την αποστολή διαφημιστικών emails, για την επικοινωνία με τα παιδιά μέσω κινητού τηλεφώνου, για τη συλλογή στοιχείων των παιδιών μέσω του Διαδικτύου και για τη χρήση των στοιχείων αυτών για διαφημιστικούς λόγους. Μελετήστε τις επιλογές αυτές προσεκτικά.

- **Βέλτιστες πρακτικές για προστασία από την ηλεκτρονική εξαπάτηση**

Μην απαντάτε ποτέ σε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν τα προσωπικά σας στοιχεία Πρέπει να είστε καχύποπτοι αν λάβετε μήνυμα από εταιρεία ή άτομο που σας ζητάει τα προσωπικά σας στοιχεία — ή που σας στέλνει προσωπικά στοιχεία ζητώντας σας να τα επαληθεύσετε. Αντί για αυτό, χρησιμοποιήστε τον αριθμό τηλεφώνου από το τραπεζικό έντυπο για να τηλεφωνήσετε. Μην τηλεφωνήσετε στον αριθμό που μπορεί να περιλαμβάνεται στο μήνυμα. Ομοίως, δεν πρέπει να δίνετε ποτέ οικειοθελώς τα στοιχεία σας σε όποιον σας τηλεφωνεί χωρίς να γνωρίζετε ποιος είναι.

Μην κάνετε κλικ σε ύποπτες συνδέσεις Μην κάνετε κλικ σε συνδέσεις που περιλαμβάνονται σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου. Η σύνδεση μπορεί να μην είναι αξιόπιστη. Αντί για αυτό, επισκεφτείτε τις τοποθεσίες Web πληκτρολογώντας τη σχετική διεύθυνση URL στο πρόγραμμα περιήγησης ή χρησιμοποιώντας τη σύνδεση Αγαπημένα.

Χρησιμοποιείτε δυναμικούς κωδικούς πρόσβασης και αλλάζετέ τους συχνά Αν ο λογαριασμός τους επιτρέπει, οι δυναμικοί κωδικοί πρόσβασης συνδυάζουν πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα ώστε να είναι ακόμα ποιο δύσκολοι να σπάσουν. Μην χρησιμοποιείτε πραγματικές λέξεις. Χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για κάθε λογαριασμό και αλλάζετέ τους συχνά. Είναι δύσκολο να θυμάστε τόσους κωδικούς πρόσβασης και μπορεί να τους χάσετε εύκολα, συνεπώς βεβαιωθείτε ότι τους έχετε σημειώσει κάπου ή αποθηκεύστε τους στη

συσκευή ως διακριτικό USB. Βεβαιωθείτε ότι τους φυλάσσετε σε κλειδωμένη τοποθεσία!

- **Μην στέλνετε προσωπικά στοιχεία σε τυπικά μηνύματα ηλεκτρονικού ταχυδρομείου** Τα συνηθισμένα μηνύματα ηλεκτρονικού ταχυδρομείου δεν είναι κρυπτογραφημένα, είναι σαν να στέλνετε μια απλή καρτ ποστάλ. Αν είναι ανάγκη να χρησιμοποιήσετε μηνύματα ηλεκτρονικού ταχυδρομείου για τις προσωπικές συναλλαγές σας, χρησιμοποιήστε το Outlook για να υπογράψετε ψηφιακά και να κρυπτογραφήσετε τα μηνύματα με ασφάλεια S/MIME (S/MIME: Οι ασφαλείς/γενικές επεκτάσεις ταχυδρομείου Internet (S/MIME) είναι μια προδιαγραφή του Internet για κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου με ψηφιακή υπογραφή.). Τα MSN®, Hotmail®, Outlook Express, Microsoft Office Outlook Web Access, Lotus Notes, Netscape και Eudora υποστηρίζουν την ασφάλεια S/MIME.

- **Συνεργαστείτε με εταιρείες που γνωρίζετε και εμπιστεύεστε** Χρησιμοποιείτε γνωστές, καθιερωμένες εταιρείες με φήμη για παροχή ποιοτικών υπηρεσιών. Μια επαγγελματική τοποθεσία Web πρέπει να συνοδεύεται πάντα από δήλωση προστασίας του ιδιωτικού απορρήτου η οποία αναφέρει συγκεκριμένα ότι η εταιρεία δεν πρόκειται να διαβιβάσει το όνομα και τα στοιχεία σας σε τρίτους.

- **Βεβαιωθείτε ότι η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση** Της διεύθυνσης Web πρέπει να προηγείται η έκφραση https:// αντί για το συνηθισμένο http:// στη γραμμή διευθύνσεων. Επίσης, κάντε διπλό κλικ στο εικονίδιο κλειδαριάς από τη γραμμή κατάστασης του προγράμματος περιήγησης για να εμφανιστεί το ψηφιακό πιστοποιητικό για την τοποθεσία. Το όνομα μετά από το στοιχείο **Εκδόθηκε σε** στο πιστοποιητικό πρέπει να αντιστοιχεί στην τοποθεσία που πιστεύετε ότι έχετε επισκεφτεί. Αν υποψιάζεστε ότι η τοποθεσία Web δεν είναι αυτή που θα έπρεπε, βγείτε αμέσως και αναφέρετέ την. Μην ακολουθήσετε καμία από τις συμπεριλαμβανόμενες οδηγίες.

- **Προστατεύστε τον υπολογιστή σας** Η χρήση τείχους προστασίας είναι σημαντική, όπως επίσης η ενημέρωση του υπολογιστή και η χρήση λογισμικού αντιμετώπισης ιών. Η προστασία το υπολογιστή είναι ιδιαίτερα σημαντική αν συνδέεστε στο Internet με καλώδιο μόντεμ ή με μόντεμ DSL.

- **Παρακολουθείτε τις συναλλαγές** Εξετάστε τις επιβεβαιώσεις των παραγγελιών σας, τις δηλώσεις της πιστωτικής κάρτας και του τραπεζικού σας

λογαριασμού μόλις τις λάβετε για να βεβαιωθείτε ότι έχετε χρεωθεί μόνο για τις συναλλαγές που πραγματοποιήσατε. Πρέπει να κάνετε αναφορά χωρίς καθυστέρηση αν προκύψουν προβλήματα με το λογαριασμό σας. Καλέστε τον αριθμό που αναγράφεται στη δήλωση του τραπεζικού λογαριασμού. Χρησιμοποιείτε μόνο μία πιστωτική κάρτα για τις ηλεκτρονικές αγορές σας ώστε να παρακολουθείτε πιο εύκολα τις συναλλαγές.

- **Χρήση πιστωτικών καρτών για συναλλαγές στο Internet** Στις περισσότερες χώρες, η προσωπική σας ευθύνη σε περίπτωση που κάποιος χρησιμοποιήσει την πιστωτική σας κάρτα χωρίς άδεια περιορίζεται σημαντικά. Σε αντίθεση, αν χρησιμοποιείτε απευθείας χρέωση από τον τραπεζικό λογαριασμό ή την κάρτα σας, η προσωπική σας ευθύνη είναι συχνά το υπόλοιπο στον τραπεζικό λογαριασμό σας. Επιπλέον, μια πιστωτική κάρτα με μικρότερο πιστωτικό όριο προτιμάται για χρήση στο Internet επειδή περιορίζει το χρηματικό ποσό που μπορεί να κλέψει κάποιος σε περίπτωση που υπάρξει παραβίαση της κάρτας. Ακόμα καλύτερα, πολλές εταιρείες έκδοσης πιστωτικών καρτών προσφέρουν στους πελάτες τους την επιλογή ηλεκτρονικών αγορών με εικονικούς αριθμούς πιστωτικών καρτών μίας χρήσεως που λήγουν μετά από έναν ή δύο μήνες. Για περισσότερες λεπτομέρειες, ρωτήστε την εταιρεία σας για πληροφορίες σχετικά με τους αναλώσιμους αριθμούς πιστωτικών καρτών.

Συμπεράσματα

Καθημερινά στον Τύπο διαβάζουμε πως αποκαλύπτεται κι από κάποιο ηλεκτρονικό έγκλημα.
Τα ηλεκτρονικά εγκλήματα παρουσιάζονται σε διάφορες νέες μορφές που δυστυχώς δεν είναι εύκολο να αντιμετωπιστούν άμεσα από μεθόδους της τεχνολογίας. Έτσι τα τεχνικά μέτρα που υπάρχουν ήδη είναι δύσκολο να αντιμετωπίσουν ένα ηλεκτρονικό έγκλημα που πιθανό να εμφανιστεί σε μία νέα μορφή.
Στην Ελλάδα το φαινόμενο είναι πιο νέο σε σχέση με άλλες χώρες παρ' όλα αυτά η Δίωξη Ηλεκτρονικού Εγκλήματος κάνει το καλύτερο δυνατό προκειμένου να αντιμετωπίσει τέτοιου είδους περιστατικά.
Τέλος, θα πρέπει να υπάρχει η κατάλληλη ενημέρωση από σχολεία και από διάφορες κοινωνικές και κυβερνητικές οργανώσεις, προκειμένου να μπορούμε να αντιμετωπίσουμε κι εμείς οι ίδιοι τέτοιου είδους φαινόμενα.

Βιβλιογραφία

ΤΟ ΔΙΑΔΙΚΤΥΟ ΩΣ ΣΥΓΧΡΟΝΟ ΟΧΗΜΑ ΘΥΜΑΤΟΠΟΙΗΣΗΣ, Συκιώτου Αθανασία, Εκδόσεις Σακκουλάς, Απρίλιος 2009

Ηλεκτρονικά εγκλήματα στον κυβερνοχώρο, Δημήτριος Κανελλόπουλος, Εκπαίδευση και Νέες Τεχνολογίες, Μάρτιος 2007

SafeLine.gr, http://www.safeline.gr, Μάρτιος 2010

Δίωξη Ηλεκτρονικού Εγκλήματος του INTERNET από την καλύτερη υπηρεσία του κόσμου και μορφές ηλεκτρονικού εγκλήματος, http://www.apodimos.com/arthra/08/Mar/TO_HLEKTRONIKO_EGGLHMA_TOY_INTERNET_KAI_MORFES_TOY/index.htm, Μάρτιος 2010

Ίντερνετ και παιδιά, http://www.internetandkids.com, 09/10/2008

Ηλεκτρονικό Έγκλημα, LAWNET SA, http://www.go-online.gr/ebusiness/specials/article.html?article_id=341, Ιούνιος 2003

Ηλεκτρονικό Έγκλημα**,** http://www.acrobase.gr/showthread.php?t=476, 16/08/2006

Σερφάρω στην τράπεζα και την Εφορία, ΤΑ ΝΕΑ online, http://www.tanea.gr/default.asp?pid=2&ct=1&artId=4528018 , Καρολίνα Παπακώστα, 23/07/2009

Δίκτυα Υπολογιστών και Νομικό Πλαίσιο, utopia.duth.gr/~kdrakato/thesis/chapter5.doc, Ιούνιος 2010

HACKING: Ηλεκτρονικό φαινόμενο ή πραγματική απειλή; http://4lyk-irakl.ira.sch.gr/HACKING.htm , Ιούνιος 2010

Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας, Κ. Στούπα, http://iiu.teikav.edu.gr/iiw/Announces/pros_asf_dik/mathima_10.pdf , 2007-2008

Συνδεσιμότητα και Επιλεκτική Αποκάλυψη σε Συστήματα Διαχείρισης Ταυτοτήτων, Θεόδωρος Μπαλόπουλος, Στέφανος Γκρίτζαλης, Εργαστήριο Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων Πανεπιστήμιο Αιγαίου Καρλόβασι, Ιούνιος 2010

Αναγνώριση πλαστών μηνυμάτων ηλεκτρονικού ταχυδρομείου και τακτικών "ψαρέματος", Microsoft Corporation, http://office.microsoft.com/el-gr/outlook-help/HA001140002.aspx , 2010

Ψηφιακές Υπογραφές, Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html , 2008