Τ Ε Χ Ν Ο Λ Ο Γ Ι Κ Ο

Ε Κ Π Α Ι Δ Ε Υ Τ Ι Κ Ο Ι Δ Ρ Υ Μ Α Π Α Τ Ρ Α Σ

ΣΧΟΛΗ:ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ:ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

«ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΟΙ ΕΜΠΟΡΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΣΕ ΑΥΤΟ»

ΦΟΙΤΗΤΡΙΕΣ: ΜΑΝΩΛΙΤΣΗ ΑΝΔΡΟΝΙΚΗ

ΤΣΕΛΙΚΑ ΓΕΩΡΓΙΑ-ΘΕΩΝΗ

ΦΩΤΙΑΔΗ ΕΥΑΓΓΕΛΙΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΡΙΑ : ΒΙΣΒΑΡΔΗ ΑΝΑΣΤΑΣΙΑ

ΠΑΤΡΑ,
ΟΚΤΩΒΡΙΟΣ 2008

ΠΡΟΛΟΓΟΣ

Το θέμα της παρούσας πτυχιακής εργασίας αποτέλεσε μία ενδιαφέρουσα πρόκληση. Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στη παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μία συναλλαγή γίνεται όταν στέλνονται προσωπικές, ιδιωτικές ή οικονομικές πληροφορίες μέσω του Internet.

Από τη μελέτη που έγινε δόθηκε η δυνατότητα κατανόησης του σημαντικού ρόλου που κατέχει η ασφάλεια στο διαδίκτυο καθώς και το ηλεκτρονικό εμπόριο στη σύγχρονη διεθνής επιχειρησιακή πραγματικότητα. Ακόμα μας δόθηκε η δυνατότητα να γνωρίσουμε και να παρουσιάσουμε την παρουσία του ηλεκτρονικού εμπορίου στην Ελλάδα και τις λειτουργίες και τομείς δραστηριοποίησης του στη χώρα μας καθώς επίσης και τις διάφορες προοπτικές εξέλιξης και ανάπτυξης.

ΠΕΡΙΕΧΟΜΕΝΑ

1.ΕΙΣΑΓΩΓΗ

Η τεράστια ανάπτυξη του διαδικτύου οδηγεί καθημερινά στην μετατροπή των δεδομένων του φυσικού κόσμου σε ψηφιακή - ηλεκτρονική μορφή. Καθώς σχεδόν οποιαδήποτε υπηρεσία ή οργανισμός, ιδρύματα, εταιρείες και ιδιώτες χρησιμοποιούν υπολογιστές με πρόσβαση στο διαδίκτυο τις περισσότερες φορές για την διαχείριση των δεδομένων τους, η αξία της πληροφορίας που συγκεντρώνεται στο διαδίκτυο αποκτά τεράστιες διαστάσεις και γίνεται ένα θέμα που ολοένα και περισσότερο συζητιέται. Σε πολλές περιπτώσεις μάλιστα, ολόκληρη η πληροφορία είναι αποθηκευμένη σε ψηφιακά μέσα, χωρίς να υπάρχει σε έντυπη ή αναλογική μορφή.

Η εξάρτηση μας στα συστήματα αυτά, και το γεγονός ότι η λειτουργικότητα και η φιλικότητα των υπολογιστικών συστημάτων έχουν αυξηθεί σημαντικά, οδηγούν σε μια ενισχυμένη πολυπλοκότητα των συστημάτων αυτών. Η πολυπλοκότητα αυτή οδηγεί σε μια πληθώρα αδυναμιών και προβλημάτων στην ασφάλεια των συστημάτων και των δεδομένων, είτε από προγραμματιστικά λάθη, είτε από κακές ρυθμίσεις, είτε από τις σχέσεις εμπιστοσύνης που δημιουργούνται, είτε από άλλους λόγους.

Ο πληθυσμός του Internet αν και έχει ακουστά πολλές περιπτώσεις παραβίασης της ασφάλειας συστημάτων και κλοπής δεδομένων, δεν έχει δεχτεί μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια. Οι περισσότεροι χρήστες βρίσκονται σε σύγχυση όσον αφορά την ασφάλεια των δεδομένων τους, μην γνωρίζοντας τους κινδύνους και τις απειλές που αντιμετωπίζουν, ενώ οι εταιρείες παροχής υπηρεσιών -είτε πρόκειται για e-mail, είτε για υποβολή φορολογικών δηλώσεων και web banking- εθίζουν τους χρήστες σε πρακτικές χαμηλής ασφάλειας και παρέχουν μια αίσθηση ότι ασχολούνται αποτελεσματικά με την ασφάλεια των δεδομένων τους.

Οι χρήστες παραβιασμένων συστημάτων αντιμετωπίζουν πολύ σοβαρούς κινδύνους, χωρίς να το γνωρίζουν τις περισσότερες φορές. Ένας

επιτιθέμενος μπορεί να παρακολουθεί ό,τι πληκτρολογείται στον υπολογιστή για να μάθει αριθμούς πιστωτικών καρτών και κωδικούς, να χρησιμοποιήσει το σύστημα για τη διακίνηση πορνογραφικού υλικού, να αποσπάσει ευαίσθητα δεδομένα, ακόμα και να πραγματοποιήσει επιθέσεις σε άλλα συστήματα μέσω αυτού, ώστε να σβήσουν τα ίχνη του.

Οι επιθέσεις στο Internet αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων. Καθημερινά ανακοινώνονται καινούργιες αδυναμίες στο λογισμικό και νέοι τρόποι επίθεσης.

Με δεδομένη την εξέλιξη αυτή, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που αυτά περιέχουν και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Όλες αυτές οι απειλές είναι σημαντικοί λόγοι για να αυξηθεί η ασφάλεια στο Internet και μεταξύ των χρηστών του. Αυτό περιλαμβάνει τη βελτίωση της ασφάλειας των συστημάτων που συνδέονται με το Internet και την ενημέρωση και εκπαίδευση των χρηστών για τις απειλές.

Αν και υπάρχει πολλή πληροφορία στο Internet για την ασφάλεια δικτύων και συστημάτων, πολλές φορές δεν μπορεί να κατανοηθεί από χρήστες με λίγες γνώσεις. Άλλες φορές η πληροφορία δεν είναι συγκεκριμένη, δεν προχωράει σε μεγάλα επίπεδα λεπτομέρειας και καταλήγει ελλιπής.

Το ηλεκτρονικό εμπόριο αποτελεί σήμερα μια αναμφισβήτητη πραγματικότητα στο διεθνές επιχειρηματικό περιβάλλον. Οι συναλλαγές που βασίζονται σε δημόσια (Internet) και ιδιωτικά δίκτυα υπολογιστών νοούνται

πλέον ως σημαντική και συχνά απαραίτητη επιχειρηματική πρακτική ενώ παράλληλα συντελούνται σημαντικές αλλαγές στο τεχνολογικό και θεσμικό περιβάλλον των επιχειρήσεων. Οι επιχειρήσεις ωθούνται στο να υιοθετήσουν μια πιο ολοκληρωμένη θεώρηση της χρήσης ψηφιακών μέσων για τη διερεύνηση και βελτίωση των δραστηριοτήτων τους: το Ηλεκτρονικό Επιχειρείν.

Στην εργασία που ακολουθεί θα αναπτύξουμε το θέμα σχετικά με την Ασφάλεια στο Διαδίκτυο και τις Εμπορικές Συναλλαγές σε αυτό.

Ειδικότερα στο κεφάλαιο 2 θα αναφέρουμε τις απαιτήσεις ασφάλειας των πληροφοριακών συστημάτων και του ηλεκτρονικού εμπορίου.

Στο κεφάλαιο 3, θα εξετάσουμε τις τεχνολογίες ασφάλειας και πιο συγκεκριμένα θα αναφερθούμε στα είδη της κρυπτογράφησης, τις ψηφιακές υπογραφές, στα ψηφιακά πιστοποιητικά, στους ψηφιακούς φακέλους και τέλος στη διαχείριση κλειδιών.

Στο κεφάλαιο 4, θα προβάλλουμε τα συστήματα ασφάλειας στο διαδίκτυο. Θα κάνουμε σαφείς τους ορισμούς και τις έννοιες δικτύου και διαδικτύου, παγκόσμιου ιστού, ηλεκτρονικού ταχυδρομείου. Επίσης θα αναλύσουμε τη χρησιμότητα των firewalls και τα είδη των πρωτοκόλλων.

Στο κεφάλαιο 5, γίνεται αναφορά στους εχθρούς και απειλές των πληροφοριακών συστημάτων, καθώς επίσης στα διαδικτυακά εγκλήματα και στους κινδύνους που κρύβονται για τα παιδιά κατά την πλοήγηση τους στο διαδίκτυο.

Στο κεφάλαιο 6, θα εξετάσουμε το ηλεκτρονικό εμπόριο. Παρακάτω παρατίθενται οι κίνδυνοι και τα προβλήματα που εμφανίζονται από την εφαρμογή των εμπορικών συναλλαγών. Επιπλέον, θα μιλήσουμε για τη προστασία των προσωπικών δεδομένων και των ηλεκτρονικών συναλλαγών.

Στο 7 και τελευταίο κεφάλαιο, θα μελετήσουμε τη νομοθεσία που υπάρχει σήμερα σχετικά με την ασφάλεια στο διαδίκτυο και στις εμπορικές συναλλαγές.

2.ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι΄αυτό άτομα (εμπιστευτικότητα, εξουσιοδότηση). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (ακεραιότητα). Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον Χ. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

Οι παραπάνω ιδιότητες, (εξουσιοδότηση, εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

2.1 ΕΛΕΓΧΟΣ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

Ο έλεγχος αυθεντικότητας είναι «ένας θετικός προσδιορισμός, με έναν βαθμό βεβαιότητας ικανοποιητικό για να επιτρέψει ορισμένα δικαιώματα ή προνόμια στο πρόσωπο ή στο αντικείμενο που προσδιορίζεται θετικά.» Στους απλούστερους όρους, είναι «η πράξη της επαλήθευσης της απαιτούμενης ταυτότητας ενός ατόμου, ενός σταθμού ή ενός δημιουργού». Σε μια ανθρώπινη τηλεφωνική επικοινωνία, ο πελάτης και ο έμπορος μπορούν να επικυρώσουν ο ένας τον άλλο από τις φωνές τους.

Οι κλασικές μέθοδοι για το συσχετισμό εικονικών και φυσικών ταυτοτήτων στον κυβερνοχώρο είναι παράλληλες με τις μεθόδους που χρησιμοποιούνται για την επικύρωση των ανθρωπίνων όντων στο φυσικό κόσμο. Οι τέσσερις κατηγορίες για τον έλεγχο αυθεντικότητας πληροφοριών είναι:

- Τι γνωρίζουμε – π.χ. τον κωδικό ή το παρασύνθημα.
- Τι κάνουμε – π.χ. πώς κάποιος γράφει το όνομά του ή τον τρόπο που μιλάει.
- Τι είμαστε – π.χ. το πρόσωπο κάποιου, τα βιομετρικά χαρακτηριστικά του όπως τα αποτυπώματα.
- Τι έχουμε – π.χ. ένα πιστοποιητικό όπως το δίπλωμα οδήγησης

Όλες αυτές οι κατηγορίες επικύρωσης χρησιμοποιούνται στον κυβερνοχώρο. Το τελευταίο παράδειγμα είναι ιδιαίτερα ενδιαφέρον: τα πιστοποιητικά διαδραματίζουν έναν κρίσιμο ρόλο στην επικύρωση των ανθρώπων (ή προγραμμάτων ή μηχανών) στον κόσμο του ηλεκτρονικού εμπορίου. Η άδεια οδήγησης για παράδειγμα, εάν υποτίθεται ότι είναι πραγματική, λέει στον έμπορο ότι κάποια στιγμή στο παρελθόν, μια αρχή πιστοποίησης έχει λάβει κάποια μέτρα για να εξασφαλιστεί ότι οι πληροφορίες που περιέχονται στην άδεια είναι (ήταν) σωστές. Στον κυβερνοχώρο, ο έλεγχος της νομιμότητας ενός πιστοποιητικού μπορεί να είναι ευκολότερος από ότι στον πραγματικό κόσμο.

Κάποιες μέθοδοι για να ελέγξουμε την αυθεντικότητα είναι:

- Ταυτότητα του χρήστη και κωδικοί. Το σύστημα συγκρίνει τον δοθέντα κωδικό με τον αποθηκευμένο κωδικό. Εάν οι δύο κωδικοί ταιριάζουν τότε ο χρήστης είναι αυθεντικός.
- Κάρτα που περιέχει μια μαγνητική ταινία στην οποία περιλαμβάνονται τα στοιχεία του χρήστη, έτσι ώστε να μην χρειάζεται να εισαχθεί κάποιο φυσικό δεδομένο εκτός από κάποιο PIN.
- Ψηφιακό πιστοποιητικό, ένα κωδικοποιημένο σύνολο δεδομένων το οποίο περιέχει πληροφορίες για τον ιδιοκτήτη, το δημιουργό, τις ημερομηνίες παραγωγής και λήξης και άλλα δεδομένα που χαρακτηρίζουν μοναδικά έναν χρήστη.
- Ένα εξωτερικό κλειδί (hardware), μικρή ηλεκτρονική συσκευή η οποία δημιουργεί ένα νέο τυχαίο κωδικό σε συγχρονισμό με τον κύριο υπολογιστή.
- Βιομετρικά – αμφιβληστροειδικός έλεγχος ή έλεγχος δακτυλικού αποτυπώματος. Κάποια μέρη του σώματος θεωρούνται αρκετά μοναδικά ώστε να επιτρέψουν τον έλεγχο αυθεντικότητας σε υπολογιστικά συστήματα βασισμένο σε κάποιο από αυτά τα χαρακτηριστικά.

Είτε ο χρήστης το γνωρίζει είτε όχι, οι ανησυχίες τους γύρω από την ασφάλεια του ηλεκτρονικού εμπορίου είναι κυρίως ο απομακρυσμένος έλεγχος πρόσβασης (remote access control). Όποτε κάποιος θέλει να πραγματοποιήσει επιχειρηματικές συναλλαγές, είτε μέσω του διαδικτύου είτε πρόσωπο με πρόσωπο, ο πελάτης και ο έμπορος πρέπει να παρέχουν αναγνώριση, επικύρωση και εξουσιοδότηση. Οι χρήστες πρέπει να είναι σίγουροι ότι γνωρίζουν επακριβώς ποιος διαχειρίζεται τον διακομιστή δικτύου (Web Server) με τον οποίο σκοπεύουν να πραγματοποιήσουν αυτές τις επιχειρηματικές συναλλαγές. Οι έμποροι χρειάζονται την αναγνώριση από τους πελάτες τους ώστε να είναι σίγουροι ότι πληρώνονται για τα προϊόντα ή τις υπηρεσίες που παρέχουνε.

Σε μία από τις πρώτες υποθέσεις παραβίασης της επικύρωσης το 1996-1997, πολλοί άνθρωποι που έβλεπαν φωτογραφίες σε διάφορους ιστότοπους βρέθηκαν προ εκπλήξεως όταν έλαβαν τους τηλεφωνικούς τους λογαριασμούς. Τα θύματα που κατέβαζαν ένα ειδικό πρόγραμμα για την προβολή των φωτογραφιών ουσιαστικά εγκαθιστούσαν ένα πρόγραμμα «Δούρειο Ίππο» (Trojan Horse) το οποίο τους αποσύνδεε αθόρυβα από τη σύνδεσή τους με τον κανονικό τους παροχέα internet και τους επανασυνέδεε (χωρίς αυτοί να ακούνε τον χαρακτηριστικό ήχο του modem) σε έναν αριθμό στη Μολδαβία της Κεντρικής Ευρώπης. Το τηλεφώνημα στην συνέχεια προωθούνταν σε έναν παροχέα στη Βόρεια Αμερική ο οποίος συνέχιζε τη σύνοδο.

2.2 ΕΞΟΥΣΙΟΔΟΤΗΣΗ

Εξουσιοδότηση είναι το να παρέχεται σε έναν χρήστη, πρόγραμμα ή διεργασία το δικαίωμα της πρόσβασης. Στον πραγματικό κόσμο συναντούμε την εξουσιοδότηση κάθε φορά που ένας έμπορος ελέγχει την πιστωτική μας κάρτα για να δει αν έχουμε το δικαίωμα να ξοδέψουμε ένα συγκεκριμένο ποσό χρημάτων στην επιχείρησή τους.

Σε ένα περιβάλλον κεντρικών υπολογιστών, η εξουσιοδότηση εξαρτάται από το λειτουργικό σύστημα και το επίπεδο της ασφάλειας του συστήματος που έχει επιβάλλει ο διαχειριστής. Η αναγνώριση και η εξουσιοδότηση ξεκινούν όταν αρχίσει μια σύνοδος. Η σύνοδος είναι μια δραστηριότητα για μια χρονική περίοδο. Με τον όρο δραστηριότητα εννοούμε τη σύνδεση σε έναν υπολογιστή/δίκτυο από έναν χρήστη και η χρονική περίοδος οροθετείται από την έναρξη της συνόδου (logon) και από τον τερματισμό της (logoff). Ωστόσο, στο διαδίκτυο, οι περισσότερες διεπαφές γίνονται χωρίς την εγκαθίδρυση μιας συνόδου, για παράδειγμα δεν υπάρχει αναγνώριση και εξουσιοδότηση όταν ένας ανώνυμος χρήστης απαιτεί πρόσβαση σε μία δημόσια σελίδα στο διαδίκτυο. Δεν

υπάρχει είσοδος (logon) ή έξοδος (logoff) σ'αυτήν την περίπτωση. Η αναγνώριση και η εξουσιοδότηση απαιτούνται μόνο όταν ο χρήστης και ο ιδιοκτήτης του ιστοτόπου συμφωνούν ώστε να εγκαθιδρύσουν μια ασφαλή σύνοδο.

Η ακεραιότητα των συνόδων και ο έλεγχος αυθεντικότητας μπορούν να παραβιαστούν με ποικίλους τρόπους. Το φαινόμενο του "Piggybacking" είναι η χρήση μιας υπάρχουσας συνόδου από κάποιον που δεν έχει την εξουσιοδότηση να την χρησιμοποιήσει. Αυτό το πρόβλημα είναι δύσκολο να το φανταστούμε στον πραγματικό κόσμο, όπου είναι απίθανο κάποιος για παράδειγμα να χρησιμοποιήσει το όνομα και την πιστωτική κάρτα κάποιου ώστε να αποκτήσει κάποια αγαθά. Στο διαδίκτυο παρόλα αυτά, είναι αρκετά κοινότυπο το φαινόμενο όπου χρήστες αρχίζουν μια συναλλαγή σε ένα τερματικό και κάποια στιγμή φεύγουν προσωρινά από τη θέση τους αφήνοντας απροστάτευτη τη σύνοδο για να κάνουν κάτι άλλο. Αν κάποιος κακόβουλος άνθρωπος καθίσει στη θέση τους εκείνη τη στιγμή, είναι πιθανό να εκμεταλλευτεί την σύνοδο προς όφελός του. Ένα συχνό πρόβλημα του piggybacking είναι η εκμετάλλευση του ηλεκτρονικού ταχυδρομείου κάποιου ατόμου ώστε να στείλει ανεπιθύμητη αλληλογραφία με τα στοιχεία αυτού του ατόμου. Σε ένα άλλο παράδειγμα μπορεί ο «απατεώνας» να μπει σε μια σύνοδο και να αλλάξει μια παραγγελία ή τη διεύθυνση στην οποία θα σταλούν τα αγαθά αλλά να πληρωθεί από την πιστωτική κάρτα του ατόμου που ξεκίνησε τη σύνοδο. Τέτοια παραδείγματα απάτης μπορεί να έχουν καταστροφικές συνέπειες για τα θύματα και κατά γενική ομολογία κάθε νέα είδηση που αφορά τέτοιου είδους απάτες μειώνουν την πεποίθηση για την ασφάλεια του ηλεκτρονικού εμπορίου.

Μια περισσότερο τεχνική επίθεση ονομάζεται πειρατεία συνόδου (hijacking). Το hijacking επιτρέπει στον επιτιθέμενο να καταλάβει ένα ανοιχτό τερματικό ή μια σύνοδο εισόδου από έναν χρήστη ο οποίος έχει εξουσιοδοτηθεί από το σύστημα. Αυτές οι επιθέσεις γενικά συμβαίνουν σε απομακρυσμένους υπολογιστές, ωστόσο μερικές φορές είναι πιθανό να γίνουν στη σύνδεση μεταξύ

του απομακρυσμένου υπολογιστή και του τοπικού υπολογιστή. Αυτή η «πειρατεία» συμβαίνει όταν ένας εισβολέας χρησιμοποιεί ψευδώς αποκτημένα προνόμια ώστε να αποκτήσει την πρόσβαση στο λογισμικό ενός συστήματος που ελέγχει την συμπεριφορά του τοπικού TCP (Transmission Control Protocol).

Μια επιτυχημένη πειρατεία επιτρέπει στον επιτιθέμενο να δανειστεί ή να κλέψει μια ανοιχτή σύνδεση (π.χ. Telnet) από έναν απομακρυσμένο πάροχο για τους δικούς του σκοπούς. Στο πιθανό ενδεχόμενο που ο γνήσιος χρήστης έχει ήδη εξουσιοδοτηθεί σε έναν απομακρυσμένο πάροχο, οποιαδήποτε είσοδος από το πληκτρολόγιο που στέλνει ο επιτιθέμενος λαμβάνονται και επεξεργάζονται σαν να είχαν σταλεί από τον χρήστη.

Εν ολίγοις, η αναγνώριση, ο έλεγχος αυθεντικότητας και η εξουσιοδότηση είναι απαραίτητα συστατικά για κάθε επιχειρηματική συναλλαγή και πρέπει να εξασφαλίζονται από τα τηλεπικοινωνιακά συστήματα και από το λογισμικό που μεσολαβεί μεταξύ του προμηθευτή και του πελάτη.

2.3 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Σε κάποιο site τις περισσότερες φορές υπάρχουν πληροφορίες που δεν θα πρέπει να προσπελαστούν από μη εξουσιοδοτημένους χρήστες. Τα λειτουργικά συστήματα διαθέτουν συνήθως ενσωματωμένους μηχανισμούς για την προστασία των αρχείων. Οι μηχανισμοί αυτοί δίνουν την δυνατότητα σε έναν διαχειριστή να ελέγχει ποιος θα έχει πρόσβαση στα περιεχόμενα των αρχείων αυτών. Ο έλεγχος και η αποτροπή της μη εξουσιοδοτημένης προσπέλασης σε εμπιστευτικά δεδομένα είναι μία πρωταρχική απαίτηση που συναντάται σε όλα σχεδόν τα ασφαλή πληροφοριακά συστήματα.

Η εμπιστευτικότητα μπορεί να επιτευχθεί και με την κρυπτογράφηση. Η κρυπτογράφηση επιτυγχάνεται με την παρεμβολή χαρακτήρων στα δεδομένα, έτσι ώστε να είναι δύσκολη και χρονοβόρα η εύρεση της αρχικής πληροφορίας

για οποιονδήποτε άλλο εκτός από τους εξουσιοδοτημένους παραλήπτες. Οι εξουσιοδοτημένοι παραλήπτες και οι ιδιοκτήτες της πληροφορίας κατέχουν τα κλειδιά για την αποκρυπτογράφηση της πληροφορίας.

Επομένως εμπιστευτικότητα είναι η κρυπτογράφηση (κωδικοποίηση) των δεδομένων ή και των μηνυμάτων και συνεπώς η προστασία τους από τρίτα, μη εξουσιοδοτημένα άτομα. Αυτό σημαίνει ότι τα δεδομένα ή τα μηνύματα δεν μπορεί ούτε καν να τα δει κάποιος τρίτος, πόσο μάλλον να τα τροποποιήσει. Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Όσο αφορά την εμπιστευτικότητα υπάρχουν και αρκετές απειλές. Αυτές περιλαμβάνουν την ανάγνωση εμπιστευτικών δεδομένων όπως εταιρικά μυστικά ή δεδομένα πιστωτικών καρτών. Οι απειλές εμπιστευτικότητας δεν αφορούν μόνο την ανάγνωση αποθηκευμένων δεδομένων, αλλά μπορούν να περιλαμβάνουν την κλοπή δεδομένων περιγραφής δικτύου, όπως τα δεδομένα που περιγράφουν τις πρακτικές ασφαλείας του διαχειριστή.

2.4 ΑΚΕΡΑΙΟΤΗΤΑ

Ακεραιότητα μπορούμε να πούμε ότι είναι η προστασία των δεδομένων ή και των μηνυμάτων από ενδεχόμενη τροποποίησή τους από τρίτα, μη εξουσιοδοτημένα άτομα. Αυτό σημαίνει ότι τα δεδομένα ή τα μηνύματα μπορεί να τα δει κάποιος τρίτος αλλά όχι και να τα τροποποιήσει. Η ακεραιότητα

βεβαιώνει ότι τα δεδομένα είναι σωστά και ότι αλλαγές χωρίς προηγούμενη άδεια μπορούν να προβλεφθούν ή τουλάχιστον να εντοπιστούν.

Επίσης, η ακεραιότητα περιλαμβάνει και αρκετές απειλές. Οι απειλές αυτές περιλαμβάνουν έναν εισβολέα που παραποιεί αποθηκευμένα δεδομένα, όπως πιστωτικές κάρτες ή την παραποίηση δεδομένων κατά τη μεταφορά, για παράδειγμα την προσθήκη κάποιας πίστωσης στον λογαριασμό πιστωτικής κάρτας του εισβολέα. Οι απειλές ακεραιότητας έχουν σαν αποτέλεσμα την απώλεια σημαντικών πληροφοριών και μπορούν να κάνουν έναν διακομιστή επιρρεπή σε επιπλέον επιθέσεις. Για παράδειγμα ένας τρόπος εισαγωγής σε κάποιο διακομιστή είναι η παραποίηση του φακέλου με τους κωδικούς, ώστε ο εισβολέας να αναγνωρίζεται σαν εξουσιοδοτημένος χρήστης. Υπάρχουν ορισμένοι τρόποι για τη μείωση αυτών των απειλών.

- Χρήση κρυπτογραφικών μεθόδων που θα κάνουν σημαντικά αρχεία μη αναγνώσιμα.
- Χρήση επιτομής μηνυμάτων για τον έλεγχο ότι σημαντικά αρχεία δεν έχουν παραποιηθεί.
- Τακτική δημιουργία εφεδρικών αντιγράφων για σημαντικά αρχεία.
- Χρήση τεχνολογίας firewall για την αποτροπή πρόσβασης στους διακομιστές που περιέχουν τα δεδομένα.

2.5 ΜΗ ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ

Γενικά, μη αποποίηση ευθύνης είναι η ικανότητα να επιβεβαιώσουμε ότι κάποιος που παίρνει μέρος π.χ. σε ένα συμβόλαιο ή σε μια επικοινωνία δεν μπορεί να αρνηθεί την αυθεντικότητα της υπογραφής του σε ένα έγγραφο ή το ότι ήταν αυτός που έστειλε κάποιο μήνυμα. Στο διαδίκτυο, η ψηφιακή υπογραφή χρησιμοποιείται όχι μόνο στο να επιβεβαιώσει ότι ένα μήνυμα ή ένα έγγραφο έχει υπογραφεί ηλεκτρονικά από το άτομο που ισχυρίζεται ότι έχει υπογράψει το έγγραφο, αλλά επίσης για να διασφαλίσει ότι αυτό το άτομο

αργότερα δεν θα μπορεί να αρνηθεί ότι εφοδιάστηκε την υπογραφή από κάπου αλλού αφού κάθε ψηφιακή υπογραφή μπορεί να δημιουργηθεί από ένα και μόνο άτομο.

Με λίγα λόγια, ο όρος μη αποποίηση ευθύνης κρυπτό-τεχνικά μπορεί να σημαίνει:

1) Κατά τον έλεγχο αυθεντικότητας, μια υπηρεσία που παρέχει αποδείξεις για την ακεραιότητα και την προέλευση των δεδομένων, το οποίο μπορεί να επιβεβαιωθεί από οποιοδήποτε τρίτο πρόσωπο οποιαδήποτε χρονική στιγμή.
2) Μια μορφή ελέγχου αυθεντικότητας που μπορεί με μεγάλη βεβαιότητα να αποδείξει τη γνησιότητα και δεν μπορεί να αμφισβητηθεί από κανέναν.

Το 1998 η επιτροπή ειδικών ηλεκτρονικού εμπορίου της κυβέρνησης της Αυστραλίας υιοθέτησε έναν τεχνικό όρο για την έννοια της μη αποποίησης ευθύνης:

Η μη αποποίηση ευθύνης είναι μια ιδιοκτησία που επιτυγχάνεται μέσα από κρυπτογραφικές μεθόδους που αποτρέπουν ένα άτομο ή μια οντότητα από το να αρνηθεί ότι έχει λάβει μέρος σε μία συγκεκριμένη πράξη που σχετίζεται με δεδομένα (για παράδειγμα μηχανισμοί για την απόδειξη της προέλευσης, του σκοπού, της δέσμευσης ή της ιδιοκτησίας)

Πρόκειται για την άρνηση του δικαιώματος για αποκήρυξη μιας ψηφιακής υπογραφής που προκαλεί μεγάλη ανησυχία και έχει ως αποτέλεσμα τη λάθος χρήση της στο καθεστώς των ψηφιακών υπογραφών. Επιπροσθέτως, ο Διεθνής Οργανισμός Τυποποίησης (ISO) δίνει το δικό του ορισμό στην έννοια της μη αποποίησης ευθύνης: Σκοπός της, σε προσαρμογή με το ISO/IEC 13888-1,-2,-3 είναι να παρέχει επιβεβαιώσιμες αποδείξεις ή στοιχεία εγγραφής δεδομένων, χρησιμοποιώντας συμμετρικές ή ασύμμετρες κρυπτογραφικές τεχνικές που δημιουργούν τιμές ελέγχου για τα παρακάτω στοιχεία:

1) Έγκριση – Η μη αποποίηση ευθύνης της έγκρισης παρέχει αποδείξεις για το ποιος είναι υπεύθυνος για την έγκριση του περιεχομένου ενός μηνύματος.
2) Αποστολή – Η μη αποποίηση ευθύνης της αποστολής είναι μια υπηρεσία που παρέχει αποδείξεις για το ποιος έστειλε ένα μήνυμα.
3) Προέλευση – Η μη αποποίηση ευθύνης της προέλευσης είναι ένας συνδυασμός των υπηρεσιών έγκρισης και αποστολής.
4) Υποβολή – Η μη αποποίηση ευθύνης της υποβολής παρέχει αποδείξεις ότι μια αρχή παράδοσης έχει αποδεχτεί ένα μήνυμα προς μετάδοση.
5) Μεταφορά – Η μη αποποίηση ευθύνης της υπηρεσίας μεταφοράς έχει αποδείξεις για τον δημιουργό του μηνύματος ότι μια αρχή παράδοσης έχει μεταβιβάσει το μήνυμα στον παραλήπτη
6) Παραλαβή – Η μη αποποίηση ευθύνης της παραλαβής διαπιστεύει ότι ο παραλήπτης έλαβε κάποιο μήνυμα.
7) Γνώση – Η μη αποποίηση ευθύνης της γνώσης παρέχει διαπιστευτήρια ότι ο παραλήπτης αναγνώρισε το περιεχόμενο του σταλμένου μηνύματος.
8) Παράδοση – Η μη αποποίηση ευθύνης της παραλαβής είναι ένας συνδυασμός των υπηρεσιών παραλαβής και γνώσης καθώς παρέχει αποδείξεις ότι ο παραλήπτης έλαβε το μήνυμα και το αναγνώρισε.

Στο περιβάλλον του ηλεκτρονικού εμπορίου, ο τεχνικός όρος της μη αποποίησης ευθύνης είτε μετακινεί το βάρος των αποδείξεων από τον αποστολέα στον υποτιθέμενο υπογράφων είτε αρνείται ολοκληρωτικά στον υπογράφων το δικαίωμα να αμφισβητήσει την ψηφιακή υπογραφή. Αυτό συμβαίνει αν μια ψηφιακή υπογραφή είναι επικυρωμένη ώστε να αναγνωρίζει τον ιδιοκτήτη του ιδιωτικού κλειδιού που χρησιμοποιήθηκε για να δημιουργηθεί η ψηφιακή υπογραφή και μετά είναι αυτό το άτομο που θα πρέπει να επωμιστεί το βάρος του να αποδείξει ότι δεν είναι δική του η ψηφιακή υπογραφή. Κάποιοι σχολιαστές έχουν φτάσει να συνηγορούν ότι αν μια ψηφιακή υπογραφή είναι

επικυρωμένη τότε ο ιδιοκτήτης του ιδιωτικού κλειδιού αποτρέπεται από το να αποκηρύξει την ψηφιακή υπογραφή.

Ο παραπάνω τεχνικός όρος της μη αποποίησης ευθύνης είναι λανθασμένος και δεν λαμβάνει υπ'όψιν την πιθανότητα της κλοπής ή της παράνομης χρήσης ενός ιδιωτικού κλειδιού. Επιπροσθέτως ο τεχνικός όρος αναφέρεται σε γεγονότα που έχουν σχέση μετά την υπογραφή και όχι με τον μηχανισμό λειτουργίας των υπογραφών. Ένας από τους βασικούς ρόλους των αξιόπιστων παρόχων είναι να φτιάξουν μια «αποθήκη» με ψηφιακά πιστοποιητικά που περιλαμβάνουν δημόσια κλειδιά που ανταποκρίνονται στα ιδιωτικά κλειδιά των ψηφιακών υπογραφών. Τα πιστοποιητικά αυτά χρησιμοποιούνται για να επαληθεύσουν ότι οι ψηφιακές υπογραφές ανταποκρίνονται στα δημόσια κλειδιά που περιλαμβάνονται στα πιστοποιητικά. Η χρήση τους όμως και πάλι δεν σχετίζεται με τη διαδικασία της υπογραφής με οποιονδήποτε τρόπο.

Αφού καμία τεχνολογία για ασφάλεια στο διαδίκτυο δεν μπορεί να θεωρηθεί απόλυτα φερέγγυα, κάποιοι ειδικοί προειδοποιούν ότι η ψηφιακή υπογραφή από μόνη της μπορεί να μην εγγυάται πάντα την μη αποποίηση ευθύνης. Συνιστάται να χρησιμοποιούνται αρκετές μέθοδοι, όπως η δειγματοληψία βιομετρικών πληροφοριών και λοιπά δεδομένα για τον αποστολέα ή αυτόν που βάζει την υπογραφή που συγκεντρωτικά θα είναι δύσκολο να τα αποποιηθεί.

3. ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

3.1 ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Αρχικά η αυθεντικοποίηση μπορεί να συσχετιστεί με την απόκρυψη του μηνύματος. Η αυθεντικοποίηση είναι κάτι που χρησιμοποιεί κανείς για να αποδείξει την ταυτότητα από κάτι που έχει, που είναι, που γνωρίζει. Είναι μέρος της αναγνώρισης και της διαδικασίας αυθεντικοποίησης. Η πιο κοινή φόρμα στην αυθεντικοποίηση είναι το username και το password. Οι περισσότεροι κωδικοί είναι κρυπτογραφημένοι. Δεν χρειάζονται αποκλειστικά να είναι κρυπτογραφημένοι, αλλά χωρίς κρυπτογράφηση η διαδικασία της αυθεντικοποίησης μπορεί να είναι αδύναμη. FTP και Telnet είναι δύο παραδείγματα από αυτό επειδή τα username και τα password μεταβιβάζονται σε clear text και ο καθένας που έχει πρόσβαση στο καλώδιο μπορεί να κάνει capture αυτούς τους κωδικούς. Τα virtual private networks (VPNs) επίσης χρησιμοποιούν αυθεντικοποίηση, αλλά αντί για clear text χρησιμοποιούν ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές για περισσότερη ακρίβεια στην αναγνώριση του χρήστη και προστασία της αυθεντικοποίησης από spoofing.

Η αυθεντικοποίηση διακρίνεται σε:

- **Αυθεντικοποίηση οντότητας:** Η διαδικασία σύμφωνα με την οποία μια οντότητα Α βεβαιώνεται για την ταυτότητα μιας άλλης οντότητας Β (άτομο, τερματικό, πιστωτική κάρτα) και ότι η Β είναι ενεργή την ώρα που γίνεται η διαδικασία της αυθεντικοποίησης. Πρόκειται για μια διαδικασία πραγματικού χρόνου, με την έννοια ότι διαβεβαιώνει πως η οντότητα που αυθεντικοποιείται είναι λειτουργική την ώρα που αυθεντικοποιείται (παρέχουν διαβεβαιώσεις μόνο για τη συγκεκριμένη χρονική στιγμή).

- **Αυθεντικοποίηση μηνύματος:** Η διαδικασία σύμφωνα με την οποία επιβεβαιώνεται ότι μια οντότητα αποτελεί την πηγή κάποιων δεδομένων τα οποία δημιουργήθηκαν κάποια στιγμή στο παρελθόν (η χρονική αυτή στιγμή συνήθως δε δηλώνεται). Μέθοδοι που χρησιμοποιούνται:
  1) Κώδικες αυθεντικοποίησης μηνύματος (MAC): Χρησιμοποιούν συμμετρικές μεθόδους.
  2) Ψηφιακές υπογραφές
- **Αυθεντικοποίηση οντότητας**

  Δύο κατηγορίες:
  1. Μονόδρομη αυθεντικοποίηση (unilateral authentication): Μόνο η μια οντότητα αυθεντικοποιεί την άλλη.
  2. Αμφίδρομη αυθεντικοποίηση (mutual authentication): Αυθεντικοποίηση και των δύο οντοτήτων.

Η αυθεντικοποίηση οντότητας γίνεται σύμφωνα με

1. κάτι που **ξέρει**
   - Password (η ασφάλεια μπορεί να αυξηθεί εάν χρησιμοποιούμε κάποια μέθοδο πρόκλησης-απόκρισης)
   - PIN
   - Ένα μυστικό ή ιδιωτικό κλειδί γνώση του οποίου αποδεικνύεται σε ένα πρωτόκολλο πρόκλησης-απάντησης (challenge-response).
2. κάτι που **έχει**
   - Security token (password generator)
   - Smart card, magnetic stripe card
   - Για να κάνουμε την αυθεντικοποίηση πιο ασφαλή συνήθως τις χρησιμοποιούμε σε συνδυασμό με κάποια μέθοδο τύπου “κάτι που ξέρει”
3. κάτι που **είναι**
   - Βιομετρικές μέθοδοι

§ Αυθεντικοποίηση μηνύματος

Γίνεται κυρίως με τρεις μεθόδους:

- Κώδικας αυθεντικοποίησης μηνύματος (MAC): Βασίζονται στη χρήση συμμετρικών κλειδιών και έτσι δεν επιτρέπουν το διαχωρισμό μεταξύ των οντοτήτων που μοιράζονται το κλειδί. Επομένως, και σε αντίθεση με τις ψηφιακές υπογραφές δε παρέχουν μη αποποίηση της προέλευσης του μηνύματος. Εάν η επίλυση διαφορών αποτελεί απαίτηση, τότε αντί αυτού συνιστάται η χρήση είτε μιας έμπιστης τρίτης οντότητας, είτε η χρήση ασύμμετρων μεθόδων.
- Ψηφιακές υπογραφές
- Επισύναψη (πριν την κρυπτογράφηση) στα κρυπτογραφημένα δεδομένα μιας μυστικής τιμής.

Η αυθεντικοποίηση εξετάζεται εδώ ως μία από τις κρυπτογραφικές λειτουργίες και συνεπώς εννοείται ότι η οντότητα που αυθεντικοποιείται κατέχει ήδη ένα ψηφιακό πιστοποιητικό. Οι μηχανισμοί αυθεντικοποίησης που βασίζονται σε ψηφιακά πιστοποιητικά έχουν τρία σημαντικά πλεονεκτήματα σε σχέση με τις συμβατικές μεθόδους που βασίζονται σε κωδικούς (passwords):

1. Η αυθεντικοποίηση με πιστοποιητικά είναι ισχυρότερη και συνεπώς ασφαλέστερη, αφού βασίζεται σε μεγάλα ασφαλώς αποθηκευμένα κλειδιά που δεν απαιτείται να απομνημονευθούν.
2. Η χρήση των πιστοποιητικών παρέχει παράλληλα αδιάψευστες πληροφορίες για την ταυτότητα της οντότητας, πολύ περισσότερες από ένα απλό όνομα χρήστη. Οι πληροφορίες αυτές μπορούν να αξιοποιηθούν κατάλληλα στη συνέχεια στον έλεγχο προσπέλασης σε πόρους και στη γενικότερη ασφαλή διαχείριση του συστήματος.
3. Δεν απαιτείται η ύπαρξη κεντρικού εξυπηρετητή αυθεντικοποίησης ούτε κεντρική διαχείριση λογαριασμών και κωδικών. Μία οντότητα

μπορεί να αυθεντικοποιηθεί από οποιαδήποτε άλλη οντότητα με την οποία συναλλάσσεται, ενώ η απόφαση για την είσοδο σε ένα σύστημα βασίζεται στην πολιτική του συστήματος σε σχέση με το ποια πιστοποιητικά χαρακτηρίζονται ως αποδεκτά.

Η γενική αρχή του μηχανισμού αυθεντικοποίησης που βασίζεται σε πιστοποιητικά είναι απλή. Μεταξύ δύο συναλλασσομένων οντοτήτων, κάθε μία αυθεντικοποιείται από την απέναντί της, αποδεικνύοντας ότι είναι κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο πιστοποιητικό που παρουσιάζει ως δικό της.

Τα βήματα συνοψίζονται ως εξής:

1. Οι δύο οντότητες ανταλλάσσουν ένα μικρό κείμενο το οποίο κρυπτογραφούν, η κάθε μία με το ιδιωτικό της κλειδί.
2. Η οντότητα που αυθεντικοποιείται παρουσιάζει στην απέναντι το πιστοποιητικό της μαζί με το κρυπτογραφημένο κείμενο που προέρχεται από το γνωστό, προσυμφωνημένο αρχικό κείμενο.
3. Η απέναντι οντότητα αποκρυπτογραφεί το κείμενο με το δημόσιο κλειδί της οντότητας που το κρυπτογράφησε, λαμβάνοντας το κλειδί από το πιστοποιητικό της.
4. Επιβεβαιώνει ότι το αποτέλεσμα της αποκρυπτογράφησης συμφωνεί με το γνωστό αρχικό κείμενο και άρα
5. Συμπεραίνει ότι ο αποστολέας είναι πράγματι ο κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο πιστοποιητικό που παρουσιάστηκε.
6. Επαναλαμβάνονται τα βήματα 2-6 και για να αυθεντικοποιηθεί και η δεύτερη οντότητα.

3.2 ΤΕΧΝΟΛΟΓΙΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Η κρυπτογράφηση σαν μέθοδος εξασφάλισης του απορρήτου των πληροφοριών είναι γνωστή από την αρχαιότητα. Με τη χρήση κωδικών συμβόλων αντί για τα γνωστά σύμβολα της αλφαβήτου, οι προκάτοχοι μας εξασφάλιζαν - ή τουλάχιστον έτσι νόμιζαν - το απόρρητο αυτό. Στην πραγματικότητα όμως, το σπάσιμο του κώδικα αυτού δεν είναι και τόσο δύσκολο. Μελετώντας τη συχνότητα εμφάνισης κάποιων χαρακτήρων και γνωρίζοντας, έστω και σε βασικό επίπεδο τη γλώσσα στην οποία είναι γραμμένο το μήνυμα, είναι εφικτή η αποκωδικοποίηση του χωρίς ιδιαίτερο κόπο. Σήμερα διαθέτουμε πολύ πιο αποτελεσματικούς αλγόριθμους κρυπτογράφησης, οι οποίοι διακρίνονται σε δυο βασικές κατηγορίες. Την κρυπτογράφηση ιδιωτικού κλειδιού ή συμβατική κρυπτογράφηση και την κρυπτογράφηση δημόσιου-ιδιωτικού κλειδιού που πρότειναν οι κρυπτολόγοι Diffie και Hellman το 1976. Παραλλαγές της δεύτερης με κάποιες προσθαφαιρέσεις χρησιμοποιούνται σήμερα ευρέως στο Internet. Τεχνικά ζητήματα που αφορούν την κρυπτογράφηση και τον τρόπο με τον οποίο αυτή γίνεται σήμερα θα παρουσιαστούν λεπτομερώς στη συνεχεία.

Η κρυπτογράφηση αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet καθώς η μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου έχει γίνει κοινός τόπος σήμερα και θα πρέπει να βρεθούν μηχανισμοί προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των χρηστών του Internet. Με τον όρο *Κρυπτογραφία* εννοούμε τη μετατροπή ενός αρχικού κειμένου σε μορφή που δεν είναι κατανοητή από κάποιον τρίτο και που αποκαλείται κρυπτογραφημένο κείμενο. Η μετατροπή αυτή γίνεται από τον αποστολέα με τη χρήση κάποιας μαθηματικής συνάρτησης.

Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Δηλαδή, είναι μια επιστήμη που στηρίζεται στα μαθηματικά για την κωδικοποίηση (encoding) και αποκωδικοποίηση (decoding) των δεδομένων που διακινούνται μέσω του Διαδικτύου. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά.

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, την χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν.

Στις μέρες μας κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός από την διασφάλιση του απόρρητου ***(privacy)***, η πιστοποίηση ταυτότητας ***(authe***ntication) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητα μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας.

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Με τη σωστή χρήση των μεθόδων κρυπτογράφησης, τα ευαίσθητα προσωπικά δεδομένα των χρηστών είναι προσβάσιμα μόνο απ’ όσους διαθέτουν την κατάλληλη εξουσιοδότηση. Με τις τεχνολογίες της κρυπτογράφησης μπορούμε να εξασφαλίσουμε ότι ένα μήνυμα θα μπορεί να διαβασθεί μόνο από τον παραλήπτη του μηνύματος καθώς στα ενδιάμεσα στάδια απ’ όπου περνάει το

μήνυμα, αυτό εμφανίζεται με ακατάληπτους χαρακτήρες και είναι μη αναγνωρίσιμο.

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασιζόταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές αλλά στηριζόταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί, ότι, εάν μας είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει, από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο με βάση τον Kahn. Επίσης ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφεύραν τη «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία, χρησιμοποίησαν για την κρυπτογράφηση, τη μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» Σχήμα (3.1), ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο

ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Σχήμα 3.1 Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα, χρησιμοποιήθηκαν κυρίως συστήματα τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας, χρησιμοποίησε και άλλα πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε,

αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες. Στην διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που ανακάλυψαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, ανακαλύφθηκε από αυτούς γύρω στον 14ο αιώνα. Η κρυπτογραφία λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός *Giovanni Batista Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολύαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

Ο *C.Wheatstone*, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση, ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και

έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά , χρονολογούνται στο 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός ιερέας Α. Κίρχερ, εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipous Aegyptiakus*». Με βάση αυτό, προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλευθούν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο, τρεις φορές. Μια στα ιερογλυφικά, μια στα ελληνικά και μια στα ιερατικά. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές, μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής

- 3000 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850 1450 π.Χ.: Γραμμική γραφή Α
- 1450 1200 π.Χ.: Γραμμική Γραφή Β

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή, δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την

γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο Μαλίων της Κρήτης. Εμφανίζεται στο Δίσκο της Φαιστού Σχήμα (3.2), που ανακαλύφθηκε το 1908, στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα, έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα, δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Σχήμα 3.2 Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή, ανακαλύφθηκαν από τον Sir Arthur Evans, το μεγάλο Άγγλο αρχαιολόγο, που ανάσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος, ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής

χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β, βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα. Σήμερα, αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής, ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν, μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά, φυλάσσονταν σε

αρχειοφυλακεία και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε, ότι επρόκειτο για κάποιο είδος ελληνικής γραφής αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά, από τους ειδικούς. Στην συνέχεια όμως, αρκετοί προσχώρησαν στην άποψη του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Κρυπτομηχανή Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων, έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματα τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β, απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα, ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η

κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma Σχήμα(3.3).

Σχήμα 3.3 : Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως από την Γερμανία

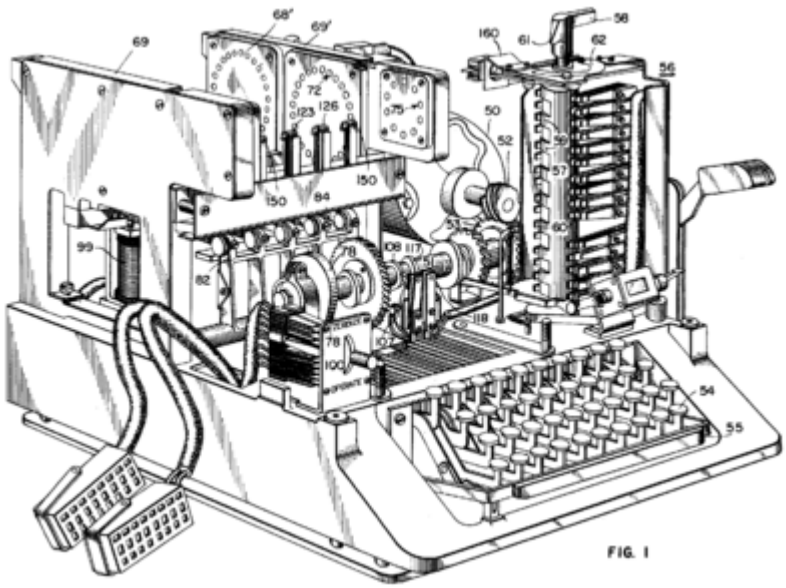
Ο Marian Rejewski, στην Πολωνία, επιτέθηκε και παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (μια ηλεκτρομηχανική κρυπτογραφική μηχανή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της χιλιετίας. Οι Πολωνοί συνέχισαν να παραβιάζουν τα μηνύματα που βασιζόταν στην κρυπτογράφηση με τον Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε κάποιες αλλαγές και οι Πολωνοί δεν μπόρεσαν να ακολουθήσουν γιατί η παραβίαση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, από τον Biuro Szyfrow, κατέληξαν με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η εργασία αυτή, συνεχίστηκε από τον Alan Turing, τον Gordon Welchman, και από πολλούς άλλους στο Bletchley Park και οδήγησε σε συνεχείς παραβιάσεις των διαφόρων παραλλαγών του Enigma. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτό-συστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην μάχη του Midway.

Το Ιαπωνικό υπουργείο εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε επίσης διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκαλέστηκε ως "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική μηχανή αποκαλούμενη Purple από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο δεύτερος παγκόσμιος πόλεμος. Οι Αμερικανοί

αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτό-μηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Σχήμα 3.4) και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, εν τούτοις με σημαντικές βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτό-μηχανών M-94. Οι Βρετανοί πράκτορες SOE χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά).

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτό-μηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του πήρε ακριβώς μερικές ώρες για να την σπάσει και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Αίνιγμα, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.



Σχήμα 3.4 : Κρυπτό-μηχανή SIGABA

Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (*Communication Theory of Secrecy Systems*) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (*Mathematical Theory of Communication*), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard)στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας

πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

3.2.1ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ (SYMMETRIC CRYPTOGRAPHY OR SECRET- KEY CRYPTOGRAPHY).

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, πιο συγκεκριμένα ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Έτσι κατά συνέπεια, το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού, για αυτό το λόγο απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται, αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

3.2.1.1 ΑΛΓΟΡΙΘΜΟΙ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

• **DES (Data Encryption Standard).**

DES είναι το ακρωνύμιο των λέξεων Data Encryption Standard. Αντιπροσωπεύει την

τυποποίηση Federal Information Processing Standard (FIPS) 46-1 που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

• **Triple-DES.**

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

• **DES-EEE3 (Encrypt-Encrypt-Encrypt):** πραγματοποιούνται τρεις συνεχόμενες

κρυπτογραφήσεις με τρία διαφορετικά κλειδιά.

• **DES-EDE3 (Encrypt-Decrypt-Encrypt):** το μήνυμα διαδοχικά κρυπτογραφείται,

αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.

• **DES-EEE2:** είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο

διαφορετικά κλειδιά.

• **DES-EDE2:** είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά. Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

• **DESX.**

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

• **AES (Advanced Encryption Standard).**

Το ακρωνύμιο AES προέρχεται από την φράση Advanced Encryption Standard. Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES. Ο DES βρίσκεται ήδη πολλά χρόνια σε χρήση και από το 1998 το NIST δεν τον ανανεώνει.

• **DSS (Digital Signature Algorithm).**

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το Digital

Signature Algorithm (DSS), που είναι μέρος του Capstone Project της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α. Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι

πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα. Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές. Τα κυριότερα θέματα κριτικής είναι η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν είχε αποκαλυφθεί.

• **RC2, RC4, RC5**

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES. Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται
εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL. Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο

αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

• **IDEA (International Data Encryption Algorithm)**

Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο hardware σε όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

• **Blowfish**

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

3.2.2 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ (PUBLIC-KEY CRYPTOGRAPHY)

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το

ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

• Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

• Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού. Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά. Κάθε χρήστης, λοιπόν έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική και δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και η επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να

αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα. Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ότι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής. Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνος που γνωρίζει την ιδιωτική κλείδα. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

3.2.2.1 ΑΛΓΟΡΙΘΜΟΙ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

• **RSA**

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA. Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς p, q και υπολογίζουμε το γινόμενο τους n = pq. Το n καλείται modulus. Διαλέγουμε ένα αριθμό e μικρότερο του n και τέτοιο, ώστε e και (p-1)(q-1) να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό d, ώστε (ed-1) να διαιρείται από το (p-1)(q-1). Τα ζευγάρια (n,e) και (n,d) καλούνται δημόσια κλείδα και ιδιωτική κλείδα, αντίστοιχα. Είναι δύσκολο να βρεθεί η ιδιωτική κλείδα d από την δημόσια κλείδα e. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού n, δηλαδή των αριθμών p και q. Ο n είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το RSA. Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς την κοινή χρήση ιδιωτικών κλείδων. Ο καθένας χρησιμοποιεί μόνο την δικιά του ιδιωτική κλείδα ή την δημόσια κλείδα οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος της σωστής ιδιωτικής κλείδας μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

Κρυπτογράφηση με το RSA

Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο μήνυμα στον χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: c = me mod n, όπου (n,e) είναι η δημόσια κλείδα του Β. Ο Β, όταν παραλάβει το

μήνυμα θα εφαρμόσει την εξής εξίσωση: m = cd mod n, όπου (n,d) η ιδιωτική κλείδα του Β. Η μαθηματική σχέση που το e και το d εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το d, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

3.2.3 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΣΥΜΜΕΤΡΙΚΗΣ ΚΑΙ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν

επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, οι διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή στους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη. Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους.

3.2.4 ΑΠΛΕΣ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

3.2.4.1 <u>ΔΙΑΦΥΛΑΞΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ</u>

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου (privacy) μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες

κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή την ιδιωτική κλείδα που αντιστοιχεί στην δημόσια κλείδα που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση. Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί να είναι αδύνατη. Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι hash values των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν ακόμα να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

3.3 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα. 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. να χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

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.

3.3.1 Η ΑΝΑΓΚΗ ΓΙΑ ΗΛΕΚΤΡΟΝΙΚΗ ΚΑΙ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Είναι γεγονός ότι η ηλεκτρονική επικοινωνία αποτελεί ένα αχανές κομμάτι της σύγχρονης τεχνολογίας που συνεχώς εξελίσσεται αλλά και που δημιουργεί ολοένα και περισσότερα, δισεπίλυτα προβλήματα. Αλλά στην ουσία, στην επικοινωνία αυτή όλα είναι απρόσωπα και στην πραγματικότητα αυτοί που επικοινωνούν είναι κάποιοι ηλεκτρονικοί υπολογιστές. Έχει χαθεί η φυσική και ενυπόγραφη σχέση που είχαμε συνηθίσει να εμπιστευόμαστε.

Δεν είμαστε σε θέση να γνωρίζουμε ποιος βρίσκεται μπροστά σ’ ένα πληκτρολόγιο, αν είναι όντως αυτός που ισχυρίζεται ότι είναι, αν τα λεγόμενά του είναι αληθινά, αν έχει κακόβουλους στόχους, όπως την προσβολή του υπολογιστή μας με ιό κοκ. Το πρόβλημα αυτό γίνεται ολοένα και πιο σοβαρό καθώς ένα μεγάλο μέρος της καθημερινής οικονομικής μας ζωής περνάει

αναγκαστικά από το σύστημα της ηλεκτρονικής συναλλαγής, είτε πρόκειται για απλές εμπορικές συναλλαγές είτε για θέματα εθνικής άμυνας και ασφάλειας.

Η ψηφιακή υπογραφή αντιπροσωπεύει ένα συγκεκριμένο γνωστό πρόσωπο ή υπηρεσία ή επιχείρηση και είναι μοναδική σε παγκόσμιο επίπεδο, ενώ η χρήση της έχει όλες τις γνωστές συνέπειες της κλασικής υπογραφής. Με τον όρο προηγμένη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή ορίζεται η ηλεκτρονική υπογραφή η οποία παράγεται αποκλειστικά με τις διαδικασίες της υποδομής δημόσιας κλείδας (PKI – Public Key Infrastructure) και η οποία μπορεί και εξασφαλίζει την αυθεντικότητα του υπογράφοντος και την ακεραιότητα και το απόρρητο του μηνύματος.

Η προηγμένη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή θεωρείται υπό προϋποθέσεις ως ισοδύναμη της ιδιόχειρης υπογραφής. Οι Πάροχοι Υπηρεσιών Πιστοποίησης είναι φυσικά ή νομικά πρόσωπα που εκδίδουν αναγνωρισμένα πιστοποιητικά και παρέχουν υπηρεσίες που έχουν σχέση με τις ηλεκτρονικές υπογραφές. Η εποπτεία και ο έλεγχος των Παρόχων Υπηρεσιών Πιστοποίησης που είναι εγκατεστημένοι στην Ελλάδα γίνεται από την Ε.Ε.Τ.Τ. (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων), αλλά δεν απαιτείται η χορήγηση άδειας στους Παρόχους Υπηρεσιών Πιστοποίησης.

Η ηλεκτρονική υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Έχει επιβεβαιωτική λειτουργία, καθώς εξασφαλίζει ότι το μήνυμα που λαμβάνει ο παραλήπτης ανήκει όντως στον αποστολέα και ότι είναι ακέραιο (όχι αλλοιωμένο), αλλά και εμπιστευτική λειτουργία, καθώς μόνο ο παραλήπτης είναι σε θέση να διαβάσει το μήνυμα και κανένας άλλος.

3.3.2 ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

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

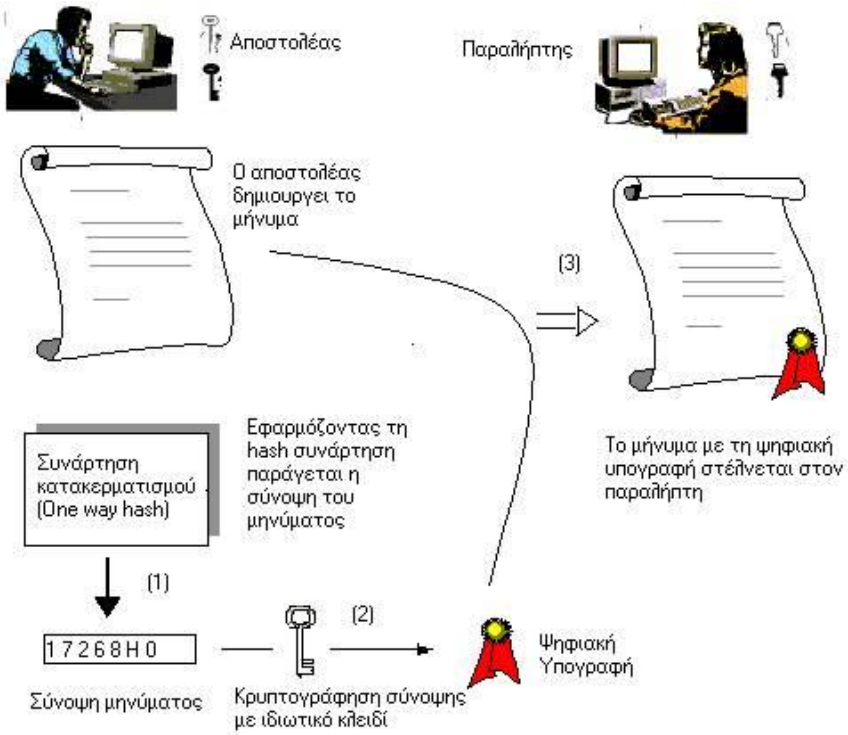
1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).

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).

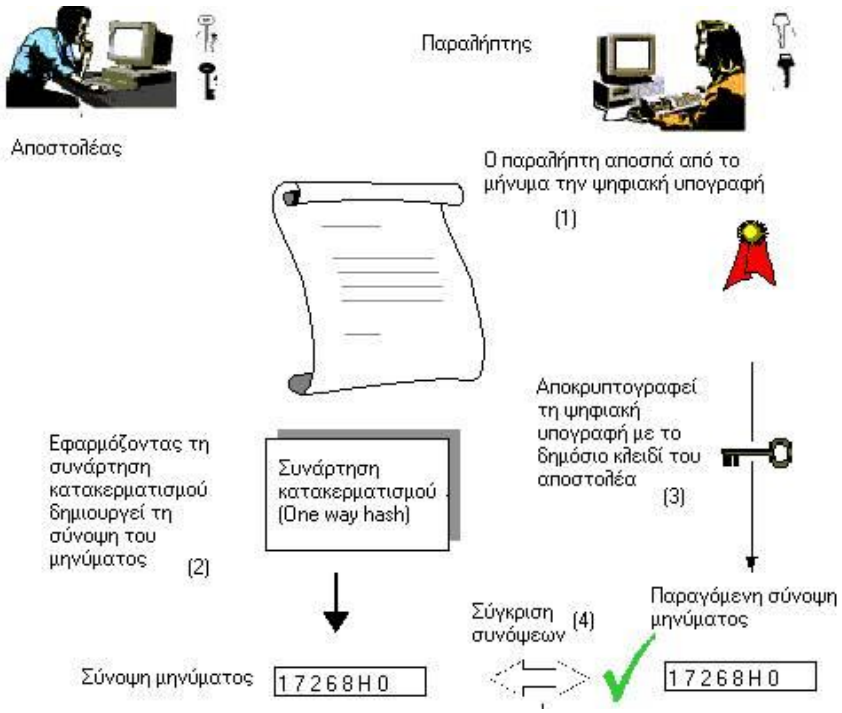
4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.

Δημιουργία ψηφιακής υπογραφής



Οι παραπάνω διεργασίες γίνονται από το ανάλογο λογισμικό στον υπολογιστή του χρήστη.

Επαλήθευση ψηφιακής υπογραφής



3.3.3 ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει πιστοποίηση ταυτότητας (authentication). Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων (integrity) και την ταυτότητα ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία του αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας hash function και της ιδιωτικής κλείδας του αποστολέα.

Ας δούμε πως λειτουργεί μία ψηφιακή υπογραφή. Έστω δύο χρήστες, ο Α και ο Β. Όταν ο Α θέλει να στείλει ένα υπογεγραμμένο έγγραφο στον Β. Το

πρώτο βήμα είναι η παραγωγή του message digest του μηνύματος. Το message digest είναι κατά κανόνα μικρότερο σε μέγεθος από το αρχικό μήνυμα. Στο δεύτερο βήμα, ο Α κρυπτογραφεί το message digest με την ιδιωτική του κλείδα. Τέλος, στέλνει το κρυπτογραφημένο message digest στον Β μαζί με το έγγραφο. Για να μπορέσει ο Β να επαληθεύσει την υπογραφή πρέπει να γνωρίζει την δημόσια κλείδα του Α και τον hash function που χρησιμοποίησε ο Α. Πρώτα θα αποκρυπτογραφήσει το message digest με την δημόσια κλείδα του Α και θα πάρει το message digest που παρήγαγε ο Α. Έπειτα, θα υπολογίσει το message digest του εγγράφου ξανά και θα το συγκρίνει με το παραληφθέν. Εάν τα δύο είναι ταυτόσημα τότε η υπογραφή επαληθεύτηκε επιτυχώς. Εάν δεν ταιριάζουν τότε ή κάποιος προσποιείται ότι είναι ο Α ή το μήνυμα τροποποιήθηκε κατά την μεταφορά του ή προέκυψε λάθος κατά την μετάδοση. Οποιοσδήποτε που γνωρίζει την δημόσια κλείδα του Α, την hash function και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε, μπορεί να επιβεβαιώσει το γεγονός ότι το μήνυμα προέρχεται από τον Α και ότι δεν αλλοιώθηκε μετά την υπογραφή του.

Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις: (α) η hash function πρέπει να είναι όσο το δυνατόν περισσότερο μη αντιστρέψιμη και (β) τα ζεύγη δημόσιας ιδιωτικής κλείδας να είναι συσχετισμένα με τους νόμιμους κατόχους τους. Για την εξασφάλιση της δεύτερης προϋπόθεσης υπάρχουν ψηφιακά έγγραφα που καλούνται πιστοποιητικά (certificates) και συνδέουν ένα άτομο με μία συγκεκριμένη δημόσια κλείδα.

3.3.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΦΑΡΜΟΓΗΣ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

Ας υποθέσουμε ότι δύο οντότητες Α και Β, που μπορεί να είναι ιδιώτες, υπηρεσίες, εταιρείες ή και άλλοι φορείς, επιθυμούν να επικοινωνήσουν με τη χρήση ψηφιακών υπογραφών. Η ψηφιακή υπογραφή της οντότητας Α αποτελείται από το ζεύγος κλειδιών I_A (ιδιωτικό κλειδί) και Δ_A (δημόσιο κλειδί). Αντίστοιχα, η ψηφιακή υπογραφή της οντότητας Β αποτελείται από το ζεύγος κλειδιών I_B (ιδιωτικό κλειδί) και Δ_B (δημόσιο κλειδί). Τα ιδιωτικά κλειδιά I_A και I_B είναι γνωστά μόνο στις οντότητες Α και Β αντίστοιχα, ενώ τα δημόσια κλειδιά τους Δ_A και Δ_B είναι γνωστά σ' όλον τον κόσμο.

Η οντότητα Α πριν στείλει το μήνυμά της, το κρυπτογραφεί κάνοντας χρήση του ιδιωτικού της κλειδιού I_A και έτσι θα μπορεί ο καθένας να χρησιμοποιήσει το αντίστοιχο δημόσιο κλειδί Δ_A για να το αποκρυπτογραφήσει. Η οντότητα Β είναι έτσι σίγουρη ότι το μήνυμα προέρχεται όντως από την οντότητα Α και όχι από κάποιον τρίτο που προσποιείται ότι είναι η οντότητα Α, καθώς το δημόσιο κλειδί Δ_A μπορεί να αποκρυπτογραφήσει μόνο το αντίστοιχο ιδιωτικό κλειδί I_A, το οποίο μόνο η οντότητα Α κατέχει.

Επίσης, η οντότητα Β είναι σίγουρη ότι το μήνυμα δεν έχει αλλοιωθεί καθ' οδόν προς τον προορισμό του από κάποιον τρίτο, καθώς κανείς δεν είναι σε θέση να γνωρίζει το ιδιωτικό κλειδί I_A που χρησιμοποιήθηκε για την κρυπτογράφησή του, αλλά ακόμα και στην περίπτωση που το κείμενο τροποποιηθεί, η οντότητα Β θα διαπιστώσει ότι το δημόσιο κλειδί δεν θα είναι σε θέση να αποκρυπτογραφήσει το μήνυμα και έτσι θα γνωρίζει ότι το μήνυμα είναι παραποιημένο.

Το παραπάνω είναι ένα παράδειγμα ενός ηλεκτρονικού μηνύματος που είναι υπογεγραμμένο με ψηφιακή υπογραφή, πρόκειται δηλαδή για ένα μήνυμα για το οποίο είμαστε σίγουροι για την ταυτότητα του αποστολέα του καθώς και για το ότι το μήνυμα αυτό είναι γνήσιο και όχι παραποιημένο. Στην περίπτωση

τώρα που η οντότητα Α θελήσει να στείλει ένα μήνυμα στην οντότητα Β που να είναι όμως και κρυπτογραφημένο, δηλ. μόνο η οντότητα Β να μπορεί να το διαβάσει και κανένας άλλος, τότε θα πρέπει να κρυπτογραφήσει το μήνυμα και με το δημόσιο κλειδί Δ_B της οντότητας Β.

Έτσι, μόνο η οντότητα Β θα μπορέσει να αποκρυπτογραφήσει το μήνυμα καθώς μόνο αυτή διαθέτει το αντίστοιχο ιδιωτικό κλειδί I_B. Θα πρέπει επιπλέον να εφαρμόσει και το δημόσιο κλειδί Δ_A της οντότητας Α για να μπορέσει να επαναφέρει το αρχικό μήνυμα. Το παραπάνω είναι ένα παράδειγμα ενός ηλεκτρονικού μηνύματος που είναι υπογεγραμμένο και κρυπτογραφημένο με ψηφιακή υπογραφή, πρόκειται δηλαδή για ένα μήνυμα για το οποίο όχι μόνο είμαστε σίγουροι για την ταυτότητα του αποστολέα του και για το ότι το μήνυμα είναι γνήσιο και όχι παραποιημένο αλλά και ότι κανείς άλλος δεν μπορεί να το δει και να το αποκρυπτογραφήσει εκτός από αυτόν για τον οποίο προορίζεται.

Για να μπορέσουν να έχουν εφαρμογή οι παραπάνω διαδικασίες, θα πρέπει να είμαστε σίγουροι ότι η ψηφιακή υπογραφή έχει εκδοθεί νόμιμα στο όνομα κάποιου χρήστη και ότι αυτός ο χρήστης έδωσε τα πραγματικά του στοιχεία όταν ζήτησε να εκδοθεί η ψηφιακή υπογραφή του. Η λύση είναι η ύπαρξη ενός αξιόπιστου οργανισμού, ο οποίος θα αναλάβει να εκδίδει και να πιστοποιεί τις ψηφιακές υπογραφές.

3.4 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Τα πιστοποιητικά είναι ψηφιακά έγγραφα που αποδεικνύουν την σχέση μεταξύ μίας δημόσια κλείδας και μίας οντότητας. Επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι μία συγκεκριμένη δημόσια κλείδα ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικης κλείδας.

Ας υποθέσουμε ότι ο Α χρειάζεται την δημόσια κλείδα του Β για να μπορέσει να εγκαταστήσει μία ασφαλή συναλλαγή. Το να ζητήσει από τον Β να του στείλει την δημόσια κλείδα του μπορεί να θέσει την όλη επικοινωνία σε ρίσκο. Εκτός από την παρακολούθηση της συναλλαγής και αντικατάστασης της δημόσιας κλείδα του Β με την δημόσια κλείδα κάποιου άλλου (επίθεση man-in-the-middle), μπορεί οποιοσδήποτε να ξεγελάσει τον Α, όταν ο Α δεν γνωρίζει και δεν μπορεί να επικοινωνήσει τηλεφωνικός με τον Β, λέγοντας πως είναι ο Β και παρουσιάζοντας μία ψεύτικη δημόσια κλείδα. Δηλαδή, έστω ότι ο Β υποστηρίζει ότι είναι ο πρωθυπουργός της Ελλάδος. Τότε ο Α θα νομίζει ότι συνδιαλέγεται με τον πρωθυπουργό της Ελλάδος και χρησιμοποιεί την δημόσια κλείδα που του παρουσίασε ο Β για να στείλει στον δήθεν πρωθυπουργό εμπιστευτικά έγγραφα.

Ένα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

- το όνομα του κατόχου,
- το όνομα του εκδοτικού οργανισμού CA ,
- την δημόσια κλείδα του ονόματος που αναγράφεται στο πιστοποιητικό,
- την ημερομηνία λήξης του πιστοποιητικού,
- ένα σειριακό αριθμό (serial number),
- την ψηφιακή υπογραφή του εκδοτικού οργανισμού.

Ένα τυπικό παράδειγμα πιστοποιητικού φαίνεται παρακάτω:

Η τυποποιημένη μορφή ενός πιστοποιητικού ακολουθεί το πρωτόκολλο X.509.Το πιστοποιητικό μεταφέρεται, συνήθως, μαζί με την ψηφιακή υπογραφή. Για την επαλήθευση της ψηφιακής υπογραφής ο παραλήπτης πρέπει να έχει την σωστή δημόσια κλείδα του αποστολέα. Επίσης, το πιστοποιητικό στέλνεται κατά την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο άκρων, για την γνωστοποίηση της δημόσιας κλείδας κάθε πλευράς στην άλλη πλευρά και για την χρήση της στην κρυπτογράφηση της επικοινωνίας. Το πιστοποιητικό δεν

χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities)

Τα πιστοποιητικά εκδίδονται από τις Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities CA), που μπορεί να είναι οποιοσδήποτε άξιος εμπιστοσύνης οργανισμός ικανός να εγγυηθεί για την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά. Ένας οργανισμός μπορεί να εκδίδει πιστοποιητικά για τους υπάλληλους του ή ένα Πανεπιστήμιο για τους σπουδαστές του ή ακόμα και μια πόλη για τους κατοίκους της. Η CA πρέπει να κατέχει ένα ζεύγος ιδιωτικής ή δημόσιας κλείδας. Με την ιδιωτική της κλείδα υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει, ενώ την εγκυρότητα της δημόσιας κλείδας πρέπει να επικυρώνει εκδοτικός οργανισμός σε υψηλότερη θέση στην ιεραρχία των CAs.

3.4.1 ΔΙΑΧΕΙΡΙΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ (CERTIFICATE MANAGEMENT)

Η εγκατάσταση μιας Αρχής Πιστοποίησης είναι μια υπευθυνότητα η οποία απαιτεί ένα στιβαρό διαχειριστικό και τεχνικό πλαίσιο. Οι Αρχές Πιστοποίησης δεν εκδίδουν μόνο πιστοποιητικά αλλά τα διαχειρίζονται κιόλας, πράγμα πού με απλά λόγια σημαίνει ότι η Αρχή καθορίζει το χρονικό διάστημα εγκυρότητας κάθε πιστοποιητικού, την ανανέωσή του, τη διατήρηση και την ενημέρωση αρχείων των πιστοποιητικών που έχουν ήδη εκδοθεί καθώς και εκείνων που δεν είναι πλέον έγκυρα, συντηρώντας λίστες ανακληθέντων πιστοποιητικών (certificate revocation lists - CRLs). Για παράδειγμα έστω ότι ο χρήστης Χ δικαιούται ενός πιστοποιητικού ως υπάλληλος στην εταιρεία στην οποία εργάζεται. Έστω τώρα ότι ο ίδιος υπάλληλος σε κάποια χρονική στιγμή εγκαταλείπει την εργασία του. Κατά συνέπεια το πιστοποιητικό του πρέπει να ανακληθεί. Για να ελεγχθεί, λοιπόν, η εγκυρότητα των υφιστάμενων

πιστοποιητικών πρέπει να ελεγχθούν οι λίστες ανακληθέντων πιστοποιητικών, διαδικασία η οποία σε καμιά περίπτωση δεν μπορεί να χαρακτηριστεί αυτοματοποιημένη.

3.5 ΨΗΦΙΑΚΟΙ ΦΑΚΕΛΟΙ (DIGITAL ENVELOPES)

Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί. Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με την δημόσια κλείδα της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

Ας υποθέσουμε ότι ο χρήστης Α θέλει να στείλει μήνυμα στον χρήστη Β. Ο Α διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με την δημόσια κλείδα του Β. Στέλνει στον Β το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο Β θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί την ιδιωτική του κλείδα για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ενός παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με την δημόσια κλείδα του κάθε παραλήπτη. Και πάλι μεταδίδεται μόνο ένα κρυπτογραφημένο μήνυμα.

Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο

πιο συνηθισμένος συνδυασμός είναι το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

3.6 ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Οι μηχανισμοί διαχείρισης κλειδιών (key management*)* και η ανταλλαγή κλειδιών *(*key exchange*),* ασχολούνται με την ασφαλή παραγωγή, διανομή και αποθήκευση των κλειδιών κρυπτογράφησης. Η εύρεση απρόσβλητων μεθόδων διαχείρισης και ανταλλαγή κλειδιών είναι πολύ σημαντική στην διατήρηση της ασφάλειας της επικοινωνίας.

Η έννοια της διαχείρισης κλειδιών αναφέρεται στα ασύμμετρα κρυπτοσυστήματα. Τα χαρακτηριστικά που πρέπει να έχει ένας μηχανισμός διαχείρισης κλειδιών είναι τα ακόλουθα. Οι χρήστες πρέπει να είναι σε θέση να μπορούν να αποκτήσουν με ασφάλεια ένα ζεύγος δημόσιας - ιδιωτικής κλείδας που θα ικανοποιεί τις ανάγκες τους για προστατευμένη επικοινωνία. Πρέπει να υπάρχει τρόπος αποθήκευσης και δημοσιοποίησης των δημόσιων κλειδιών, ενώ παράλληλα θα είναι δυνατή η ανάκτηση τους όποτε χρειάζεται. Επίσης οι δημόσιες κλείδες θα πρέπει να συσχετίζονται με σίγουρο τρόπο με την ταυτότητα του νόμιμου κατόχου. Έτσι, δεν θα μπορεί κάποιος να παρουσιάζεται σαν κάποιος άλλος, επιδεικνύοντας μία ψεύτικη δημόσια κλείδα. Τέλος οι χρήστες πρέπει να έχουν την δυνατότητα να φυλάσσουν τις ιδιωτικές τους κλείδες με ασφάλεια, οι οποίες θα είναι έγκυρες μόνο για συγκεκριμένο χρονικό διάστημα.

Η ανταλλαγή κλειδιών εφαρμόζεται στα συμμετρικά κρυπτοσυστήματα, όπου οι δύο επικοινωνούντες χρήστες πρέπει να αποφασίσουν για το κοινό μυστικό κλειδί και έπειτα να αποκτήσουν από ένα αντίγραφο αυτού, χωρίς κανένας άλλος να μάθει για αυτό.

3.6.1 ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΩΝ

Για να δουλέψει η συμβατική κρυπτογράφηση, οι δυο ομάδες σε μια ασφαλή συναλλαγή πρέπει να έχουν το ίδιο κλειδί το οποίο πρέπει να προστατεύεται από τη πρόσβαση από άλλους. Επιπλέον, οι συχνές αλλαγές κλειδιών είναι συνήθως επιθυμητές για να περιοριστούν τα δεδομένα που εκθέτονται, εάν ένας επιτιθέμενος μάθει το κλειδί. Επομένως, η δύναμη οποιουδήποτε κρυπτογραφικού συστήματος βασίζεται στη τεχνική διανομής κλειδιού, ένας όρος που αναφέρεται στα μέσα παράδοσης ενός κλειδιού σε δύο ομάδες που επιθυμούν να ανταλλάσσουν δεδομένα, χωρίς να επιτρέπουν σε άλλους να δουν το κλειδί. Η διανομή του κλειδιού μπορεί να επιτευχθεί με διάφορους τρόπους. Για δύο ομάδες Α και Β :

1. Ένα κλειδί μπορεί να επιλεχθεί από την Α και να παραδοθεί φυσικά στη Β.
2. Μία τρίτη ομάδα θα μπορούσε να επιλέξει το κλειδί και να το παραδώσει φυσικά στις Α και Β.
3. Εάν η Α και η Β έχουν χρησιμοποιήσει προηγουμένως και πρόσφατα ένα κλειδί, μία ομάδα θα μπορούσε να μεταδώσει το νέο κλειδί στην άλλη, κρυπτογραφημένα χρησιμοποιώντας το παλιό κλειδί.
4. Εάν η Α και Β έχουν μια κρυπτογραφημένη σύνδεση με μία τρίτη ομάδα Γ, η Γ θα μπορούσε να παραδώσει ένα κλειδί στις κρυπτογραφημένες ζεύξης των Α και Β.

Οι επιλογές 1 και 2 απαιτούν τη χειροκίνητη παράδοση ενός κλειδιού. Για τη κρυπτογράφηση ζεύξης, αυτή είναι μια λογική απαίτηση επειδή κάθε συσκευή κρυπτογράφησης ζεύξης πρόκειται μόνο να ανταλλάσσει δεδομένα με την αντίστοιχη της στο άλλο άκρο της ζεύξης. Ωστόσο, για την κρυπτογράφηση από άκρο σε άκρο, η χειροκίνητη παράδοση είναι άκομψη. Σε ένα κατανεμημένο σύστημα, οποιοσδήποτε υπολογιστής ή τερματικό μπορεί να

χρειάζεται να συμμετέχει σε συναλλαγές με πολλούς άλλους υπολογιστές και τερματικά κατά καιρούς. Έτσι, κάθε συσκευή χρειάζεται ένα αριθμό από κλειδιά, που παρέχονται δυναμικά. Το πρόβλημα είναι ιδιαίτερα δύσκολο σε ένα κατανεμημένο σύστημα ευρείας περιοχής.

Η επιλογή 3 είναι μια δυνατότητα είτε για την κρυπτογράφηση ζεύξης είτε για την κρυπτογράφηση από άκρο σε άκρο, αλλά εάν ποτέ ένας προσβολέας επιτύχει να κερδίσει πρόσβαση σε ένα κλειδί, τότε αποκαλύπτονται όλα τα επόμενα κλειδιά. Ακόμη και εάν γίνονται συχνές αλλαγές στα κλειδιά κρυπτογράφησης ζεύξης, αυτές πρέπει να γίνονται χειροκίνητα. Για την παροχή κλειδιών για την κρυπτογράφηση από άκρο σε άκρο, είναι προτιμότερη η επιλογή 4.

4. ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο, όχι πολλά χρόνια πριν, αποτελούσε ένα κατά πολύ μικρότερο «μέρος» συγκριτικά με σήμερα. Οι κόμβοι του ήταν διεσπαρμένοι σε μερικά ακαδημαϊκά ιδρύματα, ερευνητικά εργαστήρια και εταιρείες. Οι χρήστες του περιλάμβαναν φοιτητές, ερευνητές και γενικότερα ανθρώπους που ασχολούνταν κατά τον έναν ή τον άλλο τρόπο με την τεχνολογία και τις επιστήμες. Η υποδομή του, το διάσημο ζεύγος πρωτοκόλλων TCP/IP, είχε σχεδιαστεί για να λειτουργεί απλά και αποτελεσματικά, χωρίς να περιλαμβάνει ιδιαίτερους μηχανισμούς ή «δικλίδες».Όμως κατά την πάροδο των χρόνων υπήρχε τεράστια ανάπτυξη του διαδικτύου που οδηγεί καθημερινά στην μετατροπή των δεδομένων του φυσικού κόσμου σε ψηφιακή – ηλεκτρονική μορφή. Σχεδόν οποιαδήποτε υπηρεσία ή οργανισμός, ιδρύματα, εταιρείες και ιδιώτες χρησιμοποιούν υπολογιστές με πρόσβαση στο διαδίκτυο, τις περισσότερες φορές για την διαχείριση των δεδομένων τους. Η αξία της πληροφορίας που συγκεντρώνεται στο διαδίκτυο αποκτά τεράστιες διαστάσεις και γίνεται ένα θέμα που ολοένα και περισσότερο συζητιέται. Σε πολλές περιπτώσεις μάλιστα, ολόκληρη η πληροφορία είναι αποθηκευμένη σε ψηφιακά μέσα, χωρίς να υπάρχει σε έντυπη ή αναλογική μορφή.Η εξάρτηση μας στα συστήματα αυτά,

και το γεγονός ότι η λειτουργικότητα και η φιλικότητα των υπολογιστικών συστημάτων έχουν αυξηθεί σημαντικά, οδηγούν σε μια ενισχυμένη πολυπλοκότητα των συστημάτων αυτών. Η πολυπλοκότητα αυτή οδηγεί σε μια πληθώρα αδυναμιών και προβλημάτων στην ασφάλεια των συστημάτων και των δεδομένων, είτε από προγραμματιστικά λάθη, είτε από κακές ρυθμίσεις, είτε από τις σχέσεις εμπιστοσύνης που δημιουργούνται, είτε από άλλους λόγους. Ο πληθυσμός του Internet αν και έχει ακουστά πολλές περιπτώσεις παραβίασης της ασφάλειας συστημάτων και κλοπής δεδομένων, δεν έχει δεχτεί μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια. Οι περισσότεροι χρήστες βρίσκονται σε σύγχυση όσον αφορά την ασφάλεια των δεδομένων τους, μην γνωρίζοντας τους κινδύνους και τις απειλές που αντιμετωπίζουν, ενώ οι εταιρείες παροχής υπηρεσιών –είτε πρόκειται για e-mail, είτε για υποβολή φορολογικών δηλώσεων και web banking- εθίζουν τους χρήστες σε πρακτικές χαμηλής ασφάλειας και παρέχουν μια αίσθηση ότι ασχολούνται αποτελεσματικά με την ασφάλεια των δεδομένων τους.

Οι χρήστες παραβιασμένων συστημάτων αντιμετωπίζουν πολύ σοβαρούς κινδύνους, χωρίς να το γνωρίζουν τις περισσότερες φορές. Ένας επιτιθέμενος μπορεί να παρακολουθεί ότι πληκτρολογείτε στον υπολογιστή για να μάθει αριθμούς πιστωτικών καρτών και κωδικούς, να χρησιμοποιήσει το σύστημα για τη διακίνηση πορνογραφικού υλικού, να αποσπάσει ευαίσθητα δεδομένα, ακόμα και να πραγματοποιήσει επιθέσεις σε άλλα συστήματα μέσω αυτού, ώστε να σβήσουν τα ίχνη του. Οι επιθέσεις στο διαδίκτυο αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων. Καθημερινά ανακοινώνονται καινούργιες αδυναμίες στο λογισμικό και νέοι τρόποι επίθεσης. Με δεδομένη την εξέλιξη αυτή, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που αυτά περιέχουν και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Όλες αυτές οι απειλές είναι σημαντικοί λόγοι για να αυξηθεί η ασφάλεια στο διαδίκτυο και μεταξύ των χρηστών του. Αυτό περιλαμβάνει τη βελτίωση της ασφάλειας των συστημάτων που συνδέονται με το διαδίκτυο και την ενημέρωση και εκπαίδευση των χρηστών για τις απειλές. Αν και υπάρχει πολλή πληροφορία στο διαδίκτυο για την ασφάλεια δικτύων και συστημάτων, πολλές φορές δεν μπορεί να κατανοηθεί από χρήστες με λίγες γνώσεις. Άλλες φορές η πληροφορία δεν είναι συγκεκριμένη, δεν προχωράει σε μεγάλα επίπεδα λεπτομέρειας και καταλήγει ελλιπής.

4.1 ΤΙ ΕΙΝΑΙ ΔΙΚΤΥΟ

Τα δίκτυα υπολογιστών άρχισαν να καθιερώνονται στα εταιρικά περιβάλλοντα στις αρχές της δεκαετίας του ’80, με την εμφάνιση μικρότερων και οικονομικότερων συστημάτων.

Στα δίκτυα peer-to-peer, κάθε υπολογιστής μπορεί να ζητήσει δεδομένα και πόρους από οποιονδήποτε άλλον υπολογιστή του δικτύου. Αντίστροφα, μπορεί να προσφέρει δικά του δεδομένα και πόρους (π.χ. εκτυπωτικές εργασίες) στους άλλους υπολογιστές του δικτύου. Στα δίκτυα διακομιστή/ πελάτη, υπάρχει ένας τουλάχιστον υπολογιστής που χρησιμοποιείται αποκλειστικά για την εξυπηρέτηση των αιτήσεων των υπόλοιπων υπολογιστών του δικτύου. Αυτός ο υπολογιστής ονομάζεται διακομιστής. Ανάλογα με τη φύση των αιτήσεων που εξυπηρετεί ονομάζεται διακομιστής αρχείων, εκτυπώσεων, εφαρμογών, αλληλογραφίας, φαξ κ,λ.π. Τα τοπικά δίκτυα (LAN) είναι μικρά εταιρικά δίκτυα. Η κάλυψη που προσφέρουν δεν υπερβαίνει τα όρια ενός κτιρίου. Τα μητροπολιτικά δίκτυα (MAN) συνδέουν μικρότερα δίκτυα, καλύπτοντας ολόκληρες πόλεις. Τα δίκτυα ευρείας περιοχής (WAN) δεν υπόκεινται σε γεωγραφικούς περιορισμούς.

Τοπολογία είναι ο τρόπος σύνδεσης των υπολογιστών στο δίκτυο. Στα τοπικά δίκτυα, οι τρεις βασικές τοπολογίες είναι ο δίαυλος, ο αστέρας και ο δακτύλιος. Για να σχηματιστεί ένα δίκτυο απαιτούνται διάφορες συσκευές και εξαρτήματα: κάρτες δικτύου, καλωδίωση, διανομείς, διακόπτες, γέφυρες, πύλες, επαναλήπτες, δρομολογητές, firewalls. Σε ένα δίκτυο, υπεύθυνο για την απρόσκοπτη επικοινωνία των υπολογιστών, είναι το λειτουργικό σύστημα δικτύου. Δημοφιλή λειτουργικά συστήματα είναι το Novell Netware, τα Windows NT/2000/XP και το UNIX.

Πρωτόκολλο επικοινωνίας είναι το σύνολο των κανόνων που ρυθμίζουν την ανταλλαγή δεδομένων στο δίκτυο. Το πρωτόκολλο επικοινωνίας ενσωματώνεται στο λειτουργικό σύστημα δικτύου. Το δημοφιλέστερο σήμερα

πρωτόκολλο επικοινωνίας στους κανόνες του οποίου στηρίζεται το Διαδίκτυο, είναι το TCP/IP. Για την σύνδεση ενός υπολογιστή σε δίκτυο μέσω τηλεφωνικής γραμμής, είναι απαραίτητο το μόντεμ. Το μόντεμ μετατρέπει το ψηφιακό σήμα σε αναλογικό και αντιστρόφως.

Τα δίκτυα έφεραν αλλαγές στους εργασιακούς χώρους, επιταχύνοντας την ανταλλαγή δεδομένων, καθιστώντας εφικτή τη δημιουργία ομάδων εργασίας, την κοινή χρήση και την κεντρική διαχείριση αρχείων και πόρων, ενώ παράλληλα μείωσαν το κόστος μηχανογράφησης των εταιριών. Παράλληλα, έγιναν αιτία εμφάνισης νέων προβλημάτων, όπως η έλλειψη αυτονομίας των χρηστών, η αυξημένη πιθανότητα υποκλοπής των δεδομένων της εταιρίας, η απόλυτη εξάρτηση της επιχειρησιακής ετοιμότητας της εταιρίας από το δίκτυο και η αυξημένη πιθανότητα μόλυνσης των υπολογιστών της εταιρίας από ιούς. Ο όρος δίκτυο δεν αναφέρεται αποκλειστικά σε υπολογιστές. Το τηλεοπτικό, το ραδιοφωνικό και το τηλεφωνικό είναι τρία τυπικά παραδείγματα διαφορετικών τύπων δικτύου. Η αρχιτεκτονική του τηλεφωνικού δικτύου (μικρότερα δίκτυα που συνδέονται σε άλλα εθνικής ή ευρύτερης εμβέλειας και επικοινωνούν «μιλώντας την ίδια γλώσσα») εξασφαλίζει την παγκόσμια εξάπλωση του. Σταθερή και κινητή τηλεφωνία είναι οι δύο τύποι τηλεφωνικής επικοινωνίας. Η δεύτερη δεν απαιτεί τη φυσική σύνδεση (καλωδίωση) των συνομιλητών. Το τηλεφωνικό δίκτυο δεν μεταδίδει μόνο φωνή. Συσκευές όπως το φαξ εκμεταλλεύονται την υποδομή του τηλεφωνικού δικτύου για να μεταδώσουν εικόνες.

4.2 ΤΙ ΕΙΝΑΙ ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο έχει ανοίξει νέους ορίζοντες, τόσο στη γνώση όσο και στην επικοινωνία. Είναι στο χέρι του καθενός να γνωρίσει τις θετικές πλευρές του Διαδικτύου και να προστατευθεί από τις αρνητικές πλευρές του. Η επικοινωνία δεδομένων έχει αναχθεί σε πρωταρχικής σημασίας κομμάτι της πληροφορικής.

Δίκτυα εγκατεστημένα σε όλο το κόσμο, χρησιμοποιούνται για την συλλογή και διανομή δεδομένων πάνω σε ποικίλα θέματα. Από καιρό έχει κατανοηθεί η αναγκαιότητα διασύνδεσης όλων αυτών των επιμέρους δικτύων σε ένα ευρύτερο σύνολο, διευκολύνοντας και επιταχύνοντας την επικοινωνία. Οι προσπάθειες της κατασκευής αυτού του υπέρ – δικτύου ήταν επιτυχημένες και το αποτέλεσμα ήταν αυτό που σήμερα ξέρουμε σαν Internet. Το Internet (ή Διαδίκτυο) παρουσιάζει μεγάλη αποδοχή, πράγμα που οδηγεί στην συνεχή εξέλιξη και αναδιαμόρφωση του.

Ένα από τα μεγαλύτερα προβλήματα που έπρεπε να λυθούν ώστε το Διαδίκτυο να γίνει πραγματικότητα, ήταν η ύπαρξη πολλών τεχνολογιών δικτύων, καθεμιά από τις οποίες εξυπηρετεί μια συγκεκριμένη ομάδα ανθρώπων. Οι χρήστες του δικτύου διαλέγουν την τεχνολογία που είναι κατάλληλη για τις επικοινωνιακές τους ανάγκες. Η χρήση μίας και μόνο τεχνολογίας για την δημιουργία ενός παγκόσμιου δικτύου είναι αδύνατη, γιατί δεν υπάρχει τεχνολογία που να ικανοποιεί όλες τις απαιτήσεις. Για παράδειγμα, μερικοί χρήστες χρειάζονται δίκτυα υψηλών ταχυτήτων που καλύπτουν μικρές αποστάσεις. Για άλλους πάλι, πιο εξαπλωμένα δίκτυα, χαμηλών ταχυτήτων είναι πιο χρήσιμα.

Το Διαδίκτυο, παρ' όλα αυτά, καταφέρνει να συνενώσει όλες αυτές τις διαφορετικές τεχνολογίες, παρέχοντας ένα σύνολο συμβάσεων. Κρύβει τις λεπτομέρειες της υποκείμενης δικτυακής τεχνολογίας και επιτρέπει σε υπολογιστές από όλο τον κόσμο να βρίσκονται σε επαφή ανεξάρτητα από το δίκτυο στο οποίο συνδέονται.

4.3 ΤΙ ΕΙΝΑΙ ΠΑΓΚΟΣΜΙΟΣ ΙΣΤΟΣ

Όλοι μας σήμερα φαίνεται να χρησιμοποιούμε τους όρους Internet και Παγκόσμιος Ιστός εναλλακτικά. Αλλά όπως ήδη γνωρίζουμε, δεν είναι το ίδιο πράγμα. Το Internet είναι τεράστια διασυνδεδεμένη συλλογή διακομιστών και

δικτύων από όλο τον κόσμο, που είναι συνδεδεμένα με σπονδυλικές στήλες. Ο Ιστός είναι απλώς ένα τμήμα του Internet αν και πολλοί, αν όχι οι περισσότεροι, τελικοί χρήστες τον θεωρούν «το Internet».

Έτσι λοιπόν, τι είναι αυτό που κάνει τον Ιστό αυτό που είναι, και πως βρίσκουν το δρόμο τους εκεί οι άνθρωποι; Αν έχετε χρησιμοποιήσει τον Ιστό, φυσικά ξέρετε ήδη την απάντηση.

Αν και οι άνθρωποι θεωρούν την εξερεύνηση του Ιστού εξερεύνηση ενός γεωγραφικού χώρου με σαφώς ορισμένα σύνορα, δεν είναι έτσι. Δεν είναι καν ένα μέρος, είναι μια συλλογή εγγράφων. Τα έγγραφα αυτά είναι γνωστά ως σελίδες (pages) και οι σελίδες αυτές κατά ομάδες αποτελούν τα εκατομμύρια των τοποθεσιών (sites) που μπορεί να επισκεφθεί όποτε θέλει κάποιος ο οποίος διαθέτει πρόσβαση στο Internet.

Οι σελίδες και οι τοποθεσίες αυτές σε συνδυασμό παρουσιάζουν πληροφορίες σε έγχρωμη μορφή και που δεν περιλαμβάνουν μόνο κείμενο αλλά και γραφικά, ήχο, κίνηση, βίντεο και τους συνδέσμους (links), που με το απλό πάτημα ενός ποντικού οδηγούν έναν επισκέπτη από σελίδα σε σελίδα και από τοποθεσία σε τοποθεσία. Χάρη στις πρόσφατες εξελίξεις τις τεχνολογίας του Ιστού, οι σελίδες μπορούν να περιλαμβάνουν ακόμη και μικρά προγράμματα-σενάρια (scripts), μικροεφαρμογές (applets), και χειριστήρια Active X (Active X controls) – τα οποία προσθέτουν αλληλεπιδραστικές δυνατότητες που επιτρέπουν στο χρήστη να κάνει πράγματα πέρα από την απλή ανάγνωση της σελίδας.

4.4 ΠΡΩΤΟΚΟΛΛΑ

Τα πρωτόκολλα δικτύου είναι "γλώσσες" ειδικού σκοπού τις οποίες χρησιμοποιούν οι υπολογιστές για να επικοινωνούν μεταξύ τους. Διαφορετικά πρωτόκολλα κάνουν διαφορετικά πράγματα. Μερικά πρωτόκολλα συντονίζουν την κίνηση των μηνυμάτων, αλλά ελέγχουν την ακεραιότητα αυτών που

διαβιβάστηκαν, και άλλα μετατρέπουν τα δεδομένα από μια μορφή σε κάποια άλλη.

Η χρήση των πρωτοκόλλων δεν είναι βέβαια μοναδικό φαινόμενο στα δίκτυα υπολογιστών. Για παράδειγμα η αναγραφή των στοιχείων του αποστολέα και του παραλήπτη σε κάποιο φάκελο που πρόκειται να ταχυδρομηθεί είναι ένα είδος πρωτοκόλλου. Η διεύθυνση του παραλήπτη και η διεύθυνση του αποστολέα στο φάκελο είναι μηνύματα προς το ταχυδρομικό γραφείο, που περιγράφουν που θα πάει το γράμμα, σε διάφορες περιπτώσεις. Τα μηνύματα αυτά πρέπει να εμφανίζονται στις προβλεπόμενες θέσεις του φακέλου, και πρέπει να έχουν μια μορφή που να την καταλαβαίνει η ταχυδρομική υπηρεσία, αν θέλουμε να παραδοθεί σωστά ο φάκελος.

Το TCP/IP – Μια Οικογένεια από Πρωτόκολλα

Το TCP/IP αποτελεί μια μεγάλη συλλογή από πολλά διαφορετικά πρωτόκολλα επικοινωνίας, τα οποία βασίζονται στα δύο σημαντικότερα και αρχικά πρωτόκολλα, το TCP και το IP.

TCP – Transmission Control Protocol

Το πρωτόκολλο TCP χρησιμοποιείται για τη μετάδοση των δεδομένων από μια εφαρμογή (application) στο δίκτυο. Το TCP είναι υπεύθυνο για τη διάσπαση των δεδομένων σε μικρότερα IP πακέτα (packets) πριν αυτά αποσταλούν καθώς και για την αντίστοιχη συναρμολόγηση των πακέτων όταν αυτά φθάσουν στον προορισμό τους.

IP – Internet Protocol

Το πρωτόκολλο IP φροντίζει για την επικοινωνία με τους άλλους υπολογιστές και είναι υπεύθυνο για την αποστολή και τη λήψη (δρομολόγηση) των πακέτων δεδομένων μέσω του Internet.

HTTP – Hyper Text Transfer Protocol

Το πρωτόκολλο HTTP φροντίζει για την επικοινωνία ανάμεσα σ' έναν Web server και έναν Web browser (φυλλομετρητή). Χρησιμοποιείται για την αποστολή των αιτήσεων (requests) από έναν Web client (browser) σ' έναν Web server καθώς και για την επιστροφή του περιεχομένου (Web content), δηλ. των ιστοσελίδων (Web pages), από τον server πίσω στον χρήστη (client).

HTTPS – Secure HTTP

Το πρωτόκολλο HTTPS φροντίζει για την ασφαλή επικοινωνία ανάμεσα σ' έναν Web server και έναν Web browser. Χειρίζεται τυπικά τις συναλλαγές που γίνονται με πιστωτικές κάρτες (credit card transactions) καθώς και μ' άλλα ευαίσθητα δεδομένα.

SSL – Secure Sockets Layer

Το πρωτόκολλο SSL χρησιμοποιείται για την κωδικοποίηση (κρυπτογράφηση – encryption) των δεδομένων για να είναι έτσι ασφαλής η μεταφορά τους.

SMTP – Simple Mail Transfer Protocol

Το πρωτόκολλο SMTP χρησιμοποιείται για την αποστολή των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) από τον χρήστη σ' έναν e-mail server.

IMAP – Internet Message Access Protocol

Το πρωτόκολλο IMAP χρησιμοποιείται για την αποθήκευση (storing) και την ανάκτηση (retrieving) των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails).

POP – Post Office Protocol

Το πρωτόκολλο POP χρησιμοποιείται για το κατέβασμα (downloading) των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) από έναν e-mail server στον προσωπικό υπολογιστή (personal computer) του χρήστη.

FTP – File Transfer Protocol

Το πρωτόκολλο FTP φροντίζει για την αποστολή των αρχείων (ανέβασμα – upload και κατέβασμα – download) ανάμεσα σε υπολογιστές και κυρίως ανάμεσα σ' έναν FTP server και έναν απλό προσωπικό υπολογιστή.

NTP – Network Time Protocol

Το πρωτόκολλο NTP χρησιμοποιείται για τον συγχρονισμό της ώρας (του ρολογιού) ανάμεσα στους υπολογιστές.

DHCP – Dynamic Host Configuration Protocol

Το πρωτόκολλο DHCP χρησιμοποιείται για την κατανομή των δυναμικών IP διευθύνσεων στους υπολογιστές ενός δικτύου (network).

SNMP – Simple Network Management Protocol

Το πρωτόκολλο SNMP χρησιμοποιείται για τη διοίκηση (administration) των δικτύων υπολογιστών (computer networks).

LDAP – Lightweight Directory Access Protocol

Το πρωτόκολλο LDAP χρησιμοποιείται για τη συλλογή πληροφοριών σχετικά με χρήστες (users) και διευθύνσεις e-mail από το Internet.

ICMP – Internet Control Message Protocol

Το πρωτόκολλο ICMP φροντίζει για την αντιμετώπιση των λαθών (error handling) στο δίκτυο (network).

ARP – Address Resolution Protocol

Το πρωτόκολλο ARP χρησιμοποιείται από το IP για να βρεθεί η διεύθυνση υλικού (hardware address) μιας κάρτας δικτύου υπολογιστή που βασίζεται στην IP διεύθυνση.

RARP – Reverse Address Resolution Protocol

Το πρωτόκολλο RARP χρησιμοποιείται από το IP για να βρεθεί η IP διεύθυνση που βασίζεται στη διεύθυνση υλικού (hardware address) μιας κάρτας δικτύου υπολογιστή.

BOOTP – Boot Protocol

Το πρωτόκολλο BOOTP χρησιμοποιείται για το ξεκίνημα των υπολογιστών από το δίκτυο (network).

PPTP – Point to Point Tunneling Protocol

Το πρωτόκολλο PPTP χρησιμοποιείται για την εγκαθίδρυση μιας σύνδεσης (tunnel) ανάμεσα σε ιδιωτικά δίκτυα (private networks).

TCP/IP Email

Το email αποτελεί έναν από τους σημαντικότερους χρήστες του TCP/IP. Όταν γράφουμε ένα email, δεν χρησιμοποιούμε το TCP/IP, αλλά ένα πρόγραμμα email όπως είναι το Lotus Notes ή το Outlook ή το Outlook Express της Microsoft ή το Netscape Messenger ή το Netscape Communicator ή το ThunderBird της Mozilla ή και το Eudora. Ένα email πρόγραμμα χρησιμοποιεί τα εξής διαφορετικά πρωτόκολλα του TCP/IP :

- Στέλνει τα μηνύματά μας (emails) με το πρωτόκολλο SMTP.

- Κατεβάζει (download) τα μηνύματά μας (emails) από έναν email server με το πρωτόκολλο POP.
- Μπορεί να συνδεθεί σ' έναν email server με το πρωτόκολλο IMAP.

SMTP – Simple Mail Transfer Protocol

Το πρωτόκολλο SMTP χρησιμοποιείται για την αποστολή των e-mails. Στην ουσία φροντίζει για την αποστολή των μηνυμάτων μας σ' έναν άλλον υπολογιστή. Κανονικά το email μας στέλνεται σ' έναν email server (SMTP server) και από εκεί σ' έναν άλλον server ή και σ' άλλους servers, μέχρι να φθάσει στον τελικό του προορισμό. Το SMTP μπορεί μόνο να στείλει απλό κείμενο. Δεν μπορεί να μεταδώσει εικόνα (picture) ή ήχο (sound) ή κινούμενη εικόνα (movie).

4.5 ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών. Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοση του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι σημαντικό να διαχειριζόμαστε τη

διεύθυνση της ηλεκτρονικής μας αλληλογραφίας με την ίδια προσοχή που διαχειριζόμαστε τον αριθμό του τηλεφώνου μας.

Μερικά από τα σημαντικότερα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

α**)** Οι Ιοί

β**)** Η Ενοχλητική Αλληλογραφία (Spam mail)

γ**)** Τα μηνύματα απατηλού περιεχομένου (hoaxes mail).

Ιοί

Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι και ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο. Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του e-mail. Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (στο outlook express επιλέξτε Προβολή->Διάταξη->απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»). Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Ενοχλητική αλληλογραφία (spam mail)

Το λεγόμενο spam ή junk mail είναι μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς

επίσης και διάφοροι άλλοι τύποι e-mail (π.χ. ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων. Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.
Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος. Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

Μηνύματα απατηλού περιεχομένου (hoaxes)

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:
1. Προειδοποιητικά: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή του συστήματος.
2. Συμπαράστασης: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται.

3. Εκφοβισμού : οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.

Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος. Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

Μηνύματα οικονομικής εξαπάτησης (phishing)

Το phishing (αγγλικός νεολογισμός βασιζόμενος στη λέξη fishing=ψάρεμα) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπαιρεώσουν μία συναλλαγή. Η πλειοψηφία των

Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια «μοναδική ευκαιρία» και ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση url μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης όψεως, φαίνεται σωστή όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου. Είτε χρησιμοποιούνται εντολές javascript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστοχώρο, είτε χρησιμοποιούνται τα ίδια τα scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο.

Παρόλο που οι περισσότεροι browsers έχουν ήδη αναπτύξει τεχνολογία anti-phishing προκειμένου να ανιχνεύουν τις σελίδες που ανοίγει ο χρήστης και να τον ειδοποιούν για το αν βρίσκεται σε σελίδα phishing, τα θύματα από τέτοιες επιθέσεις αυξάνονται ανησυχητικά σε όλον τον κόσμο. Ο χρήστης πρέπει να είναι ιδιαίτερα καχύποπτος απέναντι σε τέτοια μηνύματα και να επαληθεύει το περιεχόμενό τους επικοινωνώντας με την εταιρεία η την τράπεζα που το έστειλε, όχι μέσω του μηνύματος, αλλά με τον τρόπο που χρησιμοποιούσε ως τώρα. Γενικά, οι αξιόπιστες εταιρείες και τράπεζες δεν καταφεύγουν σε γενικόλογα μηνύματα προκειμένου να εξυπηρετήσουν τους πελάτες τους, ούτε τους ζητούν να αποκαλύψουν τους κωδικούς τους.

Σήμερα κυκλοφορούν αρκετά προγράμματα anti-phishing, τα οποία είτε ελέγχουν το περιεχόμενο των ιστοσελίδων που διατρέχει ο χρήστης, είτε το περιεχόμενο των e-mail που λαμβάνει, προκειμένου να διαπιστώσουν αν πρόκειται για phishing, ενώ αποκαλύπτουν και το πραγματικό όνομα του ιστοχώρου που επισκέπτεται ο χρήστης. Τέλος, τα γνωστά προγράμματα anti-

spam μπορούν να μειώσουν τον αριθμό των απατηλών μηνυμάτων που λαμβάνει ο χρήστης.

Προστασία προσωπικών δεδομένων

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού e-mail. Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail , οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

Το chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται «δωμάτιο επικοινωνίας» (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Το chat αποτελεί μια κοινωνική δραστηριότητα ιδιαίτερα δημοφιλή ανάμεσα στους νέους, διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο γνωριμίας με ανθρώπους από όλο τον κόσμο. Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό (όπως στην περίπτωση του δημοφιλούς IRC, ή των διαφόρων τύπων messengers). Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο

καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όταν κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους. Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές, επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός ιντερνετ-καφέ, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδοφίλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι και η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς, όσο και από τους εκπαιδευτικούς.

Και μόνο η συμμετοχή σε τέτοιου είδους χώρους αποτελεί από μόνη της μια επικίνδυνη πρακτική. Σε περίπτωση όμως που δε μπορούν οι γονείς να αποτρέψουν ή να ελέγξουν τα παιδιά τους, οφείλουν τουλάχιστον να τους επιστήσουν την προσοχή, γιατί αυτά συχνά ξεγελιούνται και αποκαλύπτουν πολλά προσωπικά τους στοιχεία σε αγνώστους, οι οποίοι καταφέρνουν να κερδίσουν την εμπιστοσύνη τους. Οι συμμετέχοντες σε τέτοιου είδους συνομιλίες δε θα πρέπει με κανέναν τρόπο να αποκαλύπτουν την ταυτότητά τους, ούτε τα προσωπικά τους στοιχεία (διεύθυνση, αριθμό τηλεφώνου, e-mail, όνομα σχολείου, πόλη), να μη δέχονται ποτέ να στείλουν τη φωτογραφία τους σε αγνώστους, ούτε να τους συναντούν σε πραγματικό χώρο. Επίσης, οφείλουν να γνωρίζουν πως σε καμιά περίπτωση δεν είναι ασφαλείς λόγω της ανωνυμίας

τους. Ένας καλός χρήστης του Διαδικτύου είναι σε θέση να εντοπίσει την IP διεύθυνση του υπολογιστή τους, να αποκτήσει πρόσβαση σε προσωπικά τους αρχεία, να μολύνει τον υπολογιστή τους με ιούς ή σκουλήκια, τα οποία συχνότατα κυκλοφορούν σε τέτοιου είδους χώρους. Τα παιδιά θα πρέπει να ενθαρρύνονται να συζητούν με τους γονείς τους για τις συνομιλίες τις οποίες παρακολουθούν μέσα σε chat-rooms, να μιλάνε για τους νέους φίλους τους, όπως θα έκαναν και για τους φίλους που γνωρίζουν στην πραγματική τους ζωή, να αναφέρουν κάθε περίπτωση κατά την οποία έχουν υποστεί παρενόχληση, οποιουδήποτε είδους. Οι γονείς, με τη σειρά τους, θα πρέπει να προτρέπουν τα παιδιά τους να χρησιμοποιούν αυτή τη δυνατότητα του Διαδικτύου για να επικοινωνήσουν με φίλους τους που βρίσκονται μακριά και τους οποίους τα παιδιά ήδη γνωρίζουν, και όχι ως μέσο νέων γνωριμιών.

4.6 ΤΑΧΥΔΡΟΜΕΙΟ ΙΣΤΟΥ

Το ταχυδρομείο Ιστού είναι μια από τις πιο χρήσιμες εφαρμογές Ιστού στο διαδίκτυο, που μας επιτρέπει να έχουμε πρόσβαση, να στέλνουμε, να λαμβάνουμε και να διαχειριζόμαστε το ηλεκτρονικό ταχυδρομείο μας μέσω ενός ξεφυλλιστή Ιστού. Το μεγάλο μέρος του ταχυδρομείου Ιστού είναι ότι μπορούμε να έχουμε πρόσβαση στο ηλεκτρονικό ταχυδρομείο από σχεδόν οποιοδήποτε υπολογιστή σε όλο τον κόσμο, εφ' όσον έχει έναν ξεφυλλιστή σύνδεσης με το Διαδίκτυο και το Ιστό.

Το ταχυδρομείο Ιστού διαφέρει από το ηλεκτρονικό ταχυδρομείο παράδοσης στο οποίο οι περισσότεροι άνθρωποι ιδρύουν έναν πελάτη ηλεκτρονικού ταχυδρομείου σε έναν υπολογιστή, θίγοντας κατά συνέπεια το μόνο θέμα πρόσβασής τους σε έναν συγκεκριμένο υπολογιστή και μόνο μια θέση. Επίσης, έχει γίνει δημοφιλές από πολλές επιχειρήσεις τεχνολογίας συμπεριλαμβανομένων των μηχανών και των πυλών αναζήτησης. Μερικές από τις δημοφιλέστερες υπηρεσίες ταχυδρομείου Ιστού είναι: Yahoo mail, Google mail και Hotmail της Microsoft. Οι επιχειρήσεις αυτές προσφέρουν την

υπηρεσία ταχυδρομείου Ιστού τους δωρεάν. Πολλά άτομα ελέγχουν το ηλεκτρονικό ταχυδρομείο τους σε καθημερινή βάση, με αποτέλεσμα οι επιχειρήσεις να κερδίζουν το περισσότερο εισόδημα τους πουλώντας διαφημίσεις.

4.7 ΙΣΧΥΡΟΙ ΚΩΔΙΚΟΙ- PASSWORD

Οι κωδικοί πρόσβασης είναι τα κλειδιά που χρησιμοποιούμε για να προσπελάσουμε προσωπικά στοιχεία που έχουμε αποθηκεύσει στον υπολογιστή μας και στους διαδικτυακούς μας λογαριασμούς.

Εάν κάποιοι εγκληματίες ή άλλοι κακόβουλοι χρήστες κλέψουν τα στοιχεία αυτά, μπορούν να χρησιμοποιήσουν το όνομά μας για να ανοίξουν νέους λογαριασμούς πιστωτικών καρτών, να υποβάλλουν αίτηση για υποθήκη ή να μας εμπλέξουν σε διαδικτυακές συναλλαγές. Σε πολλές περιπτώσεις δεν θα διαπιστώσουμε ότι υποστήκαμε επίθεση παρά μόνον όταν θα είναι πλέον πολύ αργά. Ευτυχώς, δεν είναι δύσκολο να δημιουργήσουμε ισχυρούς κωδικούς πρόσβασης και να τους διατηρήσουμε ασφαλείς.

Πώς δημιουργείται ένας ισχυρός κωδικός πρόσβασης;

Για εκείνον που επιτίθεται, ένας ισχυρός κωδικός πρόσβασης θα πρέπει να φαίνεται σαν μια τυχαία ακολουθία χαρακτήρων. Για να το επιτύχουμε αυτό, ο κωδικός πρόσβασης θα πρέπει να πληρεί τα παρακάτω κριτήρια:

Να αποτελείται από πολλούς χαρακτήρες. Κάθε χαρακτήρας που προσθέτουμε στον κωδικό πρόσβασης αυξάνει την ασφάλεια που μας παρέχει στο πολλαπλάσιο. Οι κωδικοί πρόσβασής μας θα πρέπει να έχουν μήκος 8 χαρακτήρες ή περισσότερους. Το ιδανικό είναι 14 χαρακτήρες ή περισσότεροι.

Πολλά συστήματα επίσης υποστηρίζουν τη χρήση του διαστήματος στους κωδικούς πρόσβασης, έτσι ώστε να μπορούμε να δημιουργούμε μια φράση που να αποτελείται από πολλές λέξεις (μια "κωδική φράση"). Μια κωδική φράση

είναι συχνά ευκολότερο να τη θυμηθούμε από έναν απλό κωδικό πρόσβασης, ενώ είναι μεγαλύτερη και πιο δύσκολο να τη μαντέψει κανείς.

Συνδυάστε γράμματα, αριθμούς και σύμβολα. Όσο μεγαλύτερη ποικιλία χαρακτήρων έχει ο κωδικός πρόσβασής μας, τόσο δυσκολότερο είναι να τον μαντέψουν. Άλλα σημαντικά στοιχεία είναι τα εξής:

Χρησιμοποιήστε λέξεις και φράσεις που εσείς τις θυμάστε εύκολα αλλά οι άλλοι δύσκολα θα τις μαντέψουν. Ο πιο εύκολος τρόπος να θυμόμαστε τους κωδικούς πρόσβασης και τις κωδικές φράσεις είναι να τα σημειώνουμε. Οι περισσότεροι πιστεύουν ότι είναι κακό να σημειώνει κανείς τους κωδικούς πρόσβασης. Αυτό είναι λάθος, αλλά θα πρέπει να τους προστατεύουμε προκειμένου να είναι ασφαλείς και αποτελεσματικοί.

Γενικά, οι κωδικοί πρόσβασης που γράφονται σε ένα κομμάτι χαρτί είναι δυσκολότερο να αποκαλυφθούν στο Internet από τους κωδικούς που αποθηκεύονται σε λογισμικό διαχείρισης κωδικών πρόσβασης, τοποθεσία Web ή άλλο εργαλείο αποθήκευσης λογισμικού.

Δημιουργία ενός ισχυρού και εύκολου κωδικού πρόσβασης σε 6 βήματα

Χρησιμοποιήστε τα βήματα αυτά για να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης:

1.Σκεφθείτε μια φράση που να μπορείτε να τη θυμηθείτε. Αυτή θα αποτελέσει τη βάση του ισχυρού μας κωδικού ή της κωδικής μας φράσης. Χρησιμοποιούμε κάποια φράση που να μπορούμε να απομνημονεύσουμε.

2.Ελέγξτε αν ο υπολογιστής ή το διαδικτυακό σύστημα υποστηρίζει απευθείας την κωδική φράση. Αν μπορούμε να χρησιμοποιήσουμε κωδική φράση (με διαστήματα μεταξύ των χαρακτήρων) στον υπολογιστή ή στο διαδικτυακό μας σύστημα.

3.Αν ο υπολογιστής ή το διαδικτυακό σύστημα δεν υποστηρίζει κωδικές φράσεις, μετατρέψτε την σε κωδικό πρόσβασης. Παίρνουμε το πρώτο γράμμα

κάθε λέξης της φράσης που σχηματίσαμε και δημιουργούμε μια νέα λέξη, χωρίς νόημα.

4.Προσθέστε περιπλοκότητα συνδυάζοντας κεφαλαία και πεζά γράμματα και αριθμούς. Είναι χρήσιμο να χρησιμοποιούμε εναλλαγές γραμμάτων ή ανορθογραφίες.

5.Τέλος, αντικαταστήστε ορισμένους ειδικούς χαρακτήρες. Μπορούμε να χρησιμοποιούμε σύμβολα που μοιάζουν με γράμματα, να συνδυάζουμε λέξεις και άλλους τρόπους ώστε να κάνομε τον κωδικό πρόσβασης πιο περίπλοκο.

6.Ελέγξτε τον νέο σας κωδικό πρόσβασης με το Password Checker. Το Password Checker είναι μια δυνατότητα αυτής της τοποθεσίας Web που δεν κάνει καταγραφές και μας βοηθά να προσδιορίσουμε πόσο ισχυρός είναι ο κωδικός πρόσβασης που δημιουργούμε, καθώς πληκτρολογούμε.

Στρατηγικές δημιουργίες κωδικών πρόσβασης που πρέπει να αποφεύγουμε

Ορισμένες από τις συνηθισμένες μεθόδους που χρησιμοποιούνται για τη δημιουργία κωδικών πρόσβασης είναι εύκολο να τις μαντέψουν οι εγκληματίες. Για να αποφύγουμε τους ανίσχυρους και εύληπτους κωδικούς πρόσβασης:

•**Αποφύγετε τις ακολουθίες ή τους επαναλαμβανόμενους χαρακτήρες.** Τα "12345678", "222222", "abcdefg" ή τα γράμματα που γειτονεύουν στο πληκτρολόγιο δεν χρησιμεύουν για τη δημιουργία ισχυρών κωδικών.

•**Αποφύγετε την αντικατάσταση αριθμών ή συμβόλων αποκλειστικά στη βάση της ομοιότητας.** Οι εγκληματίες και οι άλλοι κακόβουλοι χρήστες που γνωρίζουν αρκετά για να προσπαθήσουν να σπάσουν τους κωδικούς μας δεν θα ξεγελαστούν από συνηθισμένες αντικαταστάσεις στη βάση της ομοιότητας, π.χ. με το να αντικαταστήσουμε το 'i' με '1' ή το 'a' με το '@', π.χ. "M1cr0$0ft" ή "P@ssw0rd". Αυτές οι αντικαταστάσεις όμως μπορούν να είναι αποτελεσματικές όταν συνδυάζονται με άλλα μέτρα, όπως το μήκος, οι ανορθογραφίες ή η χρήση πεζών-κεφαλαίων, για την αύξηση της ισχύος του κωδικού σας.

•**Αποφύγετε να χρησιμοποιήσετε το όνομα σύνδεσης.** Είναι κακό να χρησιμοποιούμε το όνομα ή το επίθετό μας, τον αριθμό μητρώου μας, την ημερομηνία των γενεθλίων μας ή παρόμοια στοιχεία των αγαπημένων μας. Αυτά θα προσπαθήσουν να χρησιμοποιήσουν πρώτα οι εγκληματίες.

•**Αποφύγετε τις λέξεις του λεξικού, σε οποιαδήποτε γλώσσα.** Οι εγκληματίες χρησιμοποιούν εξελιγμένα εργαλεία που μαντεύουν γρήγορα τους κωδικούς πρόσβασης που βασίζονται σε λέξεις πολλών λεξικών, συμπεριλαμβανομένων λέξεων γραμμένων ανάποδα, συνηθισμένων ανορθογραφιών και αντικαταστάσεων. Σε αυτές περιλαμβάνονται όλων των ειδών οι βρισιές και οι βλασφημίες.

•**Να χρησιμοποιείτε πολλαπλούς κωδικούς παντού.** Αν κάποιος από τους υπολογιστές σας ή τα διαδικτυακά συστήματα που χρησιμοποιούν αυτό τον κωδικό πρόσβασης εκτεθεί, τότε θα πρέπει να θεωρηθεί ότι εκτέθηκαν και όλες οι άλλες πληροφορίες που προστατεύονται από αυτόν τον κωδικό πρόσβασης. Είναι πολύ σημαντικό να χρησιμοποιούνται διαφορετικοί κωδικοί πρόσβασης για διαφορετικά συστήματα.

•**Αποφύγετε τη χρήση διαδικτυακών εργαλείων αποθήκευσης.** Αν οι κακόβουλοι χρήστες βρουν αυτούς τους κωδικούς πρόσβασης αποθηκευμένους διαδικτυακά ή σε δικτυωμένο υπολογιστή, έχουν πρόσβαση σε όλες σας τις πληροφορίες

4.8 ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ-FIREWALLS

Το firewall, που μπορεί να αποδοθεί στα ελληνικά με τον όρο πύρινο τείχος προστασίας ή και ηλεκτρονική πύλη ασφαλείας, είναι ένα πρόγραμμα-τείχος που σε γενικές γραμμές έχει τη δυνατότητα να εμποδίσει τους ιούς (viruses) και τα προγράμματα τύπου spyware να εγκατασταθούν στον

υπολογιστή μας. Αποτελεί μια πολύ καλή λύση προστασίας που μπορεί να χρησιμοποιηθεί τόσο από μεγάλες εταιρείες που διαθέτουν εκτεταμένο δίκτυο υπολογιστών όσο και από απλούς χρήστες που έχουν σύνδεση στο Internet τύπου dialup ή ADSL.

Ένα firewall μπορεί να ελέγξει την κίνηση (traffic) των πακέτων του Internet από και προς τον υπολογιστή μας. Μπορεί να εντοπίσει τις πιθανές επιθέσεις στον υπολογιστή μας, να αναλύσει την κίνηση και τα αρχεία που ανταλλάσσονται, να διακρίνει τις ύποπτες δραστηριότητες και να εμποδίσει την ολοκλήρωσή τους. Ένα firewall προστατεύει ένα δίκτυο από κάποιο άλλο δίκτυο, υποβάλλοντας τα διερχόμενα πακέτα πληροφοριών (εισερχόμενα και εξερχόμενα) σε μια σειρά από ελέγχους και λαμβάνει την απόφαση να τα αφήσει να διέλθουν ή να τα εμποδίσει, ανάλογα με το αν περνούν κάποια τεστ ή όχι. Στην ουσία πρόκειται για έναν ελεγκτή κυκλοφορίας δεδομένων στο Internet.

Μπορεί επίσης να ελέγξει τα προγράμματα που είναι εγκατεστημένα στον ίδιο τον υπολογιστή μας και συνδέονται στο Internet και τα οποία στέλνουν προς τα έξω ευαίσθητα προσωπικά μας δεδομένα ή αφήνουν ανοικτή μια πόρτα (backdoor) για να μπορούν οι πιθανοί hackers να ελέγξουν τον υπολογιστή μας. Ένα firewall μπορεί να κρατήσει κλειστές αυτές τις πόρτες και να μας ενημερώνει για κάθε ύποπτη κίνηση.

Ο όρος firewall είναι πολύ πιθανό να προέρχεται από την αυτοκινητοβιομηχανία, όπου με τον όρο αυτό αποκαλείται το σύστημα ασφαλείας που υπάρχει ανάμεσα στη μηχανή και στην καμπίνα των επιβατών και που προστατεύει τους τελευταίους στην περίπτωση που η μηχανή πάρει φωτιά. Με την έλευση του Internet, ο όρος firewall εισήλθε μεταφορικά και στον χώρο των υπολογιστών.

Η κάθε σοβαρή εταιρεία και ο κάθε οργανισμός που έχει συναλλαγές μέσω Internet, οφείλει να εφαρμόσει μια πολιτική ασφαλείας (security policy) και την καρδιά αυτής της πολιτικής ασφαλείας αποτελεί το firewall. Θα πρέπει

να έχουμε υπόψη μας ότι για να μπορεί να θεωρηθεί μια εφαρμογή firewall ως πετυχημένη, θα πρέπει να μπορεί να ελέγχει και τις εσωτερικές αιτήσεις εφαρμογών και υπηρεσιών που γίνονται για πρόσβαση στο Internet και όχι μόνο αυτές που γίνονται από έξω προς τα μέσα.

4.8.1 ΙΣΤΟΡΙΚΑ ΣΤΟΙΧΕΙΑ

Ο όρος firewall είναι αρκετά παλιός. Πρωτοεμφανίστηκε στις αρχές του 20^{ού} αιώνα, όταν οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα για τους εσωτερικούς τοίχους ούτως ώστε να τα κάνουν πιο ανθεκτικά στην διάδοση της φωτιάς. Σήμερα ο όρος αυτός έφτασε να σημαίνει το λογισμικό ή υλικό που παρεμβάλλεται μεταξύ δικτύων υπολογιστών ούτως ώστε να αποτρέψει την διάδοση ιών, δούρειων ίππων και τις επιθέσεις από κακόβουλους χρήστες.

Η τεχνολογία του firewall εμφανίστηκε στα τέλη της δεκαετίας του 1980, όταν ακόμη το Διαδίκτυο ήταν σε πρώιμα στάδια. Εκείνη την εποχή είχαν παρατηρηθεί αρκετές "τρύπες" ασφαλείας στο Διαδίκτυο οπότε έπρεπε να βρεθεί μία λύση. Η λύση αυτή ήταν η δημιουργία της τεχνολογίας firewall.

1η γενιά - Φίλτρα πακέτων

Το πρώτο ερευνητικό δημοσίευμα πάνω στην τεχνολογία firewall προέκυψε το 1988 όταν οι μηχανικοί της DEC (Digital Equipment Corporation) ανέπτυξαν φίλτρα πακέτων δεδομένων (data packet filters). Τα φίλτρα αυτά θεωρούνται ως η πρώτη γενιά firewall.

Τα φίλτρα πακέτων δρουν ως εξής: Διαβάζουν τα πακέτα δεδομένων που διακινούνται από το ένα δίκτυο στο άλλο και, εάν κάποιο πακέτο ταιριάζει με κάποιο συγκεκριμένο κανόνα, τότε το απορρίπτουν. Ο διαχειριστής του δικτύου είναι σε θέση να ορίσει τους κανόνες βάσει των οποίων θα απορρίπτονται τα πακέτα. Αυτός ο τύπος firewall δεν ενδιαφέρεται για το εάν κάποιο πακέτο ανήκει σε μία σύνδεση, δηλαδή δεν αποθηκεύει πληροφορίες σχετικά με την

κατάσταση των διαφόρων συνδέσεων από το ένα δίκτυο στο άλλο (stateless packet filtering). Αντιθέτως, φιλτράρει κάθε πακέτο με βάση την πληροφορία που περιέχεται στο ίδιο το πακέτο (π.χ. διεύθυνση IP προέλευσης, διεύθυνση IP προορισμού, πρωτόκολλο, αριθμός θύρας κοκ). Επειδή τα πρωτόκολλα TCP και UDP χρησιμοποιούν τις ευρέως διαδεδομένες θύρες (Well known ports), ένα firewall πρώτης γενιάς μπορεί να ξεχωρίσει τα πακέτα που αφορούν διάφορες λειτουργίες, όπως για παράδειγμα το e-mail, την μεταφορά αρχείων, την περιήγηση στο Διαδίκτυο κοκ.

2η γενιά - Φίλτρα κατάστασης

Η δεύτερη γενιά firewall αναπτύχθηκε από τρεις ερευνητές στα εργαστήρια της AT&T Bell: Dave Presetto, Howard Trickey και Kshitij Nigam.

Τα firewall της δεύτερης γενιάς δρουν όπως τα firewall πρώτης γενιάς με κάποιες επιπρόσθετες λειτουργίες. Μία από αυτές είναι το γεγονός ότι πλέον εξετάζουν και την κατάσταση (state) του κάθε πακέτου, δηλαδή την σύνδεση από την οποία προήλθε. Για τον λόγο αυτό και αναφέρονται ως φίλτρα κατάστασης (stateful firewalls). Τα φίλτρα αυτά κρατούν ανά πάσα στιγμή πληροφορίες για τον αριθμό και το είδος των συνδέσεων μεταξύ των δύο δικτύων και επιπλέον μπορούν να ξεχωρίσουν εάν ένα πακέτο αποτελεί την αρχή ή το τέλος μία νέας σύνδεσης ή μέρος μίας ήδη υπάρχουσας.

Οι διαχειριστές τέτοιων firewalls μπορούν να ορίσουν τους κανόνες βάσει των οποίων θα επιτρέπεται η δημιουργία συνδέσεων από το εξωτερικό δίκτυο (Διαδίκτυο) προς το τοπικό/εταιρικό δίκτυο. Με τον τρόπο αυτό γίνεται πιο εύκολη η πρόληψη διαφόρων ειδών επιθέσεων, όπως για παράδειγμα η επίθεση SYN flood.

3η γενιά - Επίπεδο εφαρμογών

Η τρίτη γενιά firewall βασίζεται πλέον στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI (Open Systems Interconnection). Το κύριο χαρακτηριστικό αυτής της γενιάς firewall είναι ότι μπορεί να αντιλαμβάνεται

ποια προγράμματα και πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση (πχ FTP - File Transfer Protocol, DNS - Domain Name System, περιήγηση στο Διαδίκτυο κοκ). Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μίας υπηρεσίας.

Σήμερα

Σήμερα σιγά σιγά εδραιώνονται τα firewalls 4ης γενιάς, τα οποία διαθέτουν γραφικό περιβάλλον μέσω του οποίου μπορεί ο χρήστης να κάνει τις επιλογές του όσον αφορά την ασφάλεια του δικτύου του και να θέσει τους κανόνες βάσει τον οποίων θα απορρίπτονται κάποια πακέτα ή συνδέσεις. Τα firewalls 4ης γενιάς μπορούν πλέον να ενσωματωθούν στο λειτουργικό σύστημα και συνεργάζονται στενά με άλλα συστήματα ασφαλείας, όπως για παράδειγμα το IPS - Intrusion Prevention System.

4.8.2 ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΕΝΑ FIREWALL

Ένα firewall μπορεί να είναι ένα μηχάνημα (συσκευή) ή και ένα πρόγραμμα (εφαρμογή) υπολογιστή, το οποίο χρησιμοποιείται για να επιβάλλει συγκεκριμένους κανόνες επικοινωνίας και ανταλλαγής πληροφοριών ανάμεσα σε δύο δίκτυα υπολογιστών. Το firewall παρεμβάλλεται ανάμεσα σε δύο διαφορετικά δίκτυα υπολογιστών και φιλτράρει τα διακινούμενα πακέτα πληροφοριών. Το firewall κατά τη λειτουργία του (φιλτράρισμα) λαμβάνει υπόψη του ένα σύνολο από κανόνες (κριτήρια) που ορίζονται από τον χρήστη (διαχειριστή του firewall) και με βάση αυτούς τους κανόνες επιτρέπει ή απορρίπτει την κυκλοφορία (διακίνηση) των δεδομένων ανάμεσα στα δύο δίκτυα υπολογιστών.

Θεωρείται ως ένας συνδετικός κρίκος ανάμεσα σε δύο δίκτυα υπολογιστών ή ως ένα φίλτρο δεδομένων. Αν δεν επιτρέψει την κυκλοφορία ενός πακέτου δεδομένων, η ενέργεια αυτή χαρακτηρίζεται ως block traffic, ενώ

αν επιτρέψει την κυκλοφορία ενός πακέτου δεδομένων, η ενέργεια αυτή χαρακτηρίζεται ως permit traffic. Ενώ τα προγράμματα anti-virus, anti-trojan, anti-spam κοκ έχουν συγκεκριμένο αντικείμενο απασχόλησης και μας προστατεύουν από πολύ συγκεκριμένες απειλές, ένα firewall μπορεί να μας προστατεύσει από κάθε είδους απειλή όσον αφορά τη σχέση του υπολογιστή μας ή του δικτύου μας με τον έξω κόσμο.

Θα πρέπει να έχουμε υπόψη μας ότι αν αποφασίσουμε να εγκαταστήσουμε ένα firewall και δεν το ρυθμίσουμε ώστε να λειτουργεί σωστά και αποδοτικά, τότε το πιθανότερο είναι να κάνει ζημιά και να μειώσει την απόδοση και την ευελιξία του υπολογιστή μας. Μπορούμε να φανταστούμε ένα firewall, είτε πρόκειται για συσκευή είτε για πρόγραμμα, ως τον ενδιάμεσο ανάμεσα σε δύο δίκτυα υπολογιστών. Ο χρήστης ενός οικιακού υπολογιστή ή ο administrator ενός δικτύου υπολογιστών θα πρέπει να ορίσει τους κανόνες με βάση τους οποίους θα γίνεται η κυκλοφορία των δεδομένων ανάμεσα στα δύο αυτά δίκτυα.

Μετά την εγκατάσταση ενός οποιουδήποτε firewall, ο χρήστης οφείλει να μελετήσει όλες τις επιλογές που έχει το firewall και να τις προσαρμόσει ανάλογα με τις ανάγκες του και τις τεχνικές γνώσεις που έχει. Μπορούμε να χρησιμοποιήσουμε ένα firewall (τείχος προστασίας) για να προστατεύσουμε το δίκτυό μας από επιθετικά Web sites και πιθανούς hackers. Ένα firewall παρεμβάλλεται ανάμεσα στον υπολογιστή μας ή σ’ ένα δίκτυο υπολογιστών και σ’ ένα άλλο δίκτυο, όπως είναι το Internet ή και ένα ενδοδίκτυο (Intranet).

Σε γενικές γραμμές, ένα firewall είναι ένας φράκτης για να μπορεί να κρατάει μακριά οποιονδήποτε θελήσει να κάνει κακό στο σύστημά μας. Πήρε το όνομά του καθώς η δουλειά του είναι παρόμοια μ’ αυτήν ενός φυσικού τείχους προστασίας που η αποστολή του είναι να εμποδίσει τη φωτιά από το να επεκταθεί και σε γειτονικά μέρη.

4.8.3 ΟΙ ΚΑΤΗΓΟΡΙΕΣ ΤΩΝ FIREWALLS

Οι δύο μεγάλες κατηγορίες των firewalls είναι τα Hardware Firewalls και τα Software Firewalls. Στην πρώτη κατηγορία ανήκουν είτε συσκευές που είναι αυτόνομες (stand alone) και συνδέονται αμέσως με το δίκτυο είτε υπολογιστές που η μόνη τους δουλειά είναι ο ρόλος του firewall σ' ένα δίκτυο και που έχουν εγκατεστημένα τα απαραίτητα προς τον σκοπό αυτό προγράμματα.

Στη δεύτερη κατηγορία ανήκουν προγράμματα υπολογιστών που μπορούμε να βρούμε στο εμπόριο ή στο Internet και που μπορούμε να εγκαταστήσουμε στον υπολογιστή μας. Είναι γνωστά και με τον όρο Personal Firewall.

4.8.4 ΤΙ ΚΑΝΕΙ ΕΝΑ FIREWALL

Το firewall είναι απλά ένα πρόγραμμα ή μια συσκευή hardware που φιλτράρει τις πληροφορίες που έρχονται από τη σύνδεση του Internet μέσα στο ιδιωτικό μας δίκτυο ή στον προσωπικό μας υπολογιστή. Αν ένα εισερχόμενο πακέτο ή κάποια πληροφορία εντοπισθεί από τα φίλτρα, δεν θα της επιτραπεί η είσοδος. Ας υποθέσουμε ότι εργαζόμαστε σε μια εταιρεία με 500 υπαλλήλους, οπότε θα υπάρχουν εκατοντάδες υπολογιστές που θα έχουν όλοι κάρτες δικτύου για να μπορούν να επικοινωνούν μεταξύ τους.

Επιπλέον, η εταιρεία θα έχει μια ή περισσότερες συνδέσεις με το Internet και χωρίς την ύπαρξη ενός firewall, όλοι αυτοί οι υπολογιστές θα είναι ανοικτοί για πρόσβαση από οποιονδήποτε βρίσκεται στο Internet. Κάποιος που έχει τεχνικές γνώσεις μπορεί να εισβάλλει σ' αυτούς τους υπολογιστές, θα προσπαθήσει να κάνει FTP συνδέσεις σ' αυτούς ή να κάνει telnet συνδέσεις κοκ. Αν κάποιος υπάλληλος κάνει το λάθος και αφήσει ανοικτή μια τρύπα

ασφαλείας (security hole), οι hackers θα μπορούν να εισβάλλουν στο μηχάνημα και να εκμεταλλευθούν αυτό το κενό ασφαλείας.

Αν υπάρχει εγκατεστημένο ένα firewall, τα πράγματα είναι πολύ διαφορετικά. Η εταιρεία θα τοποθετήσει ένα firewall σε κάθε σύνδεση στο Internet και το firewall μπορεί να κλείσει τις τρύπες ασφαλείας. Για παράδειγμα, μια από τις τρύπες ασφαλείας μέσα στην εταιρεία μπορεί να είναι η εξής : Από τους 500 υπολογιστές που υπάρχουν στην εταιρεία, μόνο ένας απ' αυτούς επιτρέπεται να έχει δημόσια σύνδεση FTP. Πρέπει να επιτραπούν οι FTP συνδέσεις μόνο σ' αυτόν τον υπολογιστή και να αποκλειστούν απ' όλους τους υπόλοιπους.

Η εταιρεία μπορεί να καθορίσει κανόνες σαν τον προηγούμενο για τους FTP servers, τους Web servers, τους Telnet servers. Επιπλέον, η εταιρεία μπορεί να ελέγχει το πώς οι υπάλληλοι συνδέονται στα Web sites, αν επιτρέπεται στα αρχεία να φύγουν εκτός του δικτύου της εταιρείας. Ένα firewall μπορεί να δώσει σε μια εταιρεία πολύ μεγάλο έλεγχο για τον τρόπο που χρησιμοποιούν οι χρήστες το δίκτυό της. Τα firewalls χρησιμοποιούν μια ή περισσότερες από τις εξής τρεις μεθόδους για να ελέγξουν την κυκλοφορία (traffic) που διέρχεται μέσα και έξω από το δίκτυο.

- Φιλτράρισμα Πακέτων (Packet Filtering). Τα πακέτα (packets), που είναι μικρά κομμάτια δεδομένων, αναλύονται (διέρχονται) μέσα από κάποια φίλτρα. Τα πακέτα που κατορθώνουν να περάσουν μέσα από τα φίλτρα στέλνονται στο σύστημα που τα ζήτησε και όλα τα άλλα πακέτα απορρίπτονται.
- Υπηρεσία Μεσολάβησης (Proxy Service). Οι πληροφορίες από το Internet αναχαιτίζονται από το firewall και στέλνονται μετά στο σύστημα που τις ζήτησε και το αντίστροφο.
- Αυστηρή Επιθεώρηση (Stateful Inspection). Είναι μια καινούργια μέθοδος που δεν εξετάζει τα περιεχόμενα του κάθε πακέτου αλλά αντίθετα συγκρίνει συγκεκριμένα κομμάτια κλειδιά του πακέτου με μια

βάση δεδομένων εμπιστευτικών πληροφοριών. Οι πληροφορίες που ταξιδεύουν μέσα από το firewall προς τα έξω καταγράφονται για συγκεκριμένα χαρακτηριστικά που έχουν και μετά οι εισερχόμενες πληροφορίες συγκρίνονται μ' αυτά τα χαρακτηριστικά. Αν από την σύγκριση προκύψει ένα λογικό ταίριασμα, επιτρέπεται στις πληροφορίες να διέλθουν. Αλλιώς, απορρίπτονται.

4.8.5 Η ΠΑΡΑΚΑΜΨΗ (ΞΕΓΕΛΑΣΜΑ) ΤΩΝ FIREWALLS

Πρέπει να έχουμε υπόψη μας ότι κάθε σύνδεση στο Internet παραμένει επισφαλής ακόμα και αν είναι εγκατεστημένο κάποιο firewall. Οι επίδοξοι hackers μπορούν να βρουν εργαλεία και τεχνικές ώστε να δημιουργήσουν μια σύνδεση με το εσωτερικό δίκτυο της εταιρείας και να παρακάμψουν έτσι, στην ουσία να ξεγελάσουν, το firewall. Για τον εντοπισμό και την αντιμετώπιση αυτών των διαρροών βοηθούν τα συστήματα διάγνωσης εισβολής, γνωστά και ως IDS (Intrusion Detection Systems).

Ένας από τους πιο συνηθισμένους τρόπους που χρησιμοποιούν οι εισβολείς για να παρακάμψουν ένα firewall είναι η εγκατάσταση μιας πόρτας (backdoor) στο εσωτερικό δίκτυο μιας εταιρείας, η οποία έχει τη δυνατότητα να επικοινωνήσει με μια θύρα (port) που επιλέχθηκε να είναι ανοικτή όταν έγινε η εγκατάσταση του firewall.

Οι τρόποι που χρησιμοποιούν οι εισβολείς για να ξεγελάσουν τα θύματά τους, να παρακάμψουν το ενδεχόμενα εγκατεστημένο firewall και να εισβάλουν έτσι στον υπολογιστή τους ποικίλουν. Ένας πολύ συνηθισμένος τρόπος είναι η αποστολή ενός παραπλανητικού e-mail όπου ζητούν από το υποψήφιο θύμα τους την εγκατάσταση ενός προγράμματος το οποίο θα κάνει δήθεν έλεγχο αν είναι εγκατεστημένο κάποιο άλλο επιβλαβές πρόγραμμα.

Στην πραγματικότητα, βέβαια, δεν γίνεται κανένας έλεγχος για την εγκατάσταση ενός τέτοιου προγράμματος αλλά αντιθέτως γίνεται η εγκατάσταση ενός άλλου επιβλαβούς προγράμματος. Ένας άλλος συνηθισμένος

τρόπος είναι η δωρεάν προσφορά προγραμμάτων, τα οποία μπορεί μεν να κάνουν κάποια απλή εργασία αλλά ταυτόχρονα εγκαθιστούν και κάποιο πρόγραμμα τύπου δούρειου ίππου (trojan horse) ή κάποιας πόρτας (backdoor), το οποίο είναι προγραμματισμένο να αναλάβει δράση με την πρώτη ευκαιρία ή όταν του το ζητήσει ο δημιουργός του.

4.8.6 ΡΥΘΜΙΖΟΝΤΑΣ ΕΝΑ FIREWALL

Τα firewalls μπορούν να προσαρμοστούν. Αυτό σημαίνει ότι μπορούμε να προσθέσουμε ή να αφαιρέσουμε φίλτρα με βάση κάποιες συνθήκες, μερικές από τις οποίες είναι οι εξής :

IP Διευθύνσεις (IP Addresses). Το κάθε μηχάνημα που συνδέεται στο Internet αποκτά μια μοναδική διεύθυνση που είναι γνωστή ως IP διεύθυνση (IP address). Οι IP διευθύνσεις είναι αριθμοί που αποτελούνται από 32 bits και μπορούν να παρουσιασθούν ως τέσσερις δεκαδικοί αριθμοί χωρισμένοι με τελείες. Μια τυπική IP διεύθυνση είναι σαν την εξής : 212.24.52.118. Για παράδειγμα, αν μια συγκεκριμένη IP διεύθυνση που βρίσκεται εκτός της εταιρείας διαβάζει υπερβολικά μεγάλο αριθμό αρχείων από έναν server, το firewall θα μπορεί να εμποδίσει όλη την κυκλοφορία προς ή από αυτήν την IP διεύθυνση.

Ονόματα Χώρου (Domain Names). Επειδή είναι δύσκολο να θυμάται κανείς όλη τη σειρά των αριθμών που συγκροτούν μια IP διεύθυνση και επειδή οι IP διευθύνσεις ενδέχεται να αλλάζουν μερικές φορές, όλοι οι servers που υπάρχουν στο Internet διαθέτουν και ονόματα που είναι κατανοητά από τους ανθρώπους, τα οποία είναι γνωστά με τον όρο ονόματα χώρου (domain names). Για παράδειγμα, είναι πολύ ευκολότερο για όλους μας να θυμόμαστε το www.mycompany.com παρά το 212.24.52.118. Μια εταιρεία έχει τη δυνατότητα να μπλοκάρει την πρόσβαση σε συγκεκριμένα domain names ή να επιτρέψει την πρόσβαση μόνο σε συγκεκριμένα domain names.

Πρωτόκολλα (Protocols). Το πρωτόκολλο είναι ο προκαθορισμένος τρόπος που κάποιος που επιθυμεί να χρησιμοποιήσει μια υπηρεσία, επικοινωνεί μαζί της. Ο

«κάποιος» μπορεί να είναι ένα άτομο, αλλά πιο συχνά είναι ένα πρόγραμμα υπολογιστή, όπως είναι ένας φυλλομετρητής (Web browser). Τα πρωτόκολλα αποτελούνται συνήθως από κείμενο και απλά περιγράφουν το πώς ο πελάτης (client) και ο διακομιστής (server) θα κάνουν τη συνομιλία τους. Το http είναι το πρωτόκολλο του Web. Μερικά κοινά πρωτόκολλα για τα οποία μπορούμε να ορίσουμε φίλτρα firewall είναι τα εξής :

- IP (Internet Protocol), αποτελεί το κύριο σύστημα διανομής για τις πληροφορίες που διακινούνται στο Internet.
- TCP (Transmission Control Protocol), χρησιμοποιείται για τη διάσπαση και την επανένωση των πληροφοριών (πακέτων) που ταξιδεύουν στο Internet.
- HTTP (Hyper Text Transfer Protocol), χρησιμοποιείται στις ιστοσελίδες (Web pages).
- FTP (File Transfer Protocol), χρησιμοποιείται για το κατέβασμα (download) και το ανέβασμα (upload) αρχείων.
- UDP (User Datagram Protocol), χρησιμοποιείται για τις πληροφορίες που δεν απαιτούν απόκριση (response), όπως είναι ο ήχος και το βίντεο ροής (streaming audio και video).
- ICMP (Internet Control Message Protocol), χρησιμοποιείται από έναν δρομολογητή (router) για την ανταλλαγή πληροφοριών μ’ άλλους δρομολογητές.
- SMTP (Simple Mail Transport Protocol), χρησιμοποιείται στην αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail).
- SNMP (Simple Network Management Protocol), χρησιμοποιείται για τη συλλογή πληροφοριών συστήματος από έναν απομακρυσμένο υπολογιστή (remote computer).
- Telnet, χρησιμοποιείται για να εκτελούμε εντολές σ’ έναν απομακρυσμένο υπολογιστή (remote computer).

Η εταιρεία μπορεί να ορίσει μόνο ένα ή δύο μηχανήματα για να χειρισθούν ένα συγκεκριμένο πρωτόκολλο και να καταργήσει αυτό το πρωτόκολλο σ’ όλα τα άλλα μηχανήματα.

- Θύρες (Ports). Όλα τα μηχανήματα server κάνουν τις υπηρεσίες τους να είναι διαθέσιμες στο Internet χρησιμοποιώντας αριθμημένες θύρες (ports), από μία για κάθε υπηρεσία που υπάρχει διαθέσιμη στον server. Για παράδειγμα, αν ένα μηχάνημα server τρέχει έναν Web (HTTP) server και έναν FTP server, ο Web server θα είναι διαθέσιμος στη θύρα (port) 80 και ο FTP server θα είναι διαθέσιμος στη θύρα (port) 21. Μια εταιρεία μπορεί να μπλοκάρει την πρόσβαση στη θύρα 21 σ’ όλα τα μηχανήματα εκτός από ένα μέσα στην εταιρεία.
- Συγκεκριμένες Λέξεις και Φράσεις. Μπορεί να είναι οτιδήποτε. Το firewall θα ψάξει παντού (λειτουργία sniff) σε κάθε πακέτο δεδομένων για να βρει ένα ακριβές ταίριασμα του κειμένου που υπάρχει στο φίλτρο. Για παράδειγμα, μπορούμε να καθοδηγήσουμε το firewall ώστε να μπλοκάρει όλα τα πακέτα που περιέχουν τη λέξη "go on". Το σημαντικό είναι ότι οι λέξεις θα πρέπει να ταιριάζουν ακριβώς, δηλ. το φίλτρο δεν θα εντοπίσει τη λέξη "goon", που δε περιέχει τον κενό χαρακτήρα. Μπορούμε, όμως, να συμπεριλάβουμε όσες λέξεις, φράσεις και παραλλαγές αυτών θέλουμε.

Ένα software firewall μπορεί να εγκατασταθεί στον υπολογιστή του σπιτιού μας, όπου υπάρχει σύνδεση με το Internet. Αυτός ο υπολογιστής θεωρείται ότι είναι μια πύλη (gateway) επειδή παρέχει το μοναδικό σημείο πρόσβασης ανάμεσα στο δίκτυο του σπιτιού μας και το Internet.

Μ’ ένα hardware firewall, η μονάδα του firewall αποτελεί κανονικά την πύλη (gateway) και ένα καλό παράδειγμα είναι ένας δρομολογητής (router) που διαθέτει μια ενσωματωμένη κάρτα Ethernet και ένα hub. Οι υπολογιστές στο δίκτυο του σπιτιού μας συνδέονται στον δρομολογητή (router), ο οποίος με τη σειρά του συνδέεται σ’ ένα καλωδιακό modem ή σ’ ένα DSL modem.

Μπορούμε να ρυθμίσουμε (configure) τον router μέσω ενός Web interface από τον φυλλομετρητή του υπολογιστή μας και εκεί μπορούμε να ορίσουμε τα φίλτρα ή και άλλες ρυθμίσεις.

4.8.7 ΑΠΟ ΤΙ ΜΠΟΡΕΙ ΝΑ ΜΑΣ ΠΡΟΣΤΑΤΕΥΣΕΙ ΕΝΑ FIREWALL

Υπάρχουν πολλοί τρόποι που μπορεί να χρησιμοποιήσει κάποιος ασυνείδητος για να κάνει ζημιά σε μη προστατευμένους υπολογιστές, όπως :

- Απομακρυσμένη Πρόσβαση (Remote Login). Συμβαίνει όταν κάποιος έχει τη δυνατότητα να συνδεθεί στον υπολογιστή μας και να τον ελέγξει κατά κάποιον τρόπο. Αυτό μπορεί να κυμαίνεται από το να μπορεί να δει απλά ή να έχει πρόσβαση σε αρχεία έως το να μπορεί να τρέχει προγράμματα στον υπολογιστή μας.
- Κερκόπορτες Εφαρμογής (Application Backdoors). Μερικά προγράμματα έχουν ιδιαίτερα χαρακτηριστικά που επιτρέπουν την απομακρυσμένη πρόσβαση (remote access), ενώ άλλα περιέχουν σφάλματα (bugs) τα οποία δίνουν τη δυνατότητα για την ύπαρξη κερκόπορτας ή πίσω πόρτας (backdoor), δηλ. μιας κρυφής πρόσβασης, με την οποία μπορεί να έχει κάποιος κάποιο επίπεδο ελέγχου του προγράμματος.
- SMTP Session Hijacking. Το SMTP αποτελεί την πιο κοινή μέθοδο αποστολής ηλεκτρονικού ταχυδρομείου (e-mail) στο Internet και αποκτώντας πρόσβαση σε μια λίστα από διευθύνσεις e-mail, κάποιος μπορεί να στείλει αυτόκλητα e-mail (spam) σε χιλιάδες χρήστες.
- Σφάλματα στο Λειτουργικό Σύστημα. Όπως και οι εφαρμογές, μερικά λειτουργικά συστήματα έχουν backdoors, ενώ άλλα παρέχουν απομακρυσμένη πρόσβαση με ανεπαρκείς ελέγχους ασφαλείας ή έχουν ελαττώματα (bugs) που μπορεί να εκμεταλλευθεί ένας έμπειρος hacker.
- Άρνηση Υπηρεσίας (Denial of Service). Αυτό το είδος επίθεσης είναι σχεδόν αδύνατο να αντιμετωπισθεί. Αυτό που συμβαίνει είναι ότι ο

hacker στέλνει μια αίτηση (request) στον server για να συνδεθεί σ' αυτόν. Όταν ο server απαντήσει με μια αναγνώριση (acknowledgement) και προσπαθήσει να κάνει μια σύνοδο (session), δεν θα μπορεί να βρει το σύστημα που έκανε την αίτηση (request). Κατακλύζοντας έναν server με τέτοιες αναπάντητες αιτήσεις session, ένας hacker αναγκάζει τον server να δουλεύει πολύ αργά (σέρνεται) έως ότου καταρρεύσει.

- Βόμβες e-mail (e-mail Bombs). Μια βόμβα e-mail είναι συνήθως μια προσωπική επίθεση όπου κάποιος μάς στέλνει το ίδιο e-mail εκατοντάδες ή και χιλιάδες φορές μέχρις ότου το σύστημά μας να μην μπορεί να δεχθεί άλλα μηνύματα.
- Μακροεντολές (Macros). Για να απλοποιήσουν περίπλοκες διαδικασίες ή εργασίες, πολλές εφαρμογές (applications) μάς δίνουν τη δυνατότητα να δημιουργήσουμε ένα μικρό πρόγραμμα (σενάριο εντολών, script) από εντολές που η εφαρμογή μπορεί να εκτελέσει. Αυτό το script είναι γνωστό ως μακροεντολή (macro). Οι hackers μπορούν να εκμεταλλευθούν αυτή τη δυνατότητα και να δημιουργήσουν τα δικά τους macros, τα οποία, ανάλογα με την εφαρμογή, μπορούν να καταστρέψουν τα δεδομένα ή και να προκαλέσουν την κατάρρευση του υπολογιστή μας.
- Ιοί (Viruses). Πιθανώς η πιο γνωστή απειλή είναι οι ιοί των υπολογιστών (computer viruses). Ένας ιός (virus) είναι ένα μικρό πρόγραμμα που μπορεί να αντιγράψει τον εαυτό του σ' άλλους υπολογιστές. Μ' αυτόν τον τρόπο μπορεί να διαδοθεί ταχύτατα από το ένα σύστημα στο άλλο. Το αποτέλεσμα ενός ιού μπορεί να κυμαίνεται από την εμφάνιση ενός αβλαβούς μηνύματος έως και τη διαγραφή όλων των αρχείων του υπολογιστή μας.
- Spam e-mail. Μπορεί να μην κάνει ζημιά αλλά είναι πάντα ενοχλητική, η μη ζητηθείσα ή αυτόκλητη εμπορική αλληλογραφία (spam e-mail), που αποτελεί το ηλεκτρονικό ισοδύναμο της άχρηστης διαφημιστικής αλληλογραφίας (junk mail). Το spam e-mail μπορεί να είναι και

επικίνδυνο καθώς αρκετά συχνά περιέχει συνδέσμους (links) σε Web sites, τα οποία ενδέχεται να στέλνουν cookies για να ανοίξουν έτσι μια κερκόπορτα (backdoor) στον υπολογιστή μας.

- Βόμβες Ανακατεύθυνσης (Redirect Bombs). Οι hackers μπορούν να χρησιμοποιήσουν το πρωτόκολλο ICMP για να αλλάξουν (ανακατευθύνουν) τη διαδρομή που ακολουθούν οι πληροφορίες, στέλνοντάς τες σ' έναν διαφορετικό δρομολογητή (router). Αυτός είναι κι ένας από τους τρόπους που γίνεται μια επίθεση άρνησης υπηρεσίας (denial of service attack).
- Source routing. Στις περισσότερες περιπτώσεις, η διαδρομή που ακολουθεί ένα πακέτο στο Internet (ή σ' ένα άλλο δίκτυο) καθορίζεται από τους δρομολογητές (routers) που υπάρχουν κατά μήκος της διαδρομής. Αλλά η πηγή (source), δηλ. ο αρχικός υπολογιστής, που παρέχει το πακέτο μπορεί αυθαίρετα να καθορίσει τη διαδρομή (route) που θα πρέπει να ακολουθήσει το πακέτο. Οι hackers το εκμεταλλεύονται αυτό μερικές φορές για να κάνουν τις πληροφορίες να φαίνονται ότι προέρχονται από μια έγκυρη πηγή ή ακόμη και μέσα από το ίδιο το δίκτυο. Τα περισσότερα firewalls μπορούν και εξουδετερώνουν το source routing.

Μερικές από τις παραπάνω επιθέσεις, είναι δύσκολο, αν όχι αδύνατο, να αντιμετωπισθούν με τη χρήση ενός firewall. Ενώ μερικά firewalls προσφέρουν προστασία από ιούς, αξίζει τον κόπο να εγκαταστήσουμε ένα πρόγραμμα anti-virus σε κάθε υπολογιστή του δικτύου μας. Και, αν και είναι ενοχλητικά, πολλά spam e-mails μπορούν να περάσουν μέσα από το firewall όσο εμείς λαμβάνουμε τα e-mails μας. Το επίπεδο ασφάλειας (level of security) που ορίζουμε είναι αυτό που καθορίζει πόσες πολλές απ' αυτές τις απειλές μπορούν να αναχαιτισθούν από ένα firewall. Το υψηλότερο επίπεδο ασφάλειας θα είναι το μπλοκάρισμα των πάντων.

Στην ουσία κάτι τέτοιο καταργεί την ύπαρξη μιας σύνδεσης στο Internet, αλλά ένας κοινός πρακτικός κανόνας είναι να μπλοκάρουμε τα πάντα και μετά να αρχίζουμε να επιλέγουμε τι είδος κυκλοφορίας θα επιτρέψουμε.

Μπορούμε επίσης να περιορίσουμε την κυκλοφορία (traffic) που περνάει μέσα από το firewall έτσι ώστε μόνο συγκεκριμένα είδη πληροφοριών, όπως τα e-mail, να μπορούν να περάσουν. Για τους περισσότερους χρήστες, το καλύτερο είναι να εργάζονται με τις προκαθορισμένες ρυθμίσεις που δίνονται από τον κατασκευαστή του firewall εκτός κι αν υπάρχει κάποιος πολύ συγκεκριμένος λόγος για να γίνουν αλλαγές.

Ένα από τα καλύτερα πράγματα όσον αφορά ένα firewall από την άποψη της ασφάλειας είναι ότι εμποδίζει τον οποιονδήποτε βρίσκεται έξω από το να εισβάλλει σ' έναν υπολογιστή του δικτύου μας. Μπορεί αυτό να ενδιαφέρει κυρίως τις επιχειρήσεις, αλλά και οι οικιακοί χρήστες με τη χρήση ενός firewall μπορούν να έχουν ήσυχο το κεφάλι τους.

4.8.8 ΕΤΟΙΜΑ ΠΡΟΓΡΑΜΜΑΤΑ FIREWALL

Η τελευταία έκδοση των Windows XP διαθέτει ένα προεγκατεστημένο (ενσωματωμένο) πρόγραμμα firewall, που είναι γνωστό με την ονομασία Internet Connection Firewall. Για να ενεργοποιήσουμε το ενσωματωμένο firewall των Windows XP, πηγαίνουμε στην επιλογή Συνδέσεις Δικτύου του Πίνακα Ελέγχου. Κάνουμε δεξί κλικ στη σύνδεση που μας ενδιαφέρει και επιλέγουμε Για προχωρημένους από την επιλογή Ιδιότητες του πτυσσόμενου μενού. Για να ενεργοποιήσουμε το firewall για τη συγκεκριμένη σύνδεση πρέπει να επιλέξουμε το πλαίσιο ελέγχου Protect my computer and network by limiting or preventing access to this computer from the Internet.

Το ενσωματωμένο firewall των Windows XP ενώ προσφέρει ικανοποιητική προστασία και έλεγχο για την κίνηση που γίνεται από έξω προς τα μέσα (inbound traffic), αγνοεί την προστασία και τον έλεγχο για την κίνηση που γίνεται από μέσα προς τα έξω (outbound traffic). Αν αυτό δεν μας είναι αρκετό, προγράμματα τύπου firewall προσφέρονται και από γνωστές εταιρείες

που εξειδικεύονται στην ασφάλεια των υπολογιστικών συστημάτων, όπως είναι τα εξής :

- Norton Personal Firewall της εταιρείας Symantec,
- Personal Firewall Plus της εταιρείας McAfee,
- Panda Platinum της εταιρείας Panda,
- Norman Personal Firewall της εταιρείας Norman,
- Sygate Personal Firewall της εταιρείας Sygate,
- eSafe Desktop Firewall,
- Tiny Personal Firewall της εταιρείας Tiny,
- F-Secure Firewall της εταιρείας F-Secure,
- Lockdown Millennium της εταιρείας Lockdown και
- Bit Defender της εταιρείας AVX.

Το Kerio Personal Firewall της εταιρείας Kerio αποτελεί ένα από τα ασφαλέστερα προγράμματα της κατηγορίας του και μπορεί να κάνει και έλεγχο για ιούς τύπου dialer. Όμως, το πιο δημοφιλές πρόγραμμα firewall είναι το Zone Alarm της εταιρείας Zone Labs, καθώς καταφέρνει και συνδυάζει αρμονικά την ασφάλεια με την ευκολία χρήσης. Αυτό που κάνει στην ουσία το πρόγραμμα Zone Alarm είναι να επιτρέπει ή όχι την πρόσβαση σε προγράμματα που κάνουν χρήση του Internet. Το Zone Alarm διαθέτει πέντε εικονίδια με αντίστοιχες επιλογές και με τις εξής λειτουργίες :

- Alerts. Μπορούμε να ενημερωθούμε για τις επιθέσεις που έχει δεχθεί ο υπολογιστής μας καθώς και να κρατήσουμε τα στοιχεία αυτά σ’ ένα αρχείο.
- Lock. Μπορούμε να ορίσουμε ώστε το πρόγραμμα να κλειδώνει αυτόματα τη σύνδεση με το Internet όταν διαπιστώσει ενδεχόμενο κίνδυνο.
- Security. Μπορούμε να επιλέξουμε το επίπεδο ασφαλείας που θέλουμε να έχουμε, δηλ. High, Medium ή Low.

- Programs. Εμφανίζονται όλα τα προγράμματα που εκτελούνται στον υπολογιστή μας καθώς και αυτά που κάνουν χρήση του Internet. Μπορούμε να επιλέξουμε αν θα επιτρέπεται ή όχι η εκτέλεση ενός προγράμματος ή αν θα γίνεται σχετική ερώτηση προς τον χρήστη.
- Configure. Μπορούμε να κάνουμε διάφορες ρυθμίσεις για το πρόγραμμα.

Οι εφαρμογές firewall του εμπορίου διαθέτουν έτοιμα επίπεδα ασφαλείας, όπως High, Medium και Low για παράδειγμα, τα οποία μπορούμε να επιλέξουμε και να γίνουν έτσι αυτόματα οι απαραίτητες ρυθμίσεις, στην περίπτωση που δεν γνωρίζουμε ή δεν έχουμε τον χρόνο να ασχοληθούμε με το τι ρυθμίσεις πρέπει να κάνουμε. Μπορούμε να επιλέξουμε υψηλό, μέτριο ή χαμηλό επίπεδο ασφαλείας, μ' ό,τι αυτό συνεπάγεται.

Ο καλύτερος τρόπος για να δοκιμάσουμε κατά πόσο λειτουργεί σωστά και αποδοτικά ένα firewall, είναι να επισκεφθούμε ένα από τα sites του Internet που αναλαμβάνουν να κάνουν εικονικές εισβολές στον υπολογιστή μας και να μας δείξουν τις τυχόν αδυναμίες του, όπως είναι τα http://grc.com και http://www.pcinternetpatrol.com.

4.8.9 ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΜΕ ΤΗ ΧΡΗΣΗ FIREWALL

Η πολιτική ασφαλείας του δικτύου μιας εταιρείας, η οποία χρησιμοποιεί firewall, θα πρέπει σε γενικές γραμμές να έχει υπόψη της τα εξής :

- Θα πρέπει να περνάνε μέσα από το firewall όλες οι συνδέσεις που γίνονται από το δίκτυο της εταιρείας προς το Internet.
- Θα πρέπει να ορισθεί ένας τεχνικός υπεύθυνος για την εγκατάσταση, τη ρύθμιση και τη διαχείριση του firewall, ο οποίος θα πρέπει να ακολουθεί και τακτική εκπαίδευση και ενημέρωση.
- Το εγκατεστημένο firewall θα πρέπει να παρακολουθείται και να ελέγχεται σε τακτά χρονικά διαστήματα.

- Θα πρέπει να απενεργοποιηθούν όλες οι εφαρμογές που δεν είναι απαραίτητες.
- Το firewall θα πρέπει να είναι διαθέσιμο 24 ώρες το 24ωρο.

4.8.10 ΤΙ ΜΠΟΡΕΙ ΝΑ ΚΑΝΕΙ ΕΝΑ FIREWALL

- Να εμποδίσει ιούς (viruses), σκουλήκια (worms), δούρειους ίππους (trojan horses) και άλλα προγράμματα τύπου spyware από το να εγκατασταθούν στον υπολογιστή μας και να κάνουν ζημιά.
- Να εμποδίσει την πρόσβαση στον υπολογιστή μας σε άγνωστους ή ανεπιθύμητους επισκέπτες.
- Να μας ειδοποιήσει ότι ο υπολογιστής μας δέχεται κάποια επίθεση.
- Να μας παρουσιάσει αναλυτικά στατιστικά στοιχεία σχετικά με την κίνηση από και προς τον υπολογιστή μας.
- Να εμποδίσει κάποιο πρόγραμμα τύπου dialer από το να πραγματοποιήσει υπερπόντιες τηλεφωνικές κλήσεις χωρίς τη θέλησή μας.

4.8.11 ΤΙ ΔΕΝ ΜΠΟΡΕΙ ΝΑ ΚΑΝΕΙ ΕΝΑ FIREWALL

- Να διαγράψει ιούς (viruses), δούρειους ίππους (trojan horses) και άλλα προγράμματα τύπου spyware.
- Να εμποδίσει την μη ζητηθείσα εμπορική ηλεκτρονική αλληλογραφία, γνωστή και με τον όρο spam e-mail.
- Να μας προστατεύσει από επιβλαβή προγράμματα τα οποία είτε δεν μπόρεσε να εντοπίσει ή εμείς οι ίδιοι επιτρέψαμε την εγκατάστασή τους, όπως είναι συνήθως τα προγράμματα συνομιλίας (chat) ή ανταλλαγής αρχείων (peer-to-peer).

- Να μας προστατεύσει από τις εσωτερικές απειλές, δηλ. από τους κακόβουλους χρήστες που έχουν φυσική πρόσβαση στο εσωτερικό του τοπικού δικτύου μας.

5. ΕΧΘΡΟΙ ΚΑΙ ΑΠΕΙΛΕΣ ΣΥΣΤΗΜΑΤΩΝ

Απειλή είναι οποιοδήποτε πιθανό περιστατικό, κακόβουλο ή όχι, που μπορεί να βλάψει κάποιο αγαθό. Με άλλα λόγια, απειλή είναι οτιδήποτε κακό μπορεί να συμβεί στα αγαθά. Ευπάθεια είναι μια αδυναμία που κάνει δυνατή την απειλή. Αυτό μπορεί να γίνει λόγω αδυναμιών στη σχεδίαση, λάθη στη διαμόρφωση ή λόγω ακατάλληλων και επισφαλών τεχνικών κωδικοποίησης.

Επίθεση είναι μια ενέργεια που εκμεταλλεύεται τις ευπάθειες και υλοποιεί μια απειλή. Προκειμένου να σχεδιαστεί και να αναπτυχθεί μια ασφαλής web εφαρμογή, απαιτείται η γνώση τόσο των απειλών όσο και των εχθρών του συστήματος. Είναι σημαντικό να αναλυθεί η αρχιτεκτονική της εφαρμογής και να καθοριστούν οι πιθανές ευπαθείς περιοχές που μπορούν να επιτρέψουν σε ένα χρήστη ή σε έναν επιτιθέμενο με κακόβουλες προθέσεις, να παραβιάσει την ασφάλεια του συστήματος. Παρακάτω ακολουθούν αναλυτικά οι κατηγορίες των εχθρών, παρουσιάζονται οι πιο συνήθεις απειλές καθώς και οι τεχνικές επιθέσεων που κάνουν πραγματικότητα αυτές τις απειλές.

5.1 ΕΧΘΡΟΙ

Είναι σημαντικό στην προσπάθεια παροχής ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου, να αναγνωρίζονται αρχικά «εχθροί». Οποιοσδήποτε εμπλέκεται με ζητήματα ασφάλειας ηλεκτρονικού εμπορίου θα πρέπει να τον απασχολούν οι εχθροί του συστήματος, οι προθέσεις τους καθώς και τα μέσα που διαθέτουν. Οι «εχθροί» κατηγοριοποιούνται ως εξής:

- Hackers - Crackers
- Εισβολείς

5.1.1 HACKERS- CRACKERS

Hacker ονομάζεται ένα άτομο, που χωρίς εξουσιοδότηση αποκτά παράνομη πρόσβαση σε κάποιο σύστημα υπολογιστών και στα δεδομένα του, χωρίς ωστόσο να έχει πρόθεση να προκαλέσει ζημιά.

Cracker ονομάζεται ένα άτομο που χωρίς εξουσιοδότηση, αποκτά παράνομη πρόσβαση σε ένα σύστημα υπολογιστών και στα δεδομένα του, με σκοπό την πρόκληση οικονομικής ή άλλου είδους ζημιάς και την κλοπή πληροφοριών.

Συνήθως οι hackers αντιμετωπίζουν τη δραστηριότητά τους ως μια πρόκληση και ευχαριστιούνται να μπαίνουν σε υψηλής ασφάλειας συστήματα υπολογιστών, στα οποία δεν σκοπεύουν να προκαλέσουν κανένα είδος ζημιάς. Πολλές φορές οι hackers μπαίνουν σε κάποιο σύστημα (π.χ. τραπεζικό ή κυβερνητικό) για να αποκαλύψουν τα «κενά» στην ασφάλειά τους. Αν πετύχουν το σκοπό τους, ενημερώνουν τον ενδιαφερόμενο οργανισμό για την επιτυχία τους, ελπίζοντας σε οικονομικά οφέλη.

Από την άλλη, οι crackers προσπαθούν παράνομα να μπουν σε συστήματα υπολογιστών με σκοπό να υποκλέψουν δεδομένα και να προκαλέσουν ζημιά στις πληροφορίες που βρίσκονται στους φακέλους του συστήματος. Για παράδειγμα, μόλις αποκτήσουν έναν αριθμό πιστωτικής κάρτας, τον χρησιμοποιούν προς όφελός τους.

Οι crackers συνήθως βάζουν ιούς και άλλου είδους προγράμματα που περιέχουν ειδικό κώδικα στα συστήματα στόχους, με σκοπό να προκαλέσουν σοβαρή ζημιά. Στις περισσότερες περιπτώσεις αυτοί οι κώδικες είναι:

- Ένας δούρειος ίππος, κρυμμένος σε άλλα προγράμματα που φαινομενικά δεν είναι βλαβερά.
- Ένα σκουλήκι, το οποίο δεν είναι κρυμμένο σε άλλα αρχεία, αλλά αποστέλλεται εκμεταλλευόμενο τα κενά στην ασφάλεια των δικτύων που έχουν εντοπίσει οι crackers.

- Μια λογική βόμβα, που υποδηλώνει ανενεργό κώδικα τοποθετημένο μέσα σε ένα πρόγραμμα λογισμικού και ο οποίος ενεργοποιείται σε συγκεκριμένη ημερομηνία ή συμβάν.

5.1.2 ΕΙΣΒΟΛΕΙΣ

Απαιτείται πολύς χρόνος για κάποιον που δεν γνωρίζει τόσο για να μάθει όσο και για να καταφέρει να πραγματοποιήσει μια εισβολή σε ένα ξένο σύστημα υπολογιστή. Εξαιτίας αυτού του γεγονότος υπάρχουν δύο τύποι σοβαρών εισβολέων, οι υποαπασχολούμενοι και αυτοί που πληρώνονται προκειμένου να πραγματοποιούν εισβολές. Η λέξη εισβολέας μας φέρνει στο μυαλό εφήβους που κάθονται όλη την ημέρα μπροστά σε ένα υπολογιστή. Πράγματι, αυτή η ομάδα είναι το μεγαλύτερο κομμάτι των σημερινών εισβολέων, αλλά δεν αποτελούν το μεγαλύτερο κίνδυνο. Οι εισβολείς ανήκουν στις παρακάτω κατηγορίες, με σειρά αυξανόμενης απειλής :

- **F** Ειδικοί Ασφαλείας
- **F** Έφηβοι Εισβολείς
- **F** Υποαπασχολούμενοι Ενήλικες
- **F** Εισβολείς από Ιδεολογία
- **F** Εγκληματίες Εισβολείς
- **F** Εταιρικοί Κατάσκοποι
- **F** Δυσαρεστημένοι Υπάλληλοι

Ειδικοί Ασφαλείας:

Οι περισσότεροι ειδικοί ασφαλείας είναι σε θέση να κάνουν εισβολές αλλά δεν το κάνουν για ηθικούς ή για οικονομικούς λόγους. Γνωρίζουν ότι μπορούν να κερδίσουν περισσότερα χρήματα αν αποτρέπουν τις εισβολές παρά να τις προκαλούν, οπότε ξοδεύουν το χρόνο τους παρακολουθώντας τις

κοινότητες των εισβολέων και τις τρέχουσες τεχνικές προκειμένου να γίνουν περισσότερο αποτελεσματικοί στη μάχη κατά των εισβολέων. Είναι πολλές οι εταιρίες που δραστηριοποιούνται στον κυβερνοχώρο που προσλαμβάνουν ηθικούς εισβολείς για να ελέγχουν τα συστήματα ασφαλείας τους και των μεγάλων πελατών τους. Αυτοί οι ειδικοί συχνά είναι οι πρώτοι που βρίσκουν νέες μεθόδους εισβολής και συχνά γράφουν λογισμικό για να ελέγχουν ή για να προκαλούν μια κατάσταση.

Έφηβοι Εισβολείς:

Οι έφηβοι εισβολείς είναι συνήθως σπουδαστές που κάνουν εισβολές, ενώ βρίσκονται σε κάποια βαθμίδα της εκπαίδευσης –γυμνάσιο, λύκειο ή πανεπιστήμιο. Αυτοί οι εισβολείς μπορούν να χρησιμοποιούν το δικό τους υπολογιστή ή μπορούν να χρησιμοποιούν τους ισχυρούς πόρους της σχολής τους για να κάνουν τις εισβολές τους.

Οι έφηβοι εισβολείς κάνουν βόλτες στον κυβερνοχώρο ψάχνοντας για στόχους και ενδιαφέρονται κυρίως για να εντυπωσιάσουν τους φίλους τους και να μην συλληφθούν. Συνήθως δεν βλάπτουν τους στόχους τους ενώ τις περισσότερες φορές η δράση τους δεν γίνεται καν αντιληπτή, εκτός και αν το σύστημα στο οποίο εισβάλουν ανιχνεύσει ασυνήθιστη δραστηριότητα και ειδοποιήσει τον ιδιοκτήτη ή αν ένα firewall καταγράψει την επίθεση ή εκτός και αν κάνουν κάποιο λάθος.

Αν θεωρήσουμε την κοινότητα των εισβολέων ως μια οικονομική δραστηριότητα, τότε οι έφηβοι εισβολείς είναι οι καταναλωτές. Χρησιμοποιούν τα εργαλεία που παράγονται από άλλους, χαίρονται με τις δραστηριότητές τους και γενικά παράγουν μια βάση διασκέδασης, επάνω στην οποία κάθονται οι σοβαρότεροι έφηβοι εισβολείς και υποαπασχολούμενοι ενήλικες. Καμία σοβαρή προσπάθεια ασφάλειας δεν θα τους βγάλει από το παιχνίδι.

Υποαπασχολούμενοι Ενήλικες:

Οι υποαπασχολούμενοι ενήλικες είναι είτε πρώην έφηβοι εισβολείς, οι οποίοι είτε εκδιώχθηκαν από τη σχολή τους, είτε δεν κατάφεραν να βρουν μια εργασία πλήρους απασχόλησης. Συνήθως εργασίες που πληρώνουν μόνο για τις βασικές τους ανάγκες ενώ η πρώτη τους αγάπη είναι η εισβολή. Πολλά από τα εργαλεία που χρησιμοποιούν οι έφηβοι εισβολείς κατασκευάζονται από τους ενήλικες εισβολείς.

Οι ενήλικες εισβολείς δεν είναι εγκληματίες από πρόθεση αφού δεν έχουν σκοπό να κάνουν κακό σε κανέναν. Ωστόσο συχνά δημιουργούν τα σπασίματα που εφαρμόζονται από άλλους εισβολείς για να ξεκλειδώσουν εμπορικό λογισμικό. Επίσης αυτή η ομάδα των εισβολέων γράφει τους περισσότερους ιούς λογισμικού και αποτελεί την περιβόητη συμμορία των εισβολέων. Κάνουν τις εισβολές τους για αποκτήσουν φήμη στην κοινότητα των εισβολέων, θέλουν να εντυπωσιάσουν τους όμοιούς τους, να πάρουν πληροφορίες και να κάνουν γνωστή την αντίδρασή τους στην κυβέρνηση και τις επιχειρήσεις. Η ομάδα αυτή αποτελεί το ένα δέκατο της κοινότητας των εισβολέων, αλλά είναι η πηγή του λογισμικού που γράφεται ειδικά για εισβολείς.

Οι υποαπασχολούμενοι ενήλικες αποτελούν κίνδυνο για το δίκτυο μιας εταιρίας αν αυτή κατέχει κάποιο είδος πνευματική ιδιοκτησίας που θέλει να προστατέψει, μιας και η πνευματική ιδιοκτησία δεν προστατεύεται αρκετά από το νόμο και η εισβολή δεν αποτελεί αδίκημα σε πολλές χώρες του κόσμου.

Εισβολείς από Ιδεολογία:

Οι εισβολείς από ιδεολογία είναι αυτοί που κάνουν εισβολές για να προωθήσουν κάποιο πολιτικό σκοπό. Από το 2000, η εισβολή από ιδεολογία έχει ξεφύγει από την εμφάνιση μερικών μόνο επεισοδίων και έχει φτάσει σε επίπεδο πλήρους πολέμου πληροφοριών. Η εισβολή από ιδεολογία είναι περισσότερο συνηθισμένη σε πολιτικές διαμάχες που αφορούν συνήθως σε θέματα περιβάλλοντος και εθνικισμού.

Σε μια προσπάθεια να διαδηλώσουν τις ιδέες τους, αυτοί οι εισβολείς συνήθως καταστρέφουν ιστοσελίδες ή κάνουν επιθέσεις άρνησης παροχής υπηρεσίας εναντίον των ιδεολογικών τους αντιπάλων. Συνήθως προσπαθούν να επιτύχουν ευρεία κάλυψη των κατορθωμάτων τους από τα μέσα και επειδή προέρχονται κυρίως από άλλες χώρες και έχουν την έμμεση υποστήριξη των κυβερνήσεών τους, δεν μπορούν να απαγγελθούν κατηγορίες εναντίον τους.

Αυτό το είδος εισβολής εμφανίζεται κατά κύματα, όταν συμβαίνουν μεγάλα γεγονότα στον πολιτικό στίβο, και πολλές φορές εξαιτίας του ότι αυτού του είδους οι επιθέσεις καταναλώνουν πολύ μεγάλο εύρος ζώνης, προκαλούν χαοτικές καταιγίδες.

Εγκληματίες Εισβολείς:

Οι εγκληματίες εισβολείς κάνουν εισβολές είτε για εκδίκηση, είτε για να διαπράξουν κλοπές, είτε απλώς για να ικανοποιηθούν και να προκαλέσουν καταστροφές. Αυτή η κατηγορία εισβολέων δεν αποτελούν ένα ειδικό επίπεδο ηθικού προβλήματος. Οι εγκληματίες εισβολείς είναι αυτοί που ακούγονται στις εφημερίδες να έχουν εισβάλει σε διακομιστές Internet για να κλέψουν αριθμούς πιστωτικών καρτών, για να κάνουν μεταφορές χρημάτων από τράπεζες ή να έχουν εισβάλει στο μηχανισμό τραπεζικών συναλλαγών του Internet για να κλέψουν χρήματα.

Αυτοί οι εισβολείς είναι παρόμοιοι με κάθε άλλο εγκληματία αφού προσπαθούν να κάνουν ζημιά αδιαφορώντας για το ποιος είναι το θύμα. Οι εγκληματίες εισβολείς είναι πολλοί σπάνιοι επειδή η ευφυΐα που απαιτείται για να κάνουν εισβολές συνήθως τους δίνει την ευκαιρία να βρουν κάποιο περισσότερο αποδεκτό κοινωνικά τρόπο ζωής. Παρόλα αυτά, γίνεται όλο και περισσότερο συνηθισμένο το οργανωμένο έγκλημα να απειλεί ότι θα κάνει επιθέσεις άρνησης παροχής υπηρεσιών για να ζητήσει χρήματα προστασίας από εταιρίες τα έσοδα των οποίων προέρχονται από μια δημόσια ιστοθέση. Επειδή οι επιθέσεις άρνηση παροχής υπηρεσιών δεν μπορούν να αποτραπούν, αφού

μπορεί για παράδειγμα να εμφανιστούν με την μορφή μιας μεγάλης ποσότητας νόμιμων αιτήσεων, τα θύματα συχνά αισθάνονται ότι δεν έχουν καμία άλλη επιλογή παρά να πληρώσουν.

Εταιρικοί Κατάσκοποι:

Οι πραγματικοί εταιρικοί κατάσκοποι είναι πολύ σπάνιοι επειδή είναι πολύ ακριβό και πολύ επικίνδυνο να χρησιμοποιηθούν παράνομες τεχνικές εισβολής εναντίον ανταγωνιστικών εταιριών. Αυτές οι τεχνικές χρησιμοποιούνται τις περισσότερες φορές εναντίον εταιριών υψηλής τεχνολογίας από ξένες κυβερνήσεις. Πολλές εταιρίες υψηλής τεχνολογίας είναι νέες και άπειρες στο θέμα ασφάλειας και έτσι μπορούν εύκολα να επιλεγούν από τους πεπειραμένους πράκτορες ξένων κυβερνήσεων. Αυτές οι υπηρεσίες έχουν ήδη τα χρήματα για να κάνουν κατασκοπία και επιτίθενται σε μερικές επιχειρήσεις μεσαίου μεγέθους για να υποκλέψουν τεχνολογία, η οποία θα δώσει στις εθνικές τους εταιρίες ένα ανταγωνιστικό πλεονέκτημα.

Δυσαρεστημένοι Υπάλληλοι:

Οι δυσαρεστημένοι υπάλληλοι είναι οι πιο επικίνδυνοι και οι πιθανότεροι να δημιουργήσουν προβλήματα από όλους τους εισβολείς. Ένας υπάλληλος που θεωρεί ότι δεν του έχει φερθεί καλά η εταιρία στην οποία εργάζεται, έχει και τον τρόπο αλλά και τα κίνητρα να προκαλέσει σοβαρές καταστροφές στο δίκτυο της εταιρίας. Επιθέσεις από δυσαρεστημένους υπαλλήλους δύσκολα ανιχνεύονται πριν να συμβούν, αλλά συνήθως κάποιο είδος συμπεριφοράς δίνει κάποιες γενικές ενδείξεις. Οι επιθέσεις μπορεί να είναι είτε περίπλοκες όπου ένας διαχειριστής δικτύου για παράδειγμα διαβάζει όλα τα e-mail των υπαλλήλων, είτε απλές όπου ένας υπάλληλος κάνει καταστροφές στον διακομιστή της εταιρικής βάσης δεδομένων.

Εξαιτίας των παραπάνω είναι πολύ αποδοτικό να γίνετε γνωστό σε όλους τους υπαλλήλους της εταιρίας ότι το τμήμα Πληροφορικής καταγράφει όλες τις δραστηριότητες των χρηστών για λόγους ασφαλείας. Αυτό αποτρέπει μέρος των προβλημάτων αφού οι υπάλληλοι γνωρίζουν ότι θα είναι γνωστές όλες οι ενέργειες που κάνουν στα συστήματα του δικτύου υπολογιστών της εταιρίας.

5.2 ΑΠΕΙΛΕΣ

Στις τυπικές απειλές ασφάλειας σε ένα περιβάλλον διαδικτύου, συμπεριλαμβάνονται :

F *Βλάβες συστατικών μερών (component failure):* Σχεδιαστικά λάθη ή ελαττωματικά μέρη υλικού/ λογισμικού, είναι ικανά να προκαλέσουν δυσλειτουργία σε κάποιο συστατικό του συστήματος και να οδηγήσουν έτσι σε άρνηση εξυπηρέτησης ή άλλες καταστάσεις επικίνδυνες για την ασφάλεια.

F *Παρουσίαση πληροφοριών (information browsing):* Η αποκάλυψη ευαίσθητων πληροφοριών σε μη-εξουσιοδοτημένους χρήστες, είτε είναι εισβολείς είτε είναι νόμιμοι χρήστες που επιχειρούν παράνομους τρόπους προσπέλασης, οδηγεί στην απώλεια εμπιστευτικότητας και μπορεί να προκληθεί από την εκμετάλλευση διάφορων μηχανισμών.

F *Μη-εξουσιοδοτημένη διαγραφή, μεταβολή ή εισαγωγή πληροφοριών*: Η εκούσια ή και ακούσια πρόκληση ζημιών στα πληροφοριακά αγαθά (information assets) οδηγεί στην απώλεια της ακεραιότητας των λειτουργιών/ δεδομένων των οργανισμών και των χρηστών.

F *Κατάχρηση (misuse):* Η χρήση των πληροφοριακών αγαθών αλλά και των υπόλοιπων πόρων για σκοπούς διαφορετικούς από αυτούς που έχουν προκαθορισθεί, προκαλεί άρνηση εξυπηρέτησης, αύξηση κόστους λειτουργίας των συστημάτων και δυσφήμιση των οργανισμών που τα χρησιμοποιούν.

F *Διείσδυση (penetration):* Οι εισβολείς από μη-εξουσιοδοτημένα πρόσωπα ή συστήματα μπορούν να προκαλέσουν άρνηση εξυπηρέτησης ή να

απαιτήσουν σοβαρότατα χρηματικά ποσά για την αντιμετώπιση των συνεπειών από τις παρενοχλήσεις του συστήματος.

F *Διαστρέβλωση:* Οι προσπάθειες ενός χρήστη που παρανομεί, να μεταμφιεστεί σαν ένας χρήστης με εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες ή δυσχέρειες σε ένα οργανισμό.

Οι πιθανότητες να εκδηλωθούν επιθέσεις και να πραγματοποιηθούν απειλές όπως οι προαναφερθείσες, αυξάνονται όταν προσφέρεται στο διαδίκτυο μια ευδιάκριτη εικόνα της οργάνωσης της δικτυακής υποδομής ενός συστήματος. Πάρα πολλές επιθέσεις στο Internet είναι ευκαιριακής φύσης (opportunistic), με την έννοια ότι δεν έχουν συγκεκριμένο στόχο παραβίασης. Απλά εκδηλώνονται σε ένα συγκεκριμένο σύστημα γιατί εκείνη τη στιγμή το σύστημα αυτό «φαντάζει» ως ιδανικός στόχος (τελικός ή ενδιάμεσος) για τους επίδοξους εισβολείς.

5.3 ΕΠΙΘΕΣΕΙΣ

Η πραγματοποίηση οποιασδήποτε από τις παραπάνω θεμελιώδεις απειλές, μπορεί να γίνει με μια από τις παρακάτω τεχνικές επίθεσης:

5.3.1 Η ΒΟΜΒΑ E-MAIL

Αυτό είναι ένα e-mail το οποίο είτε περιλαμβάνει ένα πολύ μεγάλο κείμενο είτε έχει ένα πολύ μεγάλο επισυναπτόμενο αρχείο. Συχνά τέτοια e-mail στέλνονται σε συμμετέχοντες σε ομάδες νέων (newsgroups) ή σε forums με τους οποίους ο αποστολέας διαφώνησε στο forum. Είναι απλά ενοχλητικά και τίποτα παραπάνω: αν έχετε μόνο μια dial-up σύνδεση και κάποιος σας στέλνει

ένα αρκετά μεγάλο αλλά άχρηστο e-mail μπορεί να χρειαστεί να περιμένετε μάταια πολύ ώρα μέχρι να το δείτε. Υπάρχουν ωστόσο σοβαρότερες περιπτώσεις όπου τέτοια μηνύματα στάλθηκαν κατά συρροή σε ένα οργανισμό ώστε να απενεργοποιηθεί ο mail server λόγω του υπερβολικού φορτίου που συνεπάγονται τα μηνύματα αυτά.

Άλλη μια σημαντική απειλή της μορφής αυτής είναι η ακούσια εγγραφή σε λίστες e-mail. Στη περίπτωση αυτή κάποιο κακόβουλο άτομο θα εγγράψει το θύμα του σε πάρα πολλές λίστες e-mail. Αυτό μπορεί να έχει ως αποτέλεσμα το θύμα να δέχεται συνεχώς e-mail. Αυτό μέχρι κάποιο σημείο μπορεί να είναι απλά ενοχλητικό. Από κάποιο σημείο και πέρα όμως μπορεί να είναι ιδιαίτερα σημαντικό για το θύμα καθώς μπορεί τα μηνύματα αυτά να γεμίσουν το χώρο αποθήκευσης του (ιδιαίτερα αν περιλαμβάνουν και επισυναπτόμενα αρχεία) και να προκαλέσουν την απώλεια πραγματικά σημαντικών μηνυμάτων καθώς δεν θα υπάρχει χώρος για την αποθήκευση τους.

5.3.2 ΕΠΙΘΕΣΕΙΣ ΑΡΝΗΣΗΣ ΥΠΗΡΕΣΙΑΣ (DENIAL OF SERVICE)

Όταν έχουμε μια επίθεση άρνησης υπηρεσίας, ένας εισβολέας εκτελεί κάποια ενέργεια η οποία είτε σταματά κάποια υπηρεσία του συστήματος είτε υποβαθμίζει την ποιότητα της. Για παράδειγμα, η εκτέλεση ενός προγράμματος το οποίο στη συνέχεια θα ξεκινήσει κάποια άλλα προγράμματα, τα οποία με τη σειρά τους θα ξεκινήσουν κάποια άλλα κ.ο.κ. θα προκαλέσει συμφόρηση στο σύστημα και συνεπώς θα εμποδίσει την παροχή των πραγματικών υπηρεσιών για τις οποίες είναι υπεύθυνο.

Μια από τις πρώτες επιθέσεις της μορφής άρνησης υπηρεσίας που εμφανίστηκαν στο Internet ήταν το διάσημο "σκουλήκι" (Worm) του Robert Morris. Ο Morris, ένας αμερικανός φοιτητής, έριξε στο Internet το

συγκεκριμένο πρόγραμμα το 1988. Το "σκουλήκι" είχε φτιαχτεί με τέτοιο τρόπο ώστε αντέγραφε τον εαυτό του σε άλλους υπολογιστές στο Internet, ώστε τελικά πολλές χιλιάδες υπολογιστές είχαν μολυνθεί.

Ένα από τα προβλήματα με τις επιθέσεις άρνησης υπηρεσίας που εμφανίζονται στο Internet είναι πως αφού το λογισμικό υλοποιείται με περίπου τον ίδιο τρόπο, κάθε λειτουργικό σύστημα που χρησιμοποιεί το TCP/IP είναι ευάλωτο σε τέτοιου είδους επιθέσεις.

5.3.3 ΙΟΙ

Οι ιοί είναι ένα είδος κακόβουλα γραμμένου κώδικα που θέτει σε κίνδυνο την ασφαλή λειτουργία του συστήματος και μπορούν να χρησιμοποιηθούν για μια ποικιλία διαφορετικών επιθέσεων. Περιγράφονται ξεχωριστά εδώ καθώς απαιτούν αρκετά υψηλό επίπεδο τεχνικών γνώσεων. Οι συνηθισμένες επιθέσεις άρνησης υπηρεσιών είναι απλές και όχι ιδιαίτερα εξεζητημένες ενώ η επίθεση με ιό απαιτεί μεγαλύτερο βαθμό τεχνικών γνώσεων.

Ένας ιός είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή - μια διαδικασία που είναι γνωστή ως μόλυνση Αφού ένας ιός εγκατασταθεί σε έναν υπολογιστή, μπορεί να αντιγράψει τον εαυτό του και σε άλλα αρχεία στον υπολογιστή.

5.3.3.1 <u>ΚΑΤΗΓΟΡΙΕΣ ΙΩΝ</u>

Υπάρχουν τρεις κύριες κατηγορίες ιών: εκτελέσιμοι ιοί, ιοί δεδομένων και ιοί οδηγών συσκευών. Ένας **εκτελέσιμος ιός** είναι ένας ιός ο οποίος προστίθεται σε ένα εκτελέσιμο αρχείο, το οποίο όταν εκτελεστεί θα έχει ως αποτέλεσμα να εκτελεστεί και ο κώδικας του ιού. Αυτός ο κώδικας στη συνέχεια θα κάνει κάποια κακόβουλη ενέργεια όπως να διαγράψει κάποια σημαντικά αρχεία. Ένας **ιός δεδομένων** είναι ένας ιός ο οποίος μολύνει ένα αρχείο που περιέχει δεδομένα αντί για εκτελέσιμο κώδικα. Συχνά τα δεδομένα

αυτά είναι συνδεδεμένα με κάποιο πρόγραμμα, το οποίο χρειάζεται τα δεδομένα για να εκτελέσει τη λειτουργία του. Για παράδειγμα, πολλά προγράμματα χρειάζονται ένα startup αρχείο το οποίο αρχικοποιεί το πρόγραμμα και ορίζει βασικές παραμέτρους της λειτουργίας του. Ένας ιός δεδομένων θα μπορούσε να μολύνει ένα τέτοιο αρχείο και να αλλάξει τα δεδομένα σε ένα τέτοιο αρχείο ώστε το πρόγραμμα δεν θα μπορεί να λειτουργήσει ή η λειτουργία του θα τεθεί σε κίνδυνο. Ένας άλλος τύπος ιού δεδομένων θα μπορούσε να προσθέσει μια καταχώρηση σε ένα αρχείο με password κι έτσι θα επέτρεπε πρόσβαση σε ένα εισβολέα. Άλλο ένα παράδειγμα είναι αυτό ενός ιού δεδομένων για έναν επεξεργαστή κειμένου, που θα μπορούσε επίσης να γραφτεί και εύκολα και που θα μπορούσε να αλλάζει τα περιεχόμενα κάθε αρχείου που ανοίγει από τον επεξεργαστή κειμένου ή ακόμη χειρότερα να το σβήνει. Μια τρίτη κατηγορία είναι οι **ιοί οδηγών συσκευών**. Αυτοί επηρεάζουν τους οδηγούς συσκευών ενός λειτουργικού συστήματος που χρησιμοποιούνται για τον χειρισμό διαφόρων στοιχείων του υπολογιστή όπως δίσκος. Ευτυχώς αυτός ο τύπος ιού εμφανιζόταν κυρίως σε παλιότερα λειτουργικά συστήματα όπως το MSDOS.

Υπάρχει επίσης ένας τρόπος κατηγοριοποίησης των ιών βάσει του τρόπου που χρησιμοποιούν για να κρύψουν την παρουσία τους στον υπολογιστή. Βάσει του κριτηρίου αυτού υπάρχουν δυο ειδών ιοί, οι **stealth ιοί** και οι **πολυμορφικοί ιοί**.

Πριν περιγράψουμε αυτούς τους δυο τύπους ιών είναι χρήσιμο να μιλήσουμε για το πως τα προγράμματα εντοπισμού ιών λειτουργούν. Τα προγράμματα αυτά λειτουργούν ελέγχοντας τα αρχεία που υπάρχουν αποθηκευμένα ψάχνοντας σε αυτά είτε γνωστούς ιούς είτε αλλαγές σε σημαντικά αρχεία, π.χ. αλλαγές σε αρχεία κώδικα του λειτουργικού συστήματος παρότι δεν υπήρξε άμεση αναβάθμιση του.

Οι ιοί Stealth κρύβουν την παρουσία τους χρησιμοποιώντας μερικές διάφορες τεχνικές, για παράδειγμα αλλάζοντας τις ημερομηνίες αλλαγής ή το

πραγματικό μέγεθος των αρχείων ώστε το πρόγραμμα εντοπισμού ιών να μην μπορεί να εντοπίσει κάποια αλλαγή και να μην θεωρεί ύποπτα αρχεία τα οποία στην πραγματικότητα είναι μολυσμένα.

Οι πολυμορφικοί ιοί μπορούν να αλλάζουν συχνά τα χαρακτηριστικά τους - για παράδειγμα το μέγεθος τους - μια διαδικασία που είναι γνωστή ως μετάλλαξη. Αυτό σημαίνει ότι είναι πολύ πιο δύσκολο για τα προγράμματα εντοπισμού ιών να τους εντοπίσουν βασιζόμενοι μόνο στα γνωστά χαρακτηριστικά τους.

Κοινοποιημένοι και μη κοινοποιημένο ιοί

Οι ερευνητές που ασχολούνται με τους ιούς υπολογιστών κατηγοριοποιούν τους ιούς είτε ως κοινοποιημένους είτε ως μη κοινοποιημένους. Οι πρώτοι είναι ιοί οι οποίοι έχουν ελευθερωθεί και μπορούν να προσβάλλουν οποιονδήποτε υπολογιστή ενώ οι δεύτεροι προορίζονται για έρευνα και δεν εξαπλώνονται πέρα από λίγους υπολογιστές.

5.3.3.2 ΔΗΜΙΟΥΡΓΙΑ ΙΩΝ

Υπάρχουν διάφοροι τρόποι δημιουργίας ιών. Μπορούν να δημιουργηθούν από την αρχή χρησιμοποιώντας μια γλώσσα όπως η C ή assembly. Χρησιμοποιούνται τέτοιες γλώσσες γιατί πρέπει ο κώδικας του ιού να είναι όσο το δυνατόν μικρότερος για να μπορεί να αποφεύγει τον εντοπισμό από προγράμματα anti-virus. Οι γλώσσες αυτές επίσης παρέχουν αρκετές δυνατότητες σχετικά χαμηλού επιπέδου που δεν προσφέρονται από άλλες γλώσσες όπως κάποιες λειτουργίες εισόδου / εξόδου. Υπάρχουν επίσης κάποια εργαλεία κατασκευής ιών τα οποία μπορούν να βρεθούν σε διάφορα μέρη στο Internet.

5.3.3.3 ΕΝΑΣ ΤΥΠΙΚΟΣ ΙΟΣ

Θα συμπληρώσουμε την ενότητα των ιών εξετάζοντας τη λειτουργία ενός συγκεκριμένου ιού βλέποντας έτσι πόσο πονηροί μπορεί να είναι οι κατασκευαστές ιών. Ο ιός αυτός είναι γνωστός σας ιός οικογένειας και φίλων. Χρησιμοποιεί επισυναπτόμενα αρχεία σε e-mails για να διαδοθεί ωστόσο το κάνει με ένα ιδιαίτερα πονηρό τρόπο.

Υπάρχει ένας ιδιαίτερα μεγάλος αριθμός ιών (εκτελέσιμων ιών ή ιών δεδομένων) που διαδόθηκαν μέσω e-mail. Το μόνο που πρέπει να κάνει ο παραλήπτης ενός μολυσμένου e-mail είναι να ανοίξει ένα επισυναπτόμενο αρχείο. Το αποτέλεσμα θα είναι να εκτελεστεί ένα πρόγραμμα που θα μολύνει τον υπολογιστή του παραλήπτη. Συχνά τέτοια e-mail έχουν μια απλή επικεφαλίδα όπως 'Γεια' ή 'Πως πάει;' που ίσως αποτελεί ένδειξη ότι ο αποστολέας είναι γνωστός του παραλήπτη και το αρχείο πιθανότατα μπορεί με ασφάλεια να ανοιχθεί. Μια άλλη ανάλογη μέθοδος είναι μέσω ηλεκτρονικών ευχετήριων καρτών, όπου τα ύποπτα επισυναπτόμενα αρχεία μπορεί να φαίνονται σαν ευχετήριες κάρτες.

Υπήρξε έντονη δημοσιότητα σχετικά με τη διάδοση ιών μέσω e-mail και σαν συνέπεια πολλοί χρήστες του Internet είναι διστακτικοί να ανοίξουν επισυναπτόμενα αρχεία από χρήστες που δεν γνωρίζουν. Αυτό είναι το ιδιαίτερο σημείο στο οποίο οι ιοί του τύπου "φίλοι και οικογένεια" αποδεικνύονται τόσο ύπουλοι. Ο ιός μπορεί μολύνει κάποιον υπολογιστή χρησιμοποιώντας κάποιο άλλο μέσο και όχι e-mail, για παράδειγμα μπορεί να μολύνει κάποιο υπολογιστή όταν ο χρήστης του κατεβάζει κάποιο δωρεάν πρόγραμμα από το κάποιο ftp site. Ανεξάρτητα από τον τρόπο με τον οποίο έγινε η μόλυνση, ο ιός στη συνέχεια θα δει τη λίστα διευθύνσεων του χρήστη και θα στείλει e-mails σε όλα τα άτομα που είναι καταχωρημένα στη λίστα διευθύνσεων του χρήστη προσποιούμενος πως είναι ο χρήστης του υπολογιστή. Το e-mail που στέλνεται θα περιέχει και ένα επισυναπτόμενο αρχείο. Οι χρήστες οι οποίοι δεν θα άνοιγαν κάποιο επισυναπτόμενο αρχείο από άγνωστο αποστολέα κατά πάσα πιθανότητα θα ανοίξουν το αρχείο που προέρχεται κατά τα φαινόμενα από

κάποιον που γνωρίζουν. Συνεπώς ο ιός θα μολύνει όλους τους υπολογιστές των ατόμων που θα ανοίξουν το αρχείο και θα στείλει ακόμα περισσότερα e-mails χρησιμοποιώντας το νέο κατάλογο διευθύνσεων κ.ο.κ.

5.3.4 ΑΝΙΧΝΕΥΤΕΣ (SCANNERS)

Ένα scanner είναι ένα πρόγραμμα το οποίο ανιχνεύει αδυναμίες ασφάλεια σε υπολογιστικά συστήματα. Είναι λίγο αμφιλεγόμενο αν θα έπρεπε να μπει αυτό το θέμα σε μια ενότητα σχετική με επιθέσεις αφού τα προγράμματα αυτά αναπτύχθηκαν για να βοηθήσουν τους διαχειριστές συστημάτων να εντοπίσουν αδυναμίες. Ωστόσο κάποια από αυτά μπορούν να χρησιμοποιηθούν για να διερευνήσουν τρόπους εισβολής σε ένα δίκτυο.

Πιθανότατα το πιο γνωστό scanner είναι το SATAN. Όταν κυκλοφόρησε το 1995 δημιούργησε σάλο καθώς ήταν το πρώτο πρόγραμμα το οποίο μπορούσε να εντοπίσει προβλήματα ενός δικτύου λειτουργώντας έξω από το δίκτυο. Υπήρχαν άλλοι δυο λόγοι για τους οποίους δημιουργήθηκε τόσος θόρυβος για το πρόγραμμα αυτό: ο πρώτος είναι ότι όταν εντόπιζε κάποια αδυναμία εμφάνιζε και ένα κατάλληλο και αρκετά αυστηρό μήνυμα σχετικά με τους κινδύνους της αδυναμίας αυτής και το δεύτερο ήταν το ίδιο το όνομα του προγράμματος, ήταν μια ένδειξη κακόβουλων προθέσεων εκ μέρους του εκάστοτε χρήστη του. Το SATAN δημιουργήθηκε από δυο σύμβουλους ασφαλείας, τον Dan Farmer και τον Weitse Venema, στο UNIX. Τα αρχικά SATAN σημαίνουν Security Administrator's Tool for Analyzing Networks.

Ένα scanner είναι ένα πρόγραμμα το οποίο ερευνά τα διάφορα στοιχεία ενός λειτουργικού συστήματος και ελέγχει αν είναι ασφαλή, για παράδειγμα μερικοί scanners για το UNIX μπορούν να ελέγχουν αν η δημοφιλής εφαρμογή ***sendmail*** είναι αρκετά ασφαλής για να αποτρέψει την εισβολή. Άλλοι scanners μπορούν να ελέγξουν την ανθεκτικότητα ενός ftp server, για παράδειγμα βρίσκοντας αν ένα πολύ μεγάλο password θα μπλοκάρει τον ftp server. Τα

scanners συνήθως είναι γραμμένα στο UNIX, αλλά τα τελευταία χρόνια έχουν δημιουργηθεί αντίστοιχα και για άλλα λειτουργικά συστήματα όπως τα Windows NT.

5.3.5 ΣΠΑΣΙΜΟ ΚΩΔΙΚΩΝ (PASSWORD CRACKERS)

Ένα password cracker είναι ένα πρόγραμμα το οποίο προσπαθεί να βρει το password κάποιου χρήστη ή το όνομα του χρήστη που αντιστοιχεί σε κάποια passwords που υπάρχουν αποθηκευμένα σε ένα αρχείο με passwords σε κάποιο υπολογιστή. Τα εργαλεία αυτά χρησιμοποιήθηκαν αρχικά από διαχειριστές συστημάτων ώστε να σιγουρευτούν ότι τα passwords που επέλεξαν οι χρήστες τους δεν μπορούσαν να εντοπιστούν εύκολα. Ωστόσο, χρησιμοποιήθηκαν επίσης κακόβουλα, για παράδειγμα για να αποκτήσουν πρόσβαση σε συστήματα όπου οι χρήστες είχαν εύκολα passwords όπως 'system' ή 'admin'.

Τα περισσότερα password crackers είτε προσπαθούν να ανακαλύψουν ένα password χρησιμοποιώντας μια μεγάλη λίστα λέξεων που επιλέγουν συχνά οι χρήστες ως passwords και δοκιμάζουν πολλά από αυτά είτε επιχειρούν να αποκτήσουν απευθείας πρόσβαση στο αρχείο των password.

5.3.6 ΠΡΟΓΡΑΜΜΑΤΑ ΥΠΟΚΛΟΠΗΣ (SNIFFERS)

Αυτά είναι εργαλεία τα οποία υποκλέπτουν πακέτα δεδομένων τα οποία ταξιδεύουν στο δίκτυο. Υπάρχει μια νόμιμη χρήση τους από τους διαχειριστές συστημάτων καθώς μπορούν να χρησιμοποιηθούν για να εντοπίσουν αδυναμίες ενός δικτύου, για παράδειγμα μπορούν να χρησιμοποιηθούν για να εντοπίσουν σημεία πολύ έντονης κυκλοφορίας όπου μπορεί να υπάρχει πρόβλημα. Χρησιμοποιούνται επίσης από προγραμματιστές κατανεμημένων συστημάτων για να πάρουν μια ιδέα της αναμενόμενης κυκλοφορίας στο δίκτυο και να προσαρμόσουν την εφαρμογή τους σε αυτή.

Ωστόσο, έχουν συχνά επίσης χρησιμοποιηθεί για την υποκλοπή σημαντικών δεδομένων. Ένας εισβολέας μπορεί να εγκαταστήσει ένα sniffer σε ένα σημαντικό σημείο ενός δικτύου, για παράδειγμα σε μια πύλη και να διαβάσει τα μηνύματα καθώς αυτά περνάνε από αυτή. Ένας πετυχημένος sniffer μπορεί να εντοπίσει εκατοντάδες, αν όχι χιλιάδες passwords μέσα σε λίγες ώρες και να τα στείλει σε ένα απομακρυσμένο υπολογιστή από όπου κάποιος μη εξουσιοδοτημένος χρήστης θα μπορεί να τα χρησιμοποιήσει για να εισβάλει στο σύστημα.

Οι επιθέσεις με sniffer είναι παραδόξως όχι πολύ συνηθισμένες, ωστόσο όταν συμβαίνουν μπορεί να θέσουν σε κίνδυνο την ασφάλεια πολλών υπολογιστών και χρηστών. Για παράδειγμα, μια πρόσφατη επίθεση με sniffer είχε ως αποτέλεσμα 268 sites (όχι υπολογιστές αλλά sites!) να έχουν σοβαρά προβλήματα ασφάλειας.

5.3.7 ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ (TROJAN HORSES)

Ένας δούρειος ίππος είναι ένα κακόβουλο κομμάτι κώδικα το οποίο υπάρχει μέσα σε ένα κατά τα άλλα αθώο πρόγραμμα και το οποίο επιχειρεί να κάνει κάτι το οποίο ο χρήστης δεν περιμένει να κάνει. Για παράδειγμα, ένα ελεύθερης πρόσβασης πρόγραμμα το οποίο παρέχει σε ένα διαχειριστή συστημάτων πληροφορίες σχετικά με τη χρήση των αρχείων σε ένα δικτυακό σύστημα, αλλά το οποίο μετά από κάποια στιγμή υποκλέπτει πληροφορίες ή αλλάζει αρχεία είναι ένας δούρειος ίππος.

Οι δούρειοι ίπποι μπορούν να χρησιμοποιηθούν για διάφορους λόγους όπως την υποκλοπή passwords και άλλων πληροφοριών ή για να καταστρέψουν πόρους (π.χ. αρχεία) και να προκαλέσουν κατάρρευση ενός συστήματος.

Το κύριο πρόβλημα με τους δούρειους ίππους είναι ότι είναι πολύ δύσκολο να εντοπιστούν. Οι λόγοι είναι δυο: ο πρώτος είναι ότι συχνά παίρνουν τη μορφή ιδιαίτερα συνηθισμένων εργαλείων ή εργαλείων που απαιτούν την

χειροκίνητη εγκατάσταση τους από το χρήστη. Για παράδειγμα, το 1997 ένας δούρειος ίππος κυκλοφόρησε με τη μορφή του δημοφιλούς προγράμματος συμπίεσης αρχείων *Stuffit* που χρησιμοποιείται στους υπολογιστές Macintosh. Αυτός ο συγκεκριμένος δούρειος ίππος έσβηνε σημαντικά αρχεία μετά την εγκατάσταση του σε έναν υπολογιστή.

Ο δεύτερος λόγος για τον οποίο είναι δύσκολο να εντοπιστούν είναι ότι υπάρχουν σε κάποιο υπολογιστή με τη μορφή ενός μεταφρασμένου προγράμματος το οποίο είναι δύσκολο να ελεγχθεί τι ακριβώς κάνει.

5.3.8 SPOOFING

Αυτός είναι ένας όρος ο οποίος χρησιμοποιείται για να περιγράψει την κατάσταση κατά την οποία ένας εισβολέας χρησιμοποιεί κάποιο υπολογιστή προσποιούμενος στο σύστημα στο οποίο επιτίθεται ότι ο υπολογιστής που χρησιμοποιεί είναι κάποιος άλλος τον οποίο το σύστημα εμπιστεύεται και συνεπώς μπορεί να εκτελέσει λειτουργίες που κανονικά δεν θα επιτρεπόταν. Το spoofing δεν απαιτεί πολλές γνώσεις σχετικά με passwords και μεθόδους πιστοποίησης χρηστών όπως οι προηγούμενες μέθοδοι. Έχει σχέση μόνο με το να νομίζει το δίκτυο ότι ο υπολογιστής που χρησιμοποιεί ο εισβολέας είναι κάποιος άλλος υπολογιστής που το δίκτυο εμπιστεύεται.

Για να καταλάβουμε πως λειτουργεί το spoofing μπορούμε να δούμε μια συγκεκριμένη μορφή της τεχνικής αυτής που λέγεται IP spoofing. Αυτή η επίθεση χρησιμοποιεί το πρωτόκολλο TCP/IP για να παρακάμψει τις κανονικές λειτουργίες πιστοποίησης σε ένα σύστημα και γίνεται χρησιμοποιώντας έναν υπολογιστή που ισχυρίζεται πως έχει μια έμπιστη IP διεύθυνση.

Cookies και ασφάλεια

Ένα cookie είναι ένα αρχείο που τοποθετείται στον υπολογιστή ενός χρήστη από έναν browser και που συνήθως περιέχει στοιχεία συναλλαγών του

χρήστη με συγκεκριμένους δικτυακούς τόπους. Για παράδειγμα, ένα cookie μπορεί να περιέχει στοιχεία για τα προϊόντα που επέλεξε και θα χρησιμοποιείται στο τέλος της συναλλαγής για να υπολογίσει το τελικό κόστος. Τέτοια cookies είναι παροδικά, ωστόσο υπάρχουν άλλα που είναι περισσότερο μόνιμα και μένουν στον δίσκο του χρήστη για πολύ καιρό. Μια συνηθισμένη χρήση τέτοιων cookies είναι να κρατάνε στοιχεία πιστωτικών καρτών για παράδειγμα ώστε να μην απαιτείται ο χρήστης να ξαναεισάγει τα στοιχεία του κάθε φορά που θέλει να κάνει μια συναλλαγή. Τα cookies είναι όμως απειλή για προσωπικά σας στοιχεία τα οποία πιθανόν δεν θέλετε να είναι γνωστά σε άλλους: είναι σχετικά εύκολο να μαζέψει κανείς στοιχεία σχετικά με τις συνήθειες σας, τις προτιμήσεις σας κ.λ.π. Αν αισθάνεστε άβολα με μια τέτοια κατάσταση υπάρχει απλή λύση: να απενεργοποιήσετε την επιλογή του browser σχετικά με την χρησιμοποίηση των cookie. Ωστόσο, αυτό μπορεί μερικές φορές να μην είναι βολικό καθώς πολλά sites θα απαιτούν τη χρήση των cookies.

Όταν ένας υπολογιστής ανοίγει μια σύνδεση με έναν άλλο χρησιμοποιώντας TCP/IP, ο πελάτης στέλνει ένα TCP πακέτο με έναν αρχικό ακέραιο αριθμό. Ο λαμβάνων υπολογιστής (ο διακομιστής) επιστρέφει ένα πακέτο το οποίο περιλαμβάνει έναν άλλο ακέραιο, οι αριθμοί αυτοί είναι γνωστοί ως αριθμοί ακολουθίας. Επίσης στέλνει μια επιβεβαίωση η οποία είναι ο αριθμός ακολουθίας του πελάτη συν ένα. Ο πελάτης στη συνέχεια πρέπει να επιστρέψει μια επιβεβαίωση η οποία περιλαμβάνει τον αριθμό του ακολουθίας του διακομιστή συν ένα. Από τη στιγμή αυτή, ο πελάτης και ο διακομιστής μπαίνουν σε μια διαδικασία διαλόγου στην οποία ο πελάτης και ο διακομιστής στέλνουν πακέτα τα οποία περιέχουν αριθμούς ακολουθίας τους οποίους η άλλη πλευρά πρέπει να επιστρέψει για να πιστοποιήσει ότι είναι αυτή που ισχυρίζεται. Οι αριθμοί ακολουθίας προσδιορίζονται από έναν αλγόριθμο του TCP/IP.

Το κύριο πρόβλημα για να επιτευχθεί το IP spoofing είναι ότι ο εισβολέας θα πρέπει να γνωρίζει τους αριθμούς ακολουθιών που δημιούργησε και έστειλε

ο διακομιστής κατά την αρχική εγκατάσταση της επικοινωνίας: ο διακομιστής θα λαμβάνει πακέτα από έναν υπολογιστή που ισχυρίζεται ότι έχει μια IP διεύθυνση αλλά τα πακέτα που στέλνει θα μεταφέρονται από το δίκτυο στον υπολογιστή που πραγματικά έχει την διεύθυνση αυτή και συνεπώς ο εισβολέας δεν θα παίρνει τις απαντήσεις για να δει τον αριθμό ακολουθίας που πρέπει να στείλει. Επειδή ο εισβολέας πρέπει να απαντήσει με πακέτα τα οποία περιέχουν τον κατάλληλο αριθμό ακολουθίας, κάθε πακέτο το οποίο θα λαμβάνεται στον διακομιστή και δεν περιέχει τον κατάλληλο αριθμό ακολουθίας θα θεωρείται ύποπτο και θα παρουσιάζεται το κατάλληλο μήνυμα.

Για να κάνει μια επίθεση IP spoofing, ο εισβολέας πρέπει να πετύχει τα εξής:

- Ο πραγματικός υπολογιστής που θα προσποιηθείτε ότι είστε πρέπει να είναι εκτός λειτουργίας. Αυτό συνήθως επιτυγχάνεται με μια επίθεση άρνησης υπηρεσίας.
- Ο υπολογιστής που θα χρησιμοποιηθεί για την επίθεση πρέπει να πάρει την IP διεύθυνση του υπολογιστή που θα προσποιηθεί ότι είναι.
- Ο υπολογιστής του εισβολέα τότε θα πρέπει να συνδεθεί με τον διακομιστή και να ξεκινήσει έναν διάλογο προσποιούμενος ότι είναι κάποιος άλλος υπολογιστής.
- Ο υπολογιστής του εισβολέα πρέπει με κάποιο τρόπο να ανακαλύψει τον αριθμό ακολουθίας που δημιούργησε ο διακομιστής. Αυτό είναι αρκετά δύσκολο αλλά όχι ακατόρθωτο. Σε μερικά τοπικά δίκτυα μπορεί επίσης να γίνει αρκετά εύκολα.

Μερικές φορές πάντως, οι αριθμοί ακολουθίας που φτιάχνει κάποιος ευάλωτος διακομιστής μπορούν να βρεθούν απλά με δοκιμή πολλών διαφορετικών σε μια σειρά πολλών διαφορετικών προσπαθειών για σύνδεση.

Συνήθως αφού κάποιος εισβολέας καταφέρει να μπει στο σύστημα, βρίσκει ένα πιο απλό και βολικό τρόπο για να συνεχίσει τη δραστηριότητα του, αλλάζοντας κάποιο password ή κάποια ρύθμιση στον διακομιστή κ.λ.π.

Αυτή είναι μια μόνο μορφή spoofing, υπάρχουν και άλλες. Το ARP spoofing για παράδειγμα. Τα αρχικά ARP σημαίνουν Address Resolution Protocol. Το πρωτόκολλο ARP είναι το κομμάτι του TCP/IP, που συνδέει φυσικές διευθύνσεις υπολογιστών (κάρτας δικτύου π.χ.) με IP διευθύνσεις. Το τμήμα του λειτουργικού συστήματος το οποίο αποθηκεύει τα απαραίτητα στοιχεία για να γίνεται η απαραίτητη μετατροπή διευθύνσεων είναι γνωστό ως ARP cache. Μια επίθεση ARP spoofing πραγματοποιείται μεταβάλλοντας την cache ώστε η IP διεύθυνση ενός υπολογιστή που ο διακομιστής εμπιστεύεται στην πραγματικότητα θα ισοδυναμεί με τη φυσική διεύθυνση του υπολογιστή του εισβολέα.

Άλλη μια μορφή spoofing είναι το DNS spoofing. Αυτό είναι μια λιγότερο σημαντική απειλή από τα δυο προηγούμενα καθώς μπορεί σχετικά εύκολα να εντοπιστεί. Ωστόσο, κάποιες επιθέσεις αυτού του είδους εξακολουθούν να συμβαίνουν ενίοτε. Σε μια επίθεση DNS spoofing μεταβάλλονται τα στοιχεία ενός DNS server ώστε να αντιστοιχεί το συμβολικό όνομα κάποιου υπολογιστή που εμπιστεύονται οι χρήστες στην IP διεύθυνση ενός υπολογιστή που χρησιμοποιείται από το άτομο που στήνει το κόλπο. Αυτό σημαίνει ότι οι υπολογιστές που θα προσπαθούν να συνδεθούν με τον υπολογιστή που εμπιστεύονται θα συνδέονται στην πραγματικότητα με κάποιον άλλο υπολογιστή, κατά τη διάρκεια της επικοινωνίας με τον οποίο θα μπορούσαν να αντληθούν σημαντικά δεδομένα. Για παράδειγμα θα μπορούσε ο χρήστης να δώσει τον αριθμό της πιστωτικής του κάρτας νομίζοντας πως πραγματικά η άλλη πλευρά θα το χρησιμοποιήσει απλά για να φέρει εις πέρας μια επιθυμητή συναλλαγή.

5.3.9 ΣΚΟΥΛΗΚΙΑ (WORMS)

Τα σκουλήκια (worms) είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντας τα ίδια ανεξέλεγκτα, αλλά συνήθως δεν προκαλούν άλλου τύπου επιπλοκές. Τα σκουλήκια μοιάζουν πολύ με τους

ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Πρόκειται για αυτόνομα προγράμματα τα οποία μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων. Για τη δημιουργία τους απαιτούνται ιδιαίτερες γνώσεις πρωτοκόλλων επικοινωνιών, ευπαθειών δικτυακών συστημάτων και ειδικών θεμάτων πάνω σε λειτουργικά συστήματα.

Μόλις ένα σκουλήκι μολύνει ένα σύστημα, αναζητεί δραστηριότητα για πιθανές συνδέσεις με άλλους υπολογιστές, οπότε αν βρει, αμέσως αντιγράφεται σε αυτούς. Όμως, πέρα από την συμπεριφορά αναπαραγωγής τους από σύστημα σε σύστημα, τα σκουλήκια συχνά εκτελούν και κακόβουλες πράξεις, που δεν περιορίζονται μόνο στην καταστροφή αρχείων. Έτσι, μέσω των δικτυακών συνδέσεων μπορούν να υποκλέψουν και να μεταφέρουν προς τους συγγραφείς τους πληροφορίες που αφορούν συνθηματικά χρηστών και άλλες ευαίσθητες αλλά και πολύτιμες πληροφορίες. Επιπλέον, μπορούν να επιφέρουν πλήρη αποδιοργάνωση των λειτουργιών ενός συστήματος ώστε να προκαλείται επίθεση άρνησης εξυπηρέτησης (denial of service). Αυτό συνήθως προκαλείται από παράλληλες και ανοργάνωτες επιθέσεις περισσότερων του ενός σκουληκιών στο ίδιο σύστημα.

Ακριβώς επειδή η μόλυνση από σκουλήκια επιτυγχάνεται μέσω δικτυακών συνδέσεων, είναι δύσκολος ο εντοπισμός των σημείων προσβολής. Για την αποφυγή της μόλυνσης από σκουλήκια επιβάλλεται ο εντοπισμός και η αντιμετώπιση όλων των ευπαθών σημείων του υπολογιστικού συστήματος από τους διαχειριστές του. Αυτό σημαίνει ότι ιδιαίτερα πρέπει να προσεχθούν τα αδύνατα σημεία όπως εύκολα συνθηματικά ή ανεξέλεγκτες δικτυακές υπηρεσίες που μπορούν να εκμεταλλευθούν τα σκουλήκια για να εισβάλλουν στο σύστημα από το δίκτυο και να το μολύνουν.

Ένας καλός τρόπος προφύλαξης από τα σκουλήκια είναι η γνώση των μεθόδων που χρησιμοποιούν για τον εντοπισμό και την αξιοποίηση των ευπαθών σημείων του συστήματος. Όπως γίνεται γενικότερα για την πρόληψη

εισβολών (intrusion prevention), η χρήση διατάξεων firewalls και ελέγχου προσπέλασης μπορούν να μειώσουν σημαντικά τους κινδύνους επίτευξης των στόχων των σκουληκιών.

5.3.10 PHISING

Ο όρος phising αναφέρεται στη διαδικασία "ψαρέματος" για λογαριασμούς και κωδικούς πρόσβασης, διαμορφώνοντας μια ψεύτικη διασύνδεση χρήστη, όπως μια ιστοθέση που φαίνεται ότι είναι πραγματική και στέλνοντας ένα μήνυμα e-mail που προσκαλεί χρήστες να συνδεθούν σε αυτή.

Για παράδειγμα, μπορεί να δεχθεί ένας χρήστης ένα μήνυμα e-mail, που δηλώνει ότι ο λογαριασμός του στην eBay πρέπει να ενημερωθεί για κάποιο λόγο. Κάνει κλικ στην ενσωματωμένη σύνδεση μέσα στο μήνυμα, και αυτό που φαίνεται μοιάζει με τη σελίδα εισδοχής στην eBay. Εισάγει το όνομα λογαριασμού και τον κωδικό πρόσβασής του και παίρνει ένα μήνυμα σφάλματος, που λέει ότι έχει πληκτρολογήσει τον κωδικό πρόσβασης λανθασμένα Όταν κάνει πάλι κλικ στη σύνδεση, εισέρχεται κανονικά και ενημερώνει τις πληροφορίες, όπως του ζητείται. Αυτό που συμβαίνει στην πραγματικότητα είναι ότι ένας εισβολέας του έστειλε ένα e-mail που περιείχε μια σύνδεση προς μια ιστοσελίδα, την οποία είχε δημιουργήσει αυτός, έτσι ώστε να μοιάζει σε εμφάνιση με την ιστοθέση της eBay. Όταν πληκτρολογήθηκε ο λογαριασμός χρήστη και ο κωδικός πρόσβασης, αυτά τα στοιχεία καταγράφτηκαν και μετά ανακατευθύνθηκε ο χρήστης στην κανονική ιστοσελίδα, οπότε τη δεύτερη φορά που εισήγαγε τον κωδικό πρόσβασης, αυτός δούλεψε σωστά.

Μια καλή διαδικασία ψαρέματος μπορεί να ψαρέψει χιλιάδες έγκυρους συνδυασμούς λογαριασμών και κωδικών πρόσβασης για ηλεκτρονικές ιστοθέσεις τραπεζών, ιστοθέσεις χρηματιστηριακών συναλλαγών ή κάθε τύπου ιστοθέσεις όπου διεξάγονται οικονομικές συναλλαγές.

Ακόμη, επειδή οι χρήστες γενικά χρησιμοποιούν τον ίδιο κωδικό πρόσβασης σε ιστοθέσεις με τις οποίες εργάζονται, οι εισβολείς μπορούν να μπουν εύκολα σε συστήματα εργασίας χρησιμοποιώντας κωδικούς πρόσβασης που έχουν ψαρέψει.

5.4 ΔΙΑΔΙΚΤΥΑΚΑ ΕΓΚΛΗΜΑΤΑ

Τα μέτρα για την ασφαλή πλοήγηση έχουν αφετηρία υπηρεσίες του παροχέα (provider) πρόσβασης στο διαδίκτυο. Ένας καλός παροχέας μπορεί να προσφέρει φιλτράρισμα των ιστοσελίδων που επισκέπτεται φιλτράρισμα των επισυναπτόμενων αρχείων στα e-mails που δέχεται ο χρήστης-πελάτης. Είναι ωστόσο συχνές οι περιπτώσεις κατά τις οποίες σελίδες που περιέχουν ακατάλληλο υλικό δεν περιέχουν τις λέξεις που φιλτράρουν τα προγράμματα αυτά ή δεν έχουν καταχωρηθεί στην μαύρη λίστα. Αντιθέτως, ιστοσελίδες που δεν περιέχουν ακατάλληλο υλικό μπορεί να απαγορεύονται επειδή περιέχουν λέξεις που φιλτράρει το πρόγραμμα. Σε αυτές τις περιπτώσεις είναι καλό ο χρήστης να ενημερώνει τον διαχειριστή του προγράμματος

(Cachemaster). Ωστόσο ακόμα και οι καλύτερες υπηρεσίες ενός παροχέα σύνδεσης δεν εξασφαλίζουν τον χρήστη από τους κινδύνους που ελλοχεύουν κατά την πλοήγηση αν ο ίδιος δεν λάβει τα κατάλληλα μέτρα προστασίας και δεν υιοθετήσει μια πολύ προσεκτική συμπεριφορά.

Ο βασικότερος κανόνας είναι η προσεκτική ανάγνωση όλων των μηνυμάτων που εμφανίζονται στην οθόνη του υπολογιστή. Ο χρήστης δε θα πρέπει σε καμία περίπτωση να κάνει κλικ στο «Ναι» ή το «Όχι» των παραθύρων χωρίς να διαβάζει το περιεχόμενό τους, ενώ θα πρέπει να κλείνει το παράθυρο χωρίς να κάνει κλικ, όταν δεν το καταλαβαίνει. Πολλές φορές κατά την πλοήγηση ανοίγουν, χωρίς να το προκαλέσει ο χρήστης, παράθυρα (pop up windows) των οποίων το περιεχόμενο ποικίλει. Αυτό μπορεί να είναι:

1. Διαφημίσεις.

2. Προειδοποιητικά μηνύματα που καλούν τον χρήστη να προβεί σε ενέργειες (αποδεχόμενος συγκεκριμένες προσφορές) με άγνωστες ή επικίνδυνες για αυτόν συνέπειες.
3. Κάλεσμα για παιγνίδια είτε κανονικά είτε τυχερά.
4. Δωρεές.
5. Δεσμοί σε σελίδες πορνογραφικού περιεχομένου και γενικά ποικιλία δελεαστικών προτάσεων.

Η ενδεδειγμένη ενέργεια είναι να κλείνουν άμεσα αυτά τα παράθυρα. Η εμφάνιση τέτοιων παραθύρων μπορεί να αποφευχθεί χρησιμοποιώντας κατάλληλα προγράμματα (pop up blockers/ killers), τα οποία προσφέρονται στο διαδίκτυο. Επισημαίνεται ότι η χρήση τέτοιων προγραμμάτων μπορεί να εμποδίσει την πρόσβαση σε κάποιες, χρήσιμες κατά τα άλλα, ιστοσελίδες. Μία τέτοια περίπτωση είναι αυτή κατά την οποία έγκυρες εταιρείες προσφέρουν μέσω pop up παραθύρων προγράμματα εφαρμογών απαραίτητα για τη σωστή εμφάνιση ενός πλήθους ιστοσελίδων (π.χ. Flash Player από την Macromedia, mwpluggin από την LCSI για το Microworlds κ.λ.π.). Σε αυτή την περίπτωση οι χρήστες μπορούν προσωρινά να απενεργοποιήσουν τον blocker.

5.4.1 ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ (E-MAIL).

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική και ταχύτατη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο, όμως ακόμα και σήμερα τα περισσότερα προγράμματα αποστολής και λήψης e-mail δεν εγγυώνται σε καμία περίπτωση τη διασφάλιση του προσωπικού απορρήτου του χρήστη ούτε και την ακεραιότητα της λειτουργίας του συστήματός του. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε

τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών.

Πιο συγκεκριμένα κύριος φορέας των μηνυμάτων e-mail είναι το πρωτόκολλο επικοινωνίας SMTP (Simple Mail Transfer Protocol). Το SMTP αναλαμβάνει τη μεταφορά μηνυμάτων από το μηχάνημα του χρήστη σε ένα διακομιστή αλληλογραφίας (mail server), καθώς και την προώθησή του από έναν mail server σε κάποιον άλλο. Κάθε εταιρεία παροχής ιντερνετικών υπηρεσιών (Internet Service Provider, ISP) διαθέτει έναν ή περισσότερους διακομιστές αλληλογραφίας, οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την αποστολή των μηνυμάτων. Όταν ένας χρήστης συνδέεται τηλεφωνικά (dialup) με τον ISP του, μπορεί να «κατεβάσει» την αλληλογραφία του από τον mail server του ISP στον υπολογιστή του, με τη βοήθεια του πρωτοκόλλου POP (Post Office Protocol) ή του IMAP (Internet Message Access Protocol). Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι ιδιαίτερα σημαντικό να διαχειριστεί τη διεύθυνση της ηλεκτρονικής του αλληλογραφίας με την ίδια προσοχή που διαχειρίζεται τον αριθμό του τηλεφώνου του. Μερικά από τα σημαντικότερα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

5.4.1.1 **ΙΟΙ**

Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι και ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο. Δε θα πρέπει λοιπόν οι χρήστες να

ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του e-mail. Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (στο outlook express επιλέξτε Προβολή->Διάταξη->απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»). Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

5.4.1.2 ΕΝΟΧΛΗΤΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ (SPAM MAIL).

Από τα πρώτα δυσάρεστα εμπόδια που κλήθηκαν (και καλούνται) να αντιμετωπίσουν οι χρήστες του Internet ήταν και είναι το spam mail. Τα τελευταία χρόνια, μάλιστα, έχει αποκτήσει και παρέα: τα διαδοχικά pop-up windows με διαφημιστικά banners που αφαιρούν από το web την βασική του γοητεία: την πλοήγηση. Είναι το λεγόμενο spam ή junk mail, δηλαδή μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ. ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Διαδικτύου και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Διαδικτύου και κινδυνεύει η ασφάλεια των δικτύων. Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην

απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα. Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος.

Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη. Ειδικότερα, το McAfee SpamKiller διακρίνεται από εξαιρετική δυνατότητα ανίχνευσης και παρεμπόδισης του spam mail, κάτι που οφείλεται στα προηγμένα τεχνολογικά "έξυπνα" φίλτρα που χρησιμοποιεί τα οποία με την σειρά τους βασίζονται σε συνδυασμούς κριτηρίων που αφορούν στον έλεγχο του περιεχομένου του μηνύματος, τη διεύθυνση του αποστολέα, το θέμα του μηνύματος, αλλά ακόμα και την προέλευσή του (χώρα προέλευσης, κόμβος - στοιχεία που προκύπτουν μέσα από την ανάλυση των headers του μηνύματος.

5.4.1.3 ΜΗΝΥΜΑΤΑ ΑΠΑΤΗΛΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ (HOAXES).

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

1. **«Προειδοποιητικά»:** είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα.

2. **«Συμπαράστασης»:** παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται.
3. **«Εκφοβισμού» :** οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες. Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως. Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know").

Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος. Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

5.4.1.4 ΤΡΟΠΟΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα e-mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού e-mail. Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail , οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

5.4.2 ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Σε μια ηλεκτρονική επικοινωνία η εμπιστοσύνη μεταξύ των συναλλασσόμενων μερών είναι πολύ σημαντική, για αυτό και θα πρέπει να δίδεται ιδιαίτερη έμφαση στο θέμα της ασφάλειας των συναλλαγών. Σήμερα, η τεχνολογία παρέχει πολύ προηγμένες λύσεις στο θέμα αυτό. Ένα ηλεκτρονικό κατάστημα που μεριμνά για την ασφάλεια των πελατών του θα πρέπει να χρησιμοποιεί και να αναφέρει ρητά όλα τα απαραίτητα συστήματα ασφάλειας καθώς και θα πρέπει να παρέχει τις απαραίτητες πληροφορίες για την πιστοποίηση της ταυτότητάς του. Όσον αφορά την ασφάλεια, ένα ηλεκτρονικό κατάστημα θα πρέπει να χρησιμοποιεί μια σειρά από «συστήματα ασφαλείας» προκειμένου να διασφαλίσει την ασφάλεια των συναλλαγών του, όπως:

1. Ένα ψηφιακό πιστοποιητικό ταυτότητας (digital ID) από κάποιο αναγνωρισμένο φορέα πιστοποίησης (οι ψηφιακές ταυτότητες επιβεβαιώνουν την ταυτότητα του συναλλασσόμενου εμπόρου)
2. Ένα πρωτόκολλο ασφαλείας (π.χ., Secure Socket Layer – SSL, ή Secure Electronic Transaction – SET).
3. Μια ασφαλή σύνδεση.

Οι έλεγχοι για την ασφάλεια και την εγκυρότητα του ηλεκτρονικού καταστήματος πρέπει να γίνονται ανεξάρτητα από το αν η πρόσβασή στο Διαδίκτυο γίνεται από τον υπολογιστή, από κινητό τηλέφωνο (π.χ. WAP) ή από την διαδραστική (interactive) τηλεόραση. Σε αυτή τη περίπτωση , οι ιδιοκτήτες ενός ηλεκτρονικού καταστήματος πρέπει να ζητούν ενημέρωση από ειδικούς για όλες τις δυνατές λύσεις και να επιλέγουν, με τη βοήθειά τους, τις πλέον κατάλληλες για την επιχείρησή τους.

Όσον αφορά την «ταυτότητα» του, ένα ηλεκτρονικό κατάστημα θα πρέπει να παρουσιάζει ρητά σε ποιόν ακριβώς έχει κατοχυρωθεί, δηλαδή ποιος είναι ο πραγματικός ιδιοκτήτης. Η ύπαρξη ενός ειδικού σήματος στην ιστοσελίδα που να πιστοποιεί την ταυτότητα (από γνωστούς δημόσιους ή ιδιωτικούς οργανισμούς) αποτελεί πλεονέκτημα. Επιπλέον, θα πρέπει να παρέχεται η δυνατότητα στον καταναλωτή, πριν προβεί σε αγορές, να επικοινωνήσει με τον τηλεφωνικό αριθμό στη φυσική έδρα του καταστήματος (είναι υποχρεωτική η αναγραφή του στην ιστοσελίδα) για να διαπιστώσει πως όντως πρόκειται για το κατάστημα που έχει επιλέξει.

Συνοπτικά, οι πληροφορίες που πρέπει να παρουσιάζει ένα ηλεκτρονικό κατάστημα στους καταναλωτές περιλαμβάνουν τα παρακάτω:

- Πραγματική ταυτότητα του εμπόρου (όνομα, γεωγραφική διεύθυνση, τηλέφωνο κ.λπ..)
- Τρόποι επικοινωνίας τόσο με ηλεκτρονικό όσο και με συμβατικό τρόπο (ηλεκτρονικό ταχυδρομείο [e-mail], fax, τηλέφωνο, κ.λπ..)

- Τελική τιμή του προϊόντος ή της υπηρεσίας συμπεριλαμβανομένων φόρων, εξόδων αποστολής, κ.λπ.
- Εγγύηση του προϊόντος.
- Μέθοδος αποστολής και χρόνος παράδοσης, δυνατότητα υπαναχώρησης, τρόπος
- πληρωμής και παράδοσης, κ.λπ..
- Τρόπος ακύρωσης της παραγγελίας σε περίπτωση λάθους ή αλλαγής γνώμης.
- Επιβεβαίωση της παραλαβής της παραγγελίας.
- Πληροφορίες για την προστασία των προσωπικών δεδομένων (privacy statement)
- Που να απευθυνθεί ο καταναλωτής για τα παράπονα του εάν κάτι δεν πάει καλά (π.χ. αργοπορημένη παράδοση ή καθόλου παράδοση).
- Πώς θα επιστραφεί το προϊόν, τι πρόσθετες επιβαρύνσεις υπάρχουν για την επιστροφή, κ.λπ.
- Ποιο δικαστήριο είναι αρμόδιο και ποιο Δίκαιο θα εφαρμοσθεί σε περίπτωση διαφοράς.

5.4.3 ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

Με τη συνεχώς αυξανόμενη εμπορευματοποίηση του Internet και τη χρήση του Web πολλές επιχειρήσεις έχουν οδηγηθεί στην υλοποίηση συστημάτων και μεθόδων ηλεκτρονικών πληρωμών προκειμένου να υποστηρίξουν πρακτικά την ανάπτυξη του ηλεκτρονικού εμπορίου στο σύγχρονο επιχειρησιακό περιβάλλον. Έτσι όχι μόνο δεν θεωρείται αρκετή η ανάπτυξη ηλεκτρονικών επιχειρήσεων χωρίς την ανάπτυξη και την εξέλιξη τέτοιων συστημάτων πληρωμών μέσα στο διαδίκτυο, αλλά είναι αδύνατο να υπάρξει ηλεκτρονικό εμπόριο χωρίς έναν τρόπο μεταφοράς χρηματικών πόρων

(πληρωμής) μέσω της ψηφιακής υποδομής. Στα πρώτα στάδια ανάπτυξης του ηλεκτρονικού εμπορίου οι πληρωμές γίνονταν εκτός του διαδικτύου με καταβολή των ποσών σε κάποια τράπεζα. Ο αναχρονιστικός όμως αυτός τρόπος χρηματικής εκκαθάρισης των διαδικτυακών συναλλαγών δε συμβάδιζε με την ταχύτητα και την αξιοπιστία που απαιτούν οι σύγχρονες διαδικτυακές συναλλαγές. Για το λόγο αυτό μια σειρά από συστήματα ηλεκτρονικών πληρωμών αναπτύχθηκε σταδιακά. Τα συστήματα αυτά είτε αποτελούσαν μια μεταφορά παραδοσιακών πρακτικών του πραγματικού κόσμου στο διαδίκτυο όπως είναι η περίπτωση on-line πληρωμών με πιστωτική κάρτα, είτε οι δημιουργοί τους προχώρησαν σε καινοτομικές λύσεις που εκμεταλλεύονται τα χαρακτηριστικά του διαδικτύου προκειμένου να προτείνουν πρωτοποριακές λύσεις όπως οι πληρωμές με ηλεκτρονικό χρήμα. Οι ηλεκτρονικές πληρωμές αποτελούν αναπόσπαστο τμήμα του ηλεκτρονικού εμπορίου.

Στη γενική του μορφή, ο όρος ηλεκτρονικές πληρωμές (electronic payments) περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες, ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις, οι οποίες εκτελούνται με τη μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας. Κάθε ηλεκτρονική πληρωμή γίνεται εξ αποστάσεως χωρίς τη φυσική παρουσία του πληρωτή και φυσικά δεν περιλαμβάνει μετρητά. Το περιεχόμενο αυτής της πληρωμής έχει τη μορφή κάποιου ψηφιακού οικονομικού μέσου (π.χ. κρυπτογραφημένους αριθμούς πιστωτικών καρτών, ηλεκτρονικές επιταγές, ή ψηφιακό χρήμα) το οποίο μέσο υποστηρίζεται από κάποιον χρηματοπιστωτικό οργανισμό, τράπεζα ή άλλον ενδιάμεσο φορέα.

Οι ηλεκτρονικές πληρωμές μπορούν να ταξινομηθούν σε τρεις κατηγορίες με βάση την τεχνολογία δικτύου που χρησιμοποιούν. Οι συναλλαγές αυτές μπορούν να πραγματοποιηθούν:

- **μέσω τηλεφώνου**: Οι πληρωμές μέσω του τηλεφωνικού δικτύου αποτελούν μια καινούργια μορφή ηλεκτρονικών πληρωμών. Στόχος είναι η εκμετάλλευση της υπάρχουσας τεχνικής υποδομής αλλά και της

σημαντικής διείσδυσης που έχει το τηλέφωνο ως τεχνολογία σε όλα τα κοινωνικά στρώματα. Πολλές επιχειρήσεις, τράπεζες αλλά και δημόσιες υπηρεσίες επιτρέπουν την εξόφληση λογαριασμών μέσω τηλεφώνου.

- **μέσω διαδικτύου**: Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η εύκολη πρόσβαση στο διαδίκτυο από την πλειοψηφία του καταναλωτικού κοινού, καθιστά τα εν λόγω συστήματα ηλεκτρονικών πληρωμών ιδιαίτερα σημαντικά στην ανάπτυξη του ηλεκτρονικού εμπορίου.
- **μέσω κινητής τηλεφωνίας (m–payments)**: Η ανάπτυξη τεχνολογιών όπως το WAP επιτρέπουν την εκτέλεση βασικών χρηματικών συναλλαγών από κινητές και ασύρματες συσκευές ανεξαρτήτως χώρου και χρόνου. Πρόκειται για ένα μέσο πιο αυτόνομο ενώ η ευρεία αποδοχή και χρήση του από το καταναλωτικό κοινό καθιστά το κινητό ηλεκτρονικό εμπόριο (m-commerce) ιδιαίτερα δημοφιλή.

5.4.4 ΣΤΗΝ ΑΜΕΣΗ ΣΥΝΟΜΙΛΙΑ (CHAT).

Το chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται «δωμάτιο επικοινωνίας» (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Το chat αποτελεί μια κοινωνική δραστηριότητα ιδιαίτερα δημοφιλή ανάμεσα στους νέους, διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο γνωριμίας με ανθρώπους απ' όλον τον κόσμο. Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου

προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό (όπως στην περίπτωση του δημοφιλούς IRC). Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις. Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όταν κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους. Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές, επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός internet-cafe, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδόφιλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι και η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς, όσο και από τους εκπαιδευτικούς.

5.4.5 ΣΤΟ ΔΙΑΜΟΙΡΑΣΜΟ ΑΡΧΕΙΩΝ

Είναι η δυνατότητα, που προσφέρει το Διαδίκτυο στους χρήστες του, να διαμοιράζονται αρχεία κάθε είδους. Πραγματοποιείται με προγράμματα (ελεύθερα ή με πληρωμή) όπως τα παρακάτω:

Προγράμματα για Windows: Aimster, Audio Galaxy, Bearshare, Gnotella, Gnucleus, Grokster, iMesh, KaZaa, Lime wire, Morpheus, Swap Nut,WinMX.

Προγράμματα για Mac: Aimster, Lime wire, Mactella.

Καθένα από τα ανωτέρω προγράμματα λειτουργεί έτσι ώστε να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή, σε όλους χρήστες, οι οποίοι είναι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα. Επομένως, κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία, στον δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας, σύγχρονη επικοινωνία μεταξύ υπολογιστών, γι' αυτό τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης (peer-to-peer) προγράμματα. Η ευρύτατη χρήση της δυνατότητας αυτής του Διαδικτύου οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείου (μουσικής, εικόνων, προγραμμάτων) με μηδαμινό κόστος για τον χρήστη. Η συγκέντρωση των ταυτόχρονα διασυνδεδεμένων χρηστών σε κάθε τέτοιο πρόγραμμα διαμοιρασμού αρχείων ανέρχεται σε μερικά εκατομμύρια. Δημιουργούνται έτσι μερικές από τις μεγαλύτερες διαδικτυακά πληθυσμιακές κοινότητες, μέσα στις οποίες διακινείται σχεδόν ανεξέλεγκτα κάθε είδους υλικό.

5.5 ΟΔΗΓΟΣ ΓΙΑ ΑΣΦΑΛΗ ΠΛΟΗΓΗΣΗ ΣΤΟ INTERNET

Λίγα είναι αυτά που δεν έχουν ειπωθεί-γραφτεί για την ασφάλεια προσωπικών δεδομένων και υπολογιστικών συστημάτων. Λίγα, όμως, είναι κι αυτά που έχουν γραφτεί ή ειπωθεί πάνω στα ίδια θέματα, που αποφεύγουν την υπερβολή και τον εντυπωσιασμό, παρουσιάζοντας παράλληλα πρακτική αξία και υψηλή χρηστικότητα για τον καθημερινό χρήστη.Σε ευαίσθητα και ταυτόχρονα "καυτά" θέματα όπως η ασφάλεια των δεδομένων, η προστασία της ανωνυμίας και η προάσπιση του ιδιωτικού απορρήτου, οι όποιες κινήσεις μας απαιτούν προσεκτικό σχεδιασμό και μεθοδικότητα. Η συχνή παρομοίωση ενός υπολογιστή συνδεδεμένου στο Internet με ένα αυτοκίνητο με ορθάνοιχτες

πόρτες και την μηχανή αναμμένη μπορεί να φαντάζει στα αυτιά ενός μέσου ή αν θέλετε ακόμα κι έμπειρου χρήστη με υπερβολή, ωστόσο δεν απέχει σημαντικά από την πραγματικότητα. Ο μόνος τρόπος για να είστε πραγματικά σίγουροι για την ασφάλεια του υπολογιστή σας δεν είναι ο χρονικός περιορισμός της σύνδεσης στο Διαδίκτυο στο απολύτως απαραίτητο, αλλά η απόλυτη αποχή από αυτό.

Το ζητούμενο, λοιπόν, δεν είναι η πλήρης διασφάλιση του απορρήτου των προσωπικών σας δεδομένων (απλά και μόνο γιατί κάτι τέτοιο αποτελεί ουτοπία) αλλά η προσπάθεια για την επίτευξη υψηλών ποσοστών ασφαλείας - γιατί όχι και του 99%! Τα "κλειδιά" για την ασφάλεια του ηλεκτρονικού υπολογιστή σας ή του δικτύου υπολογιστών σας στο σπίτι ή στο γραφείο δεν είναι άλλα από τα ειδικά προϊόντα ασφαλείας που καλύπτουν ένα ευρύ φάσμα αναγκών τόσο σε επίπεδο hardware όσο και σε επίπεδο λογισμικού (software). Ένας άλλος παράγοντας που καθορίζει το βαθμό επικινδυνότητας που παρουσιάζει ο (οι) υπολογιστής(-ές) σας είναι αυτός της διαθεσιμότητάς του, και ειδικότερα της ποιότητας και της ποσότητας αυτής.

Με απλά λόγια, το επισφαλές ενός υπολογιστή καθορίζεται όχι μόνο από το εάν αυτός είναι συνδεδεμένος σε ένα δίκτυο, αλλά και από το διάστημα που είναι συνδεδεμένος όπως επίσης και από την ταχύτητα της σύνδεσής του. Χωρίς να προχωρήσουμε (τουλάχιστον σε αυτό το σημείο σε τεχνικές λεπτομέρειες) σε γενικές γραμμές οι συνδέσεις που γίνονται με σταθερές IP διευθύνσεις (static IP ISDN, μισθωμένη γραμμή κ.λπ.) παρουσιάζουν μεγαλύτερη επικινδυνότητα από ότι οι συνήθεις PSTN dial up συνδέσεις. Για να αντιληφθείτε του λόγου του αληθές, απλά σκεφθείτε πως εάν έχετε σταθερή IP address και ένας hacker ή ένα script kiddie σας εντοπίσει (μια φορά) θα είναι σαν να γνωρίζει τη διεύθυνση του σπιτιού σας - ενώ το αντικλείδι κατά πάσα πιθανότητα θα το έχει ήδη στην διάθεσή του. Η χρήση personal firewalls, antivirus προγραμμάτων (δύο τουλάχιστον), εξειδικευμένων προγραμμάτων anti-trojan (ανάλογα με το ποιος trojan είναι σε "έξαρση" κάθε περίοδο) και λογισμικού προστασίας

προσωπικών δεδομένων είναι επιβεβλημένη. Αξίζει να σημειωθεί πως η καταπολέμηση των κινδύνων δεν τελειώνει με την εγκατάσταση δύο ή και περισσοτέρων προγραμμάτων ασφαλείας, αντιθέτως μόλις αρχίζει! Εκτός από την εγκατάσταση των προγραμμάτων απαιτείται διαρκής ενημέρωση και σωστή ρύθμιση, αλλιώς η ίδια η γραμμή προστασίας που επιχειρούμε να δημιουργήσουμε στο PC μας, μπορεί να στραφεί εναντίον μας. Κάτι άλλο που πρέπει να έχουμε υπόψη όσον αφορά στο θέμα "Ασφάλεια στον Η/Υ" είναι ότι, ως επί το πλείστον οι ψηφιακές επιθέσεις είναι απρόσωπες - δεν έχουν προσωπικό χαρακτήρα (με προφανή εξαίρεση τις επιθέσεις σε ιστοσελίδες). Οι hackers δεν έχουν κάτι εναντίον σας κι ούτε θέλουν το κακό σας, το μόνο που ζητούν είναι πρόσβαση στο υπολογιστή σας για διαφορετικούς λόγους ο καθένας (ψυχαγωγικούς ή εκπαιδευτικούς).

5.6 ΓΟΝΕΙΣ ΚΑΙ ΠΑΙΔΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τα τελευταία χρόνια, οι εξελίξεις στις Τεχνολογίες Επικοινωνιών και Πληροφορικής (ΤΕΠ) είναι δραματικές. Εμείς και τα παιδιά βομβαρδιζόμαστε καθημερινά με καινοτομίες που μόλις πριν από λίγα χρόνια έλειπαν από τη ζωή μας.

Ως γονείς, θυμηθείτε πότε ήταν η πρώτη φορά που μάθατε να χρησιμοποιείτε το Διαδίκτυο ή που στείλατε το πρώτο σας e-mail ή που συνομιλήσατε ηλεκτρονικά με κάποιους φίλους και σίγουρα θα αντιληφθείτε ότι για τους περισσότερους από εμάς αυτό έγινε πολύ πρόσφατα.

Σε αντίθεση με τα παιδιά που έχουν μεγαλώσει με αυτές τις τεχνολογίες, ένας γονέας σπάνια βρίσκει το χρόνο ή έχει το απαιτούμενο ενδιαφέρον να ενημερώνεται για τις τελευταίες εξελίξεις. Αποτέλεσμα είναι τα παιδιά, τις περισσότερες φορές, να βρίσκονται ένα βήμα μπροστά σε θέματα όπως το Διαδίκτυο.

Το Διαδίκτυο μπορεί να αποτελέσει για τα παιδιά ένα εξαιρετικό περιβάλλον για μάθηση, ενημέρωση, ψυχαγωγία, για να συνομιλήσουν με φίλους ή απλώς να χαλαρώσουν και να ερευνήσουν διάφορα θέματα. Μπορεί, όμως, το Διαδίκτυο, όπως και το καθημερινό μας περιβάλλον, να είναι και επικίνδυνο. Για παράδειγμα, όπως δε θα θέλατε τα παιδιά σας να συνομιλούν ή να συναντιούνται με άγνωστα άτομα στη καθημερινή τους ζωή, το ίδιο ισχύει και για το Διαδίκτυο. Πριν αφήσετε τα παιδιά να χρησιμοποιήσουν το Διαδίκτυο χωρίς την επιτήρησή σας, θα πρέπει να γνωρίζετε ορισμένα βασικά στοιχεία και κινδύνους που πιθανόν να αντιμετωπίσουν στον κυβερνοχώρο. Ένας από τους μεγαλύτερους κινδύνους είναι οι επιτήδειοι χρήστες που εκμεταλλεύονται την ανωνυμία που προσφέρει το Διαδίκτυο.

<u>Πώς μπορούν οι γονείς να μειώσουν τον κίνδυνο</u>

- Μιλήστε στο παιδί σας σχετικά με τους σεξουαλικούς διαφθορείς και τους πιθανούς κινδύνους που κρύβει το Διαδίκτυο.
- Τα νεαρά παιδιά δεν πρέπει να χρησιμοποιούν τα δωμάτια συνομιλίας, οι κίνδυνοι είναι εξαιρετικά μεγάλοι. Καθώς τα παιδιά μεγαλώνουν, καθοδηγήστε τα προς καλά επιβλεπόμενα δωμάτια συζητήσεων για παιδιά. Προτρέψτε ακόμη και τους έφηβους να χρησιμοποιούν επιβλεπόμενα δωμάτια συνομιλιών.
- Εάν τα παιδιά σας συμμετέχουν σε δωμάτια συνομιλιών, φροντίστε να γνωρίζετε ποια επισκέπτονται και με ποιον συζητούν. Παρακολουθήστε κι εσείς οι ίδιοι τις περιοχές αυτές για να δείτε το είδος των συζητήσεων που διεξάγονται.
- Πείτε στα παιδιά σας ποτέ να μη φεύγουν από τη δημόσια περιοχή του δωματίου συνομιλίας. Πολλά δωμάτια συνομιλίας διαθέτουν προσωπικές περιοχές όπου οι χρήστες μπορούν να έχουν συζητήσεις ένας προς έναν με άλλους χρήστες. Τα προγράμματα επίβλεψης δεν μπορούν να

διαβάσουν αυτές τις συζητήσεις. Αυτές οι περιοχές αναφέρονται συνήθως και ως περιοχές “ψιθύρων”.

- Εγκαταστήστε τον υπολογιστή που είναι συνδεδεμένος με το Διαδίκτυο σε έναν κοινόχρηστο χώρο του σπιτιού, ποτέ στο υπνοδωμάτιο του παιδιού. Είναι πολύ δυσκολότερο για έναν διαφθορέα να δημιουργήσει μια σχέση με το παιδί σας, εάν η οθόνη του υπολογιστή είναι εύκολα ορατή από άλλους. Ακόμη κι όταν ο υπολογιστής βρίσκεται σε κοινόχρηστο χώρο του σπιτιού σας, να κάθεστε μαζί με το παιδί σας όταν αυτό συνδέεται στο Διαδίκτυο.
- Όταν τα παιδιά σας είναι νεαρά, θα πρέπει να χρησιμοποιούν τη διεύθυνση ηλεκτρονικού ταχυδρομείου της οικογένειας, αντί να έχουν προσωπικό λογαριασμό. Καθώς μεγαλώνουν, μπορείτε να ζητήσετε από τον παροχέα υπηρεσιών Διαδικτύου να δημιουργήσει μια ξεχωριστή διεύθυνση ηλεκτρονικού ταχυδρομείου, αλλά η αλληλογραφία του παιδιού σας θα συνεχίσει να βρίσκεται στο δικό σας λογαριασμό.
- Πείτε στα παιδιά να μην απαντούν ποτέ σε άμεσα μηνύματα ή σε μηνύματα ηλεκτρονικού ταχυδρομείου από ξένους. Εάν τα παιδιά σας χρησιμοποιούν υπολογιστές σε χώρους εκτός της επίβλεψής σας-σε δημόσιες βιβλιοθήκες, στο σχολείο ή στα σπίτια φίλων, μάθετε ποια προστατευτικά μέτρα χρησιμοποιούνται στους υπολογιστές.
- Εάν όλες οι προφυλάξεις αποτύχουν και τα παιδιά σας συναντήσουν κάποιον διαδικτυακό διαφθορέα, μην τα κατηγορήσετε. Η ευθύνη είναι αποκλειστικά του διαφθορέα. Δράστε αποφασιστικά, ώστε να σταματήσετε την περαιτέρω επαφή του παιδιού σας με αυτό το άτομο.

<u>Πώς μπορούν τα παιδιά να μειώσουν τον κίνδυνο</u>

Υπάρχουν ορισμένες προφυλάξεις που μπορούν να πάρουν τα παιδιά σας, στις οποίες περιλαμβάνονται:

- Ποτέ να μη μεταφορτώνουν εικόνες από άγνωστη πηγή, μπορεί να είναι σεξουαλικά ακατάλληλες.
- Να χρησιμοποιούν φίλτρα ηλεκτρονικού ταχυδρομείου.
- Να ενημερώσουν αμέσως έναν ενήλικα, εάν κάτι που συμβαίνει στο Διαδίκτυο κάνει κάποιο παιδί να νιώσει άβολα ή να φοβηθεί.
- Να διαλέξουν ένα αναγνωριστικό όνομα που να μην αποκαλύπτει το γένος και να μην περιέχει λέξεις με σεξουαλικά υπονοούμενα ή να αποκαλύπτει προσωπικά δεδομένα.
- Ποτέ και σε κανένα να μην αποκαλύπτουν προσωπικά δεδομένα στο Διαδίκτυο για τους εαυτούς τους (συμπεριλαμβανομένων της ηλικίας και του φύλου) ή στοιχεία σχετικά με την οικογένεια. Ποτέ να μη συμπληρώνουν ηλεκτρονικές φόρμες προσωπικών στοιχείων.
- Να διακόπτουν κάθε επικοινωνία με ηλεκτρονικό ταχυδρομείο, συζητήσεις με άμεσα μηνύματα ή συνομιλίες εάν κάποιος αρχίσει να κάνει ερωτήσεις πολύ προσωπικές ή με σεξουαλικό υπονοούμενο.

Τι μπορείτε να κάνετε εάν το παιδί γίνει στόχος

- Εάν το παιδί σας λαμβάνει σεξουαλικά ακατάλληλες φωτογραφίες από κάποια διαδικτυακή επαφή, ή εάν λαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, άμεσα μηνύματα ή με κάποιον άλλο ηλεκτρονικό τρόπο, σεξουαλικά υπονοούμενα, καλέστε την αστυνομία. Αποθηκεύστε τυχόν στοιχεία, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις διαδικτυακών τοποθεσιών και μητρώα συνομιλιών για να τα δώσετε στην αστυνομία.

- Ελέγξτε τον υπολογιστή σας για αρχεία με πορνογραφικό υλικό ή κάποιο τύπο σεξουαλικής επικοινωνίας, αυτά αποτελούν συνήθως προειδοποιητικές ενδείξεις.
- Παρακολουθήστε την πρόσβαση του παιδιού σας σε μέσα ζωντανής ηλεκτρονικής επικοινωνίας, όπως τα δωμάτια συνομιλιών, τα άμεσα μηνύματα και το ηλεκτρονικό ταχυδρομείο. Οι διαδικτυακοί διαφθορείς συνήθως συναντούν τα υποψήφια θύματα σε δωμάτια συνομιλιών και, στη συνέχεια, επικοινωνούν μέσω ηλεκτρονικού ταχυδρομείου ή άμεσων μηνυμάτων.

Το Διαδίκτυο παρέχει ανεξάντλητους πόρους και ευκαιρίες μάθησης. Περιέχει, όμως, και πάρα πολλές πληροφορίες που μπορεί να μην είναι ούτε ωφέλιμες ούτε αξιόπιστες. Καθώς ο καθένας μπορεί να δημοσιεύσει σχόλια ή πληροφορίες στο Διαδίκτυο, οι χρήστες θα πρέπει να αναπτύξουν ικανότητες κριτικής σκέψης, ώστε να κρίνουν την ακρίβεια των πληροφοριών αυτών.

Αυτό ισχύει ιδιαίτερα για τα παιδιά, που συνήθως πιστεύουν πως "Εάν είναι στο Διαδίκτυο, πρέπει να είναι αλήθεια". Παραδοσιακά, οι έντυπες πηγές είχαν τους φύλακές τους, τους επιμελητές και τους διορθωτές που διόρθωναν τα λάθη και διέγραφαν τις ψευδείς και ανακριβείς πληροφορίες. Ωστόσο, το Διαδίκτυο, σε πολλές περιπτώσεις δεν διαθέτει ασφαλιστικές δικλείδες για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται. Μάθετε στα παιδιά σας πώς λειτουργεί το Διαδίκτυο και εξηγήστε τους ότι ο καθένας μπορεί να δημιουργήσει μια διαδικτυακή τοποθεσία, χωρίς να τον ελέγχει κανείς. Μάθετε τα παιδιά σας να χρησιμοποιούν μεγάλο εύρος πηγών πληροφοριών και να ελέγχουν, να αμφισβητούν και να διασταυρώνουν όσα βλέπουν στο Διαδίκτυο.

Γενικές συμβουλές ασφάλειας

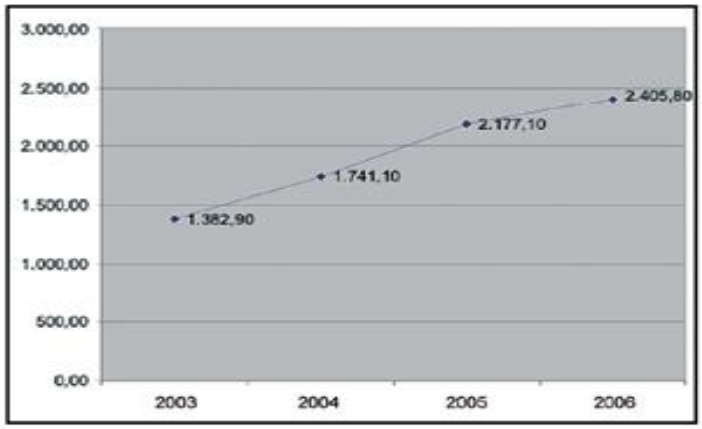
- Τοποθετήστε τους υπολογιστές με πρόσβαση στο Διαδίκτυο σε ανοικτό χώρο, από όπου μπορείτε εύκολα να επιβλέψετε τις δραστηριότητες του παιδιού σας, ιδίως για παιδιά σε μικρότερες ηλικίες.
- Συμβουλεύετε τα παιδιά σας να χρησιμοποιούν φιλικά προς σε αυτά ιστοσελίδες όπως το MSN Kids και το whatsup.com.cy.
- Διερευνήστε τα εργαλεία φιλτραρίσματος του Διαδικτύου (όπως τα εργαλεία γονικού ελέγχου του MSN Premium) ως συμπληρώματα, όχι υποκατάστατα, της γονικής επίβλεψης.
- Ενθαρρύνετε τα παιδιά σας να σας ενημερώνουν εάν κάτι ή κάποιος στο Διαδίκτυο τα κάνει να νιώθουν άβολα ή τα απειλεί. Διατηρήστε τη ψυχραιμία σας και υπενθυμίστε στα παιδιά σας ότι δε θα τιμωρηθούν εάν σας ενημερώσουν για κάτι (σημαντικό είναι να μη νομίζουν τα παιδιά ότι θα τους στερήσετε το δικαίωμα χρήσης του υπολογιστή).

5.7 ΕΚΘΕΣΗ ΠΕΠΡΑΓΜΕΝΩΝ ΕΤΟΥΣ 2006

Η προστασία των πληροφοριακών συστημάτων είναι ζωτικής σημασίας για την εύρυθμη λειτουργία οργανισμών και επιχειρήσεων. Πριν από λίγα χρόνια, η ασφάλεια των δικτύων αποτελούσε, κατά κύριο λόγο, θέμα των κρατικών μονοπωλίων που παρείχαν εξειδικευμένες πληροφορίες μέσω δημοσίων δικτύων, ιδίως του δικτύου τηλεφωνίας. Η ασφάλεια των συστημάτων πληροφορικής περιοριζόταν στους μεγάλους οργανισμούς και εστιαζόταν στον έλεγχο πρόσβασης. Σήμερα, η κατάσταση έχει μεταβληθεί σημαντικά. Σε αυτό συνετέλεσαν διάφορες εξελίξεις, όπως η απελευθέρωση των τηλεπικοινωνιών, η σύγκλιση των δικτύων και των συστημάτων πληροφοριών, καθώς και το γεγονός ότι σημαντικό πλέον μέρος των επικοινωνιών διεξάγεται διασυνοριακά ή μέσω τρίτων χωρών.

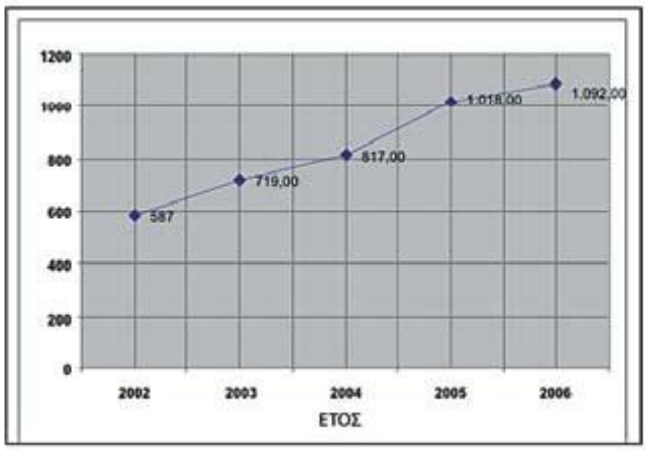
Παράλληλα, η πληροφορική έχει δημιουργήσει παγκόσμια διασυνδεσιμότητα, φέροντας σε επαφή εκατομμύρια δικτύων με εκατοντάδες εκατομμύρια μεμονωμένους προσωπικούς υπολογιστές, οι οποίοι αυξάνονται συνεχώς. Επίσης, η πληροφορική υποστηρίζει υποδομές μεγάλης σημασίας για μια χώρα, όπως εγκαταστάσεις ενέργειας και μεταφορών και τα μεγάλα χρηματοπιστωτικά ιδρύματα. Επιπλέον, παίζει σημαντικό ρόλο στη διοίκηση του σύγχρονου κράτους, των μεγάλων και μικρών επιχειρήσεων και στην παροχή υπηρεσιών στον πολίτη. Τα παραπάνω έχουν ως συνέπεια, ο όγκος των πληροφοριών που διακινείται τόσο στο διαδίκτυο όσο και στην τηλεφωνία να έχει εκτιναχθεί στα ύψη. Αυτό γίνεται αντιληπτό, αν παρατηρήσει κανείς τη σημαντική αύξηση των συνδρομητών στην κινητή τηλεφωνία παγκοσμίως (Εικόνα 1), των χρηστών διαδικτύου (Εικόνα 2), καθώς και των ευρυζωνικών συνδέσεων (Εικόνα 3) .

Εικόνα 1: Συνδρομητές Κινητής Τηλεφωνίας Παγκοσμίως (σε εκ.)



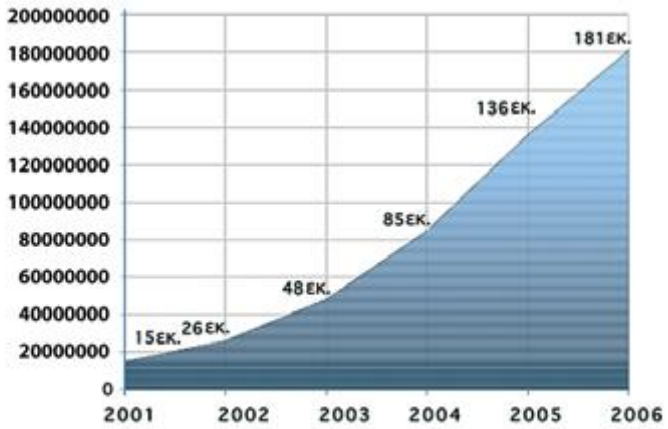
Πηγή: GSM Association

Εικόνα 2: Χρήστες Διαδικτύου Παγκοσμίως (σε εκ.)



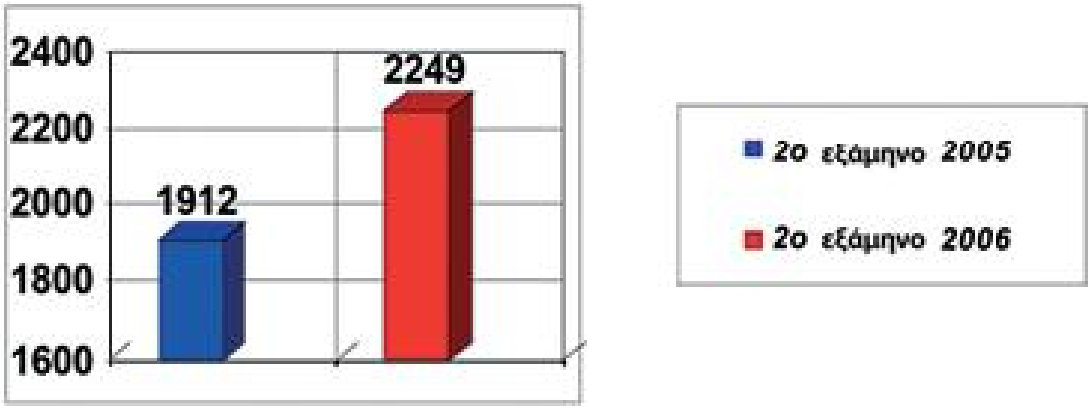
Πηγή: Internet World Statistics

Εικόνα 3: Αριθμός Ευρυζωνικών Συνδέσεων Χωρών Ο.Ο.Σ.Α.



Πηγή: Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη
Στοιχεία Έκθεσης Ιουνίου 2006

Εξαιτίας της πληθώρας των πληροφοριών και της μεγάλης ταχύτητας διακίνησής τους, τα πληροφοριακά συστήματα και τα δίκτυα είναι πλέον εκτεθειμένα σε πλήθος κινδύνων, οι οποίοι αυξάνονται σημαντικά από χρόνο σε χρόνο (Εικόνα 4) και μπορούν σήμερα να εξαπλώνονται σε ελάχιστο χρόνο, σε όλο τον κόσμο, μέσω των δικτύων πληροφοριών. Σ' αυτούς εντάσσονται, κυρίως, οι παραβιάσεις του προσωπικού απορρήτου, η βιομηχανική κατασκοπία, η κακόβουλη πρόσβαση στα αρχεία των υπολογιστών, η εισαγωγή ιών στους υπολογιστές, η δικτυακή τρομοκρατία, ο ηλεκτρονικός πόλεμος κ.λπ.

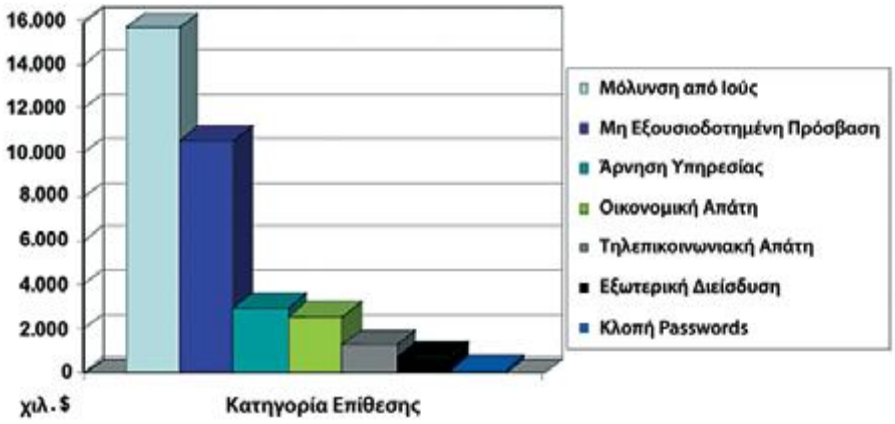


Πηγή: «Symantec Internet Security Threat Report», Σεπτέμβριος 2006.

Εικόνα 4: Εξέλιξη αριθμού κινδύνων ασφάλειας στο Διαδίκτυο

Επιπλέον, το κόστος που απαιτείται για την πρόσβαση σε πολύτιμες πληροφορίες είναι πλέον μικρό. Είναι προφανές ότι κακόβουλες προσβάσεις στα αρχεία υπολογιστών μπορούν να δημιουργήσουν τεράστια προβλήματα στην εθνική ασφάλεια, κυκλοφοριακό χάος στην εναέρια ή επίγεια κυκλοφορία, σοβαρές διακοπές στη διανομή ηλεκτρικής ενέργειας, αλλά και οικονομικό χάος, ανάλογα σε ποια δίκτυα θα υπάρξει η κακόβουλη πρόσβαση (Εικόνα 5).

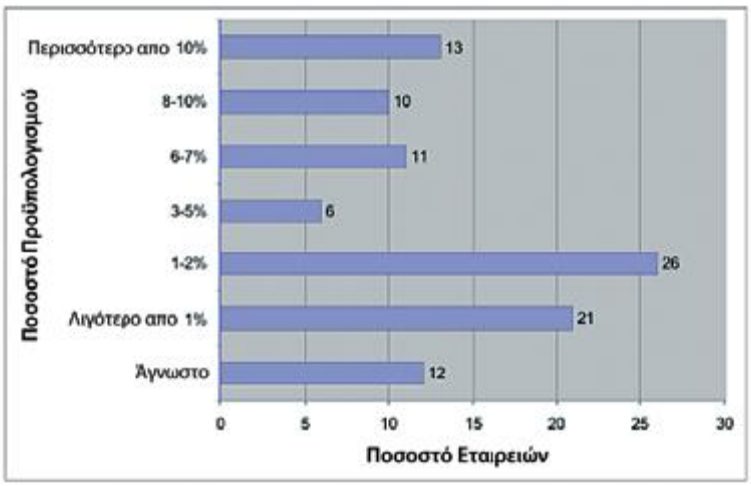
Εικόνα 5: Οικονομικές Απώλειες ανά Κατηγορία Επίθεσης



Πηγή: CSI/FBI Computer Crime and Security Survey, (δείγμα 613 εταιρειών) «Computer Security Institute», Δεκέμβριος 2006.

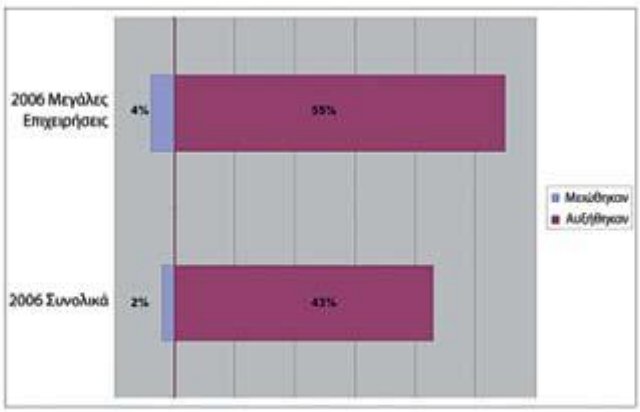
Αναμφίβολα, η ασφάλεια δικτύων και συστημάτων πληροφοριών αυξάνει την αίσθηση ελεύθερης δράσης των πολιτών, δημιουργεί νέες επιχειρηματικές ευκαιρίες και μειώνει το κόστος λειτουργίας μιας σύγχρονης επιχείρησης, της οποίας δραστηριότητες απαιτούν πολλαπλές διασυνδέσεις με τα δίκτυα επικοινωνιών. Αυτός είναι και ο λόγος, για τον οποίον οι εταιρείες, ιδιαίτερα οι μεγαλύτερες, επενδύουν συνεχώς, στην ενίσχυση της ασφάλειας των δικτύων τους με όλο και μεγαλύτερα ποσά. Σύμφωνα με έρευνα του CSI/FBI (Εικόνες 6, 7), το 13% των εταιρειών επενδύουν πάνω από το 10% του προϋπολογισμού τους στην ασφάλεια των δικτύων τους, ενώ το 55% των μεγάλων εταιρειών αύξησαν το 2006 τις δαπάνες τους για την ασφάλεια σε σχέση με την προηγούμενη χρονιά.

Εικόνα 6: Ποσοστό προϋπολογισμού πληροφορικής εταιρειών που δαπανάται για την ασφάλεια



Πηγή: CSI/FBI Computer Crime and Security Survey, (δείγμα 613 εταιρειών) «Computer Security Institute», Δεκέμβριος 2006.

Εικόνα 7: Αύξηση δαπανών για την ασφάλεια πληροφοριών



Πηγή: DTI, Information Security Breaches Survey, 2006 – Technical Report

Οι οργανισμοί, επίσης, δαπανώντας μόνο μικρό μέρος του προϋπολογισμού τους για την ασφάλεια δικτύων και πληροφοριών, προστατεύονται από πλήθος απωλειών που θα μπορούσαν να προκληθούν από κακόβουλες επιθέσεις. Γενικά, σε συνθήκες ασφάλειας αυξάνεται η αξιοποίηση

του διαδικτύου, γεγονός που έχει ως επακόλουθο τη μείωση του κόστους παραγωγής και διάθεσης προϊόντων, δεδομένου ότι βελτιώνεται η παραγωγικότητα και ο ανταγωνισμός, μηδενίζονται οι αποστάσεις και δημιουργούνται νέες αγορές και επιχειρηματικές ευκαιρίες.

Η ασφάλεια των δικτύων και πληροφοριών αναφέρεται αφενός στην προστασία οποιασδήποτε μορφής ηλεκτρονικών υπηρεσιών και συστημάτων, χρησιμοποιώντας τον κατάλληλο τεχνικό εξοπλισμό και λογισμικό, αφετέρου στη διαφοροποίηση της συμπεριφοράς των απλών χρηστών, οι οποίοι έχοντας συνειδητοποιήσει τους κινδύνους, λαμβάνουν τα απαραίτητα μέτρα για την προστασία του δικού τους υπολογιστή. Θα πρέπει ωστόσο να επισημανθεί ότι, επειδή ο τομέας των ηλεκτρονικών επικοινωνιών και εφαρμογών χαρακτηρίζεται από εξαιρετική δυναμική, οι τεχνολογικές εξελίξεις είναι συνεχείς και συχνά ανατρεπτικές. Συνεπώς, επιβάλλεται η διαρκής παρακολούθηση των συντελουμένων μεταβολών, ώστε να λαμβάνονται περαιτέρω μέτρα για την αποτροπή των νέων κινδύνων, όταν διαπιστώνεται σχετική ανάγκη.

6. ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ – ΕΜΠΟΡΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Τα τελευταία χρόνια ολοένα και μεγαλύτερος αριθμός εμπορικών συναλλαγών γίνεται μέσω του Διαδικτύου (Internet). Η δραστηριότητα αυτή είναι γνωστή ως ηλεκτρονικό εμπόριο. Το ηλεκτρονικό εμπόριο, ανάμεσα στα άλλα, περιλαμβάνει τραπεζικές εργασίες πραγματικού χρόνου (on- line banking), χρηματιστηριακές συναλλαγές, αγορά και πώληση αγαθών μέσω του Διαδικτύου. Κάθε καταναλωτής, χρησιμοποιώντας τη πιστωτική του κάρτα, μπορεί για παράδειγμα να αγοράσει ένα βιβλίο να κάνει κράτηση αεροπορικών εισιτηρίων, να νοικιάσει αυτοκίνητο, να κλείσει δωμάτια σε ξενοδοχεία ενώ κάθεται απλά στον υπολογιστή του (ή απλά χρησιμοποιώντας το κινητό του τηλέφωνο στο λεγόμενο M – commerce).

6.1 ΟΡΙΣΜΟΣ- ΕΝΝΟΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Η προσπάθεια ορισμού του ηλεκτρονικού εμπορίου είναι αρκετά δύσκολη λόγω της πληθώρας των εφαρμογών του και των διαφορετικών πεδίων χρήσης του . Σύμφωνα με ορισμένους συγγραφείς , όπως ο P. McKeon το ηλεκτρονικό εμπόριο είναι η χρήση δικτύων υπολογιστών (computer networks) προς τη βελτίωση της επιχειρησιακής επίδοσης. Άλλοι συγγραφείς αναφέρονται σε «οποιαδήποτε μορφή επιχειρησιακής συναλλαγής στην οποία τα μέρη που λαμβάνουν μέρος αλληλεπιδρούν ηλεκτρονικά και όχι μέσω φυσικών ανταλλαγών .

Εμείς ορίζοντας το απλά θα μπορούσαμε να πούμε ότι :

Το ηλεκτρονικό εμπόριο είναι η επικοινωνία και η σύναψη εμπορικών συναλλαγών μεταξύ επιχειρήσεων ή μεταξύ επιχειρήσεων και των πελατών τους , με τη χρήση ηλεκτρονικών μέσων.

Το πρόβλημα όμως με αυτό τον ορισμό είναι ότι δεν περικλείει τη φιλοσοφία του ηλεκτρονικού εμπορίου , η οποία είναι ο επανακαθορισμός του τρόπου με τον οποίο γίνονται οι εμπορικές συναλλαγές , και η οποία έχει ως στόχο την αμοιβαία ωφέλεια των επιχειρήσεων και των πελατών τους . Και αυτό συμβαίνει διότι η έννοια του ηλεκτρονικού εμπορίου σήμερα έχει επεκταθεί σημαντικά σε σχέση με την προηγούμενη δεκαετία . Περιλαμβάνει οποιαδήποτε επιχειρηματική δραστηριότητα μεταξύ επιχειρηματικών εταίρων διαμέσου ηλεκτρονικού δικτύου , κυρίως διαμέσου του Internet , και οδηγεί στην αγορά ή την πώληση αγαθών και υπηρεσιών . Η κύρια εξέλιξη μπορεί να εντοπισθεί στην μετατόπιση από την έννοια της ηλεκτρονικής συναλλαγής (στιγμιαία , περιορισμένη , δομημένη) σε αυτή της ηλεκτρονικής συνεργασίας με χρήση πληροφοριακών και επικοινωνιακών συστημάτων , τα οποία περιλαμβάνουν κείμενα , ήχο , και εικόνα . Σύμφωνα με την ευρωπαϊκή Commission , στο πλαίσιο αυτό εμπίπτουν διάφορες δραστηριότητες , όπως ηλεκτρονική εμπορία αγαθών και υπηρεσιών , παράδοση ψηφιακού περιεχομένου μέσω δικτύου (on-line) , ηλεκτρονική μεταφορά κεφαλαίων , ηλεκτρονικές αγοραπωλησίες μετοχών , ηλεκτρονικές φορτωτικές ψηφιακός σχεδιασμός , ηλεκτρονικές δημοπρασίες , δημόσιες προμήθειες , απευθείας εμπορική προώθηση προϊόντων , εξυπηρέτηση μετά την πώληση , κ.λ.π..

Οι υπηρεσίες του ηλεκτρονικού εμπορίου περιλαμβάνουν τόσο τη διάθεση προϊόντων όσο και την παροχή υπηρεσιών , αλλά και τη δωρεάν προσφορά πληροφοριών (π.χ. ξεφύλλισμα ιστοσελίδων στον Παγκόσμιο ιστό και μηχανές αναζήτησης) η οποία χρηματοδοτείται από τη διαφήμιση . Έτσι , στο πλαίσιο του ηλεκτρονικού εμπορίου εμπίπτουν παραδοσιακές (π.χ. εκπαίδευση) αλλά και καινοτομικές δραστηριότητες (π.χ. «εικονικά» πολυκαταστήματα) , οι οποίες δε νοούνται σε μη ηλεκτρονικό περιβάλλον .

Έχοντας ορίσει το ηλεκτρονικό εμπόριο ας δούμε τώρα τη διαφορά του με το ηλεκτρονικό επιχειρείν . Το πρώτο περιλαμβάνει την έννοια της συναλλαγής χρημάτων και αγαθών μεταξύ δύο ή περισσοτέρων μερών . Η

έννοια όμως του ηλεκτρονικού επιχειρείν είναι ευρύτερη γιατί περιέχει και άλλες έννοιες και δραστηριότητες , όπως την ανταλλαγή πληροφοριών και ιδεών ενδο-εταιρικά ή με συνεργάτες της εταιρίας , την εύρεση προσωπικού , την προσέλκυση επενδυτών , τη βελτιστοποίηση διαδικασιών κ.α. Τέλος , η αντίληψη ότι το ηλεκτρονικό εμπόριο αφορά μόνο τη χρήση του Internet στο εμπορικό κύκλωμα αγοράς – πώλησης θεωρείται πλέον ξεπερασμένη . Ο πολλαπλασιασμός των διαφόρων ειδών ψηφιακών δικτύων , η σύγκλιση ψηφιακών τεχνολογιών , η δημιουργία ψηφιακού περιεχομένου και υπηρεσιών καθώς και τα νέα αναπτυσσόμενα επιχειρηματικά μοντέλα , αποτελούν πλέον το περιβάλλον του ηλεκτρονικού επιχειρείν .

Το ηλεκτρονικό εμπόριο χωρίζεται επίσης σε «ολικό» και «μερικό» . το ηλεκτρονικό εμπόριο περιγράφεται με τρεις παραμέτρους : το προϊόν , τη διαδικασία της παραγγελιοδοσίας – παραγγετοληψίας και εκτέλεσης και τα συμβαλλόμενα μέρη . Όταν το προϊόν είναι ηλεκτρονικής μορφής (π.χ. λογισμικό) η διαδικασία γίνεται ηλεκτρονικά (χωρίς παρεμβολή ανθρώπινου παράγοντα) και τα συμβαλλόμενα μέρη που αποφασίζουν για την αγοραπωλησία είναι επίσης προγράμματα που ονομάζονται έξυπνοι πράκτορες , τότε ολικό ή καθαρό ηλεκτρονικό εμπόριο . Όταν το προϊόν δεν έχει ηλεκτρονική μορφή ή υπάρχει ανθρώπινη παρεμβολή , τότε μιλάμε για μερικό ηλεκτρονικό εμπόριο .

Τέλος , το ηλεκτρονικό εμπόριο χωρίζεται σε δυο σκέλη : Στη διαδικτυακή αγορά και στη διαδικτυακή έρευνα αγοράς . Η πρώτη αφορά την τεχνολογική υποδομή που απαιτείται για την ανταλλαγή στοιχείων και την αυτόματη υποστήριξη όλων των διαδικασιών που χρειάζονται για την αγορά ενός προϊόντος στο Internet . Η δεύτερη αφορά τη συλλογή των πληροφοριών και των υπολοίπων διαδικασιών που πρόκειται να ληφθούν για την επιλογή ενός προϊόντος. Δηλαδή πιο απλά :

Αν αποφασίσετε να πάτε σε ένα εμπορικό κέντρο για να βρείτε ένα πουκάμισο, σίγουρα θα επισκεφθείτε αρκετά καταστήματα . Η διερεύνηση αυτή

θα περιλαμβάνει έλεγχο της ποιότητας , του μεγέθους , του χρώματος και της τιμής διαφορετικών προϊόντων σε διαφορετικά καταστήματα . Μόλις αποφασίσετε να το αγοράσετε , το τοποθετείτε στο καλάθι σας και συνεχίζετε τις αγορές σας στο συγκεκριμένο κατάστημα . Αφού έχει ολοκληρωθεί η διαδικασία διερεύνησης και επιλογής , πηγαίνετε στο ταμείο του καταστήματος . Για την πληρωμή σας , μπορείτε ακόμη να δώσετε και την πιστωτική σας κάρτα στον ταμεία . Στο ηλεκτρονικό εμπόριο χρησιμοποιείται μεταφορικά το ίδιο λεξιλόγιο για να περιγραφούν οι διαδικασίες συλλογής πληροφοριών και τελικής αγοράς ενός προϊόντος στο Internet . Η ίδια ορολογία χρησιμοποιείται για τις συναλλαγές τόσο μεταξύ επιχειρήσεων όσο και μεταξύ επιχειρήσεων-πελατών . Όταν εξετάζετε προϊόντα στο Internet , κάνετε μια διαδικτυακή έρευνα αγοράς . Μπορείτε να τοποθετήσετε τα προϊόντα που σας ενδιαφέρουν στο δικτυακό καλάθι και μόλις ολοκληρώσετε την έρευνά σας και είστε έτοιμοι να αγοράσετε , μπορείτε να κάνετε κλικ στο πλήκτρο «purchase» , για να μεταφερθείτε σε μια σελίδα διαδικτυακής αγοράς . Για να ολοκληρωθεί η συναλλαγή θα πρέπει να δώσετε τις απαραίτητες πληροφορίες σχετικά με τη διεύθυνση αποστολής και τον αριθμό της πιστωτικής σας κάρτας .

Η διαδικτυακή έρευνα αγοράς εξασφαλίζει στους πελάτες όσες πληροφορίες χρειάζονται για να καταλήξουν σε μια ενημερωμένη αγοραστική απόφαση . Ένας καταναλωτής που ενδιαφέρεται π.χ. να αγοράσει ένα αυτοκίνητο πιθανόν να ενημερωθεί για τις τιμές και για τα χαρακτηριστικά στο Internet . Το Internet του εξασφαλίζει έναν εύκολο δρόμο εξέτασης διαφορετικών προϊόντων ώστε να συγκρίνει τα χαρακτηριστικά τους , τις δυνατότητες και τις τιμές τους . Στις συναλλαγές μεταξύ επιχειρήσεων η διαδικασία διερεύνησης της αγοράς μπορεί να συμπεριλάβει ένα extranet (ένα ιδιωτικό site) το οποίο περιέχει απαραίτητες πληροφορίες για την ολοκλήρωση μιας συμφωνίας . Ένας κατασκευαστής μπορεί να δημοσιεύσει φωτογραφίες του προϊόντος λογότυπα , case studies , τεχνικά χαρακτηριστικά ή να αναφέρεται στη διαθεσιμότητα του προϊόντος . Τη σελίδα αυτή μπορεί να την επισκεφθεί

ένας έμπορος λιανικής πώλησης , να κατεβάσει αντίγραφο του προϊόντος , όπως εμφανίζεται , ή μια φωτογραφία που θα μπορεί να τη χρησιμοποιήσει σε έναν δικό του κατάλογο ή σε μια διαφημιστική του καταχώρηση . Με τη βοήθεια του extranet ο έμπορος λιανικής μπορεί να είναι σίγουρος ότι η εικόνα που εμφανίζεται αντιστοιχεί στο προϊόν που εμπορεύεται και ότι είναι διαθέσιμο σε επαρκείς ποσότητες. Η διερεύνηση της αγοράς μέσω του Internet αυξάνει την ταχύτητα συλλογής πληροφοριών και τη διαδικασία προσπέλασης , προσφέροντας άμεση και επίκαιρη πρόσβαση σε ακριβείς πληροφορίες .

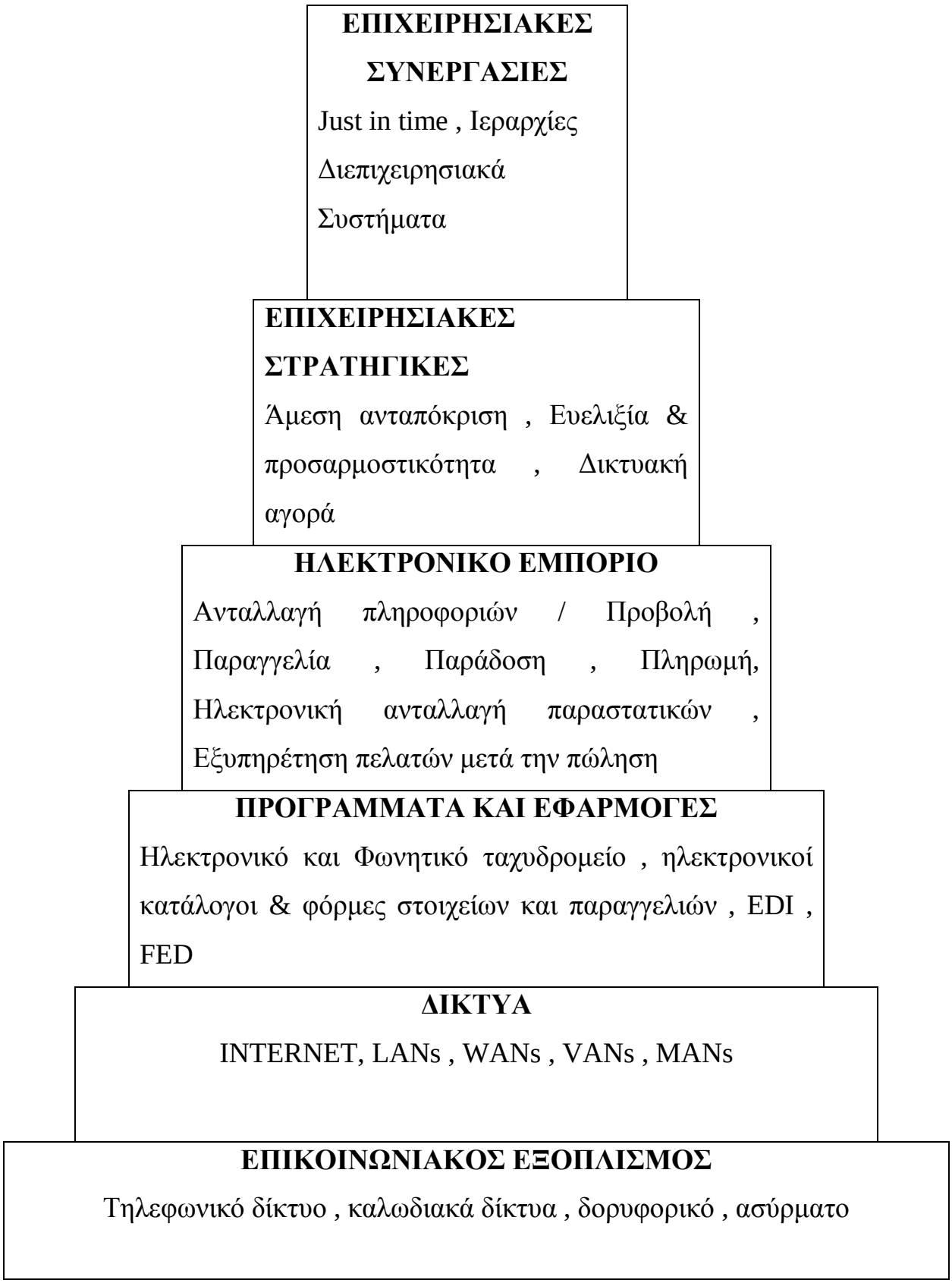
Ως διαδικτυακή αγορά ορίζεται η υποδομή που υποστηρίζει την αγορά προϊόντων στο Internet . Αν ένας καταναλωτής ενδιαφέρεται να αγοράσει είδη γραφείου , μπορεί να επισκεφθεί κάποιο ανάλογο site . Εκεί μπορεί να εξερευνήσει το διαδικτυακό κατάστημα , να επιλέξει εκείνα τα προϊόντα που τον ενδιαφέρουν και να το τοποθετήσει στο ηλεκτρονικό καλάθι αγορών . Μόλις ολοκληρώσει τη διαδικασία επιλογής , μπορεί να περάσει στη σελίδα αγοράς και να αγοράσει τα προϊόντα που επέλεξε .

Σύμφωνα με μια μελέτη της Zona research , η οποία πραγματοποιήθηκε το 1998 στην Αμερική σε 100 επιχειρήσεις με προσωπικό άνω των 500 ατόμων , απέδειξε ότι το 80 % των επιχειρήσεων χρησιμοποιούσαν το Internet για την προώθηση των προϊόντων τους , ενώ μόλις το 10 % είχε ήδη εμπλακεί στη διαδικασία της δικτυακής αγοράς . Το 45 % που ερωτήθηκαν απάντησαν ότι είχαν σκοπό να εγκαταστήσουν υποδομή διαδικτυακών πωλήσεων μέσα στα επόμενα δυο χρόνια .

Στο παρακάτω σχήμα θα προσπαθήσουμε να δείξουμε τη δομή του όλου συστήματος από τα θεμέλια , που βρίσκονται οι τηλεπικοινωνίες , οι οποίες κάνουν δυνατές τις συναλλαγές μέσω Internet, έως την κορυφή , που είναι οι σχέσεις που συνάπτουν οι επιχειρήσεις μεταξύ τους μέσω δικτύου

Οι τηλεπικοινωνίες είναι η βάση του οικοδομήματος γιατί επιτρέπουν τη δημιουργία δικτύων . Πάνω στα δίκτυα «τρέχουν τα προγράμματα και οι εφαρμογές που κάνουν το ηλεκτρονικό εμπόριο πραγματικότητα . Με τη σειρά

του , το ηλεκτρονικό εμπόριο γίνεται εργαλείο το οποίο χρησιμοποιεί η επιχείρηση με σκοπό τη διαμόρφωση στρατηγικής και την ανάπτυξη πλεονεκτημάτων έναντι των ανταγωνιστών της . Τέλος η επιχείρηση χρησιμοποιεί τι Internet συναγωνιστικά με άλλες επιχειρήσεις του κλάδου ή άλλων κλάδων , ή ακόμη και με κυβερνητικές υπηρεσίες , για πληροφόρηση και μείωση του κόστους οργάνωσης και διαχείρισης .



Σχήμα 1 : **Η πυραμίδα του ηλεκτρονικού εμπορίου**

Όπως φαίνεται και στην πιο πάνω πυραμίδα το ηλεκτρονικό εμπόριο για να γίνει εφικτό πρέπει να χρησιμοποιήσει την τεχνολογία , η οποία «πατάει» πάνω στις τηλεπικοινωνίες . Εδώ πρέπει να παρατηρηθεί ότι δεν είναι ανάγκη το Internet να «πατάει» πάνω στο τηλεφωνικό δίκτυο. Και αυτό γιατί τώρα υπάρχουν και άλλοι τρόποι λειτουργίας . Για την ώρα βέβαια το τηλεφωνικό δίκτυο είναι η προτιμότερη και συνηθέστερη μέθοδος .

Τώρα θα δούμε πως και σε ποιους τομείς επιδρά το ηλεκτρονικό εμπόριο . Οι κυριότερες δραστηριότητες πάνω στις οποίες επιδρά είναι οι εξής :

- Μάρκετινγκ, πωλήσεις και προώθηση πωλήσεων προσφορές πριν την πώληση
- Χρηματοδότηση και ασφάλιση εμπορικές συναλλαγές: παραγγελία, μεταφορά και πληρωμή, σέρβις προϊόντος και συντήρηση-υποστήριξη ανάπτυξη προϊόντος, κατανεμημένη εργασία
- Χρήση δημοσίων και ιδιωτικών υπηρεσιών επιχείρηση-δημόσια διοίκηση (παραχωρήσεις, άδειες, φόροι, κτλ.)
- Μεταφορές και λογιστική προσωπικού και υλικών
- Προμήθειες δημοσίου αυτόματο εμπόριο ψηφιακών αγαθών λογιστικά

Η όλη εμπορική συναλλαγή μπορεί να υποστηριχθεί ηλεκτρονικά, συμπεριλαμβανομένων και της μεταφοράς και της πληρωμής. Θεωρητικά ακόμα υπάρχει και η δυνατότητα να γίνεται η συνδιαλλαγή με τις δημόσιες υπηρεσίες ηλεκτρονικά, δηλαδή για πληρωμή δασμών και φόρων. Παρόλα αυτά όμως ένας αριθμός ζητημάτων όπως η προστασία και η ασφάλεια, η νομική κάλυψη δεν έχουν διευθετηθεί ακόμα ώστε να αποτελέσουν αναπόσπαστο κομμάτι του κεφαλαίου αυτού που λέγεται Ηλεκτρονικό Εμπόριο.

Θα πρέπει να γίνεται όμως ένας σαφής διαχωρισμός μεταξύ της ηλεκτρονικής μεταφοράς φυσικών αγαθών και υπηρεσιών και ανάμεσα στην ηλεκτρονική μεταφορά περιεχομένων βασισμένα αποκλειστικά σε ψηφιακή μορφή (εικόνες, ήχος, κείμενο, software).

Το Η.Ε. φυσικών αγαθών και υπηρεσιών αναπαριστά θα λέγαμε την εξέλιξη της μορφής του εμπορίου γενικότερα στη σημερινή εποχή, κεφαλαιοποιώντας τις νέες δυνατότητες που προσφέρει η τεχνολογία για να επιτευχθεί η μέγιστη αποδοτικότητα των πόρων της επιχείρησης. Παράλληλα, προσφέρει το άνοιγμα της αγοράς για νέα προϊόντα και αναβαθμισμένες υπηρεσίες μέσα από μια πρωτοποριακή άμεση συναλλαγή πελάτη-προμηθευτή. Αναμένεται να έχει μεγάλη επίδραση στον ανταγωνισμό και λιγότερη στην απασχόληση.

Ειδικότερα, το εμπόριο ηλεκτρονικού υλικού (εικόνες , ήχος , κείμενο, video , software , games , multimedia works) αναπαριστά μια επαναστατική νέα μορφή εμπορίου, στην οποία ο κύκλος των εμπορικών συναλλαγών δεν κλείνει ποτέ, μια και βρίσκεται συνέχεια μέσα στο δίκτυο. Τα εμπορευόμενα "ηλεκτρονικά αγαθά" μπορούν να δημιουργήσουν ολοκληρωτικά καινούργιες αγορές, βασιζόμενα βέβαια σε επιτυχείς λύσεις, αλλά και να φέρουν επανάσταση σε μερικές βιομηχανίες (π.χ. εκδοτικούς οίκους). Αυτή καθεαυτή η καινοτόμος μορφή εμπορίου αναμένεται να έχει μια σημαντική επίδραση στην ανταγωνιστικότητα και στη δημιουργία απασχόλησης .

6.2 ΜΟΡΦΕΣ ΕΜΦΑΝΙΣΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

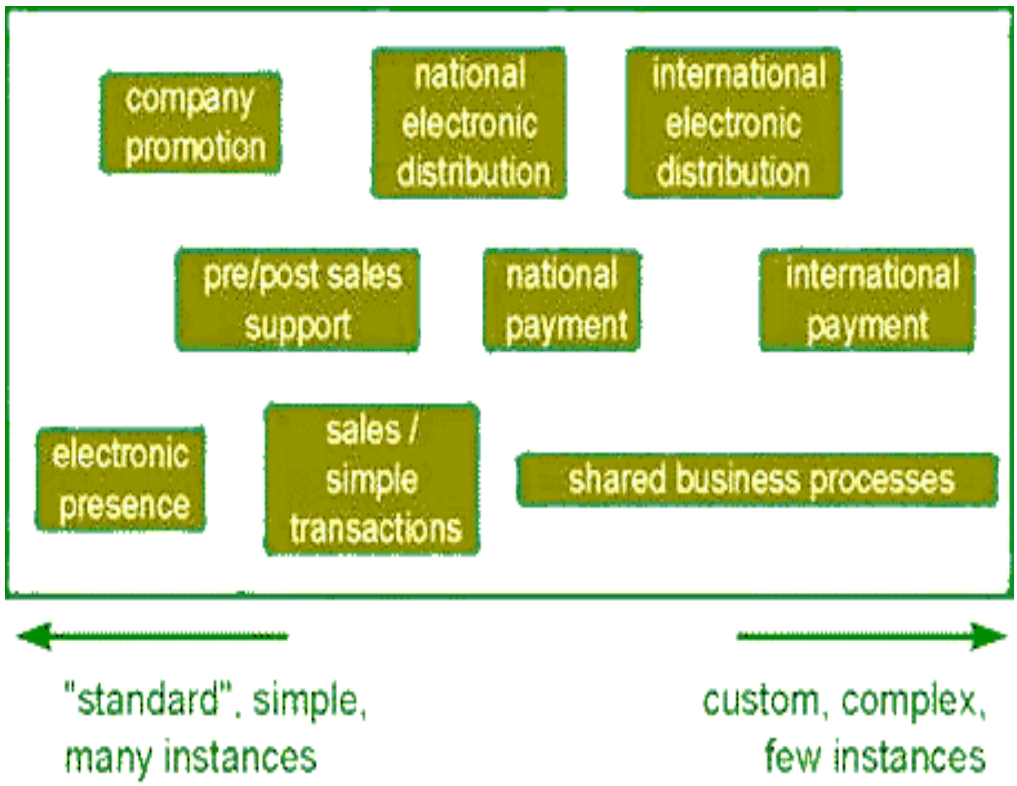
6.2.1ΕΠΠΕΔΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Υπάρχουν διάφορα και σημαντικά επίπεδα στα οποία μπορεί να συναντήσουμε το ηλεκτρονικό εμπόριο. Ποικίλλουν από μια απλή ηλεκτρονική παρουσία στο δίκτυο έως μια πλήρης ηλεκτρονική υποστήριξη εργασιών που ανήκουν σε δύο ή και παραπάνω εταιρίες και οι οποίες έχουν θεσπιστεί απ' αυτές.

Τα σημαντικότερα επίπεδα του ηλεκτρονικού εμπορίου φαίνονται και στο σχήμα. Βλέπουμε ότι γίνεται ένας διαχωρισμός μεταξύ εθνικών και διεθνών

συναλλαγών και η διάκριση αυτή δεν γίνεται τόσο από τεχνικής άποψης όσο από νομικής. Το ηλεκτρονικό εμπόριο είναι πιο περίπλοκο στο διεθνές επίπεδο επειδή ακριβώς εμπλέκονται παράγοντες όπως η φορολόγηση, οι δασμοί, οι πληρωμές και οι διαφορές που υπάρχουν στις τραπεζικές πρακτικές.

Τα κατώτερα επίπεδα του ηλεκτρονικού εμπορίου ασχολούνται βασικά με μια απλή παρουσία δικτύου, προώθηση της εταιρίας και υποστήριξη πριν και μετά την πώληση. Χρησιμοποιώντας τεχνολογία "off the selves" μπορούν να έχουν ένα φτηνό αλλά ικανό εργαλείο στα χέρια τους. Σε αντίθεση, σε πιο αναπτυγμένες μορφές συναντάμε προβλήματα τόσο νομικά όσο και τεχνολογικά. Οι εταιρίες αυτές είναι αναγκασμένες να αναπτύξουν μόνες τους τα συστήματα.



6.2.2 ΜΟΡΦΕΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Δυο είναι κυρίως οι μορφές των ηλεκτρονικών συναλλαγών και υπηρεσιών του ηλεκτρονικού εμπορίου (on line υπηρεσιών) . Η πρώτη είναι η έμμεση (off-line) διεξαγωγή ηλεκτρονικών συναλλαγών που είναι η

ηλεκτρονική παραγγελία υλικών αγαθών τα οποία πρέπει να παραδοθούν με παραδοσιακές μεθόδους (π.χ. ταχυδρομικώς) ενώ η δεύτερη είναι η άμεση (on line) διεξαγωγή των παραπάνω συναλλαγών , που είναι η παραγγελία , η πληρωμή και η παράδοση των αυλών αγαθών σε απευθείας σύνδεση , όπως είναι το λογισμικό και το ψηφιακό περιεχόμενο (π.χ. δικτυακών τόπων) καθώς και , εν γένει , πληροφοριών .

Μια μορφή ομαδοποίησης του ηλεκτρονικού εμπορίου μπορεί να γίνει βάση του πεδίου χρήσης αυτού . Τα πεδία αυτά είναι αλληλοεξαρτώμενα και αφορούν τα είδη των ηλεκτρονικών συναλλαγών που λαμβάνουν χώρα με το ηλεκτρονικό εμπόριο . Οι συναλλαγές αυτές διακρίνονται σε :

- Επιχείρηση προς πελάτη (Business to Customer , B2C)
- Επιχείρηση προς δημόσιο φορέα
- Επιχείρηση προς επιχείρηση (Business to Business , B2B)
- Καταναλωτές προς δημόσιο φορέα (Business to Administration)

Η κατηγορία εφαρμογών επιχείρηση προς πελάτη παρουσιάζει αυξανόμενη χρήση σε διεθνές επίπεδο , λόγω της ευρείας χρήσης των δυνατοτήτων του Internet , το οποίο ενδείκνυται για την αποτελεσματική προώθηση προϊόντων και υπηρεσιών σε μεγάλο εύρος πελατών . Οι επιχειρήσεις εκμεταλλευόμενες τα στρατηγικά οφέλη , που προσφέρει το ηλεκτρονικό εμπόριο και ειδικότερα η παγκοσμιοποίηση της αγοράς μέσω της οικονομίας του διαδικτύου ,δημιουργούν καινοτομικά προϊόντα και υπηρεσίες και τα προωθούν στους καταναλωτές . Έτσι έχει αναπτυχθεί μια σειρά εφαρμογών που περιλαμβάνει μεταξύ άλλων και τα ακόλουθα : υποστήριξη πελατών , ηλεκτρονική δημοσιογραφία , διαφήμιση , ηλεκτρονικές τράπεζες , κ.λ.π.

Η κατηγορία εφαρμογών επιχείρηση προς δημόσιο φορέα καλύπτει κάθε μορφή ηλεκτρονικής επικοινωνίας μεταξύ ιδιωτικών εταιριών και αρμόδιων αρχών , τόσο για τη διεκπεραίωση φορολογικών ή άλλων υποχρεώσεων , όσο και για την αυτοματοποίηση της διαδικασίας των δημοσίων προμηθευτών .

Τέτοιου είδους συναλλαγές συνήθως αφορούν τέσσερις περιπτώσεις : Φορολογία , εισαγωγές-εξαγωγές μέσω τελωνείων , δημόσιες προμήθειες και προηγμένες ηλεκτρονικές υπηρεσίες .

Οι εφαρμογές της μορφής επιχείρηση προς επιχείρηση , στοχεύουν στην απλοποίηση διαδικασιών των επιχειρήσεων , στον έλεγχο και τη μείωση του αποθέματος , στην αυτοματοποιημένη αντικατάσταση προϊόντων κ.α. Απαραίτητη προϋπόθεση για την επιτυχία των εφαρμογών της κατηγορίας αυτής είναι η συνεργασία και ο συντονισμός των επιχειρήσεων . Ένα χαρακτηριστικό παράδειγμα εφαρμογής ηλεκτρονικού εμπορίου μεταξύ επιχειρήσεων είναι η χρήση τηλεπικοινωνιακών δικτύων για να διεκπεραιωθούν ηλεκτρονικά καίριες λειτουργίες , όπως η παραγγελιοδοσία και η τιμολόγηση.

Στις περισσότερες εφαρμογές της μορφής καταναλωτών προς Δημόσιο φορέα , οι πολίτες φορολογούμενοι συναλλάσσονται με τους δημόσιους οργανισμούς χρησιμοποιώντας εφαρμογές του ηλεκτρονικού εμπορίου είτε για να ολοκληρώσουν τις φορολογικές τους υποχρεώσεις , είτε για να προμηθευτούν με τα απαραίτητα πιστοποιητικά ή βεβαιώσεις , είτε ακόμη για να εξασφαλίσουν τις απαραίτητες πληροφορίες που χρειάζονται.

Σε κάθε πεδίο Ηλεκτρονικού Εμπορίου χρησιμοποιούνται διαφορετικά είδη επικοινωνιακών δικτύων και διαφορετικές τεχνολογίες . Το Internet χρησιμοποιείται στις συναλλαγές “επιχείρηση – προς – πελάτη” . Για τις ενδοεπιχειρησιακές συναλλαγές χρησιμοποιείται το Internet , ενώ για τις συναλλαγές μεταξύ των επιχειρήσεων χρησιμοποιούνται επίσης Extranets και EDI . Η επικοινωνία αυτή μεταξύ των επιχειρήσεων ονομάζεται Διαλυσίδα . Σύμφωνα με τον κ. Γ. Δουκίδη (1998), *η διαλυσίδα είναι σχεδιασμένη να συνδέει τον αγοραστή και τον προμηθευτή προς παροχή καλύτερου συντονισμού των κοινών τους δραστηριοτήτων. Η ιδέα της διαλυσίδας προέκυψε από την αλυσίδα αξίας που κάθε επιχείρηση έχει και το γεγονός ότι στα τελικά σημεία της , η αλυσίδα αξίας της μιας επιχείρησης διασυνδέεται με την αλυσίδα αξίας μιας άλλης*

.

Θα πρέπει να σημειωθεί ότι οι ηλεκτρονικές συναλλαγές εξαρτώνται σε μεγάλο βαθμό από το μέσο που χρησιμοποιείται για τη διενέργεια τους. Με την εξέλιξη της τεχνολογίας του Διαδικτύου και τη διάδοση του τελευταίου ως ενός μέσου πληροφόρησης και επικοινωνίας παγκόσμιας εμβέλειας, διευρύνεται η σημασία του ηλεκτρονικού εμπορίου και το δίκτυο, το οποίο για το παραδοσιακό ηλεκτρονικό εμπόριο ήταν το μέσο για τη μεταφορά δεδομένων, γίνεται για το διαδικτυακό ηλεκτρονικό εμπόριο, η ίδια η αγορά.

Βεβαίως το ηλεκτρονικό εμπόριο μεταξύ των επιχειρήσεων αναπτύχθηκε ήδη πριν από την εμφάνιση του Διαδικτύου, στα πλαίσια κλειστών δικτύων- π.χ. με την ηλεκτρονική ανταλλαγή εμπορικών δεδομένων (Electronic Data Interchange – EDI) ενώ παράλληλα το (ηλεκτρονικό) λιανικό εμπόριο αναπτύχθηκε και αυτό με τη χρησιμοποίηση συστημάτων videotext, όπως ήταν λ.χ. στη Γαλλία το minitel .

Με την εξέλιξη όμως του Διαδικτύου και των υπηρεσιών του, όπως είναι ιδίως ο Παγκόσμιος Ιστός το ηλεκτρονικό εμπόριο απέκτησε ευρύτερες διαστάσεις και διευρυνόμενη σημασία και αναπτύχθηκε σε έναν κατ΄ιδίαν οικονομικό κλάδο, παρέχοντας σημαντικά πλεονεκτήματα τόσο στις επιχειρήσεις καθώς στις ηλεκτρονικές συναλλαγές εξοικονομούνται δαπάνες διαφήμισης, σύναψης και εκτέλεσης συμβάσεων, όσο και στους καταναλωτές, στους οποίους παρέχεται η δυνατότητα πρόσβασης σε μεγάλη γκάμα προϊόντων και υπηρεσιών και σε χαμηλότερες τιμές. ΄Ηδη το ηλεκτρονικό εμπόριο υπερβαίνει και αυτά ακόμη τα όρια του Διαδικτύου και εισβάλει στο χώρο της κινητής τηλεφωνίας . Επίσης θα πρέπει να τονισθεί ότι το ηλεκτρονικό εμπόριο δεν εξαντλείται στις συναλλαγές μέσω του Internet , αλλά περιλαμβάνει και όλες τις συναλλαγές που διενεργούνται με ηλεκτρονικά μέσα , όπως το τηλέφωνο , το φαξ κ.λ.π. , αλλά και τις συναλλαγές μέσω κλειστών δικτύων .

6.2.3 ΠΕΔΙΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Το ηλεκτρονικό εμπόριο μπορεί να εφαρμοστεί σε μια ευρεία γκάμα επιχειρηματικών λειτουργιών που περιλαμβάνουν :

- Ανταλλαγή πληροφοριών για προϊόντα και υπηρεσίες (πριν την πώληση) . Η ανταλλαγή αυτή των πληροφοριών η διαφήμιση και η ενημέρωση για τα προϊόντα και τις υπηρεσίες είναι ίσως η πλέον διαδεδομένη χρήση του ηλεκτρονικού εμπορίου . Για παράδειγμα , πάρα πολλές επιχειρήσεις διαθέτουν ηλεκτρονικές σελίδες μέσω των οποίων διαφημίζουν τις υπηρεσίες και τα προϊόντα που παρέχουν . Οι περισσότερες προσφέρουν παράλληλα και επιπλέον υπηρεσίες στους πελάτες τους που εμπίπτουν συνήθως σε μια από τις επόμενες κατηγορίες .
- Υποστήριξη πελάτη (πριν και μετά την πώληση) . Πολλές επιχειρήσεις δημιουργούν ομάδες συζητήσεων και επαφών με τους πελάτες τους , οι οποίοι με τον τρόπο αυτό μπορούν να επικοινωνούν όχι μόνο με τον προμηθευτή , αλλά και μεταξύ τους , ανταλλάσσοντας ιδέες και ερωτήσεις .
- Δημιουργία ηλεκτρονικών επιχειρήσεων (virtual enterprises) –Εμπορικά κέντρα . Το ηλεκτρονικό εμπόριο παρέχει τη δυνατότητα δημιουργίας ηλεκτρονικών επιχειρήσεων στο δίκτυο . Επιπλέον πολλές μικρομεσαίες (κυρίως) επιχειρήσεις δημιουργούν Ηλεκτρονικά Εμπορικά Κέντρα , δηλαδή ομάδες επιχειρήσεων που συνεργάζονται ηλεκτρονικά . Μια ηλεκτρονική επιχείρηση αποτελείται από δυο ή περισσότερα ηλεκτρονικά καταστήματα και παρέχει τη δυνατότητα στις επιχειρήσεις να δημιουργήσουν ισχυρούς και ανταγωνιστικούς ομίλους εταιριών . Το γεγονός αυτό φαίνεται να αλλάζει το συσχετισμό δυνάμεων μεταξύ των επιχειρήσεων . Οι πελάτες μπορούν να δουν πληροφορίες για τα προϊόντα της εταιρίας και να τα παραγγέλνουν πληρώνοντας μέσω ηλεκτρονικών συστημάτων πληρωμών . Οι παραγγελίες των πελατών μεταφέρονται

μέσω Internet στον κατάλληλο προμηθευτή και τα προϊόντα αποστέλλονται μέσω ταχυδρομείου . Ο πελάτης έχει τη δυνατότητα να παρακολουθεί το σημείο στο οποίο βρίσκεται η παραγγελιά του ανά πάσα στιγμή .

- Ηλεκτρονικές Τράπεζες . Αρκετές τράπεζες έχουν δημιουργήσει ηλεκτρονικές υπηρεσίες παρέχοντας ένα σύνολο δυνατοτήτων στους πελάτες τους . Οι ηλεκτρονικές τράπεζες επιτρέπουν στους πελάτες να χρεοπιστώνουν λογαριασμούς μέσα από το Internet , να μεταφέρουν κεφάλαια από ένα λογαριασμό σε έναν άλλο ή ακόμη και να κάνουν αίτηση για προέγκριση δανείου ή απόκτηση πιστωτικής κάρτας . Άλλες υπηρεσίες που προσφέρονται από τις τράπεζες είναι η εξυπηρέτηση των οικονομικών συναλλαγών των ιδεατών καταστημάτων και η διεκπεραίωση των μηνυμάτων EDI , EFT , SWIFT , κλπ .
- Ηλεκτρονική διανομή . Στα πλαίσια της ηλεκτρονικής διανομής μπορούν να ενταχθούν υπηρεσίες on-line διάχυσης πληροφοριών με μηδαμινό , συνήθως , κόστος χρήσης .
- Ανάπτυξη κοινών επιχειρηματικών διαδικασιών (shared business processes) μεταξύ επιχειρήσεων. Τέτοιες διαδικασίες φέρνουν σε στενή επαφή τους συμμετέχοντες στο εμπορικό κύκλωμα , συσφίγγοντας τους επιχειρηματικούς δεσμούς και δυσχεραίνοντας με αυτό τον τρόπο την αλλαγή συνεργατών (lock-in) .

6.3 ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Αρκετοί είναι οι κίνδυνοι και τα προβλήματα που εμφανίζονται στην εφαρμογή του ηλεκτρονικού εμπορίου. Ορισμένα από αυτά αφορούν τις επιχειρήσεις και άλλα τους καταναλωτές. Επίσης υπάρχουν προβλήματα που αφορούν γενικότερα την Ελληνική αγορά του ηλεκτρονικού εμπορίου. Οι κίνδυνοι αφορούν κυρίως την ασφάλεια των ηλεκτρονικών συναλλαγών. Τα

προβλήματα οφείλονται κυρίως στην περιορισμένη διείσδυση του Διαδίκτυο στις επιχειρήσεις ιδιαίτερα μικρού και μεσαίου μεγέθους, σε διαρθρωτικά προβλήματα της τραπεζικής αγοράς καθώς και στην γενικότερη καταναλωτική κουλτούρα που επιδρά αρνητικά στη χρήση συστημάτων ηλεκτρονικού εμπορίου.

6.3.1 ΠΡΟΒΛΗΜΑΤΑ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ ΠΟΥ ΑΦΟΡΟΥΝ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

- Απουσία περιεχομένου για πώληση :Ένας από τους βασικότερους λόγους για τους οποίους δεν έχει ακόμα αναπτυχθεί το ηλεκτρονικό εμπόριο στην Ελλάδα είναι η απουσία περιεχομένου προς πώληση. Μέχρι τώρα στην Ελλάδα το ηλεκτρονικό εμπόριο γνωρίζει επιτυχία σε ελάχιστα καταναλωτικά είδη και κυρίως στα βιβλία, τα λουλούδια και τα cd. Αν και υπάρχουν ηλεκτρονικά καταστήματα που διαθέτουν προς πώληση πολλά είδη όπως ηλεκτρονικές συσκευές ή ακόμα και είδη για το σπίτι ο αριθμός τους δεν είναι ιδιαίτερα σημαντικός ενώ δεν έχουν την ίδια επιτυχημένη πορεία με τα είδη που προαναφέραμε. Γενικότερα αυτή την στιγμή και παρά τις όποιες μεμονωμένες προσπάθειες, οι Έλληνες καταναλωτές δεν έχουν στην διάθεσή τους μια ευρεία γκάμα προϊόντων τα οποία μπορούν να αγοράσουν ηλεκτρονικά. Ενώ και για τα είδη που είναι διαθέσιμα μέσω του διαδικτύου δεν υπάρχουν πολλά ηλεκτρονικά καταστήματα που να τα προσφέρουν ώστε να υπάρχει δυνατότητα σύγκρισης όπως υπάρχει στον φυσικό κόσμο.
- Το πρόβλημα των ηλεκτρονικών πληρωμών στις επιχειρήσεις :ένα από τα πιο σημαντικά ζητήματα που σχετίζονται άμεσα με τη χρήση και τη διάδοση του Ηλεκτρονικού Εμπορίου αφορά το επίπεδο ασφαλείας των ηλεκτρονικών συναλλαγών. Έως τώρα στην Ελλάδα, έχουν υλοποιηθεί εφαρμογές ηλεκτρονικών πληρωμών που απευθύνονται κυρίως σε καταναλωτές (B2C). Η πλειοψηφία των υλοποιήσεων αυτών δεν μπορεί να θεωρηθεί επιτυχημένη

καθώς δεν έχει καταφέρει να συγκεντρώσει κρίσιμη μάζα πελατών που θα διασφαλίσουν την βιωσιμότητα των υλοποιήσεων. Η πιο συνηθισμένη πρακτική μεταξύ των εταιριών που προσφέρουν συστήματα ηλεκτρονικών πληρωμών είναι να συνεργαστούν με κάποια από τις τράπεζες που προσφέρουν ηλεκτρονικές πλατφόρμες όπως η Τράπεζα Πειραιώς, η Εγνατία Τράπεζα και η Eurobank. Παρά όμως τις καινοτομικές λύσεις και την σχετική ασφάλεια που εγγυάται η παρουσία μιας μεγάλης τράπεζας που λειτουργεί το σύστημα ηλεκτρονικών πληρωμών, το μεγαλύτερο μέρος των προσπαθειών αυτών δεν στέφθηκε με επιτυχία καθώς δεν κατόρθωσαν να προσελκύσουν τον αναγκαίο αριθμό καταναλωτών ώστε να δημιουργήσουν αγορές.

Αυτό έχει σαν αποτέλεσμα οι περισσότερες Ελληνικές τράπεζες να μην έχουν στα άμεσα σχέδιά τους την πραγματοποίηση επενδύσεων για την δημιουργία συστημάτων ηλεκτρονικών πληρωμών καθώς το όφελος από μια τέτοια επένδυση δεν είναι ορατό ενώ το κόστος είναι αρκετά υψηλό. Επιπλέον, υπάρχει και το προηγούμενο της ηλεκτρονικής τραπεζικής όπου οι τράπεζες προέβησαν σε σημαντικές επενδύσεις οι οποίες δεν έδωσαν τα αναμενόμενα αποτελέσματα, καθώς από το1999 μειώθηκε η ζήτηση για τις υπηρεσίες Internet Banking.

- Διατήρηση συναλλακτικών ηθών που δεν επιτρέπουν την δημιουργία συστημάτων ηλεκτρονικών συναλλαγών: Η ύπαρξη επιτυχημένων συστημάτων ηλεκτρονικών συναλλαγών μεταξύ των εταιριών (B2B) θα δημιουργούσε τις απαραίτητες προϋποθέσεις για την περαιτέρω εξάπλωση και υιοθέτηση των συστημάτων αυτών και από τους καταναλωτές. Αυτή την στιγμή στην Ελλάδα λειτουργούν τέσσερις μεγάλες ηλεκτρονικές αγορές. Όμως ,σε καμία από αυτές, αν και είναι εφικτό από τεχνική άποψη, δεν προσφέρεται η δυνατότητα πραγματοποίησης πληρωμών ηλεκτρονικά. Ο βασικός λόγος για τον οποίο δεν έχει ζητηθεί από τους μετέχοντες στην ηλεκτρονική αγορά η ενεργοποίηση των συστημάτων ηλεκτρονικών πληρωμών είναι κυρίως η πρακτική που ακολουθείται μεταξύ των συναλλασσομένων εταιριών σε όλη την Ελλάδα. Η

ύπαρξη συστημάτων ηλεκτρονικών πληρωμών σημαίνει ότι οι επιχειρήσεις θα πρέπει να εγκαταλείψουν την πρακτική των μεταχρονολογημένων επιταγών που αποτελεί τον συνηθέστερο τρόπο εξόφλησης στον εμπορικό κόσμο. Όπως είναι φυσικό μια τέτοια αλλαγή δεν είναι δυνατόν να επέλθει άμεσα. Αυτό που απαιτείται κυρίως είναι η εξομάλυνση των υπαρχόντων συναλλακτικών ηθών και στη συνέχεια η μεταφορά των νέων πρακτικών στο διαδίκτυο.

- Προσέγγιση καταναλωτών νεαρών ηλικιακών ομάδων: Οι ηλικιακές ομάδες που είναι περισσότερο εξοικειωμένες με την χρήση των νέων τεχνολογιών είναι οι έφηβοι και οι νέοι μέχρι 25 ετών. Το βασικό πρόβλημα με αυτές τις ομάδες του πληθυσμού είναι ότι παρόλο που είναι οι πιο θετικές στις αγορές μέσω διαδικτύου δεν διαθέτουν τα απαραίτητα κεφάλαια προκειμένου να χρησιμοποιήσουν ένα από τα συστήματα ηλεκτρονικών πληρωμών τα περισσότερα εκ των οποίων σχετίζονται με την κατοχή πιστωτικής κάρτας ή τραπεζικού λογαριασμού. Για τον λόγο αυτό, οι Ελληνικές τράπεζες, που αποτελούν και την βασική κινητήριο δύναμη πίσω από την ανάπτυξη συστημάτων ηλεκτρονικών πληρωμών, δημιουργούν σταδιακά τέτοια συστήματα τα οποία θα είναι προσβάσιμα και στις νεαρές ηλικίες. Στόχος αυτής της στρατηγικής είναι η παροχή της δυνατότητας αγορών σε εκείνες τις πληθυσμιακές ομάδες που είναι περισσότερο διατεθειμένες να πραγματοποιήσουν αγορές μέσω διαδικτύου και η σταδιακή δημιουργία κρίσιμου μεγέθους που θα μπορέσει να δικαιολογήσει περισσότερες επενδύσεις σε τέτοια συστήματα.
- Κατακερματισμός της τραπεζικής αγοράς στην Ελλάδα: μέχρι τώρα στην Ελλάδα δεν υπάρχει κοινή υποδομή σε επίπεδο συστημάτων μεταξύ των εταιριών. Κάθε τράπεζα αναπτύσσει τα δικά της συστήματα με αποτέλεσμα η αγορά να είναι πλήρως κατακερματισμένη. Χαρακτηριστικό είναι το παράδειγμα της Πορτογαλίας όπου οι πληρωμές είναι κεντρικοποιημένες και ελέγχονται από το διατραπεζικό σύστημα της χώρας. Ο πελάτης βλέπει ένα κοινό interface στις συναλλαγές του, το οποίο προέρχεται από την VISA, ενώ η

εκκαθάριση των συναλλαγών γίνεται κεντρικά από το διατραπεζικό σύστημα. Τα πλεονεκτήματα ενός τέτοιου τρόπου οργάνωσης εντοπίζονται στο γεγονός ότι δημιουργούνται οικονομίες κλίμακας, συγκεντρώνεται εύκολα κρίσιμος όγκος πελατών ενώ η ανάπτυξη εμπιστοσύνης είναι σαφώς ευκολότερη. Παρόμοιο τρόπο οργάνωσης έχει και η Ισπανία με τη διαφορά ότι υπάρχου περισσότερα από ένα διατραπεζικά συστήματα. Ενδιαφέρον, παρουσιάζει και η περίπτωση της Βουλγαρίας όπου υπάρχει ανεπτυγμένο ένα ιδιαίτερα εξελιγμένο διατραπεζικό σύστημα που θα μπορούσε να υποστηρίξει κεντρικοποιημένες ηλεκτρονικές συναλλαγές. Η εξόρμηση όμως των Ελληνικών Τραπεζών στα Βαλκάνια και η μεταφορά της ελληνικής νοοτροπίας αυτούσιας σε αυτή την χώρα οδηγεί σε σταδιακό κατακερματισμό του διατραπεζικού συστήματος της Βουλγαρίας. Αυτό οφείλεται στο γεγονός ότι κάθε τράπεζα ακολουθώντας το ελληνικό μοντέλο αναπτύσσει η ίδια τις τεχνολογικές λύσεις που επιθυμεί.

- Προβλήματα που σχετίζονται με τον υπάρχοντα τεχνολογικό εξοπλισμό και τις μεθοδολογίες που ακολουθούνται: Ο υπάρχον τεχνολογικός εξοπλισμός είναι καθοριστικής σημασίας για την εφαρμογή νέων τεχνολογιών στην επιχείρηση. Έλλειψη μηχανογραφικής υποδομής ή έλλειψη λειτουργικότητάς της προκαλεί αδυναμία εκμετάλλευσης της πληροφορίας που ανταλλάσσεται μεταξύ των διαφόρων συστημάτων. Η τεχνολογία είναι ένας καταλύτης που επιτρέπει αποτελεσματική επικοινωνία. Η ανταλλαγή πληροφορίας μέσω ηλεκτρονικών μεθόδων απαιτεί την υιοθέτηση προτύπων, ώστε να μπορεί να επιτευχθεί η επικοινωνία υπολογιστικών συστημάτων. Ένα από τα πλέον σημαντικά θέματα που αφορούν στο περιεχόμενο της εμπορικής πληροφορίας είναι η ενιαία κωδικοποίηση των ειδών. Η κοινή γλώσσα (κωδικοποίηση) είναι απαραίτητη προκειμένου αποστολέας και παραλήπτης να επικοινωνήσουν αποτελεσματικά. Ειδικά στο τμήμα της εμπορικής επικοινωνίας οι νέες τεχνολογίες προϋποθέτουν την χρήση κοινά αποδεκτών κωδικοποιήσεων οι οποίοι χρησιμοποιούνται ευρύτατα στο διεθνές εμπορικό περιβάλλον. Έλλειψη της κοινής κωδικοποίησης συνεπάγεται έλλειψη αποτελεσματικής επικοινωνίας.

Ένα πολύ βασικό στοιχείο του ηλεκτρονικού εμπορίου είναι οι on-line τιμοκατάλογοι η διαχείριση των οποίων είναι μια διαδικασία πολύ πιο πολύπλοκη από ότι φαίνεται. Οι περισσότεροι on-line κατάλογοι προϊόντων περιέχουν ανακριβείς συντομεύσεις και φτωχές περιγραφές. Επιπλέον περιέχουν λάθη που έχουν συσσωρευτεί κατά τη διάρκεια των χρόνων όπως: διαφορετικές μονάδες μέτρησης, ξεπερασμένα προϊόντα, λανθασμένους κωδικούς κλπ. Πριν ένας κατάλογος μεταφερθεί στο Internet, συνήθως χρειάζεται σημαντικές αλλαγές που απαιτούν από την μία μεριά ανθρώπινη εργασία και από την άλλη βοήθεια της τεχνολογίας. Τα περιεχόμενα του καταλόγου, πρέπει να κατηγοριοποιηθούν με κατάλληλο τρόπο ώστε να είναι δυνατή η αναζήτηση προϊόντων με βάση κωδικούς, κατηγοριοποιήσεις, ομάδες και χαρακτηριστικά προϊόντων. Η κατηγοριοποίηση των καταλόγων είναι μια κρίσιμη διαδικασία που απαιτεί ειδικές ικανότητες και έχει μεγάλες επιπτώσεις στο πόσο εύκολα οι πελάτες της ηλεκτρονικής αγοράς θα βρίσκουν τα προϊόντα που θέλουν να προμηθευτούν. Συνήθως οι μεγάλες επιχειρήσεις επιθυμούν να φιλοξενούν οι ίδιες καταλόγους των βασικών προμηθευτών τους, αλλά ανακαλύπτουν σταδιακά ότι αυτή η διαδικασία απαιτεί μεγαλύτερη προσπάθεια από αυτή που μπορούν να αντέξουν. Μια ακόμη μεγάλη πρόκληση είναι αυτή της ανανέωσης του περιεχομένου των ηλεκτρονικών καταλόγων. Κατά μέσο όρο οι προμηθευτές αλλάζουν τους καταλόγους τους κατά 25% κάθε χρόνο όσο αφορά τις περιγραφές των προϊόντων, και κατά 125% τις τιμές τους. Επομένως, είναι σημαντικό το κόστος της ανανέωσης και πολλές επιχειρήσεις δεν είναι ικανές να τους συντηρήσουν σωστά.

- Προβλήματα που σχετίζονται με το υπάρχον νομικό και θεσμικό πλαίσιο:

Η κάθε εμπορική επιχείρηση υπόκεινται σε κανόνες και νόμους που επιβάλλονται από το Ελληνικό Δημόσιο και από τις Κοινοτικές οδηγίες της Ευρωπαϊκής Ένωσης. Οι νέες τεχνολογίες επαγγέλλονται επικοινωνία χωρίς χαρτιά, ενώ κάποια παραστατικά, σύμφωνα με την υπάρχουσα νομοθεσία, απαιτείται να υπάρχουν σε έντυπη μορφή. Ένα παράδειγμα είναι το Δελτίο

Αποστολής που πρέπει να συνοδεύει κάθε προϊόν κατά την μεταφορά του. Ένα βήμα προς τον εκσυγχρονισμό του μηχανογραφικού συστήματος TAXIS αναμένεται να κάνει το υπουργείο Οικονομίας και Οικονομικών μέχρι το τέλος του έτους σύμφωνα με άρθρο της εφημερίδας «Ημερησία», «*Ηλεκτρονικό αποτύπωμα στα τιμολόγια*» που δημοσιεύθηκε την Τρίτη 20 Απριλίου 2004 και αναφέρει μεταξύ άλλων : «Ηλεκτρονικό φρένο» στα πλαστά και εικονικά τιμολόγια που έχουν κατακλύσει την αγορά ετοιμάζεται να βάλει το υπουργείο Οικονομίας και Οικονομικών. Το σχέδιο που επεξεργάζεται, σύμφωνα με πληροφορίες, το οικονομικό επιτελείο προβλέπει την ηλεκτρονική σήμανση αντί της σημερινής διάτρησης των τιμολογίων που χρησιμοποιούν στις συναλλαγές τους οι επιχειρήσεις. Συγκεκριμένα, όλα τα τιμολόγια θα αποκτήσουν ένα μοναδικό ασφαλή ηλεκτρονικό αριθμό σήμανσης. Η πιστότητα και αυθεντικότητα κάθε τιμολογίου ελέγχεται και θα διασταυρώνεται από τον ίδιο τον επιχειρηματία μέσω ενός ειδικού ηλεκτρονικού προγράμματος του Taxis. Δηλαδή, κάθε επιχειρηματίας θα μπορεί να διαπιστώνει αν είναι πλαστό ή εικονικό ένα τιμολόγιο εισάγοντας τον μοναδικό αριθμό του στο ειδικό ηλεκτρονικό πρόγραμμα του taxis. Όμως, για την εφαρμογή του νέου μέτρου απαιτείται η αναβάθμιση του υπάρχοντος μηχανογραφικού συστήματος Taxis, η οποία θα υλοποιηθεί μέσω διαγωνισμού -πιθανότατα μέχρι το τέλος του έτους.

6.3.2 ΤΑ ΠΡΟΒΛΗΜΑΤΑ ΠΟΥ ΑΦΟΡΟΥΝ ΤΟΥΣ ΚΑΤΑΝΑΛΩΤΕΣ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Δεν είναι όμως μόνο οι επιχειρήσεις που αντιμετωπίζουν κινδύνους και προβλήματα στην εφαρμογή του ηλεκτρονικού εμπορίου. Είναι και οι καταναλωτές αντιμέτωποι με πολύ σοβαρές προκλήσεις οι οποίες έχουν σχέση με το ηλεκτρονικό εμπόριο και ιδιαίτερα με τις ηλεκτρονικές συναλλαγές και την ασφάλειά τους. Τα προβλήματα αυτά αποτελούν ανασταλτικό παράγοντα για την διάδοση του ηλεκτρονικού εμπορίου στους καταναλωτές.

Διάφοροι κίνδυνοι και προβλήματα που έχουν να αντιμετωπίσουν οι καταναλωτές κατά την εκτέλεση των ηλεκτρονικών τους αγορών είναι τα παρακάτω:

- Ασφάλεια των ηλεκτρονικών συναλλαγών: Ένας από τους σημαντικότερους παράγοντες που λαμβάνεται υπ' όψη από τους καταναλωτές για την πραγματοποίηση ηλεκτρονικών αγορών και κατά συνέπεια συναλλαγών είναι το επίπεδο της ασφάλειας που παρέχουν οι διενεργούμενες ηλεκτρονικά συναλλαγές. Οι πιο συχνές περιπτώσεις μη εξουσιοδοτημένων ηλεκτρονικών παραβιάσεων είναι οι ιοί που δημιουργούν πολλές φορές σοβαρά προβλήματα σε χρήστες του διαδικτύου. Λιγότερο συχνά αλλά περισσότερο σοβαρά είναι τα κρούσματα επιθέσεων που σημειώνονται κατά καιρούς στα συστήματα δικτύου μεγάλων εταιριών του διαδικτύου τα οποία έχουν σαν αποτέλεσμα τον εντοπισμό και την αποκρυπτογράφηση μυστικών κωδικών πρόσβασης, την υποκλοπή προσωπικών στοιχείων που μεταφέρονται μέσω του διαδικτύου καθώς και την τροποποίηση αποθηκευμένων αρχείων. Όλα αυτά δημιουργούν σοβαρές ανησυχίες στους καταναλωτές για την συνολική ασφάλεια των συναλλαγών που πραγματοποιούνται μέσω του διαδικτύου, αλλά και γενικότερα του ηλεκτρονικού εμπορίου. Έτσι περιορίζουν τις ηλεκτρονικές συναλλαγές μέχρι να γίνει το διαδίκτυο περισσότερο ασφαλές για τους χρήστες. Κάτω από αυτές τις συνθήκες είναι φυσικό οι εταιρίες που δραστηριοποιούνται στο χώρο του διαδικτύου να προσπαθούν να αναπτύξουν άμεσα μέτρα προστασίας των σελίδων τους, ιδίως αυτών που αφορούν το ηλεκτρονικό εμπόριο. Ήδη το υπάρχον σύστημα χρησιμοποιεί κάποιο επίπεδο κρυπτογράφησης μέσω του οποίου έχει κανείς κάποιο σχετικό έλεγχο της πρόσβασης στο δίκτυο. Με την επίτευξη καλύτερων επιπέδων ασφαλείας όλο και περισσότεροι χρήστες θα εμπιστεύονται το διαδίκτυο για τις αγορές και τις συναλλαγές τους.
- Η ευχέρεια πρόσβασης στα ηλεκτρονικά μέσα: Η αποδοχή από τους καταναλωτές των ηλεκτρονικών αγορών προαπαιτεί την ευχερή πρόσβαση των καταναλωτών στα ηλεκτρονικά μέσα. Στην Ελλάδα η διείσδυση του Internet

ανερχόταν τον Μάρτιο του 2004 σύμφωνα με τελευταία έρευνα της GFK Market Analysis, που δημοσιεύτηκε την Παρασκευή 7 Μαΐου 2004 στην Ναυτεμπορική, *ανερχόταν στο 28%, σε σύγκριση με 25% την αντίστοιχη περίοδο Μαρτίου 2003. Σύμφωνα με την ίδια έρευνα όσον αφορά το ηλεκτρονικό εμπόριο (e-commerce) η πιο ενεργητική ομάδα είναι άτομα ηλικίας 35-44 χρονών με ποσοστό 12%.* Τα ποσοστά αυτά δεν είναι ιδιαίτερα ικανοποιητικά καθώς είναι χαμηλότερα από τα αντίστοιχα των άλλων χωρών της Ευρωπαϊκής Ένωσης. Αυτό αποδεικνύει ότι οι Έλληνες καταναλωτές δεν έχουν την καλύτερη δυνατή πρόσβαση στα ηλεκτρονικά μέσα κάτι που περιορίζει τις ηλεκτρονικές αγορές τους.

- Η απροθυμία μετακίνησης από τα συμβατικά παλαιά μέσα: Ένας ακόμη παράγοντας που επηρεάζει την υιοθέτηση των νέων τεχνολογιών άρα και του ηλεκτρονικού εμπορίου είναι η απροθυμία των καταναλωτών να μετακινηθούν από τα παλαιά και γνωστά σε αυτούς μέσα διενέργειας αγορών στα οποία είναι εξοικειωμένοι, εάν αισθάνονται ότι αυτά καλύπτουν επαρκώς τις ανάγκες τους. Ιδιαίτερη αδράνεια παρατηρείται στους καταναλωτές που ανήκουν σε παλαιότερες γενεές όσο αφορά την εγκατάλειψη καθιερωμένων τρόπων αγορών και την υιοθέτηση της νέας τεχνολογίας και του ηλεκτρονικού εμπορίου. Σύμφωνα με τον Efraim Turban (2000) *οι πελάτες δεν εμπιστεύονται έναν άγνωστο πωλητή (μερικές φορές δεν εμπιστεύονται ακόμη και τους γνωστούς), τις συναλλαγές χωρίς χαρτιά και τα ηλεκτρονικά χρήματα. Ακόμη ορισμένοι πελάτες θέλουν να αγγίζουν αντικείμενα όπως υφάσματα, για να ξέρουν ακριβώς τι αγοράζουν. Έτσι η μετάβαση από τα φυσικά στα εικονικά καταστήματα μπορεί να είναι δύσκολη*. Παρά τις επιφυλάξεις αυτές ο χρόνος και η εξοικείωση πιθανότατα θα κάμψουν τελικά τη διστακτικότητα αυτή των καταναλωτών.
- Ο παράγοντας τιμής-κόστους: Ένας άλλος παράγοντας ο οποίος επηρεάζει σημαντικά τους καταναλωτές, ως προς την απόφασή τους να υιοθετήσουν τα καινούργια προϊόντα υψηλής τεχνολογίας όπως το ηλεκτρονικό εμπόριο, είναι η σχέση τιμής-κόστους αυτών. Το κόστος απόκτησης ηλεκτρονικού υπολογιστή

είναι αρκετά σημαντικό ενώ το κόστος χρήσης του Internet αν και παρουσιάζει πτωτική τάση στην Ελλάδα είναι από τα υψηλότερα μεταξύ των χωρών της Ευρωπαϊκής Ένωσης. Το κόστος χρήσης του Internet αποτελεί πρωταρχικό παράγοντα για την επιβαλλόμενη διάδοσή του. Χαρακτηριστικό παράδειγμα αποτέλεσε μια ιδιωτική εταιρεία στην χώρα μας η οποία προσέφερε δωρεάν πρόσβαση στο διαδίκτυο και κατόρθωσε να συγκεντρώσει περισσότερους από τους μισούς συνδρομητές του Internet στη χώρα, δηλαδή περισσότερους από ότι είχαν όλες μαζί οι εταιρείες παροχής επί πληρωμή πρόσβασης στο διαδίκτυο. Το γεγονός αυτό επιβεβαιώνει την μεγάλη σημασία που έχει ο παράγοντας της κοστολόγησης των προσφερομένων υπηρεσιών για την απρόσκοπτη εξάπλωση του διαδικτύου άρα και του ηλεκτρονικού εμπορίου κατ' επέκταση.

6.3.3 ΔΙΑΦΟΡΟΙ ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΕΠΗΡΕΑΖΟΥΝ ΑΡΝΗΤΙΚΑ ΤΗΝ ΔΙΑΔΟΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ:

Ø Η ανάγκη για ηλεκτρονική δικτύωση όλων των διαδικασιών-διοικητικών και παραγωγικών μιας εταιρίας είναι αναγκαία προκειμένου να μιλάμε για ηλεκτρονικές συναλλαγές και (B2B) εφαρμογές. Η έλλειψη αυτή σε συνάρτηση με την απουσία των απαιτούμενων γνώσεων Η/Υ από αρκετά μέλη και στελέχη των εταιρειών αποτελεί τροχοπέδη στην εξέλιξη και ολοκλήρωση των ηλεκτρονικών συναλλαγών μεταξύ των επιχειρήσεων.

Ø Παρατηρείται συχνά η συμμετοχή εταιριών σε περισσότερα από ένα e-marketplaces με ότι αυτό συνεπάγεται π.χ. καταγραφή των ίδιων προϊόντων με διαφορετικό κωδικό, σύγχυση στο αγοραστικό κοινό κ.λ.π. Έτσι προκύπτει η ανάγκη κοινά αποδεκτής κωδικοποίησης των προϊόντων ανεξάρτητα από την ηλεκτρονική αγορά που ανήκει η κάθε εταιρεία.

Ø Η έλλειψη πληροφόρησης σε επίπεδο στελεχών και διοίκησης σχετικά με τα οφέλη μιας επιχείρησης από την συμμετοχή της σε (B2B) εφαρμογές είναι βασικός παράγοντας για τον σκεπτικισμό και τον δισταγμό που παρατηρείται

από τον Ελληνικό επιχειρηματικό κόσμο. Επίσης υπάρχει έλλειψη επιτυχημένων παραδειγμάτων που να μπορούν να αποδείξουν την αποτελεσματικότητα από τις εφαρμογές (B2B).

Ωστόσο, παρά τα προβλήματα και τους κινδύνους που οι επιχειρήσεις και οι καταναλωτές έχουν να αντιμετωπίσουν κατά την εφαρμογή του ηλεκτρονικού εμπορίου η εξέλιξή του είναι γεγονός. Καθώς συσσωρεύεται εμπειρία από τους καταναλωτές και τις επιχειρήσεις και βελτιώνεται η τεχνολογία οι ωφέλειες από το ηλεκτρονικό εμπόριο όλο και αυξάνονται καταλήγοντας σε ένα μεγαλύτερο βαθμό υιοθέτησής του.

6.4 ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Ο διαρκώς αυξανόμενος όγκος συναλλαγών μέσω διαδικτύου έχει καταστήσει απαραίτητη την ανάπτυξη και διάδοση καινοτομικών συστημάτων ηλεκτρονικών πληρωμών. Στόχος των συστημάτων αυτών είναι να μπορούν να υποστηρίξουν τα ιδιαίτερα χαρακτηριστικά των συναλλαγών στο διαδίκτυο όπως ταχύτητα και αμεσότητα χωρίς όμως παράλληλα να θυσιάζουν βασικά πλεονεκτήματα των παραδοσιακών μέσων πληρωμών όπως είναι η ασφάλεια και η ευκολία.

Τα συστήματα ηλεκτρονικών πληρωμών ασχολούνται με οποιοδήποτε είδος υπηρεσίας δικτύου που περιλαμβάνει ανταλλαγή χρημάτων για αγαθά ή υπηρεσίες. Τα αγαθά μπορεί να είναι φυσικά όπως βιβλία, ή ηλεκτρονικά όπως ηλεκτρονικά έγγραφα, φωτογραφίες, μουσική. Όμοια οι υπηρεσίες μπορεί να είναι φυσικές όπως κράτηση μιας πτήσης, ή ηλεκτρονικές όπως ανάλυση χρηματιστηριακής αγοράς σε ηλεκτρονική μορφή. Σε ένα τυπικό σύστημα ηλεκτρονικών πληρωμών μέσω του διαδικτύου, για να γίνει δυνατή μια συναλλαγή πρέπει τόσο ο πελάτης όσο και ο έμπορας να έχουν πρόσβαση στο διαδίκτυο και επίσης πρέπει να έχουν από ένα τραπεζικό λογαριασμό σε κάποια

τράπεζα ή χρηματοπιστωτικό οργανισμό. Η τράπεζα (ή χρηματοπιστωτικός οργανισμός) του πελάτη και του έμπορα συνδέονται
μεταξύ τους μέσω ενός διατραπεζικού δικτύου και έτσι μπορούν να έρθουν σε επαφή.

Μια τυπική συναλλαγή στο διαδίκτυο (**Σχήμα 6.1**) αποτελείται από τα εξής βήματα:

Ο πελάτης επισκέπτεται το δικτυακό τόπο (site) του εμπόρου και επιλέγει τα προϊόντα που επιθυμεί. Έπειτα στέλνει πληροφορίες στον έμπορο σχετικά με τον τρόπο πληρωμής. Δηλαδή αν ο πελάτης επιθυμεί να πληρώσει με την πιστωτική του κάρτα, στέλνει στον έμπορο τον αριθμό της πιστωτικής του κάρτας και κάποιες άλλες πληροφορίες (π.χ. ημερομηνία έκδοσης της κάρτας κλπ.). Ο έμπορος προωθεί τις πληροφορίες που έλαβε από τον πελάτη στην τράπεζα του, προκειμένου να εξακριβώσει την εγκυρότητα του τρόπου πληρωμής (π.χ. της πιστωτικής κάρτας).

Στη συνέχεια η τράπεζα του έμπορα ζητά έγκριση πληρωμής από την τράπεζα του πελάτη π.χ. από τον οργανισμό έκδοσης της πιστωτικής του κάρτας. Η τράπεζα του πελάτη παρέχει έγκριση πληρωμής (αν π.χ. η συγκεκριμένη πιστωτική κάρτα μπορεί να χρεωθεί) και μεταβιβάζει το συμφωνημένο πληρωτέο ποσό από το λογαριασμό του πελάτη στην τράπεζα του έμπορα. Η τράπεζα του έμπορα ενημερώνει τον έμπορο πως η συναλλαγή είναι έγκυρη και πως έχει πληρωθεί το συγκεκριμένο χρηματικό ποσό της αξίας των προϊόντων που έχει αγοράσει ο πελάτης. Τέλος ο έμπορος αποστέλλει τα προϊόντα ή παρέχει τις συμφωνημένες υπηρεσίες στον πελάτη, σύμφωνα με την παραγγελία.

Σχήμα 6.1: Τυπική Συναλλαγή Πληρωμής.

Σημειώνεται ότι η όλη διαδικασία της συναλλαγής είναι τελείως διάφανη στους δύο τελικούς χρήστες. Ο πελάτης εμπιστεύεται την τράπεζα του και αγοράζει τα προϊόντα που θέλει, χωρίς να γνωρίζει καμιά από τις υπόλοιπες ενέργειες που μεσολαβούν μέχρι την τελική παράδοση των προϊόντων στο σπίτι του. Από την άλλη πλευρά, ο έμπορος εμπιστεύεται τη δική του τράπεζα η οποία και εγγυάται την πληρωμή των προϊόντων που πωλεί εκείνος, χωρίς να γνωρίζει περισσότερες λεπτομέρειες.

6.4.1 ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ

Οι πιστωτικές κάρτες έχουν τύχει ευρείας χρήσης στο διαδίκτυο επειδή διαθέτουν σημαντικά πλεονεκτήματα έναντι των εναλλακτικών μεθόδων πληρωμής. Κατ' αρχήν είναι διεθνώς γνωστές και αποδεκτές από τους εμπόρους, επιτρέποντας έτσι την πραγματοποίηση ακόμη και διεθνών συναλλαγών. Επιπλέον η χρήση τους στις ηλεκτρονικές συναλλαγές δεν διαφέρει και πολύ από την χρήση τους στις φυσικές συναλλαγές. Στις φυσικές

συναλλαγές ο πελάτης δίνει την κάρτα του στον έμπορα για χρέωση χέρι με χέρι, ενώ στις ηλεκτρονικές συναλλαγές ο πελάτης δίνει στον έμπορα τις πληροφορίες της κάρτας του μέσω του διαδικτύου. Αυτό έχει σαν αποτέλεσμα την πραγματοποίηση συναλλαγών χωρίς σημαντικές επενδύσεις από την πλευρά των εμπόρων αλλά και χωρίς αλλαγή στη συμπεριφορά των καταναλωτών.

Κατά την πληρωμή μέσω πιστωτικών καρτών στο διαδίκτυο ο πελάτης κοινοποιεί στον έμπορα τον αριθμό της πιστωτικής του κάρτας, καθώς και άλλες πληροφορίες της κάρτας όπως εκδότη, ημερομηνία λήξεως κλπ. Ο έμπορας ζητά έγκριση από την τράπεζα του η οποία σε συνεργασία με την τράπεζα του πελάτη (οργανισμό έκδοσης της κάρτας) δίνουν ή όχι έγκριση. Σε περίπτωση έγκρισης, ειδοποιείται ο έμπορος ότι η δαπάνη εγκρίθηκε και στέλνει τα προϊόντα στον πελάτη. Η τράπεζα του πελάτη προωθεί τα χρήματα στο λογαριασμό του έμπορα μέσω του διατραπεζικού συστήματος, και χρεώνει το ποσό στο λογαριασμό της πιστωτικής κάρτας του πελάτη. Σε τακτά χρονικά διαστήματα (συνήθως κάθε μήνα) η τράπεζα του πελάτη τον ειδοποιεί για τις συναλλαγές και τις δαπάνες του. Αυτός ο τρόπος πληρωμής παρέχει άμεση πρόσβαση στους τραπεζικούς λογαριασμούς του αγοραστή και του πωλητή και καταγράφει άμεσες μεταβολές στους λογαριασμούς τους.

Με την εμφάνιση του ηλεκτρονικού εμπορίου έχουν γίνει μεγάλης κλίμακας απάτες, κυρίως με κλεμμένους αριθμούς πιστωτικών καρτών. Η έγκριση που απαιτείται στα συστήματα πληρωμών είναι μια μορφή προστασίας. Είναι σημαντικό οι αριθμοί των πιστωτικών καρτών (και γενικά οι πληροφορίες πληρωμής) να είναι δυσανάγνωστες σε όλους, εκτός από τον πελάτη και την τράπεζα του. Δεν υπάρχει λόγος ο έμπορας να γνωρίζει τον αριθμό της πιστωτικής κάρτας του πελάτη. Για το λόγο αυτό, τα δεδομένα πληρωμής στέλνονται κρυπτογραφημένα υπό μορφή μηνύματος μέσα στο διαδίκτυο καθώς υπάρχει πιθανότητα το μήνυμα να υποκλαπεί.

Η χρήση της πιστωτικής κάρτας για αγορές σε ένα δικτυακό τόπο, αποτελεί έναν ασφαλή τρόπο πληρωμής. Για παράδειγμα, η easyJet έχει ήδη

διεξάγει πολλά εκατομμύρια κρατήσεις θέσεων μέσω Διαδικτύου. Χρησιμοποιούν πολλά βήματα ασφάλειας, έτσι ώστε να μπορούν να εγγυηθούν την απόλυτη ασφάλεια των δεδομένων των πελατών τους κατά την αγορά πτήσεων της easyJet μέσω Διαδικτύου.

Όλες οι ευαίσθητες πληροφορίες, συμπεριλαμβανομένων των προσωπικών δεδομένων, κρυπτογραφούνται και παραμένουν εμπιστευτικές. Αυτό σημαίνει ότι οι πληροφορίες μπορούν να ανταλλαχθούν μόνο ανάμεσα στο πελάτη και την easyJet και ότι κανείς τρίτος δεν μπορεί να αποκτήσει πρόσβαση σε αυτά τα δεδομένα. Στο πρόγραμμα πλοήγησης του πελάτη εμφανίζεται συνήθως το σύμβολο μίας κλειδαριάς, το οποίο συμβολίζει την κάλυψη μίας ιστοσελίδας από αυτό το σύστημα ασφάλειας.

Όλες οι πληροφορίες του ιστορικού της κράτησης, οι οποίες σχετίζονται με την πιστωτική κάρτα, το όνομα και τη διεύθυνση του πελάτη κρατούνται σε έναν ασφαλή υπολογιστή. Μετά την ολοκλήρωση της συναλλαγής δεν διατηρούνται ενεργά αρχεία των προσωπικών δεδομένων ή των στοιχείων της πιστωτικής κάρτας των επιβατών στους διακομιστές της easyJet (web servers).

6.4.2 ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΤΑΓΕΣ

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών, που τώρα υπογράφονται και μεταβιβάζονται ηλεκτρονικά, και μπορούν να έχουν όλες τις παραλλαγές των κοινών επιταγών, όπως ταξιδιωτικές επιταγές ή πιστοποιημένες επιταγές. Μια επιταγή χρησιμοποιείται για να μεταφέρει ένα μήνυμα προς την τράπεζα του αποστολέα για τη μεταφορά ενός συγκεκριμένου χρηματικού ποσού από το λογαριασμό του αποστολέα στο λογαριασμό κάποιου άλλου. Σε αντιστοιχία με την παραδοσιακή διαδικασία η ηλεκτρονική επιταγή αποστέλλεται αρχικά στον αποδέκτη του χρηματικού ποσού, ο οποίος την υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό. Στη συνέχεια η εξοφλημένη και

επικυρωμένη επιταγή επιστρέφεται στον αποστολέα ο οποίος τη χρησιμοποιεί ως απόδειξη πληρωμής. Μια ηλεκτρονική επιταγή έχει τα ίδια χαρακτηριστικά με μια έντυπη επιταγή. Είναι ένα ηλεκτρονικό έγγραφο που περιέχει τον αριθμό της επιταγής, το όνομα του πληρωτή, τον αριθμό λογαριασμού του πληρωτή και το όνομα της τράπεζας, το όνομα του δικαιούχου πληρωμής (αποδέκτη), το πληρωτέο ποσό, τη μονάδα χρήματος που χρησιμοποιείται, την ημερομηνία λήξης, την ηλεκτρονική υπογραφή του πληρωτή και την ηλεκτρονική επικύρωση του δικαιούχου πληρωμής.

Οι ηλεκτρονικές επιταγές χρησιμοποιούν την τεχνολογία των ψηφιακών υπογραφών. Από πλευράς ασφάλειας η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη, αφού ο αποστολέας μπορεί να προστατέψει τον εαυτό του από μια απάτη. Κάτι τέτοιο επιτυγχάνεται με την κρυπτογράφηση του αριθμού λογαριασμού του με το δημόσιο κλειδί της τράπεζας του, με αποτέλεσμα να μην αποκαλύπτεται στον έμπορα ο αριθμός του λογαριασμού. Σε μια συναλλαγή πληρωμής με ηλεκτρονικές επιταγές ο πελάτης παραγγέλλει κάποια προϊόντα από τον έμπορα και για πληρωμή του στέλνει μια ηλεκτρονική επιταγή ψηφιακά υπογεγραμμένη. Ο έμπορας γνωρίζοντας το δημόσιο κλειδί του πληρωτή, μπορεί να επιβεβαιώσει την ορθότητα της ψηφιακής υπογραφής και έτσι να επικυρώσει τη συγκεκριμένη επιταγή. Μετά την παραλαβή και επικύρωση της επιταγής, ο έμπορας στέλνει τα προϊόντα στον πελάτη. Η τράπεζα του πελάτη αποσύρει το ποσό πώλησης από το λογαριασμό του πελάτη και μέσω του διατραπεζικού συστήματος το εν λόγω ποσό πιστώνεται στο λογαριασμό του έμπορα.

6.4.3 ΗΛΕΚΤΡΟΝΙΚΟ ΧΡΗΜΑ

Το ηλεκτρονικό χρήμα είναι ένα σύγχρονο μέσο πληρωμής στο διαδίκτυο. Οι περισσότεροι αναλυτές συμφωνούν πάνω στο γεγονός, ότι η ανάπτυξη του ηλεκτρονικού εμπορίου οδηγεί αντίστοιχα στην ανάπτυξη του

ηλεκτρονικού χρήματος. Η χρήση ηλεκτρονικού χρήματος για την αγορά καταναλωτικών αγαθών μοιάζει να προτιμάται από πολλούς καταναλωτές, καθώς μπορεί να οδηγήσει στην ολοκλήρωση της διαδικασίας πολύ πιο γρήγορα από τη συμπλήρωση όλων των στοιχείων της πιστωτικής κάρτας. Τα σχήματα ηλεκτρονικού χρήματος στηρίζονται είτε σε κάρτες αποθηκευμένης αξίας είτε σε ειδικό λογισμικό. Στην πρώτη περίπτωση η κάρτα περιέχει ένα χρηματικό ποσό ανάλογο με αυτό που έχει προπληρώσει ο κάτοχος της. Η κάρτα μπορεί να είναι είτε ανώνυμη είτε ονομαστική. Ο κάτοχος της μπορεί να τη γεμίζει κάθε φορά με το ποσό που επιθυμεί. Για λόγους ασφάλειας, η κάρτα προστατεύεται από ένα κωδικό. Στα σχήματα ηλεκτρονικού χρήματος μέσω λογισμικού πραγματοποιείται έκδοση ηλεκτρονικών νομισμάτων από έναν παροχέα υπηρεσιών πληρωμών (συνήθως τράπεζα). Τα ηλεκτρονικά αυτά νομίσματα είναι αποθηκευμένα σε ένα ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη ο οποίος μπορεί να τα χρησιμοποιήσει για αγορές μέσω διαδικτύου. Το βασικό πλεονέκτημα των σχημάτων ηλεκτρονικών πληρωμών και στις δύο περιπτώσεις είναι ότι μπορεί να διατηρηθεί η ανωνυμία των συναλλαγών που είναι ιδιαίτερα σημαντική για τους πελάτες. Ως ηλεκτρονικό χρήμα, η Ευρωπαϊκή Κεντρική Τράπεζα ορίζει «την αποθήκευση χρηματικής αξίας σε ψηφιακή μορφή μέσω μιας συσκευής που μπορεί να χρησιμοποιηθεί ευρέως για την πραγματοποίηση πληρωμών σε δίκτυα χωρίς τη χρήση τραπεζικών λογαριασμών. Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο απόθεμα. Ενώ τα δίκτυα θα είναι είτε ανοικτά δηλαδή θα επιτρέπουν την άμεση μεταφορά χρημάτων μεταξύ αποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται από συγκεκριμένο τραπεζικό λογαριασμό αποκλειστικά».

Ωστόσο, γενικά με τον όρο ηλεκτρονικό χρήμα περιγράφεται κάθε μορφή μεταφοράς χρήματος μεταξύ δύο ή περισσότερων μερών που γίνεται με ψηφιακό τρόπο και χωρίς τη μεσολάβηση κάποιου υλικού μέσου. Τα χαρακτηριστικά που πρέπει να έχει το ηλεκτρονικό χρήμα είναι τα εξής:

• Ικανοποιητικό επίπεδο ασφάλειας.

• Ανωνυμία.

• Μεταφερσιμότητα (από μια μορφή σε άλλη π.χ. από ηλεκτρονικά νομίσματα σε μετρητά).

• Διαιρετότητα (να μπορεί να διαιρεθεί σε όσα τμήματα ίσης συνολικής αξίας θέλει ο
κάτοχος).

• Ευρεία αποδοχή.

• Ευχρηστία.

• Σταθερή αξία (προστασία από πληθωρισμό, υποτίμηση κλπ.).

Σε μια συναλλαγή πληρωμής με ηλεκτρονικό χρήμα ο πελάτης αρχικά έχει προμηθευτεί ψηφιακά νομίσματα από την τράπεζα του ή κάποιον άλλο οργανισμό έκδοσης ψηφιακών νομισμάτων. Με τα νομίσματα που αγόρασε ο πελάτης μπορεί να κάνει αγορές στο διαδίκτυο. Επειδή συνήθως τα ψηφιακά νομίσματα χρησιμοποιούνται για αγορές αγαθών ή υπηρεσιών χαμηλού κόστους, ο έμπορος πολλές φορές δίνει τα προϊόντα χωρίς να ζητήσει έγκριση πληρωμής. Στη συνέχεια ο έμπορος στέλνει αίτημα εξαγοράς νομισμάτων στην τράπεζα του.

Μέσω του διατραπεζικού δικτύου η τράπεζα του έμπορα εξαργυρώνει τα νομίσματα στον οργανισμό που τα έκδωσε και πιστώνει το λογαριασμό του έμπορα με το ισοδύναμο ποσό. Ο οργανισμός έκδοσης νομισμάτων για να εξασφαλίσει ότι το κάθε νόμισμα χρησιμοποιείται μόνο μια φορά, καταγράφει τον αύξοντα αριθμό του κάθε νομίσματος καθώς αυτό ξοδεύεται. Αν ο αριθμός αυτός είναι ήδη καταγραμμένος στη βάση δεδομένων ο οργανισμός διαπιστώνει απάτη, ακυρώνει το νόμισμα πριν τη συναλλαγή και ειδοποιεί τον έμπορο.

6.4.4 ΗΛΕΚΤΡΟΝΙΚΟ ΠΟΡΤΟΦΟΛΙ

Το ηλεκτρονικό πορτοφόλι είναι ένα νέο εργαλείο πληρωμών που προσφέρει σημαντικά πλεονεκτήματα τόσο στους καταναλωτές, όσο και στους εμπόρους και χαράζει την πορεία προς την αντικατάσταση των μετρητών, τουλάχιστον όσον αφορά τις καθημερινές μικροσυναλλαγές και γενικότερα συμβάλει στη διευκόλυνση των συναλλαγών μέσω ηλεκτρονικού εμπορίου.

Υπάρχουν δύο είδη ηλεκτρονικού πορτοφολιού:

Προπληρωμένες κάρτες: Οι κάρτες αυτές έχουν το μέγεθος και τη μορφή πιστωτικών καρτών και χρησιμοποιούνται για συναλλαγές στο διαδίκτυο. Οι εν λόγω κάρτες μπορεί να είναι είτε ονομαστικές είτε ανώνυμες. Σε περίπτωση που είναι ονομαστικές, κάθε πελάτης παίρνει από την τράπεζα του μια κάρτα αποθηκευμένης αξίας, στην οποία μεταφέρει χρήματα από το λογαριασμό του, και τη χρησιμοποιεί για τις αγορές του στο διαδίκτυο και όχι μόνο. Για λόγους ασφάλειας και ευελιξίας υπάρχει μια τάση οι κάρτες αυτές να είναι έξυπνες κάρτες. Στη δεύτερη περίπτωση όπου η κάρτα είναι ανώνυμη, ο κάτοχος της μπορεί να τη χρησιμοποιεί για τις αγορές του στα ηλεκτρονικά καταστήματα εύκολα, ανώνυμα και με ασφάλεια οποιαδήποτε ώρα της ημέρας επιθυμεί. Ένα άλλο πλεονέκτημα της ανώνυμης κάρτας είναι ότι η κάρτα μπορεί να μεταβιβαστεί από ένα άτομο σε ένα άλλο, ενώ η ονομαστική δεν μπορεί να μεταβιβαστεί. Η χρήση προπληρωμένων καρτών δημιουργεί έναν εναλλακτικό τρόπο πληρωμής ώστε να είναι δυνατή η χρήση του διαδικτύου για την πραγματοποίηση αγορών ακόμα και από εκείνους τους καταναλωτές που είναι επιφυλακτικοί στη χρήση της πιστωτικής κάρτας για λόγους ασφάλειας.

Ειδικό λογισμικό: Χρησιμοποιείται ένας ειδικά διαμορφωμένος τύπος λογισμικού (ιδεατό πορτοφόλι) για την αποθήκευση χρηματικής αξίας με τη μορφή ψηφιακών νομισμάτων. Τα ψηφιακά αυτά νομίσματα που είναι αποθηκευμένα στο ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη, μπορούν να χρησιμοποιηθούν για αγορές στο διαδίκτυο. Γενικά, ένα

Ηλεκτρονικό Πορτοφόλι διαθέτει ένα συγκεκριμένο χρηματικό ποσό και μπορεί να χρησιμοποιηθεί για αγορές στα συνεργαζόμενα με την τράπεζα που το εκδίδει, ηλεκτρονικά καταστήματα. Το ηλεκτρονικό πορτοφόλι παρέχει μέγιστη ασφάλεια, καθώς το ποσό χρέωσης δε μπορεί να υπερβεί το αποθηκευμένο ποσό που υπάρχει στο πορτοφόλι.

6.4.5 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Μια έξυπνη κάρτα είναι μια πλαστική ίση σε μέγεθος με μια πιστωτική κάρτα, στην οποία έχει ενσωματωθεί ένα ολοκληρωμένο κύκλωμα (chip). Το ολοκληρωμένο κύκλωμα μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Το κύριο πλεονέκτημα των έξυπνων καρτών είναι ότι παρέχουν φυσική προστασία των αποθηκευμένων δεδομένων. Μια από τις πλέον ενδιαφέρουσες ιδιότητες των έξυπνων καρτών είναι ότι είναι εξαιρετικά δύσκολο να αντιγραφούν.

Με την αύξηση της διαθέσιμης υπολογιστικής δύναμης και μνήμης μεγαλώνει και ο αριθμός των εφαρμογών με έξυπνες κάρτες. Οι έξυπνες κάρτες χρησιμοποιούνται ήδη στις εφαρμογές ηλεκτρονικού εμπορίου.

Οι έξυπνες κάρτες διευκολύνουν την εφαρμογή των υποδομών δημοσίου κλειδιού, οι οποίες χρησιμοποιούνται ευρέως στο ηλεκτρονικό εμπόριο. Οι υποδομές δημοσίου κλειδιού μπορούν να εξασφαλίσουν υψηλό επίπεδο εμπιστοσύνης στις ηλεκτρονικές συναλλαγές. Επιπλέον παρέχουν ακεραιότητα δεδομένων, ασφάλεια και ιδιωτικότητα. Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν τα ιδιωτικά κλειδιά με ασφάλεια. Σε αντίθετη περίπτωση τα ιδιωτικά κλειδιά αποθηκεύονται στους υπολογιστές των κατόχων τους, όπου είναι τρωτά σε επιθέσεις εισβολέων με σκοπό την απόκτηση τους. Η μεταφορά του ιδιωτικού κλειδιού μέσα στην έξυπνη κάρτα διευκολύνει ιδιαίτερα τις ηλεκτρονικές συναλλαγές. Όπως είναι γνωστό, για να γίνει μια ηλεκτρονική συναλλαγή απαιτείται η ανταλλαγή ευαίσθητων προσωπικών δεδομένων μεταξύ

των συναλλασσόμενων πλευρών. Οι έξυπνες κάρτες αποτελούν ένα άριστο μέσο για τη μεταφορά ευαίσθητων προσωπικών δεδομένων όπως για παράδειγμα αριθμούς πιστωτικών καρτών, κλειδιά κρυπτογράφησης και αποκρυπτογράφησης κλπ.

Οι κάρτες αυτές μπορούν επιπλέον να αντικαταστήσουν κάρτες όπως οι τηλεκάρτες, οι πιστωτικές κάρτες, οι κάρτες ανάληψης μετρητών και άλλες παρόμοιες κάρτες. Μπορούν επίσης να χρησιμοποιηθούν ως προπληρωμένες κάρτες για την αποθήκευση ψηφιακών νομισμάτων. Μια τέτοια κάρτα πολλαπλών εφαρμογών που χρησιμοποιείται στις ηλεκτρονικές συναλλαγές είναι η Java Card.

6.4.6 ΔΙΑΔΙΚΤΥΑΚΕΣ ΤΡΑΠΕΖΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Σύμφωνα με έρευνες, όλο και περισσότεροι ιδιώτες αλλά και επιχειρήσεις στην Ελλάδα προτιμούν να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω Διαδικτύου. Τα αποτελέσματα της Εθνικής Έρευνας για τις Νέες Τεχνολογίες και την Κοινωνία της Πληροφορίας δείχνουν ότι το 2001 περίπου 150.000 πελάτες (1%-1,5% του πληθυσμού) πραγματοποίησαν τραπεζικές συναλλαγές ηλεκτρονικά. Το 2002 ο αριθμός αυτός ξεπέρασε τους 250.000 (2,5% του συνολικού πληθυσμού). Σύμφωνα με εκτιμήσεις τραπεζών, το 2001 ο τζίρος από on-line τραπεζικές συναλλαγές έφθασε τα 2 δισ. ευρώ. Το 2002 το ποσό αυτό εκτιμάται ότι αυξήθηκε σε 10 δισ. ευρώ, ενώ αναμένεται να υπερβεί τα 40 δισεκατομμύρια. Σύμφωνα με στοιχεία της Τράπεζας Πειραιώς, οι συναλλαγές μέσω Winbank Internet παρουσιάζουν ραγδαία ανάπτυξη: το 2003 οι εγχρήματες συναλλαγές αυξήθηκαν με ρυθμό της τάξεως του 150% έναντι του 2002. Επίσης, το 50% όλων των πληρωμών ΙΚΑ πραγματοποιείται online, ενώ οι ηλεκτρονικές χρηματιστηριακές συναλλαγές υπερβαίνουν το 15% επί του συνόλου.

Η εξάπλωση του e-banking είναι ραγδαία σε όλο τον κόσμο. Ειδικοί εκτιμούν ότι στο μέλλον οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών. Ενδεικτικά, στη Γερμανία το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες e-banking, στη Σουηδία το 28%, στη Βρετανία το 7%.

Παρά τις εξελιγμένες μεθόδους για τη διασφάλιση των τραπεζικών συναλλαγών, η συχνότητα των ηλεκτρονικών επιθέσεων αυξάνεται τα τελευταία χρόνια. Η αύξηση αυτή προκαλεί ανησυχία στους ειδικούς, καθώς διακυβεύονται τεράστια ποσά, ειδικά στις περιπτώσεις κατά τις οποίες θύματα απάτης γίνονται επιχειρήσεις. Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους για να επιτύχουν τους σκοπούς τους. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Έρευνες ειδικών σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είτε είχαν την ακούσια συνήθως βοήθεια και κάποιου που εργαζόταν στην τράπεζα, είτε υπέκλεψαν κωδικούς χρηστών.

Οι επιχειρήσεις-πελάτες είναι συνήθως προσεκτικές και χρησιμοποιούν συστήματα ασφαλείας στα δίκτυά τους. Την ίδια "σοφία" ή προσοχή δεν δείχνουν και οι ιδιώτες πελάτες, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι απλοί χρήστες γίνονται εύκολα θύματα προγραμμάτων που στην πραγματικότητα ανοίγουν "τρύπες" ασφάλειας στο σύστημα και με τον τρόπο αυτό επιτρέπουν σε επιτήδειους να έχουν πρόσβαση σε αυτό και να κινούνται μέσα σε αυτό ανενόχλητοι.

Ωστόσο και οι επιχειρήσεις δεν είναι πάντοτε ασφαλείς. Σε ορισμένες περιπτώσεις, εταιρίες συνεργάζονται με τράπεζες προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με εταιρικούς πελάτες. Οι τράπεζες ενίοτε επιτρέπουν στις εταιρίες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, οι επιτήδειοι μελετούν τον τρόπο με τον οποίο οι επιχειρήσεις επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα.

Μόλις βρεθεί μια αδυναμία, μεταφέρουν με λίγες απλές κινήσεις ολόκληρους εταιρικούς λογαριασμούς στις προσωπικές τους θυρίδες. Να σημειωθεί, πάντως, πως η πρακτική αυτή, η διαχείριση δηλαδή τραπεζικού δικτύου από εταιρικό πελάτη, δεν συνηθίζεται στην Ελλάδα. Εξάλλου μέχρι σήμερα δεν έχουν δει το φως της δημοσιότητας περιπτώσεις απάτης στον τομέα του ελληνικού e-banking.

6.4.6.1 Η ΣΗΜΕΡΙΝΗ ΤΟΥΣ ΕΦΑΡΜΟΓΗ ΣΤΗΝ ΕΛΛΑΔΑ

Το e-banking (ή Internet banking) υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές. "Μεταφέρει" την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω Διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών, παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών, καθώς και πλήθος άλλων υπηρεσιών. Οι πελάτες (ιδιώτες και επιχειρήσεις) ωφελούνται σημαντικά από τη χρήση των υπηρεσιών e-banking, καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με την τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για τις ΜΜΕ το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος.

Με το e-banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής. Συχνό είναι και το φαινόμενο των προσφορών ή της εφαρμογής ευνοϊκότερων όρων στην παροχή προϊόντων μέσω Internet, γεγονός που από μόνο του είναι ικανό να προσελκύσει σημαντική μερίδα καταναλωτών που αναζητούν προσφορές. Οι βασικότερες υπηρεσίες που παρέχουν μέσω Internet οι ελληνικές τράπεζες είναι οι εξής:

- Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς.
- Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ιδίου νομίσματος.
- Πληροφορίες σχετικά με τις πρόσφατες κινήσεις των τηρούμενων λογαριασμών.
- Δυνατότητα έκδοσης και αποστολής παλαιότερων κινήσεων των τηρούμενων

λογαριασμών.

- Παραγγελία μπλοκ επιταγών.
- Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκ επιταγών.
- Εντολές αγοραπωλησίας μετοχών.
- Ενημέρωση για την κίνηση των προσωπικών αμοιβαίων κεφαλαίων.
- Δυνατότητα υποβολής αιτήσεων εμβασμάτων.
- Αλλαγή του απορρήτου κωδικού PIN.
- Προσωπικά μηνύματα.

Σε πολλές ευρωπαϊκές χώρες, όπου τα συστήματα πληρωμών είναι περισσότερο

ανεπτυγμένα και τυποποιημένα, ο προσανατολισμός των τραπεζών στρέφεται σταδιακά στην παροχή πρόσθετων υπηρεσιών προς τις επιχειρήσεις (corporate sites), πεδίο στο οποίο η γκάμα των επιλογών είναι ιδιαίτερα διευρυμένη.

6.5 ΔΙΑΦΟΡΕΣ ΜΟΡΦΕΣ ΕΜΦΑΝΙΣΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΑΓΟΡΑ.

Με την ολοένα και ταχύτερη ανάπτυξη των τεχνολογιών και των επικοινωνιών στη χώρα μας και ειδικότερα με τη ραγδαία, το τελευταίο καιρό, ανάπτυξη του Internet,η μορφή αλλά και η δραστηριότητα του εμπορίου

αλλάζει. Έτσι έχουμε μια νέα μορφή εμπορίου, το ηλεκτρονικό εμπόριο, έχει κάνει δυναμική εμφάνιση και διεκδικεί σημαντικό μερίδιο από το παραδοσιακό εμπόριο.

Το ηλεκτρονικό εμπόριο στην Ελλάδα εμφανίζεται με 2 τύπους δραστηριότητας και διάφορες μορφές έτσι ώστε τόσο ο καταναλωτής όσο και οι διάφορες επιχειρήσεις να έχουν τη δυνατότητα να πραγματοποιήσουν κάθε είδους συναλλαγές. Ως προς τους τύπους μπορεί κανείς να διακρίνει το **έμμεσο ηλεκτρονικό εμπόριο,** όπου η παραγγελία των προϊόντων γίνεται μέσω ηλεκτρονικού υπολογιστή, τα οποία στη συνέχεια παραδίδονται στον πελάτη με παραδοσιακά μέσα, και το **άμεσο ηλεκτρονικό εμπόριο**, όπου ολόκληρη η διαδικασία γίνεται ηλεκτρονικά (π.χ. πώληση προγραμμάτων λογισμικού).
Παρακάτω δίνεται ένας πίνακας για να δούμε συνοπτικά τι ακριβώς είναι το έμμεσο και άμεσο ηλεκτρονικό εμπόριο:

Έμμεσο Η.Ε.	**Άμεσο Η.Ε.**
Ηλεκτρονική παραγγελία προϊόντων Τα αγαθά παραδίδονται με παραδοσιακούς τρόπους (π.χ ταχυδρομείο, ιδιωτικές υπηρεσίες διανομής) Εξαρτάται από εξωτερικούς παράγοντες(π.χ. αποτελεσματικότητα συστήματος μεταφορών)	Ηλεκτρονική παραγγελία προϊόντων Πληρωμή και παράδοση άϋλων αγαθών και υπηρεσιών(π.χ. λογισμικό, ψυχαγωγικό περιεχόμενο) Υποστήριξη ηλεκτρονικών εμπορικών συναλλαγών σε παγκόσμιο επίπεδο

Από την άλλη πλευρά οι πιο συνηθισμένες μορφές ηλεκτρονικού εμπορίου αφορούν:

E-shopping: εδώ έχουμε τα λεγόμενα ηλεκτρονικά καταστήματα-ηλεκτρονικές αγορές όπου ο καταναλωτής, η επιχείρηση και το κράτος μπορούν να

εκτελέσουν ηλεκτρονικές συναλλαγές είτε με τη μορφή αγαθών είτε με τη μορφή υπηρεσιών, μπορούν επίσης οι εκάστοτε ενδιαφερόμενοι να πάρουν πληροφορίες για τα προϊόντα η τις υπηρεσίες που ενδιαφέρονται, δηλαδή ηλεκτρονικό εμπόριο δεν είναι μόνο η αγορά αλλά και η πληροφόρηση, η διαφήμιση.

Το e-shopping χωρίζεται σε υποκατηγορίες ανάλογα με τα μέρη που συμμετέχουν σε μια ηλεκτρονική συναλλαγή:

α)**επιχειρήσεις προς επιχειρήσεις**:Αυτή η κατηγορία είναι η λεγόμενη ‘’business to business’’, εδώ υπάρχουν συναλλαγές μεταξύ των επιχειρήσεων με παραγγελιές και πληρωμές μέσα από τα δίκτυα τηλεπικοινωνιών. Με την εφαρμογή της μορφής αυτής οι επιχειρήσεις στοχεύουν στη απλοποίηση των διαδικασιών παραγγελιάς, στην αυτοματοποιημένη αντικατάσταση των προϊόντων , στην επίτευξη καλύτερων προσφορών για τα προϊόντα με σκοπό τη μείωση του κόστους και τη μεγιστοποίηση του κέρδους. Βέβαια, απαραίτητη προϋπόθεση για την επιτυχία αυτής της μορφής είναι ο συντονισμός και η διαρκής και αποτελεσματική συνεργασία των επιχειρήσεων μεταξύ τους.

Σύμφωνα με τον γενικό διευθυντή της Intel κ. Rob Eckelman σε άρθρο του (Αύγουστο του 2000), *η οικονομία του internet επιβάλλει τον επαναπροσδιορισμό της πολιτικής των επιχειρήσεων παγκοσμίως. Η χρήση του internet για επιχειρηματικές συναλλαγές μεταξύ των εταιριών των χωρών της Ευρώπης (και της Ελλάδας) αυξάνεται με εκρηκτικούς ρυθμούς. Είναι άλλωστε χαρακτηριστικό ότι ως το 2004 το 87% των εσόδων που αναμένονται από το ηλεκτρονικό εμπόριο(τουλάχιστον 509 δισεκατομμύρια ευρώ) θα προέρχεται από συναλλαγές μεταξύ επιχειρήσεων(business to business).*

β)**επιχειρήσεις προς καταναλωτές**:Αυτή είναι η πιο γνωστή στους χρήστες internet μορφή ηλεκτρονικού εμπορίου, γνωστή ως ‘’business to customer’’, η οποία θα μπορούσε να χαρακτηριστεί και ως λιανικό ηλεκτρονικό εμπόριο. Η κατηγορία αυτή παρουσιάζει μια συνεχή αυξανόμενη χρήση σε παγκόσμιο επίπεδο, λόγω των δυνατοτήτων του internet, το οποίο ενδείκνυται για την

αποτελεσματική προώθηση προϊόντων και υπηρεσιών σε μεγάλο εύρος πιθανών πελατών. Οι επιχειρήσεις εκμεταλλευόμενες τα πλεονεκτήματα και τα οφέλη που προσφέρει το ηλεκτρονικό εμπόριο και συγκεκριμένα η παγκοσμιοποίηση της αγοράς μέσω του διαδικτύου δημιουργούν προϊόντα και υπηρεσίες με διάφορες καινοτομίες και τα προωθούν στους καταναλωτές .

γ)**δημόσιος φορέας προς επιχείρηση**:Σε αυτή τη κατηγόρια περιλαμβάνεται η κάθε μορφής ηλεκτρονική επικοινωνία μεταξύ ιδιωτικών εταιριών και των αρμόδιων αρχών, τόσο για τη διεκπεραίωση φορολογικών η άλλων υποχρεώσεων, όσο και για την αυτοματοποίηση της διαδικασίας των δημόσιων προμηθειών. Οι συναλλαγές των επιχειρήσεων με τους δημόσιους φορείς αφορούν συνήθως τέσσερις περιπτώσεις :

1. φορολογία
2. εισαγωγές-εξαγωγές μέσω τελωνείων
3. δημόσιες προμήθειες
4. προηγμένες ηλεκτρονικές υπηρεσίες

δ)**δημόσιος φορέας προς πολίτες- καταναλωτές**: Στην κατηγόρια αυτή οι πολίτες –καταναλωτές συναλλάσσονται με τους δημόσιους οργανισμούς χρησιμοποιώντας το διαδίκτυο είτε για εκπλήρωση των φορολογικών τους υποχρεώσεων είτε για να προμηθευτούν κάποια πιστοποιητικά ή βεβαιώσεις είτε ακόμη και για να πάρουν τις απαραίτητες πληροφορίες σχετικά με θέματα που τους ενδιαφέρουν π.χ. μισθοί, συντάξεις, επιδόματα.

<u>E-marketing</u>:

Για κάθε marketer ένα μέσο που επιτρέπει το one to one marketing είναι πάντοτε ενδιαφέρον. Όταν δε αυτό μπορεί να γίνει ταυτόχρονα σε εκατομμύρια χρήστες με πολύ μικρό κόστος και με αποτελεσματικό τρόπο, τότε δεν είναι δυνατόν να προσπεραστεί με αδιαφορία.

Πράγματι είναι διάφορα χαρακτηριστικά που καθιστούν μοναδικό το ίντερνετ για δραστηριοποίηση στο marketing και κατ`επέκταση στο

ηλεκτρονικό εμπόριο. Πρώτα από όλα το e-marketing είναι μέσο αμφίδρομης επικοινωνίας . Επίσης η επικοινωνία μπορεί να είναι ή να δείχνει προσωπική.

Βέβαια όλα αυτά δείχνουν ότι το e-marketing μπορεί να παίξει ρόλο στην αύξηση των κερδών των εταιριών όμως πρέπει να γίνουν κάποια βήματα για να εξελιχθεί στην ελληνική αγορά:

- Δημιουργία εταιρικών sites με στόχο την προβολή της εταιρίας, την ενημέρωση γύρω από αυτήν και βέβαια τη δυνατότητα ηλεκτρονικής αγοράς των προϊόντων της,
- Ηλεκτρονικά newsletters η μηνύματα ηλεκτρονικού ταχυδρομείου, κυρίως ενημερωτικού αλλά και αγοραστικού χαρακτήρα. Αυτό θα βοηθήσει γιατί όταν ο χρηστής επιλέγει να λαμβάνει μηνύματα με θέματα που τον ενδιαφέρουν, τότε τα αποτελέσματα συνήθως είναι θετικά.
- Διαφημιστικές καταχωρήσεις σε sites που έχουν μεγάλη κίνηση. Έτσι ώστε να προβάλλεται η εταιρία παγκοσμίως σε πολλούς χρηστές ταυτόχρονα.

E-government:

Προσπαθώντας να δώσουμε έναν ορισμό για την έννοια ηλεκτρονική διακυβέρνηση η e-government θα λέγαμε ότι πρόκειται για την τεχνολογική εξέλιξη της δημόσιας διοίκησης αλλά και την αμφίδρομη σχέση της με το σύνολο των φορέων από τους οποίους περιστοιχίζεται, αλλά και με τους πολίτες μέσω της αξιοποίησης και της χρήσης της σημερινής τεχνολογίας.

Με την εφαρμογή αυτής της μορφής ηλεκτρονικού εμπορίου επιτυγχάνεται η αρτιότερη εξυπηρέτηση του πολίτη, αύξηση της αποτελεσματικότητας του κράτους και των οργάνων του αλλά επίσης έχουμε και την εξοικονόμηση σημαντικών πόρων τόσο για το κράτος όσο και για τον υπόλοιπο κόσμο.

Συγκεκριμένα έχουμε διάφορους τομείς που διευκολύνονται όσοι συμμετέχουν σε αυτή τη μορφή ηλεκτρονικού εμπορίου:

- **Τοπική και περιφερειακή αυτοδιοίκηση:**

Οι καινοτομίες που έχουν προωθηθεί σε τοπικό επίπεδο (δήμος, νομαρχία, περιφέρεια) είναι ιδιαίτερα σημαντικές. Οι δημοτικοί σύμβουλοι μπορούν να ανταλλάσσουν γνώσεις και πληροφορίες μέσω εσωτερικών δικτύων, ενώ οι πολίτες θα έχουν πρόσβαση σε διάφορες υπηρεσίες μέσω ηλεκτρονικών σελίδων και περίπτερων πολυμέσων. μάλιστα σύμφωνα με άρθρο της εφημερίδας ‘’τα νέα’(Απρίλιο του 2004):*όλο και περισσότεροι φορολογούμενοι προτιμούν τον δρόμο του διαδικτύου προκείμενου να υποβάλλουν τη φορολογική του δήλωση. Αυτό προκύπτει από τα επίσημα στοιχεία της Γενικής Γραμματείας Πληροφοριακών Συστημάτων για την πορεία υποβολής των φετινών φορολογικών δηλώσεων σύμφωνα λοιπόν με αυτά τα στοιχεία, έως και την τέταρτη εβδομάδα υποβολής των δηλώσεων έχουν κατατεθεί ηλεκτρονικά στο σύστημα* taxis net *39.344 φορολογικές δηλώσεις, αριθμός πολύ μεγαλύτερος από περασμένα έτη.*

Αυτή η προτίμηση συμβαίνει πλέον γιατί οι φορολογούμενοι αποφεύγουν τη ταλαιπωρία της επίσκεψης στην εφορία αλλά αποφεύγουν και το χάσιμο χρόνου καθώς μπορούν ακόμη και τα σαββατοκύριακα να καταθέσουν τη φορολογική τους δήλωση ανά πάσα στιγμή. Επίσης ηλεκτρονική κατάθεση της δήλωσης συνεπάγεται γρήγορη Αποστόλη του εκκαθαριστικού, το οποίο συμφέρει ιδιαίτερα αυτούς που δικαιούνται επιστροφή φόρου.

- **Αγορά εργασίας:**

Η τεχνολογία συμβάλλει στη δημιουργία νέων θέσεων με τη δημιουργία ενός ηλεκτρονικού σημείου επικοινωνίας για όλους τους παράγοντες της αγοράς εργασίας. Έτσι οι εργοδότες δημοσιεύουν τις αγγελίες τους στο internet και όσοι αναζητούν εργασία δημοσιεύουν το βιογραφικό τους.

- **Άμυνα:**

Οι ένοπλες δυνάμεις μπορούν να χρησιμοποιήσουν την τεχνολογία τόσο σε διοικητικό όσο και σε επιχειρησιακό επίπεδο. Με τη χρήση υπολογιστικών συστημάτων που εντοπίζουν με ακρίβεια την πληροφορία, έχουμε αποφασιστική συμβολή στη διαδικασία λήψης αποφάσεων, εκμηδενισμό των δυσλειτουργιών και στήριξη της αξιοκρατίας.

- **Δικαιοσύνη:**

Το υπάρχον σύστημα απονομής της δικαιοσύνης χαρακτηρίζεται και αντιμετωπίζεται από πολλούς ως χρονοβόρο και γραφειοκρατικό. Με τη σωστή χρήση της τεχνολογίας μειώνονται οι αναβολές στην εκδίκαση υποθέσεων και έτσι έχουμε αύξηση της αποτελεσματικότητας , ενώ τεκμηριώνεται ακόμη περισσότερο η αξιοπιστία του συστήματος.

- **Υγειά:**

Οι υγειονομικές υπηρεσίες απαιτούν τη συνεργασία μεταξύ οικογενειακών γιατρών, νοσοκομείων, ασφαλιστικών φορέων, φαρμακειών και κρατικών υπηρεσιών. Σήμερα κάθε παράγοντας των υπηρεσιών υγείας έχει το δικό του σύστημα πληροφορικής .έτσι μέσω της ηλεκτρονικής διακυβέρνησης θα είναι δυνατόν να επικοινωνούν όλοι αυτοί οι παράγοντες ηλεκτρονικά και θα αποφεύγεται η ταλαιπωρία τόσο των ασθενών όσο και των υπόλοιπων φορέων.

- **Εκπαίδευση:**

Με τις νέες τεχνολογικές εφαρμογές της πληροφορικής και τις κατάλληλες υποδομές ο ρόλος του σχολείου αναβαθμίζεται κατά πολύ .Το διαδίκτυο είναι εργαλείο-κλειδί τόσο στα χέρια των δασκάλων όσο των γονέων και των μαθητών. Χαρακτηριστικό παράδειγμα είναι η υλοποίηση του εκπαιδευτικού προγράμματος ‘’ΟΔΥΣΣΕΑΣ 2004’’μέσω τηλεδιασκέψεων στα σχολικά συγκροτήματα. Στο πρόγραμμα αυτό συμμετέχουν δέκα σχολεία:έξι από την Κύπρο και τέσσερα από την Ελλάδα που έγιναν 6 τηλεδιασκέψεις μεταξύ των σχολείων με διαφορετικές ενότητες η καθεμία και θα μπορούν τα παιδία

να ανταλλάξουν απόψεις μεταξύ τους και γενικότερα αυτό θα είναι κάτι πολύ εποικοδομητικό για όλους τους εμπλεκόμενους φορείς..

Σύμφωνα με τον κ. Παναγιώτη Γεωργιάδη σε συνέντευξη του τον Ιανουάριο του 2004, *μέσα στο 2004 θα ολοκληρώσουμε δυο πολύ σημαντικά βήματα. Αρχής γενόμενης από το Φεβρουάριο, θα κατατεθεί στη βουλή το ειδικό νομοσχέδιο για τη νέα δομή της δημόσιας διοίκησης το οποίο περιλαμβάνει και πολλά ποιοτικά χαρακτηριστικά. Για παράδειγμα στο κεφαλαίο αξιολόγησης ανθρώπινου δυναμικού επισημαίνεται ότι ένα ανώτατο στέλεχος της δημόσιας διοίκησης πρέπει να κατανοεί τις εξελίξεις της ηλεκτρονικής διακυβέρνησης, να τις προωθεί και , σίγουρα να μην τις αναστέλλει. Το δεύτερο σημαντικό βήμα αφορά στη δημιουργία μιας λευκής βίβλου για τη δημόσια διοίκηση, μια εξειδικευμένη έκδοση που θα οδηγήσει τους ανθρώπους που εργάζονται στη δημόσια διοίκηση να σκέφτονται με όρους προοπτικής*.

Όμως πρέπει να εκπληρωθούν και κάποιες άλλες προϋπόθεσης για τη περαιτέρω εξέλιξη αυτής της μορφής στην Ελλάδα:

- **Καθορισμός πρότυπων:**

Τα πληροφοριακά συστήματα που υπάρχουν αυτή τη στιγμή στη διοίκηση δεν έχουν σχεδιαστεί εκτιμώντας συνολικά τις ανάγκες .Με το καθορισμό των πρότυπων θα έχουμε ενιαία ροή της πληροφορίας από σύστημα σε σύστημα στο δημόσιο τομέα και θα δίνουν τη δυνατότητα τόσο στους πολίτες όσο και στις επιχειρήσεις για καλύτερη πρόσβαση σε ολοκληρωμένες κρατικές υπηρεσίες.

- **Υποδομή δικτύων:**

Η ανάπτυξη των ευριζωνικών δικτύων αναμένεται να αποτελέσει τη βάση για την ηλεκτρονική διακυβέρνηση. Αυτό φαίνεται και από τη συνέντευξη του κ. Γεωργιάδη (Ιανουάριο του 2004):*το 2004 θα είναι πρωταγωνιστής τα ευρυζωνικά δίκτυα, τα κονδύλια για την ανάπτυξη τους είναι αρκετά, και αποτελούν έναν από τους κρίσιμους παράγοντες για το e-government στην Ελλάδα είναι αυτός που θα ανοίξει το δρόμο. Στην επαρχία ήδη λαμβάνονται*

πρωτοβουλίες. Για παράδειγμα, σε πανεπιστήμιο της Πελοποννήσου μόνοι τους οι φοιτητές μετέτρεψαν την πολυκατοικία που μένουν σε ευρυζωνική. Ακολουθώντας τη πορεία των νέων αποφασίσαμε στο υπουργείο εσωτερικών να προχωρήσουμε σε διαγωνισμό έτσι ώστε το κτίριο του υπουργείου μας να γίνει ευρυζωνικό.

- **Δημιουργία on-line πολίτη:**

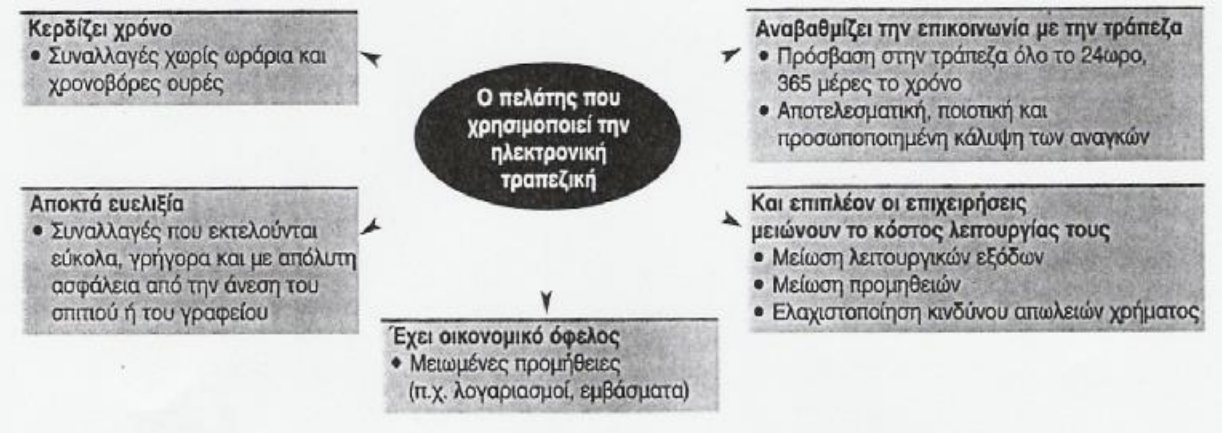
Η διοίκηση πρέπει να αναλάβει πρωτοβουλίες ώστε να ενθαρρύνει τη συμμετοχή των πολιτών στην ηλεκτρονική διακυβέρνηση. Δηλαδή γα παράδειγμα, πρέπει να επιδοτήσει τους πολίτες για την αγορά ηλεκτρονικού υπολογιστή, γιατί σήμερα είναι το βασικότερο μέσο για πρόσβαση στο διαδίκτυο.

E-banking:

Στο σημερινό επαγγελματικό χώρο, σημαντικές προτεραιότητες για κάθε άνθρωπο και επιχείρηση προσαρμοσμένο στις τεχνολογικές εξελίξεις είναι η ταχύτητα και η αξιοπιστία των συναλλαγών.

Με την ηλεκτρονική τραπεζική η αλλιώς e-banking αναβαθμίζεται η επικοινωνία του πελάτη με τις τράπεζες που συνεργάζεται, και αυτό γιατί αποφεύγονται οι χρονοβόρες ουρές στα τραπεζικά καταστήματα, οι δεσμεύσεις τραπεζικού ωραρίου αλλά και η ανάγκη φυσικής μετακίνησης και παρουσίας στις τράπεζες.

Πλέον οι συναλλαγές εκτελούνται μέσω διαδικτύου, εύκολα, άμεσα, γρήγορα, και κυρίως με απόλυτη ασφάλεια. Μερικά από τα οφέλη που αποκομίζει κανείς με τη χρήση της ηλεκτρονικής τραπεζικής φαίνονται στην παρακάτω εικόνα:



Μέσω του e-banking μπορούμε να εκτελούμε σχεδόν όλες τις τραπεζικές και χρηματιστηριακές συναλλαγές που κάνουμε και στο κατάστημα. Μπορούμε δηλαδή με τη χρήση του διαδικτύου να φέρνουμε τη τράπεζα παντού κοντά μας. Μάλιστα, ειδικά για τις επιχειρήσεις υπάρχουν επιπλέον τεχνικές για την ασφάλεια τους αλλά και δυνατότητες συναλλαγών για κάλυψη των ιδιαίτερων αναγκών τους.

Ορισμένοι τομείς του συνολικού χρηματοπιστωτικού τομέα που έχουν ήδη δραστηριοποιηθεί για να επιτευχθούν ανταγωνιστικά πλεονεκτήματα σε αυτή τη μορφή ηλεκτρονικού εμπορίου είναι:

α) Ο τομέας παροχής επενδυτικών/ χρηματιστηριακών υπηρεσιών,

προσφέροντας:

- Χρηματοοικονομικές αναλύσεις
- Ενημέρωση χαρτοφυλακίου των μετοχών και τις τιμής τους που υπάρχουν στην τράπεζα.
- Διεκπεραίωση αγοραπωλησίας μετοχών και ενημέρωση για την τύχη της εντολής που δώσατε η ακόμη και ακύρωση των εντολών πριν τη πραγματοποίηση τους.
- Ενημέρωση σχετικά με το χαρτοφυλάκιο αμοιβαίων κεφαλαίων μας.
- Υποβολή αιτήσεων για συμμετοχή σε δημόσιες έγγραφες στο Χ.Α.Α.

β) Ο τομέας παροχής λιανικών τραπεζικών υπηρεσιών μέσω διαδικτύου, ο

τομέας αυτός προσφέρει εφαρμογές home banking δηλαδή:

- Ενημέρωση για το υπόλοιπο του λογαριασμού μας.
- Μεταφορά χρημάτων από ένα λογαριασμό μας σε άλλο.
- Πληρωμή λογαριασμών ΟΤΕ, ΔΕΗ.
- Πληρωμή εργοδοτικών εισφορών του ΙΚΑ και των ασφαλιστικών εισφορών του ΤΕΒΕ.
- Δυνατότητα υποβολής αιτήσεως δανείου.
- Πληρωμή του Φ.Π.Α., εφόσον υποβάλλουμε φορολογική δήλωση μέσω TAXIS net.
- Πληρωμή των δόσεων δανείων.
- Ανάλυση υπόλοιπου πιστωτικής κάρτας
- Δυνατότητα να παράσχουμε πλήρη η μερική πρόσβαση για τη διαχείριση των λογαριασμών μας σε άτομα που δεν είναι δικαιούχοι.

Η ασφάλεια αλλά και το απόρρητο των συναλλαγών μέσω e-banking είναι εξαιρετικής σημασίας για τις τράπεζες, για αυτό έχουν λάβει όλα τα μέτρα προφύλαξης και χρησιμοποιούν αυστηρές μεθόδους ασφάλειας ενώ δεσμεύονται για το απόρρητο όλων των προσωπικών πληροφοριών που συλλέγονται μέσω e-banking.

Η ασφάλεια διασφαλίζεται με:

1. Προσωπικούς κωδικούς πρόσβασης:

   Χρήση προσωπικών κωδίκων πρόσβασης που παρέχονται από την τράπεζα (user ID και PIN) για την αναγνώριση του πελάτη και τη σύνδεση του με την υπηρεσία e-banking.

2. Κρυπτογράφηση:

   Ολες οι πληροφορίες από την έναρξη ως τη λήξη της σύνδεσης με την τράπεζα κρυπτογραφούνται (SSL 128-bit encryption),

ενώ έχουμε έλεγχο της πρόσβασης χρησιμοποιώντας ειδικά συστήματα ασφάλειας (Firewall).

3. Αυτόματη αποσύνδεση:

   Αν δεν υπάρξει δραστηριότητα για ένα καθορισμένο χρονικό διάστημα έχουμε αυτόματη αποσύνδεση από το σύστημα, αυτό προστατεύει τον πελάτη από ανεπιθύμητη πραγματοποίηση ηλεκτρονικών συναλλαγών από τρίτο.

Η πρώτη ολοκληρωμένη και πιο βραβευμένη υπηρεσία στο χώρο του e-banking είναι η winbank που παρέχεται από την τράπεζα Πειραιώς στην ελληνική αγορά και αποτελεί παράδειγμα για την ηλεκτρονική τραπεζική στην Ελλάδα αλλά και στην Ευρώπη γενικότερα. Μάλιστα το κορυφαίο επίπεδο παροχής υπηρεσιών φαίνεται και από τις διακρίσεις που έχει ως τώρα. Έχει κατακτήσει μέσα σε τρία χρόνια παρουσίας στο χώρο 12 διακρίσεις, με κορυφαία αυτή που την έφερε στο υψηλότερο σκαλί του βάθρου στην Ευρώπη στο διαγωνισμό ‘’The European banking technology awards 2001’’, όπου βραβεύτηκε στη κατηγόρια ‘’Best online and multichannek banking team’’.

6.6 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ "ΕΠΙΧΕΙΡΕΙΝ".

Από την προηγούμενη δεκαετία μέχρι και σήμερα είμαστε όλοι μάρτυρες της ραγδαίας εξέλιξης της τεχνολογίας του Διαδικτύου και του ηλεκτρονικού εμπορίου, η οποία όμως έχει δημιουργήσει πολλούς κινδύνους για τους χρήστες του, αφού είναι πάρα πολλές οι τεχνολογικές δυνατότητες για την ηλεκτρονική παρακολούθηση τους.

Έχει διαπιστωθεί κυκλοφορία προσωπικών δεδομένων σε μεγάλη έκταση, αφού και η απλή περιήγηση στο Διαδίκτυο δεν παραμένει ανώνυμη για τον χρήστη. Και μάλιστα, όταν ο χρήστης αναφέρει στοιχεία τεχνικής φύσεως και όχι προσωπικά δεδομένα, όπως είναι τα δεδομένα σύνδεσης στο Διαδίκτυο ή η

διεύθυνση του ηλεκτρονικού ταχυδρομείου, αυτά μπορούν να χρησιμεύσουν στο να αποκαλυφθεί η ταυτότητα του. Επίσης, μεγάλες διαστάσεις έχει λάβει το ζήτημα της δημιουργίας πορτραίτων προσωπικότητας των χρηστών του Διαδικτύου από επιχειρήσεις σχετικά με τις προτιμήσεις και τις ανάγκες τους, έτσι ώστε να προσαρμόσουν το διαφημιστικό τους marketing. Για να γίνει όμως αυτό, χρειάζεται καταγραφή και συλλογή προσωπικών δεδομένων.

Πέρα από τα παραπάνω, δεν πρέπει να ξεχνάμε ότι η ροή πληροφοριών μέσω Διαδικτύου αποκτά και διασυνοριακή διάσταση και έτσι, προσωπικά δεδομένα μεταφέρονται για επεξεργασία σε χώρες που δεν διαθέτουν νομοθεσία για την προστασία τους. Μάλιστα, σύμφωνα και με τον Ιγγλεζάκη (2003) "*...επειδή είναι αδύνατος ο έλεγχος της επεξεργασίας των προσωπικών δεδομένων και οι χρήστες δεν διαθέτουν δικαίωμα ενημέρωσης και πρόσβασης στις πληροφορίες που τους αφορούν, οι χώρες αυτές χαρακτηρίζονται ως "οάσεις δεδομένων" (data heavens, Datenhoasen).*

Με βάση λοιπόν τα παραπάνω καταλαβαίνουμε ότι χρειάζεται να υπάρχουν κάποιες νομικές ρυθμίσεις σχετικά με την προστασία προσωπικών δεδομένων στο Διαδίκτυο. Έτσι, λοιπόν, στη χώρα μας υπάρχει ένα γενικό νομικό πλαίσιο για αυτόν τον λόγο, που περιλαμβάνει τους νόμους 2472/1997 και 2774/1999. Κορμός όμως για την προστασία στη χώρα μας είναι κυρίως το πρώτο νομοθετικό κείμενο.

Αναλύοντας λοιπόν τις γενικές διατάξεις του νόμου 2472/1997 βλέπουμε ότι, θεμελιώδης στο δίκαιο της προστασίας των προσωπικών δεδομένων είναι η αρχή της νομιμότητας, σύμφωνα με την οποία η συλλογή και επεξεργασία των δεδομένων αυτών επιτρέπεται μόνο εφόσον πληρούνται οι προϋποθέσεις του νόμου. Και βασική προϋπόθεση στο σημείο αυτό, είναι η συγκατάθεση του υποκειμένου των δεδομένων, η οποία ορίζεται στο άρθρο 2 ως η "ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και με πλήρη επίγνωση με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας

τα προσωπικά δεδομένα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, καθώς και τα στοιχεία του υπεύθυνου επεξεργασίας".

Με αυτόν τον τρόπο αποκλείεται η σιωπηρή συγκατάθεση κατά την οποία ο χρήστης δεν πληροφορείται όλων των παραπάνω. Όσον αφορά τώρα το έγγραφο τύπο για την παροχή της συγκατάθεσης, εφόσον ορίζεται από το νόμο ότι δεν χρειάζεται ο τύπος, είναι δυνατή η παροχή της σε απευθείας σύνδεση (on line) διαφορετικά απαιτείται η χρήση προηγμένης ηλεκτρονικής υπογραφής. Ειδική όμως, είναι η περίπτωση των ευαίσθητων προσωπικών δεδομένων, όπως είναι η φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, οι θρησκευτικές πεποιθήσεις, η υγεία, η ερωτική ζωή ή τα σχετικά με ποινικές διώξεις και καταδίκες, η επεξεργασία των οποίων επιτρέπεται μόνο με άδεια της Αρχής Προστασίας Προσωπικών Δεδομένων.

Σε όλες τις παραπάνω περιπτώσεις, εκτός από την αρχή της νομιμότητας που προαναφέραμε ισχύει και η αρχή του σκοπού καθώς και η αρχή της προσφορότητας.

Σύμφωνα λοιπόν με το άρθρο 4 του νόμου, η πρώτη αρχή σημαίνει, ότι τα δεδομένα πρέπει να συλλέγονται με θεμιτό και νόμιμο τρόπο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία για τους σκοπούς αυτούς, ενώ η δεύτερη αρχή σημαίνει ότι τα δεδομένα πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται για τους σκοπούς της επεξεργασίας. Επιπροσθέτως, απαγορεύεται η συλλογή προσωπικών δεδομένων για μελλοντικές ανάγκες, καθώς και η αυθαίρετη αλλαγή του σκοπού της επεξεργασίας.

Ένα άλλο στοιχείο που ορίζει ο νόμος είναι, τα δικαιώματα των υποκειμένων των δεδομένων, όπως είναι το δικαίωμα της ενημέρωσης - στο στάδιο της συλλογής δεδομένων - (άρθρο 11), το δικαίωμα πρόσβασης στα

δεδομένα (άρθρο 12), το δικαίωμα αντίρρησης (άρθρο 13) και το δικαίωμα προσωρινής δικαστικής προστασίας (άρθρο 14).

Τέλος, ο νόμος 2472/1997 στο άρθρο 9 ρυθμίζει τη διαβίβαση προσωπικών δεδομένων στο εξωτερικό. Εδώ έχουμε διάκριση για το αν η διαβίβαση γίνεται σε χώρα της Ευρωπαϊκής ένωσης ή σε χώρα τρίτου κράτους. Στην πρώτη περίπτωση η διαβίβαση είναι ελεύθερη, ενώ στη δεύτερη περίπτωση χρειάζεται άδεια από την Αρχή προστασίας προσωπικών δεδομένων, η οποία παρέχεται μόνο εάν η χώρα προορισμού των δεδομένων εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.

Εκτός όμως, από το νόμο 2472/1997 έχουμε και τον 2774/1999 που αποτελεί πράξη προσαρμογής της ελληνικής νομοθεσίας προς την κοινοτική οδηγία 97/66 ΕΚ, και σχετίζεται με την επεξεργασία προσωπικών δεδομένων στο πλαίσιο παροχής διαθέσιμων στο κοινό τηλεπικοινωνιακών υπηρεσιών σε δημόσια τηλεπικοινωνιακά δίκτυα. Σύμφωνα, πάντως, με τον κ. Ιγγλεζάκη, (2003)"*αν και αναφέρεται ρητά ότι ο νόμος βρίσκει εφαρμογή στις υπηρεσίες του Διαδικτύου, γίνεται δεκτό ότι εφαρμόζεται σε όλη την έκταση του τομέα των τηλεπικοινωνιών, συνεπώς δε, και στο Διαδίκτυο*".

Από τις γενικές αρχές του νόμου ορίζεται ότι οποιαδήποτε χρήση τηλεπικοινωνιακών υπηρεσιών προστατεύεται από τις ρυθμίσεις του νόμου 2225/1994 για το απόρρητο των επικοινωνιών. Η ρύθμιση αυτή είναι βασική, καθώς αν δεν διασφαλίζεται το απόρρητο, τότε δεν έχει νόημα η προστασία δεδομένων. Ακολούθως, ορίζεται ότι η επεξεργασία δεδομένων επιτρέπεται μόνο όταν παρέχεται η συγκατάθεση του χρήστη ή όταν η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης. Επίσης, η επεξεργασία των δεδομένων πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της (αρχή της αναγκαιότητας) και ο φορέας παροχής διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας δεν επιτρέπεται να χρησιμοποιεί προσωπικά δεδομένα για σκοπούς που έχουν σχέση με τη διαφήμιση ή την εμπορική έρευνα αγοράς προϊόντων και υπηρεσιών, όπως και να τα διαβιβάζει

σε τρίτους, εκτός και αν ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεση του. Άλλη ρύθμιση του νόμου είναι ότι η επιλογή του εξοπλισμού και των τεχνικών μέσων για την παροχή τηλεπικοινωνιακών υπηρεσιών πρέπει να έχει ως κριτήριο και σκοπό την επεξεργασία όσο το δυνατόν λιγότερων προσωπικών δεδομένων.

Επίσης, σύμφωνα με το άρθρο 5 τα δεδομένα κίνησης (δηλαδή τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της) Web logs αφού υποβληθούν σε επεξεργασία για την πραγματοποίηση της κλήσης, μόλις αυτή λήξει, αυτά πρέπει να απαλείφονται ή να καθίστανται ανώνυμα. Έτσι, λοιπόν, δεν δύνανται στο να χρησιμοποιούνται για τη δημιουργία προφίλ των χρηστών.

Τελειώνοντας την αναφορά μας σε αυτόν τον νόμο, πρέπει να αναφερθεί ότι σύμφωνα με τον κ. Γ. Ιγγλεζάκη (2003)"*αν και οι κανόνες αυτού του νόμου είναι πρόσφοροι για την ρύθμιση της κυκλοφορίας προσωπικών δεδομένων στο Διαδίκτυο, δεν περιλαμβάνονται αντίστοιχοι σχετικά με το ζήτημα της δημιουργίας πορτραίτων των χρηστών του Διαδικτύου και το ζήτημα της επεξεργασίας των δεδομένων μη προσωπικού χαρακτήρα από την χρήση του Διαδικτύου*".

Τελευταία οδηγία της Ευρωπαϊκής Ένωσης που έχει εκδοθεί, σχετικά με την προστασία των προσωπικών δεδομένων είναι η 202/58/ΕΚ. Αυτή εκδόθηκε με σκοπό την αναθεώρηση της οδηγίας 97/66/ΕΚ και την προσαρμογή του προηγούμενου νομικού καθεστώτος στα νέα δεδομένα που γεννά η εξέλιξη της τεχνολογίας και η εξέλιξη του Διαδικτύου. Η καινούργια οδηγία διαφοροποιείται ουσιωδώς από την προηγούμενη οδηγία ως προς την ορολογία και την υιοθέτηση νέων εννοιών. Έτσι, για παράδειγμα, ως χρήστης νοείται το φυσικό ή νομικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας (άρθρο 2).

Γενικά πάντως, η οδηγία αυτή βρίσκει εφαρμογή στην επεξεργασία προσωπικών δεδομένων στα πλαίσια της παροχής διαθέσιμων στο κοινό υπηρεσιών τηλεπικοινωνιών σε δημόσια δίκτυα ηλεκτρονικής επικοινωνίας στην Κοινότητα (άρθρο 3). Αυτό σημαίνει ότι εκτός από τις τηλεπικοινωνιακές υπηρεσίες που είναι διαθέσιμες στο κοινό, σε δημόσια τηλεπικοινωνιακά δίκτυα - όπως ορίζει η οδηγία 97/66/ΕΚ στο άρθρο 3 - η καινούργια οδηγία βρίσκει εφαρμογή και σε δημόσια δίκτυα ηλεκτρονικής επικοινωνίας όπως είναι το Διαδίκτυο.

Επιπλέον, η οδηγία αυτή όπως και η προηγούμενη υποχρεώνει τον φορέα παροχής υπηρεσιών να λαμβάνει τα αναγκαία τεχνικά και οργανωτικά μέτρα ασφαλείας και σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος παραβίασης του δικτύου να ενημερώνει τους χρήστες για τους κινδύνους αυτούς, καθώς και σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την ασφάλεια των επικοινωνιών τους. Περαιτέρω, προβλέπεται η υποχρέωση των κρατών μελών να κατοχυρώσουν το απόρρητο των επικοινωνιών ειδικότερα, ορίζεται ότι πρέπει να απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των δεδομένων κίνησης από πρόσωπα εκτός των χρηστών, χωρίς την συγκατάθεση των χρηστών. Επίσης, η οδηγία αναφέρεται στα αυτοεγκαθιστώμενα αρχεία cookies.

Σύμφωνα με τον κ. Ιγγλεζάκη,(2003) "*οι επισκέψεις των καταναλωτών σε ένα ηλεκτρονικό κατάστημα και οι συναλλαγές τους αφήνουν ψηφιακά ίχνη. Αυτά τα ψηφιακά ίχνη χρησιμοποιούνται συχνά για την δημιουργία καταναλωτικού προφίλ*".

Αυτή λοιπόν η οδηγία, περιέχει ειδική ρύθμιση για το εν λόγω κατασκοπευτικό λογισμικό και σύμφωνα με αυτή, η τεχνολογία cookies απαγορεύεται να χρησιμοποιείται εν αγνοία του καταναλωτή και χωρίς τη συγκατάθεσή του, ακόμη και αν προβλέπεται να χρησιμοποιηθεί για θεμιτούς σκοπούς.

Γίνεται ευρύτερα δεκτό ότι η ραγδαία ανάπτυξη της τεχνολογίας της πληροφορικής και του Διαδικτύου εγκλείει αυξημένους κινδύνους για το δικαίωμα της προστασίας των προσωπικών δεδομένων. Και σύμφωνα με τον κ. Ιγγλεζάκη(2003) "...*το παραδοσιακό οπλοστάσιο του δικαίου της προστασίας προσωπικών δεδομένων δεν επαρκεί για την αντιμετώπιση των νέων προβλημάτων που αναφαίνονται. Μόνη ενδεδειγμένη λύση είναι η εισαγωγή ειδικής νομοθεσίας, σε τομείς όπως είναι οι ηλεκτρονικές επικοινωνίες, και εδώ η συμβολή του κοινοτικού νομοθέτη είναι σημαντική*".

Απαιτείται πάντως, και η εγρήγορση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και η άσκηση εποπτείας στον τομέα του ηλεκτρονικού εμπορίου, ώστε να αναδεικνύονται τα προβλήματα από τη χρήση της τεχνολογίας του Διαδικτύου, και να γίνεται δυνατή η επεξεργασία κατάλληλων λύσεων.

7. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου (internet) . Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στο πεδίο του εγκλήματος στον κυβερνοχώρο (cyber crime), όπως άλλωστε συμβαίνει και στα εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) χωρίς την κατοχή αυτών των τεχνικών γνώσεων . Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις. Ο συνδυασμός των δύο βασικών, αλλά και διαφορετικών τρόπων σκέψεως αποτελεί "τον σταυρό του μαρτυρίου" για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

Ένα εξίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με την νομική πλευρά του θέματος από ποινική άποψη, είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων. Είναι ευνόητο ότι, η έλλειψη αυτή οφείλεται στο γεγονός ότι, το έγκλημα στον κυβερνοχώρο αποτελεί νέα μορφή εγκλήματος. Αποτελεί κοινή διαπίστωση ότι, η ανάπτυξη των σχετικών νομικών θεμάτων από αστική και εμπορική άποψη έχει διερευνηθεί σε μεγαλύτερη έκταση, από ότι η αντίστοιχη ποινική πλευρά. Αυτό οφείλεται στην μεγάλη επιρροή του κυβερνοχώρου, τόσο στο αστικό (σύναψη συμβάσεων εξ αποστάσεως δια του κυβερνοχώρου κλπ), όσο και στον οικονομικό τομέα (ηλεκτρονικό εμπόριο, νέα οικονομία κλπ).

Σε κάθε περίπτωση όμως ο μελετητής των σχετικών με τον κυβερνοχώρο θεμάτων θα πρέπει να καταφεύγει στα διάφορα (πολυπληθή) τεχνικά περιοδικά για τους ηλεκτρονικούς υπολογιστές, καθώς και σε δημοσιεύματα του

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

7.1 Η ΝΟΜΙΚΗ ΕΝΝΟΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

Η Ελληνική νομοθεσία δεν προσδιορίζει την έννοια του διαδικτύου ή του κυβερνοχώρου. Κατά συνέπεια οι έννοιες αυτές λαμβάνονται από την τεχνολογία. Ετσι λοιπόν, ως διαδίκτυο (internet) μπορεί να οριστεί η παγκόσμια συλλογή δικτύων και πυλών, που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ τους , ενώ ως κυβερνοχώρος μπορεί να οριστεί το σύνολο των ηλεκτρονικών κόσμων, όπως το internet, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών, όπου δηλαδή η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση . Στο άρθρο 2 του Ν 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών προσδιορίζονται οι έννοιες "δίκτυο καλωδιακής τηλεόρασης", "ιδιωτικό δίκτυο", "παροχή ανοικτού δικτύου" και "τηλεπικοινωνιακό δίκτυο". Δεν προσδιορίζεται όμως η έννοια του διαδικτύου ή του κυβερνοχώρου.

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

7.2 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΗΣ ΕΝΝΟΙΑΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

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

βιβλιογραφία . Ομοίως ούτε στην Ελληνική βιβλιογραφία υπάρχει ορισμός του εγκλήματος στον κυβερνοχώρο.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το ``κοινό`` ή "συμβατικό έγκλημα" και η μόνη διαφορά που το διακρίνει απ΄ αυτό είναι ότι, διαπράττεται σε διαφορετικό περιβάλλον , (δηλ. σε ηλεκτρονικό περιβάλλον και σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται κατά την άποψή μας πλήρως στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται). Μια άλλη κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικώς σε περιβάλλον του κυβερνοχώρου. Με το παραπάνω λοιπόν κριτήριο τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν:

α) Σε εγκλήματα που διαπράττονται τόσο σε " κοινό " περιβάλλον, όσο και στο διαδίκτυο (internet) π.χ. η συκοφαντική δυσφήμηση διαπράττεται και με την χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail). Η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το έγκλημα αυτό τελεστεί σε "περιβάλλον internet" (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

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

γ) Σε "Γνήσια εγκλήματα κυβερνοχώρου" (Cyber crimes) με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς έχει σχέση με τον κυβερνοχώρο. Μια τέτοια αξιόποινη συμπεριφορά μπορεί να θεωρηθεί η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου. Τέτοια εγκλήματα δεν υπάρχουν ακόμα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία. Δηλαδή τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικώς σε περιβάλλον διαδικτύου. Σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

7.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

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

Είναι εύκολο (easy) στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ συχνά δεν αφήνει ίχνη (όπως στα κοινά εγκλήματα είναι τα δακτυλικά αποτυπώματα). Μπορεί να διαπραχθεί χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του. Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σε όσους έχουν ροπή ή τάση στην παιδοφιλία ή χρήση παιδικής πορνογραφίας (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (News groups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (IRC- Internet Relay Chat).

Οι "εγκληματίες του κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα π.χ. αποστέλλουν ηλεκτρονικά μηνύματα ή επιστολές (e-mail) ανωνύμως ή και με ψευδή στοιχεία. Είναι έγκλημα "χωρίς πατρίδα", παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους. Κατά κανόνα είναι πολύ δύσκολο να προσδιοριστεί ο (πραγματικός) τόπος τελέσεως του. Ακόμα όμως και αν προσδιοριστεί αυτός, είναι ακόμα πιο δύσκολο να εντοπιστεί ο δράστης. Η εξωτερίκευσή του μπορεί να εντοπίζεται στην Α χώρα πλην όμως τα αποδεικτικά στοιχεία μπορεί να βρίσκονται στο άλλο άκρο της γης ή και να βρίσκονται ταυτόχρονα σε πολλούς τόπους.

Για την διερεύνησή του απαιτείται κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (δηλ. του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος, και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Περιπτώσεις που το έγκλημα στον κυβερνοχώρο (cyber-crime) περιορίζεται στα όρια ενός μόνο κράτους είναι (θεωρητικώς τουλάχιστον) ελάχιστες και σπάνιες.

Οι παραδοσιακές (κοινές) Συμβάσεις για αμοιβαία Δικαστική Συνδρομή δεν επαρκούν, λόγω της φύσεως του αποδεικτικού υλικού, δηλαδή της ηλεκτρονικής απόδειξης (electronic evidence) που πρέπει να εντοπιστεί και να κατασχεθεί σε συνδυασμό με την ταχύτητα ενεργείας των διωκτικών Αρχών.

Δεν υπάρχουν επαρκή στατιστικά στοιχεία, όχι μόνο στον Ελληνικό, αλλά και στον Διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου (cyber-crimes) καταγγέλλονται. Και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια ο ``σκοτεινός αριθμός`` της εγκληματικότητας στον χώρο του διαδικτύου είναι ``ακόμα πιο σκοτεινός``, από ότι στον ``κοινό`` εγκληματικό χώρο.

Η Αστυνομική διερεύνηση γενικότερα, αλλά και η ανακριτική του προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και

εξειδικευμένες γνώσεις. Εξειδικευμένες γνώσεις επίσης απαιτούνται και για όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (Εισαγγελείς, Δικαστές, Δικηγόρους).

7.4 ΣΧΕΣΗ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΕΓΚΛΗΜΑΤΟΣ ΠΟΥ ΤΕΛΕΙΤΑΙ ΜΕ ΗΛΕΚΤΡΟΝΙΚΟ ΥΠΟΛΟΓΙΣΤΗ

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

Ως ηλεκτρονικό έγκλημα μπορεί να οριστεί αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών Ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer related crime ή computer crime) μπορεί να χαρακτηριστεί κάθε παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη επεξεργασία ή μετάδοση δεδομένων .

Σημειώνεται ότι, ο ορισμός αυτός διατυπώθηκε για πρώτη φορά το 1983 από ειδική ομάδα εμπειρογνωμόνων του ΟΑΣΑ, που συνεστήθη ειδικώς για να εξετάσει το θέμα της ηλεκτρονικής εγκληματικότητας. Ο ορισμός αυτός βέβαια είναι πολύ ευρύς και είναι ευνόητο ότι, μόνον ως ``οδηγός`` μπορεί να χρησιμοποιηθεί. Η οριστικοποίησή του επαφίεται στον Εθνικό Νομοθέτη και στη νομολογία των Δικαστηρίων.

7.5 ΣΥΝΗΘΗ ΕΓΚΛΗΜΑΤΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

Τα πλέον συνηθισμένα εγκλήματα που παρουσιάζονται αυτή την στιγμή στον κυβερνοχώρο είναι : Οι απάτες (με πιστωτικές κάρτες ή μη), η διακίνηση παιδικής πορνογραφίας, εγκλήματα κατά της Εθνικής Ασφάλειας (οδηγίες για

κατασκευή Βομβών, εισβολή σε συστήματα ασφαλείας, που έχουν σχέση με την εθνική υποδομή) ,οδηγίες για παρασκευή ναρκωτικών . Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν: σε εγκλήματα κατά των προσωπικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον περιουσιακών αγαθών .

7.6 Η ΝΟΜΙΚΗ ΕΝΝΟΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο, που με ακρίβεια καθορίζει ο νόμος για το συγκεκριμένο θέμα. Το ίδιο συμβαίνει βέβαια και με την έννοια της ασφάλειας. Άρα για το νομικό ασφάλεια στο διαδίκτυο σημαίνει αυτό που ο νόμος ορίζει ως ασφάλεια στο διαδίκτυο. Ο νόμος επίσης καθορίζει και το περιεχόμενο όλων εκείνων των επιμέρους εννοιών που αναφέρονται στον βασικό ορισμό της ασφάλειας. Έτσι αν π.χ. ο νομοθέτης ορίσει ως ασφάλεια στο διαδίκτυο "τον κίνδυνο να επέλθει κάποια βλάβη", θα πρέπει να ορίσει ταυτόχρονα και τους όρους "κίνδυνο" και "βλάβη".

Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό. Θα λέγαμε, χωρίς επιφύλαξη ότι, ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικώς ότι, ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό . Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Έτσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επόμενα, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την απάτη την σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέρος της επιβολής ή

εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).

Συμπερασματικός μπορεί να λεχθεί ότι, η έννοια της ασφάλειας στο διαδίκτυο δεν έχει καθοριστεί ακόμα από το νομοθέτη. Κατά τον καθορισμό της όμως, πρέπει να ληφθούν υπόψη οι βασικές Αρχές του Δικαίου, όπως αυτές προσδιορίζονται στο Ελληνικό Σύνταγμα και στους ισχύοντες Διεθνείς Κανόνες.

7.7 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΟΥ ΟΡΟΥ "ΑΣΦΑΛΕΙΑ" ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Στο διαδίκτυο ``διακινούνται`` πληροφορίες - δεδομένα (data) που έχουν σχέση με την προσωπική και ιδιωτική σφαίρα του ατόμου (χρήστη ή μη χρήστη του διαδικτύου). Κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα ``αδιάκριτα βλέμματα``. Κατά συνέπεια απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. Η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, αποτελούν μερικές από τις βασικότερες Αρχές του δικαίου. Είναι ευνόητο ότι, οι θεμελιώδεις αυτές Αρχές πρέπει να εφαρμόζονται και στον κυβερνοχώρο. Ο υπερβολικός αστυνομικός έλεγχος (αστυνόμευση) του κυβερνοχώρου, δηλαδή η ευρεία διατύπωση του όρου ασφάλεια έρχεται ή ενδεχομένως να έρχεται σε αντίθεση με τις παραπάνω Αρχές. Δεν μπορούμε να ομιλούμε για κρατικό έλεγχο, καθότι η έννοια του κράτους και της κρατικής κυριαρχίας είναι έννοιες άγνωστες στο διαδίκτυο.

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής, όσο και από νομικής απόψεως. Από τεχνική άποψη διότι, κάθε τεχνικός τρόπος που αποβλέπει στην ασφάλεια του διαδικτύου, μπορεί να εξουδετερωθεί και συνήθως εξουδετερώνεται, από ένα άλλο τρόπο "αντιασφάλειας". Από νομική άποψη

διότι, ο νομοθέτης δεν "προφταίνει" να παρακολουθεί τις τεχνολογικές εξελίξεις και τις κοινωνικές επιπτώσεις και συνέπειες τους, ώστε να μπορέσει να τις ρυθμίσει. Με άλλα λόγια οι αλλαγές στην τεχνική δομή του κυβερνοχώρου και κατά συνέπεια στη νομική αντιμετώπισή του, είναι τόσο ραγδαίες, που, εάν το θέμα δεν "σταθεροποιηθεί" κάπου από τεχνολογικής απόψεως, ο νομοθέτης δεν θα καταφέρει να λάβει οποιοδήποτε μέτρο , σε ουσιαστικό ή δικονομικό επίπεδο.

7.8 ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΓΕΝΙΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ

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

Ο Ν. 1805/88, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes), δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα. Όταν καταρτιζόταν ο νόμος αυτός το διαδίκτυο δεν είχε λάβει τις σημερινές του διαστάσεις και κατά συνέπεια δεν είχε γίνει αισθητή η ανάγκη καταρτίσεως ειδικότερης νομοθεσίας. Η διατύπωση όμως του νόμου αυτού έχει γίνει με τέτοιο τρόπο (συνδυασμός τεχνικών και νομικών εννοιών), που είναι εμφανής η επιθυμία του συντάκτη, να περιλάβει στο μέλλον και κάθε μορφή συμπεριφοράς, που θα δημιουργήσει η εξέλιξη της τεχνολογίας.

Ανεξάρτητα όμως από το εάν ο παραπάνω Ν. 1805/1988 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής , το βέβαιον είναι ότι, δεν επαρκεί να "καλύψει" τα εγκλήματα που έχουν παρουσιαστεί από την χρήση του διαδικτύου. Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

7.9 Η ΝΟΜΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ "ΧΑΚΕΡ" ΚΑΤΑ ΤΟ ΓΕΝΙΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ

Σύμφωνα με το άρθρο 370Γ§2 Π.Κ., όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών , εφ΄ όσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή . Αν η πράξη αναφέρεται στις διεθνείς σχέσεις του κράτους ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. Η πράξη αυτή διώκεται μόνο ύστερα από έγκλιση του παθόντα. Διευκρινίζεται δε ότι, το άρθρο 148 Π.Κ., το οποίο στην §2 αποτελεί κακούργημα, αναφέρεται στην κατασκοπεία, που διαπράττεται από πολίτη, παραπέμπει δε (το άρθρο 148 Π.Κ.) και στο άρθρο 146, το οποίο αναφέρεται στην παραβίαση των μυστικών της πολιτείας, όταν διαπράττεται βέβαια από πολίτη και όχι από στρατιωτικό. Το τελευταίο αυτό σημαίνει ότι, εάν ο χάκερ, ο οποίος εισήλθε παράνομα στα ηλεκτρονικά δεδομένα του Υπουργείου Εθνικής Αμύνης, έλαβε στην κατοχή του ή στη γνώση του αντικείμενα ή ειδήσεις, που τα συμφέροντα της πολιτείας ή των συμμάχων της επιβάλουν να τηρηθούν απόρρητα απέναντι σε ξένη κυβέρνηση τιμωρείται με φυλάκιση μέχρι ενός έτους. Αν όμως ο υπαίτιος ενήργησε με σκοπό να χρησιμοποιήσει τα ανωτέρω αντικείμενα ή ειδήσεις για να τα διαβιβάσει σε άλλον ή να τα ανακοινώσει έτσι ώστε να μπορούν να εκθέσουν σε κίνδυνο το συμφέρον του κράτους και ιδίως την ασφάλειά του ή κάποιου από τους συμμάχους του, τιμωρείται με ποινή κάθειρξης.

Αξιοσημείωτο είναι επίσης ότι, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα. Διευκρινίζεται ότι, το

παραπάνω άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και προστέθηκε με το άρθρο 4 Ν. 1805/1988. Αυτό σημαίνει ότι, η θέσπιση του συγκεκριμένου άρθρου δεν αποβλέπει στην προστασία της ασφάλειας στον κυβερνοχώρο, αλλά στην προστασία του απορρήτου. Δεν είναι λοιπόν υπερβολικό να λεχθεί ότι, η ύπαρξη της εννοίας του "χάκερ" στην ελληνική νομοθεσία αποτελεί ένα τυχαίο γεγονός, που οφείλεται στην ευρεία διατύπωση του άρθρου 370 Γ §2 Π.Κ. Η Ελληνική νομοθεσία επίσης δεν προσδιορίζει τις έννοιες των διαφόρων κατηγοριών "χάκερς", όπως είναι οι cracker κλπ .

Λέγοντας απόρρητο εννοούμε το δικαίωμα του κατόχου των δεδομένων να αποκλείει άλλους από την πρόσβαση σ΄ αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου από ουσιαστική έννοια. Στο άρθρο 370 Β §1 ορίζεται ότι, ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Είναι ευνόητο βέβαια ότι, η παραπάνω διάταξη του άρθρου 370 Γ §2 Π.Κ. θα εφαρμοστεί κατά την περίπτωση εκείνη που ο δράστης απλώς θα έχει εισέλθει χωρίς δικαίωμα σε σύστημα υπολογιστών, χωρίς να προκαλέσει οποιαδήποτε άλλη βλάβη. Σε περίπτωση δε, που από την χωρίς δικαίωμα διείσδυσή του έχει επέλθει και παραβίαση άλλων έννομων αγαθών, η νομική αντιμετώπιση είναι κάθε φορά ανάλογη. Έτσι π.χ. στην πλέον γνωστή υπόθεση "χάκιγκ", που απασχόλησε την Ελληνική νομική πράξη τον Ιούλιο του 2000, εναντίον του Έλληνα "χάκερ" γνωστού ως cyberia ασκήθηκε ποινική δίωξη και για παράβαση του άρθρου 386 Α Π.Κ. σε βαθμό κακουργήματος. Το άρθρο αυτό, το οποίο περιλαμβάνεται στα εγκλήματα κατά των περιουσιακών δικαιωμάτων, προστατεύει την περιουσία.

7.10 ΝΟΜΙΚΟΣ ΟΡΙΣΜΟΣ ΤΟΥ "ΧΑΚΕΡ"

Σύμφωνα λοιπόν με όσα αναφέρθηκαν παραπάνω για το άρθρο 370 Γ Π.Κ., ως Χάκερ, μπορεί να οριστεί το άτομο εκείνο, το οποίο, χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών. Οι χάκερς εμφανίστηκαν για πρώτη φορά κατά την δεκαετία του 1970 στις ΗΠΑ, ως δράστες κατά των τηλεπικοινωνιακών συστημάτων. Σήμερα εμφανίζονται με δύο μορφές: α)με την μορφή εισόδου (διείσδυσης) σε σύστημα υπολογιστών, χωρίς την πρόκληση βλάβης και β)με την μορφή εισόδου (διείσδυσης) σε σύστημα υπολογιστών, με πρόκληση βλάβης. Το είδος της βλάβης που θα προκαλέσει εξαρτάται από τις συγκεκριμένες περιπτώσεις. Στην δεύτερη αυτή περίπτωση έχει επικρατήσει ο όρος "κράκερ", ο οποίος όμως είναι και αυτός όρος τεχνικής φύσεως και όχι νομική έννοια. Από άποψη νομικής επιστήμης, η εξέταση της προσωπικότητας του χάκερ αποτελεί αντικείμενο της επιστήμης της εγκληματολογίας .

7.11 ΝΟΜΙΚΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΗΝ ΥΠΑΡΞΗ "ΧΑΚΙΝΓΚ" ΚΑΤΑ ΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ

Για την ουσιαστική εφαρμογή του άρθρου 370 Γ §2 Π.Κ. πρέπει να συντρέχουν οι παρακάτω προϋποθέσεις:

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

β) η πρόσβαση αυτή να γίνεται χωρίς δικαίωμα, δηλαδή χωρίς την συγκατάθεση του κατόχου των στοιχείων. Σε περίπτωση που υφίσταται η συγκατάθεση αυτή, είναι ευνόητο ότι, δεν θεμελιώνεται η αντικειμενική υπόσταση του εγκλήματος του άρθρου 370 Γ §2 Π.Κ. Σε περίπτωση που ο

δράστης είναι στην υπηρεσία του νομίμου κατόχου των στοιχείων, τότε τεκμαίρεται ότι, αυτός έχει το δικαίωμα νόμιμης πρόσβασης στα στοιχεία. Αυτό συνάγεται από την §3 του ίδιου άρθρου 370 Γ §2 Π.Κ., σύμφωνα με την οποία η πράξη της §2 τιμωρείται, μόνον αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

Η έλλειψη δικαιώματος πρόσβασης τεκμαίρεται ιδίως όταν, γίνεται (η πρόσβαση) με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει νόμιμος κάτοχός τους. Ως τέτοια μέτρα ασφαλείας θεωρούνται οι κωδικοί λέξεων (passwords) οι κωδικοί αριθμοί χρηστών, μαγνητικές κάρτες κλπ. Η διατύπωση του άρθρου 370 Γ§2 Π.Κ. είναι "αρκούντως ευρεία", ώστε να περιλαμβάνει κάθε πρόσβαση σε δεδομένα και αρχεία. Στην ευρεία αυτή διατύπωση του, οφείλεται και το γεγονός ότι, μπορεί να υπαχθεί στο άρθρο αυτό η ενέργεια του "χάκερ", δηλαδή το "χάκιγκ". Αλλωστε, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα. Το έγκλημα του άρθρου 370 Γ§2 Π.Κ. είναι έγκλημα διακινδύνευσης και όχι έγκλημα βλάβης.

7.12 ΕΙΔΙΚΕΣ ΠΟΙΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΣΤΟ ΧΩΡΟ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

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

α) Σύμφωνα με το άρθρο 11 του Ν. 2867/2000 η κατά παράβαση των άρθρων 5 (αναφέρεται στην χορήγηση γενικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) και 6 (αναφέρεται στην χορήγηση ειδικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) άσκηση τηλεπικοινωνιακών δραστηριοτήτων τιμωρείται με φυλάκιση τουλάχιστον δώδεκα (12) μηνών και με χρηματική ποινή.

Επίσης, όποιος παραβαίνει με οποιονδήποτε τρόπο τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής και τήρησης του απορρήτου των κάθε είδους δεδομένων που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο (2) ετών και χρηματική ποινή, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις. Σε περίπτωση που ο παραβάτης της παρούσας διάταξης ανήκει στο προσωπικό τηλεπικοινωνιακής επιχείρησης, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον τριών (3) ετών.

Ο τεχνικός εξοπλισμός και τα μέσα που χρησιμοποιήθηκαν για την τέλεση των παραπάνω αξιόποινων πράξεων δημεύονται. Σε περιπτώσεις πολλαπλών ή καθ' υποτροπή παραβάσεων προβλεπόμενων στον παρόντα νόμο, όπως εκάστοτε ισχύει, ή στον Ποινικό Κώδικα, σε σχέση με τα ανωτέρω αδικήματα, επιβάλλονται αθροιστικά οι βαρύτερες ποινές.

β) Σύμφωνα επίσης με το άρθρο 13 Ν.2774/22.12.99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, όποιος κατά παράβαση του νόμου αυτού χρησιμοποιεί, επεξεργάζεται, μεταδίδει, ανακοινώνει, δημοσιοποιεi δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο. τιμωρείται με φυλάκιση και χρηματική ποινή.

Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις πράξεις της Αρχής που επιβάλλουν τις διοικητικές κυρώσεις των περιπτώσεων γ' (προσωρινή ανάκληση αδείας), δ' (οριστική ανάκληση αδείας) και ε' (καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων) της παρ. 1 του άρθρου 21 του ν. 2472/1997 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή. Οι διατάξεις των παραγράφων 6 έως και 14 του άρθρου 22 του Ν. 2472/1977 εφαρμόζονται και επί των πράξεων των προηγουμένων παραγράφων.

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

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

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

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

4. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και εάν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) έτους και με χρηματική ποινή.

5. Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις αποφάσεις της Αρχής, που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με την παρ. 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με την παρ. 2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ', δ' και ε' της παρ. 1

του άρθρου 21 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9, καθώς και εκείνος που δεν συμμορφώνεται προς τη δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

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

7. Αν από τις πράξεις των παρ.1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και με χρηματική ποινή.

7.13 ΑΡΜΟΔΙΕΣ ΥΠΗΡΕΣΙΕΣ ΓΙΑ ΤΗΝ ΕΡΕΥΝΑ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Στα λεγόμενα τεχνολογικώς αναπτυγμένα κράτη, όπου το έγκλημα στον κυβερνοχώρο ``ανθεί``, έχουν συσταθεί ειδικές υπηρεσίες για την έρευνα και καταπολέμηση του νέου αυτού εγκλήματος. Ενδεικτικώς αναφέρεται ότι στις Η.Π.Α. το F.B.I. έχει συστήσει το National Infrastructure Protection Center (NIPC), με παραρτήματα σε διάφορες πολιτείες για την έρευνα των σχετικών εγκλημάτων. Στα πλαίσια μάλιστα της ``Ηλεκτρονικής Αστυνομίας`` έχει συσταθεί ειδική μονάδα, που έχει ως αντικείμενο το ``σπάσιμο`` των κωδικών των ηλεκτρονικών επιστολών (e-mails), που χρησιμοποιούν οι έμποροι ναρκωτικών και τα δίκτυα παιδεραστίας . Ομοίως έχει συσταθεί ειδικό σώμα Εισαγγελέων, οι οποίοι ύστερα από κατάλληλη εκπαίδευση, ασχολούνται με το έγκλημα στον κυβερνοχώρο . Παρόμοια εκπαίδευση έχει γίνει και στους Δικαστές. Στην Scotland Yard έχει συσταθεί το Computer Fraud Squad. Στον Καναδά έχει συσταθεί το the Royal Canadian Mounted Police Computer Crime Unit.

Δεκάδες συναντήσεις, συνέδρια κ.λ.π, γίνονται κάθε χρόνο από τις παραπάνω υπηρεσίες για θέματα σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Επίσης έχουν εκδοθεί δεκάδες γραπτές οδηγίες (guide lines) και Κώδικες Πρακτικής (Code of Practice), που απευθύνονται στους δημόσιους εκείνους λειτουργούς, οι οποίοι είναι επιφορτισμένοι με την έρευνα και την καταπολέμηση των σχετικών εγκλημάτων. Ενδεικτικώς αναφέρεται ο Κώδικας Πρακτικής του Τμήματος Εμπορίου και Βιομηχανίας (DTI) της Βρετανίας (The British Code of Practice - Department of Industry).

7.14 ΓΕΝΙΚΑ ΓΙΑ ΤΙΣ ΕΡΕΥΝΕΣ ΠΟΥ ΕΧΟΥΝ ΣΧΕΣΗ ΜΕ ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Οι δικαστικές-Αστυνομικές έρευνες που γίνονται προς διακρίβωση εγκλημάτων του κυβερνοχώρου, ουδεμία σχέση έχει με τις έρευνες , που μέχρι τώρα γνωρίζουμε . Στις μέχρι τώρα "παραδοσιακές" έρευνες ο ερευνών έψαχνε σε συγκεκριμένο χώρο π.χ. δωμάτια, συρτάρια κλπ. για να εντοπίσει το αναζητούμενο αντικείμενο. Σήμερα έχει να ψάξει files , note pads , botes, dada, κρυπτογραφημένα στοιχεία κλπ. Μπορεί το προς έρευνα αντικείμενο να βρίσκεται μπροστά στα μάτια του ερευνητή και να μην μπορεί να το εντοπίσει , εάν δεν έχει τις απαραίτητες τεχνικές γνώσεις . Ερωτάται λοιπόν, πως θα διεξαχθεί σε μια τέτοια περίπτωση η αστυνομική έρευνα ; Ο "παραδοσιακός Εισαγγελέας " και η "παραδοσιακή αστυνομία" δεν επαρκούν πλέον για την εξιχνίαση των σχετικών εγκλημάτων.

Ένα άλλο πρόβλημα είναι ότι στην κοινή έρευνα το αντικείμενο βρίσκεται σ΄ ένα σημείο . Αντίθετα στο έγκλημα του κυβερνοχώρου το αντικείμενο μπορεί να βρίσκεται σε πολλούς υπολογιστές οι οποίοι μάλιστα μπορεί να βρίσκονται σε διάφορες χώρες. Το πρόβλημα του τόπου τελέσεως είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζεται κατά την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, δεδομένου ότι, η ίδια

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

Σε κάθε περίπτωση όμως δημιουργείται πρόβλημα όχι μόνο σε θέματα Δικαστικής και Αστυνομικής συνεργασίας, αλλά και σε θέματα κατά τόπον αρμοδιότητος ως προς την εκδίκαση της πράξεως. Η έννοια επίσης των γεωγραφικών συνόρων είναι άγνωστη στα εγκλήματα του κυβερνοχώρου. Ειδικότερα, όταν οι υπολογιστές (computers) είναι συνδεδεμένοι μεταξύ τους, ολόκληρος ο πλανήτης αποτελεί " μία χώρα". Κατά συνέπεια οι μέχρι τώρα Διεθνείς Συμβάσεις περί αμοιβαίας Δικαστικής Συνδρομής και Συνεργασίας, είναι "παραχωρημένες" στο πεδίο του εγκλήματος στον κυβερνοχώρο. Η Δικαστική συνεργασία στα συγκεκριμένα θέματα του κυβερνοχώρου, για να είναι αποτελεσματική, πρέπει να είναι ταχύτατη.

7.15 ΝΟΜΟΘΕΤΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ.

Ένας από τους σημαντικότερους παράγοντες, που συντέλεσε στην συρρίκνωση της επιχειρηματικότητας στο Διαδίκτυο, ήταν η έλλειψη ξεκάθαρων νομοθετικών ρυθμίσεων για σημαντικά θέματα των ψηφιακών συναλλαγών.

Η απότομη τεχνολογική ανάπτυξη και η αρχική ραγδαία εξάπλωση του ηλεκτρονικού εμπορίου βρήκαν απροετοίμαστη την νομοθεσία σε παγκόσμιο επίπεδο, η οποία αποδείχτηκε ελλιπής και αδύναμη να προσαρμοστεί τόσο γρήγορα στα νέα δεδομένα. Πάντως, το μεγάλο αυτό νομικό κενό προκάλεσε η ίδια η φύση του Διαδικτύου. Τα κυριότερα χαρακτηριστικά του, τα οποία

εμποδίζουν την καθολική εφαρμογή της ισχύουσας νομοθεσίας για τις ηλεκτρονικές συναλλαγές είναι:

- η παγκόσμια παρουσία του Internet**,** που καταλύει τα σύνορα και δημιουργεί μια νέα, κοινή αγορά, προσβάσιμη από κάθε γωνιά του πλανήτη και έρχεται σε αντίθεση με την εδαφικότητα των νομοθετικών ρυθμίσεων (κάθε χώρα έχει το δικό της δίκαιο που ρυθμίζει με διαφορετικό τρόπο τις έννομες σχέσεις).
- η αποϋλοποίηση όλων των αντικειμένων**,** εφόσον τα πάντα μετατρέπονται, πλέον, σε δεδομένα, τα οποία μεταφέρονται σε ηλεκτρονική μορφή (bits and bytes). Έτσι παύει να υπάρχει η παραδοσιακή έννοια του «πράγματος» και έχουμε ένα καινούργιο αγαθό.
- η χρησιμοποίηση της τεχνολογίας σε όλο το κομμάτι της συναλλαγής που τροποποιεί πλήρως τα υφιστάμενα συναλλακτικά ήθη. Έτσι, δεν υπάρχει συγκρίσιμο προηγούμενο και αποκλείεται η αναλογική εφαρμογή προγενέστερων δικαστικών αποφάσεων.

Επιπλέον, οι μέθοδοι marketing στο ηλεκτρονικό εμπόριο δεν είναι πλέον οι ίδιες: η προσέγγιση του καταναλωτή μέσω της χρήσης της εικονικής πραγματικότητας είναι πιο άμεση και εύκολη σε σχέση με πιο παραδοσιακές μεθόδους. Έτσι, λοιπόν, σύμφωνα με τον Γ. Κατσουλάκο(2001) «*ο καταναλωτής έρχεται αντιμέτωπος με μεγαλύτερους κινδύνους ως προς την αποτελεσματικότητα των αγορών του μέσω του Διαδικτύου ενώ η ποιότητα των νέων προϊόντων για την παραγγελία των οποίων χρησιμοποιείται το Διαδίκτυο, η διεθνοποίηση των συναλλαγών και η συχνή έλλειψη πληροφοριών σχετικά με τις δυνατότητες των προϊόντων αυξάνουν την ανασφάλεια από μέρους των καταναλωτών σχετικά με τις αγορές τους*.

Για αυτούς τους λόγους η Ευρωπαϊκή Ένωση πραγματοποιεί σταδιακά μια συντονισμένη προσπάθεια αντιμετώπισης του προβλήματος, θέλοντας να θέσει σταθερές νομικές βάσεις που να δημιουργούν ένα δίχτυ ασφαλείας για τις ηλεκτρονικές συναλλαγές. Βασικός γνώμονας είναι η αύξηση των συναλλαγών (εμπορικών και μη) στο Internet με τις απαραίτητες όμως υποδομές που να

αποδίδουν την κατάλληλη νομική ισχύ σε κάθε επίπεδο ηλεκτρονικής συναλλαγής, ενώ παράλληλα να ανοίγουν το δρόμο για την πλήρη αποδοχή τους.

Έτσι, έχει κατά καιρούς, εκδώσει διάφορες συστάσεις και οδηγίες προς τα κράτη μέλη, όπως είναι οι εξής:

- Οδηγία 2002/65ΕΚ για την εξ αποστάσεως εμπορία χρηματοπιστωτικών υπηρεσιών προς τους καταναλωτές.
- Οδηγία 99/44/ΕΚ σχετικά με ορισμένες πτυχές της πώλησης και των εγγυήσεων καταναλωτικών αγαθών.
- Οδηγία 97/55/ΕΚ για την τροποποίηση της οδηγίας 84/450/ΕΟΚ σχετικά με την παραπλανητική διαφήμιση προκειμένου να συμπεριληφθεί η συγκριτική διαφήμιση.
- Σύσταση 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.
- Οδηγία 93/13/ΕΟΚ σχετικά με τις καταχρηστικές ρήτρες των συμβολαίων που συνάπτονται με καταναλωτές.
- Οδηγία 1999/34/ΕΚ σχετικά με θέματα ευθύνης λόγω ελαττωματικών προϊόντων.

Πάντως, και η ελληνική έννομη τάξη προσπαθεί να προσαρμοστεί στην νέα εμπορική πραγματικότητα κυρίως με την προσαρμογή των Ευρωπαϊκών νομοθετημάτων στο εσωτερικό δίκαιο. Παρόλο που παρουσιάζεται γενικά μια καθυστέρηση στην υπόθεση κάποιων επιμέρους Οδηγιών και σε πολλά σημεία χρειάζεται η δημιουργία πιο λεπτομερειακών ρυθμίσεων, αρχίζει και παίρνει μορφή το νομοθετικό εκείνο καθεστώς που να αρμόζει στο ηλεκτρονικό εμπόριο. Η ειδική νομοθεσία, σε συνδυασμό με τις προγενέστερες γενικές διατάξεις παρέχουν σήμερα τη βάση για την προστασία των ηλεκτρονικών συναλλαγών, ενώ παράλληλα τις αναγνωρίζουν ως νόμιμη συναλλακτική πρακτική. Έτσι, λοιπόν, στη χώρα μας οι Αρμόδιες Αρχές και τα Υπουργεία έχουν εκδώσει εξειδικευμένους κανονισμούς, νόμους και προεδρικά διατάγματα

για το ηλεκτρονικό εμπόριο και την προστασία του καταναλωτή. Μερικά από αυτά είναι τα εξής:

- Προεδρικό Διάταγμα 131/2003, προσαρμογή της οδηγίας 2000/31/ΕΚ σχετικά με ορισμένες πτυχές των υπηρεσιών της Κοινωνίας της Πληροφορίας ιδίως του ηλεκτρονικού εμπορίου στην εσωτερική αγορά.
- Κανονισμός ΕΕΤΤ 248/71 για την Παροχή Πιστοποίησης ηλεκτρονικής υπογραφής.
- Προεδρικό Διάταγμα 150/2001, προσαρμογή στην Οδηγία 99/99/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.
- Προεδρικό Διάταγμα 301/2002 για την προσαρμογή της Ελληνικής Νομοθεσίας προς τις διατάξεις της Οδηγίας 1998/27/ΕΚ για τα ασφαλιστικά μέτρα στην προστασία των καταναλωτών, το οποίο τροποποιεί τον νόμο 2251/1994 (τον οποίο θα δούμε παρακάτω).
- Υπουργική απόφαση Αριθμός ζ1-178/2001 (ΦΕΚ 255 β΄). Συναλλαγές που γίνονται με κάρτες - Καταναλωτική πίστη.
- Νόμος 2251/1994 για την προστασία του καταναλωτή και ειδικότερα το άρθρο 4 για τις συμβάσεις που συνάπτονται από απόσταση.

Εδώ θα πρέπει να αναφέρουμε ότι σύμφωνα με τον Γ. Κατσουλάκο(2001) «*ο νόμος 2251/1994 αποτελεί τη βάση για την προστασία του καταναλωτή στο Ηλεκτρονικό Εμπόριο και την αρχή ότι η ανάπτυξη νέων τεχνολογιών δεν θα πρέπει να μειώσει τα δικαιώματα των πολιτών*». Ο νόμος 2251/1994 περί προστασίας του καταναλωτή παρέχει τα εξής:

-Η χρήση τεχνολογιών επικοινωνίας για την οριστικοποίηση συμβολαίων από απόσταση δεν επιτρέπεται να παραβιάζει τα προσωπικά δεδομένα και την ιδιωτική ζωή του καταναλωτή.

-Απαγορεύεται η χρήση, χωρίς τη σύμφωνη γνώμη του καταναλωτή, τεχνολογιών επικοινωνιών όπως είναι τηλεφωνικές κλήσεις, αυτόματη κλήση,

χρήση Fax, χρήση ηλεκτρονικού ταχυδρομείου ή άλλα μέσα ηλεκτρονικής επικοινωνίας για την αίτηση συμβολαίων.

Άλλη μια οδηγία από την Ευρωπαϊκή Ένωση σχετικά με την διαφάνεια, υιοθετήθηκε και αναμένεται να μεταφερθεί στις εθνικές νομοθεσίες. Αυτή διασφαλίζει την προστασία του καταναλωτή μέσω ενός μηχανισμού σύμφωνα με τον οποίο αγωγές σε σχέση με βλάβες, οι οποίες έχουν προκληθεί λόγω λάθους ή παροδηγητικών πληροφοριών ή υπηρεσιών, θα εξετάζονται από τις αρμόδιες υπηρεσίες και από τα τοπικά δικαστήρια, έχοντας δικαιοδοσία επί του προμηθευτή της υπηρεσίας.

Επιπροσθέτως, είναι σημαντικό να γνωρίζουμε ότι βάσει των νόμων και των οδηγιών της Ευρωπαϊκής Ένωσης, σχετικά με την ασφάλεια των ηλεκτρονικών συναλλαγών στο Διαδίκτυο θα πρέπει να παρέχονται από τον έμπορο κάποιες πληροφορίες. Αυτές συμπεριλαμβάνουν τα παρακάτω:

- Ταυτότητα του εμπόρου (όνομα, γεωγραφική διεύθυνση κ.λ.π.)
- Τρόποι επικοινωνίας με τον έμπορο ηλεκτρονικά και παραδοσιακά (ηλεκτρονικό ταχυδρομείο - e.mail, fax, τηλέφωνο κ.λ.π.)
- Τελική τιμή του προϊόντος ή της υπηρεσίας (φόροι, έξοδα αποστολής κ.λ.π.

•Μέθοδος αποστολής και χρόνος παράδοσης, δυνατότητα υπαναχώρησης, τρόπος πληρωμής και παράδοσης κ.λ.π.

•Τρόπος ακύρωσης της παραγγελίας σε περίπτωση λάθους ή αλλαγής γνώμης.

•Επιβεβαίωση της παραλαβής της παραγγελίας.

•Πληροφορίες για την προστασία των προσωπικών δεδομένων (εάν μετά τη συναλλαγή θα διαγραφούν τα στοιχεία του από τη λίστα του εμπόρου, εάν δεν περάσουν σε άλλες εταιρείες κ.λ.π.

•Που απευθύνεται για τα παράπονά του. Εάν κάτι δεν πάει καλά (π.χ. αργοπορημένη παράδοση ή καθόλου παράδοση).

•Πως θα επιστραφεί το προϊόν, πρόσθετα έξοδα για την επιστροφή κ.λ.π.

•Ποιο δικαστήριο είναι αρμόδιο και ποιο Δίκαιο θα εφαρμοστεί σε περίπτωση διαφοράς.

Τελειώνοντας, με αφορμή την τελευταία από τις παραπάνω πληροφορίες είναι σημαντικό να γνωρίζουμε ότι, καθώς το Ηλεκτρονικό Εμπόριο αφορά και τις πωλήσεις προϊόντων και υπηρεσιών προς καταναλωτές διαφορετικών χωρών, στα πλαίσια των χωρών της Ευρωπαϊκής Ένωσης, σε περίπτωση διαφωνίας ο καταναλωτής μπορεί να απευθυνθεί στο δικαστήριο του τόπου κατοικίας του (άρθρο 15c του κανονισμού που αναθεώρησε τη Σύμβαση των Βρυξελλών για τη δωσιδικία, ΕΕΚ L 012, 16/01/2001). Το δε Δίκαιο που θα εφαρμοστεί από το δικαστήριο καθορίζεται από τη Σύμβαση της Ρώμης (ΕΕΚ C 1997) και στις περισσότερες περιπτώσεις είναι το Δίκαιο της χώρας του καταναλωτή.

Τέλος, βρίσκεται σε τελικό στάδιο το Προεδρικό Διάταγμα για το ηλεκτρονικό εμπόριο, με έμφαση στην εξώδικη επίλυση διαφορών, τη συνεργασία των κρατών-μελών για την επίλυση των προβλημάτων των καταναλωτών, τη θέσπιση κανόνων δεοντολογίας, τη σύναψη των ηλεκτρονικών συμβάσεων, τις πληροφορίες που πρέπει να παρέχονται στις εμπορικές επικοινωνίες (διαφημιστικά, χορηγίες, προσφορές κ.λ.π.) και τον τόπο εγκατάστασης των φορέων παροχής υπηρεσιών.

Με αυτό λοιπόν το νομικό πλαίσιο θα μπορούν οι επιχειρήσεις και οι καταναλωτές να αξιοποιούν με τον καλύτερο τρόπο τις δυνατότητες του ηλεκτρονικού εμπορίου.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Είναι κοινή πια παραδοχή πως όσο περνάει ο καιρός και αυξάνονται οι χρήστες του δικτύου, τόσο περισσότερο πλησιάζει το Internet την διάρθρωση και λειτουργία μιας πραγματικής κοινωνίας με δική της γλώσσα, συνήθειες, κώδικα συμπεριφοράς και ηθικής. Όπως όμως συμβαίνει σε κάθε κοινωνία, μερικά μέλη της, δεν ενστερνίζονται τις ηθικές αρχές του συνόλου, αλλά προτιμούν να λειτουργούν σε βάρος των πολλών αποκομίζοντας οικονομικά κυρίως οφέλη. Βέβαια, ακόμη και οι απατεώνες του δικτύου δεν μπορούν να ξεφύγουν από τους περιορισμούς που αυτό επιβάλλει. Οι τρόποι που χρησιμοποιούνται μέσα στο δίκτυο είναι πιο εγκεφαλικοί. Δεν είναι όμως λιγότερο επικίνδυνοι.

Η απώλεια ψηφιακών δεδομένων αποτελεί μια από τις μεγαλύτερες μη υπολογιζόμενες ζημιές για μια σύγχρονη κοινωνία. Η προστασία δεδομένων από εξωτερικούς ή και εσωτερικούς κινδύνους όπως επίσης και η διασφάλιση της ομαλής λειτουργίας των υπολογιστικών συστημάτων ενός οικιακού ή εταιρικού δικτύου πρέπει να συγκαταλέγονται μεταξύ των προτεραιοτήτων όλων. Η μόλυνση ενός ή και περισσοτέρων συστημάτων από ψηφιακό ιό πολύ συχνά έχει ως αποτέλεσμα την καταστροφή ζωτικών δεδομένων για ένα πρόσωπο ή μια εταιρεία. Ένας hacker μπορεί να χρησιμοποιήσει εταιρικά ή προσωπικά δεδομένα με τρόπο ιδιαίτερα επιβλαβή για την ίδια την εταιρία ή το άτομο, χρησιμοποιώντας τα για οποιοδήποτε λόγο αυτός επιθυμεί.

Τα θετικά στοιχεία της χρήσης του διαδικτύου είναι πλέον ευρέως γνωστά όπως η παροχή πληροφοριών για όλα σχεδόν τα θέματα, η εκπαίδευση μέσω διαδικτύου καθώς και η άμεση ή έμμεση επικοινωνία μεταξύ των χρηστών. Το στοιχείο όμως που πρέπει να γίνει ευρύτερα γνωστό με κάθε τρόπο σε όλους τους χρήστες και ιδιαίτερα σε παιδιά και εφήβους είναι οι κίνδυνοι που ελλοχεύουν και που δεν είναι άμεσα ορατοί ή αισθητοί καθώς η επικοινωνία μέσω διαδικτύου διαφέρει κατά πολύ από τα συμβατικά μέσα επικοινωνίας μια και η όλη δραστηριότητα πραγματοποιείται μέσα σε έναν

εικονικό χώρο. Επίσης θα πρέπει οι χρήστες να γνωρίζουν που να απευθυνθούν σε περίπτωση κινδύνου και πώς να προφυλαχτούν από αυτούς.

Ένα άλλο σημαντικό σημείο που πρέπει να τονιστεί είναι ότι κίνδυνοι του διαδικτύου παραμονεύουν και στα κινητά τηλέφωνα. Μπορεί λοιπόν να υπάρχει ένα ποσοστό του πληθυσμού που δεν γνωρίζει και δεν χρησιμοποιεί Η/Υ και διαδίκτυο αλλά χρησιμοποιεί το διαδίκτυο από το κινητό τηλέφωνο. Το γεγονός αυτό είναι ιδιαίτερα ανησυχητικό, γιατί οι κίνδυνοι που υπάρχουν στο διαδίκτυο δεν είναι αποκλειστικότητα του Η/Υ αλλά αποτελούν αναπόσπαστο μέρος της χρήσης των κινητών τηλεφώνων. Στο σημείο αυτό πρέπει να αναφέρουμε ότι οι νέοι και κυρίως ανήλικοι καταναλωτές πιο περίεργοι και πιο ευάλωτοι, πολλές φορές «αγοράζουν» από το κινητό τους ακόμη και υλικό απαγορευμένο για την ηλικία τους. Να θυμίσουμε ότι κινητό τηλέφωνο, στην Ελλάδα, έχει στην κατοχή του το μεγαλύτερο ποσοστό των παιδιών ηλικίας άνω των 11 ετών, επειδή αποτελεί μέσο άμεσης επικοινωνίας της δυάδας γονιού-παιδιού, αντιλαμβανόμαστε πόσο κρίσιμη έχει γίνει πλέον η κατάσταση. Το στοιχείο αυτό οδηγεί στο συμπέρασμα ότι πρέπει να γίνεται ενημέρωση για τους κινδύνους που διατρέχουν τα παιδιά από την χρήση του κινητού τηλεφώνου. Επιπλέον, όσον αφορά τον υπολογιστή, μπορούμε να προστατέψουμε τα παιδιά είτε με την εγκατάσταση φίλτρων όπου απαγορεύουν την είσοδο του ανήλικου χρήστη σε ακατάλληλες ιστοσελίδες, είτε θέτοντας χρονικό όριο στα παιδιά στην παραμονή τους στο “μαγικό” διαδίκτυο, είτε με επιτήρηση των γονιών.

Εξίσου σημαντικό είναι οι ίδιοι οι γονείς να μάθουν στα παιδιά τους να σερφάρουν με ασφάλεια στον καταπληκτικό αλλά αχανή κόσμο του διαδικτύου, να χρησιμοποιούν την πλειάδα των πληροφοριών που παρέχει σωστά, και να αποφεύγουν τους πιθανούς κινδύνους

Υπερσύγχρονα εργαλεία λογισμικού και εξειδικευμένες τεχνικές επίθεσης σε συστήματα υπολογιστών έχουν αρχίσει να χρησιμοποιούν όλο και περισσότερο οι εγκληματίες του Διαδικτύου, με στόχο να είναι περισσότερο αποτελεσματικοί στις παράνομες δραστηριότητές τους - κυρίως οικονομικής

φύσεως -, αλλά και να μη γίνονται αντιληπτοί. Βέβαια δεν είναι μόνο οι διαρκώς εκσυγχρονιζόμενες μέθοδοι που κερδίζουν έδαφος, πολλοί από τους εγκληματίες του Διαδικτύου εμμένουν και στη χρήση των «παραδοσιακών» τρόπων όπως το spam και το phising, η οποία βαίνει αυξανόμενη.

Σημαντικό για την ασφάλεια του ηλεκτρονικού υπολογιστή είναι τα ειδικά προϊόντα ασφαλείας, που καλύπτουν τόσο σε επίπεδο hardware (ο «ορατός» εξοπλισμός ενός συστήματος)όσο και σε επίπεδο λογισμικού (software). Επίσης το επισφαλές ενός υπολογιστή καθορίζεται από το διάστημα που είναι συνδεδεμένος όπως επίσης και από την ταχύτητα της σύνδεσής του. Η χρήση firewalls, antivirus (αντιβιοτικών) προγραμμάτων και λογισμικού προστασίας προσωπικών δεδομένων είναι υποχρεωτική. Για να είναι ολοκληρωμένη η προστασία εκτός από την εγκατάσταση των προγραμμάτων απαιτείται διαρκής ενημέρωση.

Η επίτευξη της σχετικής ασφάλειας σε όλες τις διαδικτυακές δραστηριότητές δεν είναι καθόλου δύσκολη υπόθεση. Το μόνο που απαιτείται είναι να τηρούν οι χρήστες με σχεδόν θρησκευτική ευλάβεια μια σειρά κανόνων, οι οποίοι θα τους απαλλάξουν και θα τους προστατεύουν από κάθε λογής κίνδυνο που μπορεί να συναντήσουν στο Παγκόσμιο Διαδίκτυο.

Ο παγκόσμιος ιστός είναι εξαιρετικά ωφέλιμος για τις μικρές και μεσαίες επιχειρήσεις, αφού προσφέρει πρόσβαση σε απομακρυσμένες αγορές που ανήκαν ως τώρα σε μεγαλύτερες επιχειρήσεις. Ταυτόχρονα όμως με τα τόσα πλεονεκτήματα και οφέλη που προκύπτουν από τη χρήση του διαδικτύου, παρουσιάζονται και ορισμένες προκλήσεις, βασικότερη των οποίων είναι η ασφάλεια Είναι πολύ σημαντικό λοιπόν να γίνει έγκαιρα κατανοητή, από τις επιχειρήσεις και την πολιτεία, η αναγκαιότητα να υποστηρίξουν με διάφορους τρόπους την ασφαλή διακίνηση των πληροφοριών μέσω του διαδικτύου ώστε οι καταναλωτές να το εμπιστεύονται και να το προτιμούν. Οι επιχειρήσεις πρέπει να αναπτύξουν συστήματα ασφαλείας για τα ηλεκτρονικά τους καταστήματα ενώ και η πολιτεία οφείλει να βοηθήσει για να αυξηθεί η διείσδυση του

διαδικτύου έτσι ώστε περισσότεροι πολίτες να έχουν την δυνατότητα πραγματοποίησης ηλεκτρονικών αγορών. Κάτω από αυτές τις προϋποθέσεις οι προοπτικές του ηλεκτρονικού εμπορίου στην Ελλάδα διαφαίνονται αρκετά καλές. Για να επωφεληθούμε από τα πλεονεκτήματα και τις προοπτικές του ηλεκτρονικού εμπορίου είναι απαραίτητο να γίνει σε όλους τους φορείς γνωστή η αναγκαιότητα του ηλεκτρονικού εμπορίου. Όσο πιο γρήγορα το κατανοήσουν αυτό οι Έλληνες επιχειρηματίες και καταναλωτές τόσο πιο εύκολα θα προσαρμοστεί η Ελλάδα στην νέα παγκόσμια πραγματικότητα που διαμορφώνει το ηλεκτρονικό εμπόριο, το εμπόριο του μέλλοντος!

ΠΑΡΑΡΤΗΜΑΤΑ

CASE STUDY 1:ΠΛΑΙΣΙΟ Α.Ε.

ΔΡΑΣΤΗΡΙΟΤΗΤΑ:

Αντιπροσωπείες, αποκλειστικές εισαγωγές, εξουσιοδοτημένοι πωλητές και εμπόριο Η/Υ, περιφερειακών, λογισμικού, αναλώσιμων, χαρτιού και ειδών χαρτοπωλείου, μηχανών και επίπλων γραφείων, τηλεφωνικών συσκευών, υλικών γραφικών τεχνών, κινητών τηλεφώνων και αξεσουάρ. Συναρμολόγηση Η/Υ. Σέρβις. Εγγραφή συνδρομητών και υπηρεσίες κινητής τηλεφωνίας.

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

- Ίδρυση της Εταιρείας

- Συναρμολόγηση και εμπορία υπολογιστών

- Νέο κατάστημα στο Φάρο Ψυχικού

- Κέντρο αποθήκευσης & διανομής και νέο κατάστημα στη Μεταμόρφωση. Κατάστημα ολοκληρωμένου service & αναβάθμισης Η/Υ στην οδό Ζαΐμη.

- Νέο σύστημα απ' ευθείας πωλήσεων & αποστολών μέσω τηλεφώνου, FAX & Direct Mail.

- Εξειδικευμένο κατάστημα ειδών σχεδίου, ζωγραφικής & γραφικών τεχνών στην οδό Στουρνάρη 19.

- Δύο νέα καταστήματα στη Γλυφάδα και στη Θεσσαλονίκη.

- Είσοδος της Εταιρείας στο Χρηματιστήριο.
  Πρώτη παρουσίαση στο Διαδίκτυο.
  Νέα καταστήματα στο Περιστέρι και στην Πάτρα.

- Νέα καταστήματα στο Ηράκλειο Κρήτης και στο Σύνταγμα.

- Νέα καταστήματα στην Αγία Παρασκευή και στην Καλλιθέα.

- Νέο κατάστημα στη Μεταμόρφωση
- Νέο Κέντρο Service στη Γλυφάδα

- Η εταιρία πριν την δημιουργία της ιστοσελίδας της περιοριζόταν στους εξής τρόπους προώθησης των προϊόντων της :

1. Εισαγωγή διαφημιστικών φυλλαδίων της εταιρίας σε εφημερίδες ευρείας ανάγνωσης

2. Συμμετοχή σε μεγάλο αριθμό εκθέσεων

3. Διαφήμιση μέσω των ΜΜΕ (τηλεόραση, ραδιόφωνο, κτλ)

4. Δημιουργία ποικίλλων ,προσιτών στο ευρύ κοινό και εύκολων στην χρήση καταλογών με τα προϊόντα της

5. Χρήση του ελεκτρονικού ταχυδρομείου (μέθοδος spam)

- Με την δημιουργία της ιστοσελίδας της η εταιρία αποσκοπούσε κατά κυρίως λόγο στην προώθηση των προϊόντων της και μέσω του διαδυκτίου .Μια επένδυση με ευοίωνο μέλλον καθώς το ίντερνετ αποτελούσε και αποτελεί ένας ταχύτατα αναπτυσσόμενος τομέας και του εμπορίου. Αξιοσημείωτο επίσης είναι το γεγονός ότι το ηλεκτρονικό εμπόριο είχε ήδη και μάλιστα επιτυχημένα δοκιμαστεί στης Η.Π.Α. , καθώς και σε άλλα ανεπτυγμένα κράτη του σύγχρονου κόσμου
- Επίσης η ιστοσελίδα του ΠΛΑΙΣΙΟ προσφέρει υπηρεσίες και στους μέτοχους ή επιχειρηματικά ενδιαφερόμενους επισκέπτες της με υποσέλιδες με τίτλο ‘’ business-to-business ‘’ και ‘’ ενημέρωση επενδυτών ‘’ παρέχοντας πλήθος πληροφοριών στους εκάστοτε ενδιαφερόμενους.
- Ένα άλλο σημείο στο οποίο και πρέπει να σταθούμε είναι η επικυρωμένη ασφάλεια των προσωπικών δεδομένων των επισκεπτών της ιστοσελίδας ως μέλη και μη .
- Έτσι η εταιρία έχει λειτουργικά , ευκαιριακά αλλά κυρίως στρατηγικά οφέλη

Η ΙΣΤΟΣΕΛΙΔΑ WWW.PLAISIO.GR

- Εντυπωσιακά είναι τα αποτελέσματα που παρουσίασε το πρώτο ηλεκτρονικό κατάστημα στην Ελλάδα www.plaisio.gr. Μέσα σε αυτό το χρόνο, περισσότεροι από 500.000 χρήστες επισκέφθηκαν το ηλεκτρονικό κατάστημα, πραγματοποιώντας 4.000 παραγγελίες, ενώ τα εγγεγραμμένα μέλη του ανέρχονται σε 15.000. Σε ημερήσια βάση, οι χρήστες που επισκέπτονται το κατάστημα ξεπερνούν τους 2.400, ενώ η διάρκεια παραμονής τους φτάνει τα 11 λεπτά, κατά μέσο όρο. Ένα από τα βασικά πλεονεκτήματα του www.plaisio.gr είναι η ευκολία και η ταχύτητα, με την οποία ο επισκέπτης μπορεί να επιλέξει και να παραγγείλει τα προϊόντα που χρειάζεται, και να τα παραλάβει στο χώρο του μέσα σε 24 ώρες.

  (Από το Weekly Telecom , 2000)

- Σε 57,6 εκατ. ευρώ ανήλθαν οι ενοποιημένες πωλήσεις κατά το πρώτο τρίμηνο του 2004, της ΠΛΑΙΣΙΟ COMPUTERS A.E.B.E., σημειώνοντας αύξηση 34,3%. Τα κέρδη προ φόρων έφθασαν τα 2,2 εκατ. ευρώ, πραγματοποιώντας αύξηση 19,4%, ενώ τα κέρδη προ Φόρων, Τόκων και Αποσβέσεων (EBITDA) ανήλθαν στα 3,4 εκατ. ευρώ από 2,8 εκατ. ευρώ

το 2003 εμφανίζοντας αύξηση 20,8%.Με το μοντέλο του πολυκαναλικού συστήματος η ΠΛΑΙΣΙΟ COMPUTERS A.E.B.E., έχει διαμορφώσει ένα πρωτοποριακό μηχανισμό παροχής υπηρεσιών, ο οποίος αποτελεί τον κύριο μοχλό, της συνεχόμενης υψηλής ανάπτυξης, προσφέροντας πλήρη εξυπηρέτηση στην επιχείρηση και στον ιδιώτη καταναλωτή, καλύπτοντας πολλαπλά κάθε ανάγκη τους. Η αποτελεσματικότητα του επιχειρηματικού μοντέλου συμπληρώνεται με τον συνδυασμό υψηλής ανάπτυξης με μηδενικό δανεισμό. (Απο το www.presspoint.gr)

ΠΡΟΤΑΣΕΙΣ ΠΡΟΣ ΒΕΛΤΙΩΣΗ ΤΗΣ ΙΣΤΟΣΕΛΙΔΑΣ

Το site της εταιρίας ΠΛΑΙΣΙΟ A.E.B.E. είναι άρτια δομημένο με σωστή οργάνωση και πληρότητα πληροφοριών , παρέχοντας ταχύτητα στην σύνδεση και την πλοήγηση , καθώς και ασφάλεια στους επισκέπτες του.
Οι οποιεσδήποτε παρακάτω αναφερόμενες πιθανές ατέλειες σε καμία περίπτωση δεν αφαιρούν από την άξια του.

Προτάσεις για βελτίωση του site :

- Η μηχανή αναζήτησης της ιστοσελίδας έχει ακόμη προοπτική βελτίωσης

- Η σύνδεση με την ιστοσελίδα της κατασκευάστριας εταιρίας χρήζει βελτίωσης καθώς σε πολλές περιπτώσεις ή δεν είναι εφικτή ή πραγματοποιείται σύνδεση με την κεντρική σελίδα του κατασκευαστή και όχι με την υποσελίδα που αναφέρεται στο εκάστοτε προϊών.

- Σε ελάχιστες υποσελίδες δεν έχει γίνει πρόσφατη ενημέρωση.

- Επιπρόσθετα η δημιουργία μιας υποσελίδας με προσφορές θα προσέθετε στο ενδιαφέρον του επισκέπτη για το site.

- Η προσθήκη επιπλέον δικαιωμάτων στους επισκέπτες-μέλη θα υποκινούσε πολλούς επισκέπτες στην εγγραφή τους ως μέλη.

- Τέλος η προσθήκη και άλλων γλωσσών εκτός από ελληνικά και αγγλικά στην επιλογή μετάφρασης της ιστοσελίδας θα ήταν χρήσιμη

CASE STUDY 2: ΑΤΛΑΣ (Εταιρικά Δίκτυα Ηλεκτρονικών Υπολογιστών. Ο Άτλας στην Επιχείρηση της Νέας Οικονομίας)

Τα δίκτυα Η/Υ έχουν σημειώσει αλματώδη ανάπτυξη τα τελευταία χρόνια, αφού αποτελούν απαραίτητο συστατικό της εταιρικής υποδομής ενώ ταυτόχρονα η χρήση τους μεταβάλλει τον τρόπο της επιχειρηματικής οργάνωσης καθώς αυξάνει την ταχύτητα και απλοποιεί την ανταλλαγή πληροφοριών τόσο ενδοεταιρικά όσο και στην επικοινωνία με το επιχειρηματικό περιβάλλον.

Η σύνδεση με το Internet είναι πρώτο βήμα για κάθε οργανισμό στην προσπάθειά του να επικοινωνήσει με τον κόσμο της πληροφορίας. Ωστόσο η συστηματικότερη προσπάθεια στην εκμετάλλευση των δυνατοτήτων των δικτύων δίνεται με την ανάπτυξη μιας αξιόπιστης και λειτουργικής δικτυακής υποδομής η οποία θα διασυνδέει τα τμήματα και θα βοηθήσει στην αναβάθμιση των παρεχόμενων υπηρεσιών. Η αναβάθμιση των δικτυακών υπηρεσιών μιας

εταιρίας προσφέρει σειρά πλεονεκτημάτων μερικά από τα οποία παρουσιάζονται παρακάτω.

Στο πλαίσιο κάλυψης αυτών των συγκεκριμένων αναγκών, η εταιρεία SYNET παρέχει και υποστηρίζει ολοκληρωμένες λύσεις πληροφορικής, που περιλαμβάνουν την ανάπτυξη και υλοποίηση μηχανογραφικών εφαρμογών και τηλεδικτύων, την παροχή συμβουλευτικών υπηρεσιών και υπηρεσιών σχεδιασμού, υπηρεσίες διαμόρφωσης και δικτύωσης κτιριακών εγκαταστάσεων, τεχνική υποστήριξη και συντήρηση. Παρακάτω ακολουθεί ένα παράδειγμα ανάπτυξης δικτύου για κάλυψη αναγκών μιας τυπικής ελληνικής εταιρείας:

Ενδοεταιρική επικοινωνία: Η ενδοεταιρική επικοινωνία που για χρόνια χρησιμοποιούσε τις παραδοσιακές τεχνικές με ανταλλαγή σημειωμάτων και fax, τείνει να αντικατασταθεί με υπηρεσίες ηλεκτρονικού ταχυδρομείου και διαχείρισης εγγράφων**.** Ο αυτοματοποιημένος σύγχρόνος τρόπος επικοινωνίας μειώνει το χρόνο διεκπεραίωσης μεγάλου όγκου πληροφοριών γρήγορα και εύκολα με το μικρότερο λειτουργικό κόστος. Επιπλέον η εξέλιξη των δικτύων προσφέρει δυνατότητες τηλεδιάσκεψης και τηλεκπαίδευσης με χρήση του εταιρικού δικτύου, γεγονός που μειώνει τόσο το κόστος συγκέντρωσης του προσωπικού όσο και το χρόνο οργάνωσης και διεξαγωγής της διάσκεψης.

Ενοποίηση δικτύων φωνής και δεδομένων: Η ενοποίηση των δικτύων φωνής και δεδομένων είναι η νέα τάση στη δημιουργία δικτύων πολλαπλών υπηρεσιών. Με αυτόν τον τρόπο είναι δυνατή η διασύνδεση των τηλεφωνικών κέντρων με στόχο την πληρέστερη κάλυψη των αναγκών επικοινωνίας με τους πελάτες και συνεργάτες της, αλλά και τη μείωση του κόστους επικοινωνίας. Η μεταξύ των καταστημάτων τηλεφωνική επικοινωνία δεν χρησιμοποιεί το υπεραστικό δίκτυο του τηλεπικοινωνιακού φορέα αλλά την υπάρχουσα δικτυακή υποδομή μειώνοντας αισθητά τα τηλεπικοινωνιακά τέλη.

Δίκτυο πολλαπλών υπηρεσιών: Η ανάπτυξη ενός δικτύου πολλαπλών υπηρεσιών προσφέρει μία επικοινωνιακή υποδομή η χρήση της οποίας συμμετέχει στη λειτουργία της επιχείρησης. Οι ανάγκες από την επικοινωνιακή

υποδομή αυξάνουν με τη χρήση των υπηρεσιών που προσφέρει. Η εξοικείωση του προσωπικού με τις υπηρεσίες συντελεί στην αύξηση της χρήσης των εφαρμογών οι οποίες με την σειρά τους ζητάνε περισσότερα από το δίκτυο. Η δυνατότητα αναβάθμισης του δικτύου είναι προϋπόθεση στην επιλογή των λύσεων. Επιπλέον, η σταθερότητα, λειτουργικότητα και διαθεσιμότητα του δικτύου είναι καθοριστικοί παράγοντες της σωστής ανάπτυξης και σχεδίασής του. Η χρήση του δικτύου αυξάνει τις απαιτήσεις και οδηγεί το μηχανισμό λειτουργίας της εταιρίας να βασίζεται όλο και περισσότερο στο επικοινωνιακό δίκτυο. Για το λόγο αυτό το δίκτυο θα πρέπει να είναι σε θέση να διαθέτει χαρακτηριστικά σταθερότητας σε πιθανές αστοχίες συστημάτων ή γραμμών. Οι ανάγκες κάθε εταιρίας για την ανάπτυξη της δικτυακής υποδομής διαφέρουν ανάλογα με τον προσανατολισμό της, τη γεωγραφική κατανομή των καταστημάτων της, αλλά και τη χρήση των πληροφοριών που επιθυμεί να διαχειριστεί μέσω του δικτύου. Στην συνέχεια προσθέτουμε ένα παράδειγμα σχεδιασμού δικτύου. Στην συνέχεια προσθέτουμε ένα παράδειγμα σχεδιασμού δικτύου που εφαρμόζεται σε μια σύγχρονη ελληνική εταιρία. Στο παράδειγμα αυτό παραθέτουμε θέματα σχεδιασμού προκειμένου να δείξουμε τη μεθοδολογία που ακολουθείται στην ανάπτυξη σύγχρονων δικτύων πολλαπλών υπηρεσιών.

Οι κυριότερες απαιτήσεις που τίθενται από τυπικές εμπορικές εταιρίες οι οποίες επιθυμούν να δημιουργήσουν δικτυακή υποδομή για τη διασύνδεση των γραφείων και υποκαταστημάτων τους, σε διαφορετικές πόλεις είναι:

- Να εξυπηρετηθεί η επικοινωνία των εφαρμογών τους: Windows, Networking, εφαρμογές λογιστηρίου και αποθήκης, μεταφορά ταχυδρομείου, σύνδεση με Internet κλπ.
- Μεγάλη διαθεσιμότητα του δικτύου τους, ειδικά αν αυτό χρησιμοποιείται κατά την παραγωγική διαδικασία. Απώλεια δικτύου ή σύνδεσης με το Internet σε πολλές εταιρίες σημαίνει απώλεια χρόνου εργασίας για μέρος του προσωπικού.

- Διασύνδεση τηλεφωνικών κέντρων από τις υπάρχουσες γραμμές, η οποία θα προσφέρει σημαντική μείωση του κόστους των τηλεφωνικών τελών για την επικοινωνία των καταστημάτων.
- Χρήση προϊόντων τηλεδιάσκεψης στα πλαίσια της οπτικοακουστικής επικοινωνίας τόσο με πελάτες όσο και μεταξύ στελεχών της εταιρίας.
- Ανάπτυξη επιχειρηματικών δραστηριοτήτων και εφαρμογή τηλεργασίας μέσω του Internet.
- Πρόσβαση στο δίκτυο της εταιρίας από απόσταση για τους εργαζόμενους της εταιρίας που μετακινούνται συχνά και θέλουν να έχουν πρόσβαση στις εφαρμογές στο γραφείο τους.

Ας υποθέσουμε ότι η εταιρία διαθέτει γραφεία στις πόλεις Αθήνα, Θεσσαλονίκη, Λάρισα και Ηράκλειο. Τότε ισχύουν τα ακόλουθα:

-το δίκτυο έχει κέντρο τα γραφεία της εταιρίας στην Αθήνα και αναπτύσσεται με μισθωμένα ψηφιακά κυκλώματα προς τις άλλες πόλεις. Το ψηφιακό δίκτυο ISDN χρησιμοποιείται τόσο ως εναλλακτικό στην περίπτωση πρώτης γραμμής όσο και ως ενισχυτικό του διαθέσιμου εύρους διασύνδεσης στην περίπτωση που απαιτείται περισσότερο εύρος κάποιες χρονικές στιγμές.

- η λειτουργία της συνδιάσκεψης θα γίνεται σε ώρες με μικρότερο φόρτο στο δίκτυο για να μην επηρεάζεται η λειτουργία των εφαρμογών.

-η σύνδεση στο ιντερνετ πρέπει να ακολουθεί τις συνθήκες ασφάλειας και επιπλέον να επιτρέπει την ασφαλή σύνδεση των υπάλληλων της εταιρίας μέσω του ιντερνετ στο δίκτυο της εταιρείας για χρήση συγκεκριμένων εφαρμογών. η αντιμετώπιση του δικτύου αυτού έγινε λαμβάνοντας υπόψη την υπάρχουσα υποδομή η οποία με κατάλληλες αναδιατάξεις και αναβαθμίσεις διαμορφώθηκε με τρόπο που να ικανοποιεί τις προαναφερόμενες απαιτήσεις του πελάτη.

Α. Βασική δικτυακή υποδομή

Το δίκτυο δεδομένων αποτελείται από τα τοπικά δίκτυα των καταστημάτων και τη διασύνδεση αυτών μέσων ψηφιακών και ISDN γραμμών. η ενεργοποίηση του ISDN κυκλώματος γίνεται είτε για την αποκατάσταση της επικοινωνίας μετά από πτώση του ψηφιακού κυκλώματος είτε για την επαύξηση του διαθέσιμου εύρους στην περίπτωση αυξημένου φορτίου στην κύρια γραμμή. η ασφάλεια στις κλήσεις ISDN εξασφαλίζεται δίπλα με κωδικούς έλεγχου και με αναγνώριση κλήσης. στην περίπτωση ενεργοποίησης του ISDNλόγω φόρτου ορίστηκε ως κριτήριο το 75% του φορτίου της κύριας γραμμής .η ενεργοποίηση του ISDNδικτύου γίνεται με τρόπο ώστε οι χρεώσεις να εμφανίζονται στο γραφείο της Αθηνάς. έτσι αν η ενεργοποίηση του ISDN γίνει από τα επαρχιακά καταστήματα εφαρμόζεται η λειτουργία του call back και τη διεκπεραίωση της κλήσης αναλαμβάνει το ISDN της Αθηνάς.

Β. Ασφάλεια

Η σύνδεση του δικτύου μιας εταιρίας στο ιντερνετ ανοίγει την πρόσβαση στο μεγαλύτερο δίκτυο σε παγκόσμιο επίπεδο. Η σύνδεση αυτή είναι ίσως η πλέον αναγκαία μπορεί ωστόσο να δημιουργήσει πολλά προβλήματα όσον αφορά στην προστασία του δικτύου της εταιρίας από πιθανές επιθέσεις μέσω ιντερνετ. Στο case study που παρουσιάζουμε η προστασία του δικτύου ελέγχεται με τη χρήση συστήματος προστασίας firewall πάνω στο οποίο έχει αναπτυχθεί η πολιτική προστασίας, που στηρίζεται στις ακόλουθες αρχές :

-το εσωτερικό δίκτυο έχει διευθύνσεις ιδιωτικών δικτύων για να αποτρέπει την απευθείας πρόσβαση των τερματικών στο ιντερνετ. για την υλοποίηση του χρησιμοποιείται η τεχνική network address translation για την επικοινωνία με το ιντερνετ

-οι χρηστές του εσωτερικού δικτύου συνδέονται στο ιντερνετ για χρήση συγκεκριμένων υπηρεσιών οι οποίες έχουν οριστεί στο firewall. Ειδικότερα για τις υπηρεσίες WEB και FTP η πρόσβαση στο ιντερνετ επιτρέπεται μόνο από τον εσωτερικό proxy-cashe server

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ/BOOKS:

- Alfred, Glossdrenner (1995), Internet έξυπνα τρυκ, Αθήνα: Nubis.
- Beekman, George (2005), Εισαγωγή στην Πληροφορική, Αθήνα: Γκιούρδας.
- Cohen, Alan (1999), Δίκτυα Υπολογιστών, Αθήνα: Ίων.
- Douglas E. Comer (1996), Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet, Αθήνα: Κλειδάριθμος.
- Falk, Bennett (1996), Εξερευνήστε το Internet, Αθήνα: Κλειδάριθμος.
- Snell, Ned (2000), Μάθετε το Internet σε 24 ώρες, Αθήνα: Γκιούρδας.
- Stallings, William (2003), Επικοινωνίες υπολογιστών και δεδομένων, Αθήνα: Τζιόλα.
- Tanenbaum Andrew και Maarten Van Steen (2005), Κατανεμημένα συστήματα: Αρχές και υποδείγματα, Αθήνα: Κλειδάριθμος.
- Tanenbaum, Andrew (2000), Δίκτυα Υπολογιστών, Αθήνα: Παπασωτηρίου.
- Αλεξόπουλος, Άρης και Λαγογιάννης Γεώργιος(1999), Τηλεπικοινωνίες και Δίκτυα Υπολογιστών, Αθήνα: Γκιούρδας.
- Γκιμπερίτης, Βαγγέλης (2000), Internet οδηγός για όλους, Αθήνα: Τζιόλα.
- Κομνηνός Θ., Σπυράκης Π. (2002), Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων,Αθήνα: Ελληνικά Γράμματα.
- Παναγιωτόπουλος Π.,Δραγώνας Γ., Σκούρλας Χ.,(2001), Τηλεπληροφορική και Δίκτυα Υπολογιστών, Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

ΕΛΛΗΝΙΚΗ ΑΡΘΡΟΓΡΑΦΙΑ:

- Αγγελούδης Στέλιος, «*Ηλεκτρονικό εμπόριο*», Notizie, No6, Ιταλία 2000
- Αναστασιάδης Αναστάσιος , «*Οι επιχειρήσεις στον κυβερνοχώρο*», Οικονομικός Ταχυδρόμος, Αθήνα 15 Οκτωβρίου 1998
- Κρασοπούλου Παναγιώτα, «*Τα πλεονεκτήματα του ηλεκτρονικού εμπορίου*», Ευρωενωσιακό Οικονομικό Δελτίο Διοικήσεως Επιχειρήσεων, Αθήνα,14 Αυγούστου 2003
- Λυραντωνάκης Α., «*Το ηλεκτρονικό εμπόριο στο Internet:Ανάγκη για μια κοινή γλώσσα συνεννόησης*», Ευρωενωσιακό Οικονομικό Δελτίο Διοικήσεως Επιχειρήσεων, Αθήνα, Ιανουάριος-Φεβρουάριος 1999

ΔΙΑΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ:

- http://athina.cs.unipi.gr
- http://dspace.lib.uom.gr
- http://eos.uom.gr
- http://homebank.nbg.gr
- http://imap.org
- http://news.promnos.net
- http://noc.auth.gr/services/personal/certificates
- http://office.microsoft.com/el-gr/project
- http://spinellis.gr
- http://w3.bsa.org/hellas//antipiracy/greece
- http://web.auth.gr
- http://www.aboutbooks.gr
- http://www.acci.gr
- http://www.aegean.gr/culturatelc/kalionatis

- http://www.aegean/culturaltec.skammas/
- http://www.ahepahosp.gr/files/itsecnotes.pdf
- http://www.athos.gr
- http://www.bicepirus.gr/enti/seminario/ecommerce/ppt
- http://www.ca.grnet.gr/faq.php
- http://www.cardisoft.gr
- http://www.cisco.com/global/GR/media
- http://www.cuteftp.com
- http://www.cybercash.com
- http://www.dart.gov.gr
- http://www.diaplous.org/library/nomothesia.php
- http://www.dide.flo.sch.gr/plinet/lutorials/lutorials-cryptography-digital signature.html
- http://www.dide.flo.sch.gr/plinet/tutorialsfirewalls.html
- http://www.dlib.ionio.gr/ctheses/0304tab522k/Sklavenitis_Authencity.doc
- http://www.ebusinessforum.gr/engine/index
- http://www.ebusiness-lab.gr
- http://www.eett.gr/opencms.sites/EETT/electronic_communications/digital signature/introesign.html
- http://www.el.wikipedia.org/wiki/firewall
- http://www.esee.gr
- http://www.etender.info/index
- http://www.e-yliko.gr
- http://www.ftpplanet.com
- http://www.goonline.gr/ebusiness/specials/article
- http://www.goonline.gr/ebusiness/specials/article.htm/articleid
- http://www.inf.teilam.gr
- http://www.islab.demokritos.gr/gr/html/mgogoulos/eisagogi.htm
- http://www.it.nom.gr/project/multimedia_technology/extra/append10.htm

- http://www.lawnet.gr
- http://www.makthes.gr
- http://www.malawicichidhomepage.com/greek/articlesgreek/fishywwebsite.greek.html
- http://www.microsoft.com/technet/prodtechonol/winxpro/el/maintain/sp2chngs.mspx
- http://www.pctdata.com
- http://www.pki.gr
- http://www.roland.gr
- http://www.rub.cti.gr
- http://www.rug.cti.gr/bouras/ergasies/foitites/asfaleia internet.doc
- http://www.saferinternet.org
- http://www.setco.org
- http://www.syros.aegean.gr
- http://www.techblog.gr
- http://www.tech-faq.co/ylang/el/firewall.shtml
- http://www.utopia.duth.gr/kdrakato/thesis/chapter2.doc
- http://www.w3.org/security/security-resource