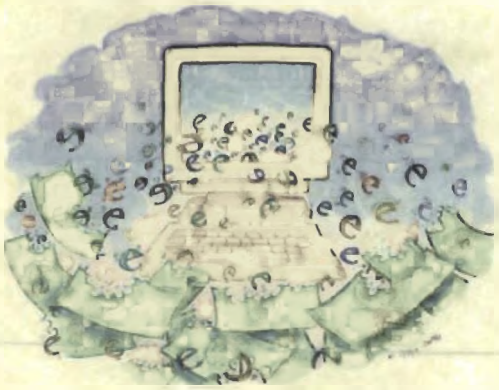
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ



ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ
ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗΝ
ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: INTERNET ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΣΠΟΥΔΑΣΤΡΙΑ: ΣΤΕΦΟΠΟΥΛΟΥ ΣΤΑΥΡΟΥΛΑ

ΕΙΣΗΓΗΤΡΙΑ: ΠΑΛΙΑΤΣΑ ΒΑΣΙΛΙΚΗ

Μεσολογγι 2008

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 4

Εισαγωγή

Η έκρηξη των νέων τεχνολογιών πληροφορικής, που περιστρέφονται γύρω από τη λογική των δικτύων και της χρήσης Ηλεκτρονικών Υπολογιστών, δημιουργούν σήμερα μια νέα παγκόσμια πραγματικότητα στις επιχειρηματικές συνεργασίες.

Οι καινούργιες δυνατότητες διασύνδεσης και επικοινωνίας, μεταξύ επιχειρήσεων πάσης φύσεως, οργανισμών και τελικών καταναλωτών, δημιουργούν ένα επιχειρηματικό περιβάλλον με εντελώς νέα χαρακτηριστικά, καινούργια ισορροπία δυνάμεων και νέους οικονομικούς "παίκτες".

Το εμπόριο, με την αξιοποίηση των δυνατοτήτων που προσφέρει η νέα ηλεκτρονική επικοινωνία, αλλάζει δραστικά τη φιλοσοφία και τις τεχνικές τού παραδοσιακού εμπορίου. Το Ηλεκτρονικό Εμπόριο αναδεικνύεται ως κύριος στρατηγικός στόχος αλλά και ως μείζον εργαλείο για την ανάπτυξη των επιχειρήσεων. Αποτελεί μία σύγχρονη επιχειρηματική πρακτική, που σκοπό έχει τη μείωση του κόστους και τη βελτίωση της ποιότητας των προϊόντων και των υπηρεσιών, αλλά και την επίσπευση των απαιτούμενων διαδικαστικών χρονικών περιθωρίων.

Στην καθημερινή ζωή, το Ηλεκτρονικό Εμπόριο συνδέεται με την αγορά και πώληση πληροφοριών, προϊόντων και υπηρεσιών, όπως η ηλεκτρονική ανταλλαγή δεδομένων, το ηλεκτρονικό ταχυδρομείο, οι ηλεκτρονικές πληρωμές και άλλα. Με τον τρόπον αυτόν η χρήση των τεχνολογιών πληροφορικής επιτρέπει την άσκηση νέων εμπορικών δραστηριοτήτων, που περιλαμβάνουν από διαφημίσεις στο Internet έως και πραγματοποίηση ηλεκτρονικών ανταλλαγών. Το ηλεκτρονικό εμπόριο παρουσιάζει σημαντικές ευκαιρίες και οφέλη για όλες τις κατηγορίες επιχειρήσεων:

- Βελτιωμένη ανταγωνιστικότητα
- Βελτιωμένη ποιότητα προϊόντων και υπηρεσιών
- Εξειδικευμένες υπηρεσίες από τους προμηθευτές προς τους πελάτες.
- Άμεση κάλυψη αναγκών
- Ελαχιστοποίηση κόστους παραγωγής και τιμών

Το Internet χρησιμοποιεί την *τεχνολογία μεταγωγής πακέτων* για τη μεταφορά πληροφοριών. Τα δεδομένα κόβονται σε κομμάτια που ονομάζονται ***πακέτα.*** Σε κάθε πακέτο μπαίνει μια «επικεφαλίδα» με τις διευθύνσεις του υπολογιστή – αποστολέα και του υπολογιστή – παραλήπτη, για παράδειγμα,

128.17.42.9	255.8.12.46	ΚΑΛΗΜΕΡΑ
Από	Προς	Δεδομένα

Κάθε πακέτο δεδομένων αριθμείται. Ο υπολογιστής – **παραλήπτης** και ο υπολογιστής – **αποστολέας,** αλλά όχι οι ενδιάμεσοι υπολογιστές, παρακολουθούν τους αριθμούς των πακέτων και ανταλλάσσουν μεταξύ τους πληροφορίες. Ο παραλήπτης λαμβάνει το πρώτο πακέτο, το δεύτερο, το τρίτο κτλ. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο, είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, το ξαναζητάει, και ο αποστολέας είναι υπεύθυνος για την αναμετάδοση του. Ο παραλήπτης ελέγχει, επίσης, αν το περιεχόμενο των πακέτων φτάνει σωστά. Η *διαδρομή* που ακολουθεί ένα πακέτο μέσα από το «σύννεφο» των συνδέσεων δεν είναι προκαθορισμένη.

Τα δίκτυα στο Internet συνδέονται μεταξύ τους με ειδικούς υπολογιστές που ονομάζονται ***δρομολογητές*** **(routers)** ή ***πύλες*** **(gateways).** Ο δρομολογητής είναι λοιπόν ένας υπολογιστής που συνδέει δύο ή περισσότερα δίκτυα (ίδιου ή διαφορετικού τύπου). Η δουλειά τους είναι να **δρομολογούν** τα πακέτα των δεδομένων μέσα από τα διάφορα δίκτυα που αποτελούν το Internet, μέχρις ότου τα επιδώσουν στον προορισμό τους. Ο δρομολογητής ελέγχει την επικεφαλίδα του πακέτου και, αν ο παραλήπτης βρίσκεται στο ίδιο δίκτυο με τον αποστολέα, στέλνει κατευθείαν το πακέτο στον παραλήπτη, χωρίς να χρειαστεί να διαβεί τα όρια του δικτύου. Διαφορετικά, το προωθεί στον επόμενο δρομολογητή που είναι συνδεδεμένος με το δίκτυο κ.ο.κ., μέχρις ότου το πακέτο προωθηθεί τελικά

στο δρομολογητή που είναι συνδεδεμένος στο ίδιο δίκτυο με τον παραλήπτη.

Οι δρομολογητές διατηρούν πίνακες από τους οποίους προσδιορίζουν την κατεύθυνση που πρέπει να πάρει ένα πακέτο, προκειμένου να φτάσει στον προορισμό του. Κάθε φορά, το πακέτο μετακινείται όλο και πιο κοντά στον προορισμό του, έως ότου, τελικά, τον φτάσει. Ανάλογα με την κίνηση, ή σε περίπτωση που ένα τμήμα του δικτύου παρουσιάζει πρόβλημα και βρίσκεται προσωρινά σε αχρηστία, οι δρομολογητές επιλέγουν εναλλακτικούς δρόμους.

Κάθε *υπολογιστής*, κάθε *τόπος*, κάθε *σελίδα* με πληροφορίες, κάθε *χρήστης* που συνδέεται στο Internet έχει τη δική του διεύθυνση. Το σύστημα διευθύνσεων του Internet επιτρέπει σε κάποιον υπολογιστή να συνδέεται με κάποιον άλλον, λόγω του ότι κάθε υπολογιστής έχει το δικό του μοναδικό όνομα και διεύθυνση, όπως κάτι ανάλογο γίνεται και στο διεθνές τηλεφωνικό δίκτυο, όπου κάθε χρήστης έχει ένα μοναδικό αριθμό τηλεφώνου.

Η διεύθυνση ενός υπολογιστή στο **Internet** αναφέρεται και ως **IP διεύθυνση (IP Address)** και αποτελεί την «ταυτότητα» του στο διαδίκτυο. Κάθε διεύθυνση αποτελείται από τέσσερα νούμερα (*αριθμός δικτύου* και *αριθμός υπολογιστή* μέσα στο συγκεκριμένο δίκτυο). Εκτός της αριθμητικής διεύθυνσης μπορεί να προσδιορίζεται και με ένα όνομα. Τα ονόματα αυτά αποδίδονται με κάποιες συμβάσεις μέσω του συστήματος **DNS (Domain Name System).** Για παράδειγμα στη IP Address **147.52.16.2** αντιστοιχεί το όνομα **crete.csd.uch.gr.** Έχουμε, λοιπόν, ως δεδομένο *ότι:*

Κάθε υπολογιστής είναι μοναδικός στο Internet.

Σε έναν υπολογιστή όμως του **Internet**, μπορούν να έχουν πρόσβαση περισσότεροι από ένας χρήστες. Κάθε χρήστης διαθέτει ένα **λογαριασμό**

(account) που περιλαμβάνει το *όνομα χρήστη* και τον *κωδικό πρόσβασης*. Δηλαδή, κάθε χρήστης έχει τη δική του ταυτότητα, το δικό **του όνομα χρήστη (user ID),** το οποίο του επιτρέπει να ξεχωρίζει από τους άλλους χρήστες που χρησιμοποιούν τον ίδιο υπολογιστή. Για να πάρει άδεια να συνδεθεί, πρέπει να επιβεβαιώσει την ταυτότητά του, παρέχοντας στο σύστημα το προσωπικό του μυστικό **κωδικό (password).**

Συνδυάζοντας το γεγονός ότι κάθε υπολογιστής είναι μοναδικός στο Internet και κάθε χρήστης μοναδικός στον υπολογιστή που χρησιμοποιεί, καταλήγουμε στο ότι:

Κάθε χρήστης είναι μοναδικός σε όλο το Internet !!!

Η **ηλεκτρονική ταχυδρομική διεύθυνση** (το ηλεκτρονικό ταχυδρομικό κουτί) κάθε ***χρήστη*** προκύπτει από το όνομα που φέρει ο χρήστης στο σύστημά του, το σύμβολο ¨@¨ που ονομάζεται **at** (στην Ελλάδα μερικοί το αναφέρουν και με τον όρο παπάκι) και το όνομα του ***υπολογιστή*** που του εξασφαλίζει την πρόσβαση στο Internet ή εξυπηρετεί την αλληλογραφία του.

Όνομα_χρήστη@όνομα_υπολογιστή

Π.χ. papadakis@eap.gr και chatzip@dide.ach.sch.gr (οι διευθύνσεις μας) ή mail@primeminister.gr (η διεύθυνση του πρωθυπουργού της Ελλάδας).

1.3 Χρήση διαδικτύου στη Ελλάδα

Ένα από τα μεγαλύτερα ποσοστά αύξησης της χρήσης του Διαδικτύου σε τριμηνιαία βάση την τελευταία διετία είχαμε το τελευταίο τρίμηνο στη χώρα μας, όπως προκύπτει από τα στοιχεία της πιο πρόσφατης έκδοσης της πανελλαδικής έρευνας «Metron Forum» της Metron Analysis.

Συγκεκριμένα, η έρευνα δείχνει ότι το 27,3% των Ελλήνων άνω των 18 ετών χρησιμοποιεί το Internet, όταν το περασμένο Μάρτιο ήταν στο 15,9%. Σύμφωνα με την Metron Analysis, το ποσοστό αυτό σημαίνει ότι οι ενήλικοι Έλληνες χρήστες του Διαδικτύου φθάνουν στα 2,4 εκατομμύρια. Η αύξηση κατά 1,4 ποσοστιαίες μονάδες είναι ένα αρκετά υψηλό νούμερο και πιθανότατα οφείλεται στον έντονο ανταγωνισμό που υπάρχει στην αγορά των ευρυζωνικών συνδέσεων που έχει ως αποτέλεσμα το κόστος της γρήγορης πρόσβασης στο Διαδίκτυο να είναι αρκετά προσιτό.

Πάντως, οι ρυθμοί ανάπτυξης θα πρέπει να αυξηθούν προκειμένου να πλησιάσουμε τους ευρωπαϊκούς μέσους όρους διείσδυσης που κινούνται σε πολλά κράτη-μέλη της Ευρωπαϊκής Ένωσης σε επίπεδα ακόμη και άνω του 50%. Προφίλ. Όσον αφορά το προφίλ του χρήστη, η έρευνα της Metron Analysis δείχνει ότι δεν έχουν υπάρξει σημαντικές αλλαγές.

Η χρήση του Διαδικτύου παρουσιάζει υψηλότερα ποσοστά στους άνδρες απ' ότι στις γυναίκες (32% έναντι 22,9%), ενώ οι απόφοιτοι ΑΕΙ και ΤΕΙ παρουσιάζουν πολύ υψηλότερα ποσοστά σε σχέση με τους απόφοιτους Λυκείου (59,9% έναντι 28,6%).

Επίσης το Internet είναι περισσότερο διαδεδομένο στις μικρότερες ηλικίες.

Έτσι, στους νέους 18-24 ετών το ποσοστό διείσδυσης φθάνει στο εντυπωσιακό 67,1%, για να πέσει στην κατηγορία 25-34 ετών στο 44,2% και στο 31% στους Έλληνες ηλικίας 35-44 ετών.

Σχετικά καλό (20,6%) είναι το ποσοστό χρήσης στην κατηγορία 45-54 ετών, ενώ μόλις 9,2% των ηλικίας 55-64 ετών Ελλήνων «σερφάρει». Αναμενόμενο είναι το μόλις 1% για τους άνω των 65 ασχολούνται με το Internet, όπως και ένας στους δύο μισθωτούς του δημοσίου τομέα (49,9%).
Πιο χαμηλά κινούνται τα ποσοστά στους εργαζόμενους στον ιδιωτικό τομέα (37,3%) και στους ελεύθερους επαγγελματίες (32%) και στους ανέργους

(34,9%). Εκεί που πρέπει να δοθεί μεγαλύτερη προσοχή από όλους όσοι προωθούν το Διαδίκτυο στη χώρα μας είναι στους γεωργούς (μόλις 5,6% χρησιμοποιεί το Internet), στις νοικοκυρές (5,1%) και στους συνταξιούχους (3,2%). Αυξητική τάση καταγράφεται όσο μετακινούμαστε προς ανώτερα κοινωνικά στρώματα, με τη διείσδυση να είναι στο 53,5% στην ανώτερη τάξη και στο 42,8% στην μεσαία τάξη, ενώ για τους μικρομεσαίους (31,5%) και τους εργάτες (14%) τα ποσοστά είναι σχετικά χαμηλά. Οι περισσότεροι Έλληνες χρήστες του Διαδικτύου ασχολούνται με το μέσο εδώ και αρκετά χρόνια, καθώς το 56,3% δηλώνει ότι συνδέεται για περισσότερα από 5 χρόνια. Το 24,9% άρχισε να «σερφάρει» πριν τρία χρόνια, ενώ το 2,1% ξεκίνησε μέσα στο τελευταίο εξάμηνο.

Καθημερινή ενασχόληση

Αξιοπρόσεκτο είναι ότι το 85,1% των Ελλήνων χρηστών συνδέονται τουλάχιστον μία φορά την εβδομάδα. Μάλιστα, για το 37,8% αποτελεί κομμάτι της καθημερινότητάς του, ενώ μόλις το 2,4% δηλώνει ότι χρησιμοποιεί το μέσο σπανιότερα από 1 φορά το μήνα. Πάντως, για τους περισσότερους χρήστες το Internet είναι κάτι που έχει με το σπίτι, καθώς το 61,5% το χρησιμοποιεί εκεί. Το 34,5% δήλωσε ότι συνδέεται και στην εργασία, ενώ για το 16,3% τα Internet cafe είναι εκεί απ όπου «σερφάρουν».

"Σερφάρισμα" αλλά και ενημέρωση

Η απλή περιήγηση στις διάφορες ιστοσελίδες και η αναζήτηση επαγγελματικών πληροφοριών είναι ο κύριος λόγος χρήσης του Διαδικτύου (58,3%), ενώ τα ενημερωτικά sites δείχνουν επίσης εξαιρετικά δημοφιλή, καθώς το 51,3% διαβάζει νέα και ειδήσεις στο Internet.

Σε υψηλά επίπεδα κινούνται ακόμη η αναζήτηση πληροφοριών για χόμπι (36,8%), η πληροφόρηση για ταξίδια (33,8%), τα online παιχνίδια (24,1%),

το «κατέβασμα» τραγουδιών (24,1%), οι ιατρικές πληροφορίες (15,4%) και το «κατέβασμα» ταινιών (15,1%).

Για επικοινωνία με άλλους χρήστες μέσω chat το χρησιμοποιεί το 14,9%, ενώ στο 6,7% ανέρχεται το ποσοστό εκείνων που κάνουν και τηλεφωνικές κλήσεις μέσω Internet.

Τέλος, το 12,5% κάνει και αγορές από ηλεκτρονικά καταστήματα.

1.4 Υπηρεσίες διαδικτύου και τεχνολογίες που χρησιμοποιούνται στο ηλεκτρονικό εμπόριο (e-commerce)

Οι υπηρεσίες και τεχνολογίες που χρησιμοποιούνται στις εφαρμογές του Ηλεκτρονικού Εμπορίου είναι οι εξής :

- Ηλεκτρονικό Ταχυδρομείο (electronic mail – e-mail)
- Ηλεκτρονικές Τράπεζες
- Παγκόσμιος Ιστός (world wide web – www)
- Ηλεκτρονικοί Κατάλογοι – (Electronic-catalogs or e-cat)
- Μεταφορά αρχείων (File Transfer Protocol – FTP)
- Λίστες Ηλεκτρονικού Ταχυδρομείου (Mailing Lists)
- Συνομιλίες (Chat)/IRC (Internet Relay Chat)
- Οι κοινότητες ή Ειδησεογραφικές ομάδες (communities or newsgroups)
- Ηλεκτρονικός Πίνακας Ανακοινώσεων (Bulletin Board Services – BBS)
- Εικονικές Κοινότητες (Virtual Communities)
- Telnet
- Finger
- Gopher
- Τηλεδιάσκεψη
- Τηλεσύνδεση (Remote Login)
- Ηλεκτρονικές Φόρμες (Electronic-Forms or e-forms)

- Γραμμωτοί κώδικες (Bar Codes)
- Πολυμέσα (Multimedia)
- Μηχανές Αναζήτησης
- Δικτυακά Παιχνίδια

1.4.1 Ηλεκτρονικό Ταχυδρομείο (E-mail)

Η ηλεκτρονική αλληλογραφία είναι η πιο δημοφιλής από τις υπηρεσίες του Internet. Το ηλεκτρονικό ταχυδρομείο είναι ένα σύστημα για τη μετάδοση μηνυμάτων μεταξύ υπολογιστών. Τα μηνύματα μπορούν να περιέχουν πληροφορίες σε διάφορες μορφές. Μια ηλεκτρονική επιστολή έχει τη δυνατότητα να περιλαμβάνει, εκτός από κείμενο, εικόνες, ήχους, κινούμενες εικόνες,video, μια εφαρμογή, μέσα στο μήνυμά σας ή ως επισυναπτόμενα αρχεία.

Ως χρήστης e-mail, μπορείτε να στέλνετε μηνύματα σ' άλλους χρήστες e-mail μέσω υπολογιστή, άνετα, γρήγορα και φθηνά. Σας παρέχει επίσης έναν αποτελεσματικό μηχανισμό για τη μετάδοση της πληροφορίας σε έναν ή πολλούς ανθρώπους (mailing lists) ταυτόχρονα. Υποστηρίζει επιπλέον βοηθητικές λειτουργίες όπως:

- Την κοινοποίηση αντιγράφου (CC, Carbon Copy – Αντιγραφή με καρμπόν)
- Την ιδιωτική κοινοποίηση (BCC, Blind Carbon Copy – Τυφλή Αντιγραφή με καρμπόν)
- Την προώθηση μηνύματος
- Την διαχείριση εισερχομένων μηνυμάτων
- Την αποθήκευση, ταξινόμηση και ανάκληση μηνυμάτων.

1.4.1.1 Τι χρειάζεται για να αποκτήσετε e-mail

Ο κάθε χρήστης, για να παραλάβει και να διαβάσει τα μηνύματα του από την ηλεκτρονική γραμματοθυρίδα ή για να στείλει κάποιο μήνυμα, θα πρέπει:

- Να έχει πρόσβαση σε έναν υπολογιστή, συνδεδεμένο στο διαδίκτυο.
- Είτε να έχει εγγραφεί σε μια **web-υπηρεσία για ηλεκτρονική αλληλογραφία,** είτε να έχει αποκτήσει ένα λογαριασμό e-mail από έναν παροχέα υπηρεσιών και εγκατεστημένο κάποιο από τα **ειδικά προγράμματα διαχείρισης αλληλογραφίας.**

Μόλις αποκτήσετε ένα λογαριασμό e-mail (**e-mail account**) και έχετε ένα πρόγραμμα αλληλογραφίας εγκατεστημένο στον υπολογιστή σας (ή ακόμα με απευθείας πρόσβαση στο WEB μέσω μιας υπηρεσίας web-mail), μπορείτε να αρχίσετε να αξιοποιείτε τις υπηρεσίες του ηλεκτρονικού ταχυδρομείου. Η γνώση μερικών βασικών λειτουργιών είναι αρκετή για να ξεκινήσετε.

1.4.1.2 Διεύθυνση e-mail χρήστη (Γραμματοθυρίδα)

Κάθε χρήστης, για να μπορεί να στέλνει ή να λαμβάνει μηνύματα έχει μια μοναδική ηλεκτρονική διεύθυνση.

Μια **ηλεκτρονική διεύθυνση,** αποτελείται από δύο τμήματα που είναι χωρισμένα με το χαρακτήρα @. Το πρώτο μέρος περιλαμβάνει το **όνομα χρήστη (user name),** που είναι ο ιδιοκτήτης της γραμματοθυρίδας, και το δεύτερο μέρος το **όνομα της περιοχής (domain)** που βρίσκεται η γραμματοθυρίδα.

Η περιοχή μιας ηλεκτρονικής διεύθυνσης διαβάζεται ευκολότερα από δεξιά προς τα αριστερά. Τα τελευταία γράμματα μιας ηλεκτρονικής διεύθυνσης περιγράφουν τη χώρα ή τη μορφή του νομικού προσώπου στο οποίο ανήκει. Για παράδειγμα:

.gr	Ελλάδα (Greece)
.uk	Μεγάλη Βρετανία (United Kingdom)
.it	Ιταλία (Italy)
.fr	Γαλλία (France)

ενώ

.com	commercial (εμπορική εταιρία)
.edu	education (εκπαιδευτικό ίδρυμα ή οργανισμός)
.gov	government (κυβέρνηση)
.mil	military (στρατιωτικός οργανισμός)
.org	organization (οργανισμός)

1.4.1.3 Λίστα νέων μηνυμάτων

Τα μηνύματά σας φθάνουν και αποθηκεύονται στον εξυπηρετητή (**server**) της υπηρεσίας που σας παρέχει το e-mail. Όταν ανοίξετε τον υπολογιστή σας και εκτελεστεί η διαδικασία λήψης των μηνυμάτων, τότε αυτά μεταφέρονται στο δικό σας υπολογιστή και εμφανίζονται στη λίστα των νέων μηνυμάτων.

Μόλις ανοίξετε το πρόγραμμα ηλεκτρονικού ταχυδρομείου ή την προσωπική σας σελίδα στην υπηρεσία υποστήριξης ηλεκτρονικού ταχυδρομείο, η λίστα των νέων μηνυμάτων δίνει συνοπτικά στοιχεία για κάθε επιστολή που έχετε λάβει όπως : Ημερομηνία, Αποστολέας, Μέγεθος μηνύματος, Θέμα μηνύματος.

1.4.1.4 Σύνταξη νέας επιστολής και αποστολή

Η σύνταξη μιας νέας επιστολής ξεκινά συνήθως με την εντολή «Νέο μήνυμα». Για να στείλετε ένα ηλεκτρονικό μήνυμα χρειάζεται να συμπληρώσετε τα παρακάτω πεδία:

Προς :

Πληκτρολογείτε τη διεύθυνση του παραλήπτη ή την επιλέγετε από το Βιβλίο Διευθύνσεων. Μπορείτε να στείλετε ταυτόχρονα το μήνυμα σας σε περισσότερους παραλήπτες.

Θέμα :

Η γραμμή του θέματος είναι ένα από τα σημαντικότερα εργαλεία για τη διαχείριση των μηνυμάτων, ιδιαίτερα όταν η εισερχόμενη αλληλογραφία αρχίζει να αυξάνεται σε όγκο. Το θέμα πρέπει να είναι κατατοπιστικό για το τι περιέχει η επιστολή σας. Συνοδεύετε πάντοτε το μήνυμά σας με ένα σύντομο και αντιπροσωπευτικό τίτλο θέματος.

Κοιν. :

Κοινοποίηση. Συμπληρώστε το πεδίο αυτό, αν θέλετε το ίδιο μήνυμα να πάει και σε άλλους παραλήπτες.

Ιδιαίτ. Κοιν. :

Ιδιαίτερη Κοινοποίηση. Αυτό το πεδίο είναι ίδιο με το προηγούμενο με τη διαφορά ότι οι αποδέκτες που θα περιληφθούν εδώ δε θα γίνουν γνωστοί στους υπόλοιπους αποδέκτες.

Επισύναψη :

Στη γραμμή αυτή εμφανίζονται τα αρχεία που έχετε επισυνάψει στην επιστολή.

1.4.1.5 Περιοχή κυρίως μηνύματος :

Ο κύριος χώρος για το μήνυμα. Τα σύγχρονα προγράμματα διαθέτουν και εργαλεία μορφοποίησης, μορφή εμπλουτισμένου κειμένου (HTML) και

μπορούν εκτός από κείμενο να συμπεριλάβουν μια εικόνα, έναν ήχο, κινούμενη εικόνα.

1.4.1.6 Η υπηρεσία Web-mail

Η υπηρεσία Web-mail μας δίνει τη δυνατότητα διαχείρισης μιας ηλεκτρονικής γραμματοθυρίδας, χωρίς την χρησιμοποίηση κάποιου ειδικού προγράμματος ηλεκτρονικού ταχυδρομείου. Η διαχείριση γίνεται μόνο με τη χρήση του φυλλομετρητή. Η υπηρεσία αυτή διευκολύνει ιδιαίτερα τους χρήστες που βρίσκονται σε μετακίνηση και χρειάζονται πρόσβαση στην ηλεκτρονική τους γραμματοθυρίδα. Το σημαντικότερο πλεονέκτημα είναι ότι μπορούμε να βλέπουμε τα e-mail μας πολύ εύκολα οπουδήποτε στον κόσμο και ότι προσφέρεται συνήθως δωρεάν. Τα κυριότερα μειονεκτήματά της είναι ότι η αποστολή και η λήψη μηνυμάτων απαιτεί περισσότερο χρόνο και ότι στις περιπτώσεις που προσφέρεται δωρεάν υπάρχει περιορισμός στο μέγεθος των επισυναπτόμενων αρχείων και στο μέγεθος της γραμματοθυρίδας μας.

1.4.2 ΜΕΤΑΦΟΡΑ ΑΡΧΕΙΩΝ (FILE TRANSFER PROTOCOL – FTP)

Ο όρος **FTP** προέρχεται από τα λεξικά των λέξεων **File Transfer Protocol** (Πρωτόκολλο Μεταφοράς Αρχείων) που είναι το σύνολο των προδιαγραφών στις οποίες βασίζεται η μεταφορά αρχείων.

Το FTP είναι ένα από τα πρωτόκολλα που περιλαμβάνονται στο συνδυασμό πρωτοκόλλων TCP/IP, στον οποίο, ως γνωστόν, στηρίζεται το Internet. Δίνει τη δυνατότητα μεταφοράς αρχείων από τον υπολογιστή σας σε άλλο υπολογιστή (upload) αλλά και να "κατεβάσετε" (download) αρχεία από έναν απομακρυσμένο υπολογιστή στον υπολογιστή σας.

Όπως και οι περισσότερες υπηρεσίες του Internet έτσι και η FTP χρησιμοποιεί το σύστημα Πελάτη/Εξυπηρετητή (Client/Server). Για να χρησιμοποιήσουμε το FTP τρέχουμε στον υπολογιστή μας ένα πρόγραμμα που ονομάζεται πελάτης FTP (FTP Client) και για να συνδεθούμε με έναν απομακρυσμένο υπολογιστή στον οποίο εκτελείται ένα άλλο πρόγραμμα που ονομάζεται Εξυπηρετητής FTP (FTP Server). Χρησιμοποιώντας το πρόγραμμα πελάτη δίνουμε κάποιες εντολές. Για παράδειγμα στέλνοντας μια εντολή που ζητά από τον FTP server να μας στείλει ένα αντίγραφο κάποιου αρχείου που βρίσκεται στον δίσκο του, ο server ανταποκρίνεται στέλνοντας το συγκεκριμένο αρχείο. Στην συνέχεια το πρόγραμμα πελάτης λαμβάνει το αρχείο το οποίο αποθηκεύει στον δίσκο του υπολογιστή μας.
Για να έχουμε πρόσβαση σε ένα FTP server πρέπει να έχουμε κάποιον λογαριασμό σ' αυτόν δηλαδή να είμαστε καταχωρημένοι και να έχουμε User Name (όνομα χρήστη) και Συνθηματικό πρόσβασης (Password).

Υπάρχει όμως και η υπηρεσία Anonymous FTP σε κάποιον server που μας επιτρέπει να συνδεθούμε σε έναν σε έναν FTP server και να πάρουμε αρχεία χωρίς να είμαστε καταχωρημένοι σαν χρήστες στον server. Στην περίπτωση αυτή το όνομα χρήστη είναι το anonymous και το Συνθηματικό πρόσβασης είναι η προσωπική μας διεύθυνση E-mail. Η υπηρεσία Anonymous FTP δεν μπορεί να χρησιμοποιηθεί σε οποιοδήποτε FTP server αλλά μόνο σε αυτούς που έχουν διαμορφωθεί κατάλληλα να παρέχουν αυτήν την υπηρεσία.

Όταν κάνουμε anonymous FTP σε κάποιον server δεν μπορούμε να μεταφέρουμε αρχεία από τον δικό μας υπολογιστή στον server ούτε να επέμβουμε στον δίσκο του server π.χ. να δημιουργήσουμε ευρετήρια, να διαγράψουμε ή να μετονομάσουμε αρχεία. Αλλά και αν ακόμη έχουμε λογαριασμό σε κάποιον FTP server το τι μπορούμε να κάνουμε εξαρτάται από τα δικαιώματα που μας έχουν εκχωρηθεί.

Η υπηρεσία FTP είναι από τις πρώτες υπηρεσίες του Internet και μέχρι πριν μερικά χρόνια ήταν ο μοναδικός τρόπος για το κατέβασμα (download) αρχείων. Σήμερα το κατέβασμα αρχείων μπορεί να γίνει και μέσω της υπηρεσίας WWW με ταχύτητες μικρότερες όμως από ότι με FTP.

1.4.3 Παγκόσμιος Ιστός (World Wide Web – WWW)

Τα αρχικά www είναι συντομογραφία της γνωστότερης υπηρεσίας του Internet, του World Wide Web (Παγκόσμιος Ιστός) ή απλά Web. Τα συναντάμε συχνά σαν συνθετικό διευθύνσεων, όπως π.χ. www.teimes.gr (η διεύθυνση του ΤΕΙ Μεσολογγίου), www.microsoft.com (η διεύθυνση της εταιρείας Microsoft), καθώς κάθε ΤΕΙ, εταιρεία ή οργανισμός με παρουσία στο Internet προσφέρει συνήθως την υπηρεσία αυτή.

Το www γεννήθηκε στο εργαστήριο CERN της Ελβετίας το 1993 και αποτελεί ένα ισχυρό και εύχρηστο μέσο για την προσπέλαση, αναζήτηση και ανεύρεση πληροφοριών στο Internet. Σήμερα, λέγοντας Internet πολλοί εννοούν το www, μιας και αυτό είναι πλέον το επικρατέστερο μέσο για την πλοήγηση στον ωκεανό πληροφορίας στο Internet. Το www διασυνδέει πληροφορίες που είναι αποθηκευμένες σε χιλιάδες υπολογιστές του Internet, διάσπαρτους σε ολόκληρο τον κόσμο. Οι χρήστες του Διαδικτύου μπορούν να προσπελαύνουν τις διαθέσιμες πληροφορίες χρησιμοποιώντας ένα πρόγραμμα που ονομάζεται browser (πρόγραμμα πλοήγησης).

Οι πληροφορίες είναι οργανωμένες σε ηλεκτρονικές σελίδες που ονομάζονται Web σελίδες ή ιστοσελίδες και συνδέονται μεταξύ τους με συνδέσμους. Μια συλλογή Web σελίδων που βρίσκεται αποθηκευμένη σε ένα συγκεκριμένο σημείο του διαδικτύου και διατίθεται δημόσια ονομάζεται Web site, π.χ. το σύνολο των σελίδων που βρίσκονται αποθηκευμένες στη διεύθυνση www.teimes.gr αποτελεί το Web site του ΤΕΙ Μεσολογγίου. Η αρχική σελίδα ενός web site είναι το σημείο εισόδου προς τις υπόλοιπες σελίδες της συλλογής και ονομάζεται home page.

Μπορούμε να φανταστούμε το www σαν μια βιβλιοθήκη : τα web sites – κομβικά σημεία του web – μπορούν να παρομοιαστούν με βιβλία, καθένα από τα οποία αποτελείται από ένα σύνολο σελίδων. Η αρχική σελίδα του site μπορεί να παρομοιαστεί με το εξώφυλλο ή τον πίνακα περιεχομένων ενός βιβλίου. Οι σελίδες και οι σύνδεσμοι που τις συνδέουν σχηματίζουν έναν ιστό πληροφοριών. Μέσω των συνδέσμων ο χρήστης έχει τη δυνατότητα να μεταπηδά από μια σελίδα σε άλλες.

Βασικό χαρακτηριστικό του www είναι η παγκοσμιότητα του. Οι σελίδες που διασυνδέει μπορεί να βρίσκονται οπουδήποτε στον κόσμο. Σαν τελικοί

χρήστες όμως, τις προσπελαύνουμε όλες με ομοιόμορφο τρόπο και έχουμε ίση πρόσβαση προς αυτές χωρίς πρόσθετα έξοδα μεγάλων αποστάσεων ή περιορισμούς.

Το www, όπως είναι γνωστό στους χρήστες του, λειτουργεί με hypertext-linked κείμενα, επιτρέποντας τους να μετακινούνται από ένα χώρο πληροφορίας σε άλλον, με το πάτημα ενός πλήκτρου στο ποντίκι. Οι πληροφορίες αυτές μπορεί να είναι κείμενα, ήχος, γραφικά, ακόμη και video. Το μόνο που βλέπει ο χρήστης, είναι μία εύκολα προσβάσιμη σελίδα με πληροφορίες, απλούστατη στην κατανόησή της.

1.4.3.1 Πώς λειτουργεί το W.W.W. (World Wide Web)

Το www είναι ακόμη ένα παράδειγμα του πελάτη / εξυπηρετητή, στο οποίο δικτυωμένοι υπολογιστές μοιράζονται τη δουλειά που απαιτεί μια διαδικασία. Στο www η επικοινωνία μεταξύ του πελάτη και του εξυπηρετητή γίνεται σύμφωνα με το πρωτόκολλο HTTP (Hyper Text Transfer Protocol).

Εμείς εκτελούμε στον υπολογιστή μας ένα πρόγραμμα πελάτη, πιθανότατα το Netscape Communicator ή το Internet Explorer. Οι πελάτες για την υπηρεσία www ονομάζονται αναζητητές (browsers). Μέσω του browser συνδεόμαστε με έναν απομακρυσμένο υπολογιστή που περιέχει τη σελίδα που θέλουμε να δούμε και στον οποίο εκτελείται ένα άλλο πρόγραμμα που ονομάζεται εξυπηρετητής web (web server). Ο web είναι υπεύθυνος για τη διαβίβαση της σελίδας και ο browser για την παρουσίασή της στην οθόνη του υπολογιστή μας.

Ο browser υποβάλλει την αίτησή του στον web server και περιμένει μέχρις ότου έρθει η απάντηση, οπότε παραλαμβάνει τη σελίδα που ζητήθηκε, που πλέον «φορτώνεται» στη μνήμη του τοπικού μας μηχανήματος, και την εμφανίζει στην οθόνη μας. Κατόπιν η σύνδεση κλείνει. Μόλις ζητήσουμε μια άλλη σελίδα, π.χ. κάνοντας κλικ πάνω σε έναν σύνδεσμο, η ίδια διαδικασία αρχίζει ξανά. Αυτό επαναλαμβάνεται πολλές φορές, σε αντίθεση π.χ. με το FTP που διατηρεί ανοικτή γραμμή

καθ' όλη τη διάρκεια της σύνδεσης. Αυτός ακριβώς ο τρόπος επικοινωνίας εξηγεί και τα πολλαπλά μηνύματα που πιθανόν να βλέπουμε στην τελευταία γραμμή της οθόνης του browser όταν προσπαθεί να εμφανίσει μία web σελίδα ("Contacting Host...", κ.λ.π.).

Η κατανομή της εργασίας μεταξύ του browser του web server επιτυγχάνει τη διαδικασία με πολλούς τρόπους, αλλά σημαίνει επίσης ότι οι δημιουργεί web σελίδων δεν μπορούν να ελέγξουν την τελική τους εμφάνιση, η οποία εξαρτάται από το πώς είναι διαμορφωμένος ο browser. Για παράδειγμα, ο δικός μας ο browser μπορεί να χρησιμοποιεί τη γραμματοσειρά Times-Roman για την παρουσίαση του κειμένου, ενώ ο browser ενός άλλου χρήστη μπορεί να χρησιμοποιεί τη γραμματοσειρά Helvetica.

Καθώς «σερφάρουμε» στο Internet χρησιμοποιώντας τον browser μας, προβάλλουμε στην οθόνη του υπολογιστή μας σελίδες που μπορεί να προέρχονται από πολλούς διαφορετικούς web servers. Από την ίδια web σελίδα μπορεί να ξεκινούν σύνδεσμοι προς άλλες σελίδες που βρίσκονται διασκορπισμένες σε διάφορους web servers ανά τον κόσμο. Έτσι καθώς επιλέγουμε συνδέσμους, ταξιδεύουμε από υπολογιστή σε υπολογιστή μέσα στον Κυβερνοχώρο του Internet.

1.4.4 Usenet

Το Usenet είναι μια υπηρεσία του Διαδικτύου, όπως ακριβώς ο Παγκόσμιος Ιστός (Web). Συγκεκριμένα, πρόκειται για μια υπηρεσία, ή ένα σύστημα, όπως το περιγράφουν οι περισσότεροι, που αποτελείται από ομάδες συζήτησης. Το Usenet ξεκίνησε (με τη μορφή που το γνωρίζουμε σήμερα) λίγο πριν από το 1980 και είναι από τις παλαιότερες υπηρεσίες του Internet. Μια ομάδα συζήτησης είναι ουσιαστικά ένα σύνολο ανθρώπων που συζητούν και ανταλλάσσουν πληροφορίες για ένα συγκεκριμένο θέμα. Υπάρχουν χιλιάδες τέτοιες ομάδες και εκατομμύρια ανά τον κόσμο άνθρωποι που συμμετέχουν. Πρόκειται για ένα σημαντικό επικοινωνιακό εργαλείο και μοιάζει σε πολλά σημεία με το ηλεκτρονικό ταχυδρομείο. Στο Usenet βέβαια δεν υπάρχουν ηλεκτρονικές διευθύνσεις και το «μήνυμα»

μιας ομάδας συζήτησης μπορεί να το διαβάσει οποιοσδήποτε. Θα μπορούσαμε να το περιγράψουμε ως ένα ανοιχτό ταχυδρομείο, στο οποίο οι επισκέπτες έχουν πρόσβαση σε ολόκληρη την αλληλογραφία των μελών του. Τα μέλη κάθε ομάδας συζήτησης ανταλλάσσουν πληροφορίες και συζητούν θέματα που ανήκουν σε συγκεκριμένη κατηγορία. Υπάρχουν ομάδες συζήτησης που ασχολούνται με τον κινηματογράφο, τη μαγειρική, τους υπολογιστές, την επιστήμη, τον αθλητισμό κ.λ.π. Έτσι, όλα τα θέματα εμπίπτουν σε μια συγκεκριμένη κατηγορία και, για να βρείτε αυτό που σας ενδιαφέρει, ανατρέχετε στην αντίστοιχη ομάδα συζήτησης.

Η φιλοσοφία της υπηρεσίας είναι απλή : οι χρήστες του Διαδικτύου στέλνουν «μηνύματα» (ονομάζονται επίσης «άρθρα» ή «δημοσιεύσεις») στις ομάδες συζήτησης, με τα οποία καταθέτουν απόψεις, εκφράζουν απορίες, ζητούν πληροφορίες και γενικότερα επικοινωνούν. Τα άρθρα αυτά ταξιδεύουν σε όλο τον κόσμο και αποτελούνται συνήθως από κείμενο, αλλά μπορεί να περιλαμβάνουν και εικόνες. Με τα κατάλληλα προγράμματα έρχονται σε επαφή με την ομάδα συζήτησης που τους ενδιαφέρει, βλέπουν συνοπτικά τα άρθρα που περιέχουν και επιλέγουν όσα θέλουν να διαβάσουν. Με τα ίδια επίσης προγράμματα, δημιουργούν και στέλνουν τα δικά τους άρθρα.

1.4.4.1 Η Ελευθερία στο Usenet

Στο Usenet δεν υπάρχουν λογοκρισία, νόμοι, έλεγχος. Είμαστε ελεύθεροι να γράψουμε και να «δημοσιεύσουμε» οτιδήποτε. Είναι ένας «δικτυακός τόπος» όπου συγκεντρώνονται άνθρωποι από όλο τον κόσμο για να εκφράσουν τις απόψεις τους, να αντιπαρατεθούν, να μοιραστούν γνώσεις και να πάρουν πληροφορίες. Σε αυτό τον καταιγισμό άρθρων δεν είναι δυνατόν να μην υπάρχουν προσβλητικά, ανούσια, ακόμα και υβριστικά κείμενα. Κάποιες ομάδες συζήτησης εποπτεύονται από ανθρώπους που ελέγχουν την καταλληλότητα των μηνυμάτων και πράττουν αναλόγως. Οι περισσότερες, όμως, δεν υφίστανται έλεγχο και μπορεί κανείς να συναντήσει κάθε λογής κείμενα. Με τα χρόνια, οι χρήστες του Usenet

έμαθαν να ακολουθούν κάποιους άγραφους κανόνες συμπεριφοράς, ώστε το σύστημα να μην καταλήξει να γίνει ένας σκουπιδότοπος κειμένων, αλλά να λειτουργεί για την εξυπηρέτησή τους. Πρώτα από όλα πρέπει να είστε ευγενικοί στα κείμενά σας και να μην προσβάλλετε άλλα μέλη της ομάδας συζήτησης. Επίσης, απαγορεύονται η αποστολή άχρηστων μηνυμάτων, άσχετων δηλαδή με το θέμα συζήτησης των ομάδων, καθώς και τα άρθρα με διαφημιστικό περιεχόμενο. Αν κάποιος παραβεί αυτούς τους κανόνες, το πιο πιθανόν είναι τα μέλη της ομάδας να του κάνουν συστάσεις για να συμμορφωθεί. Οι αποστολείς κακόβουλων μηνυμάτων πρέπει να αγνοούνται: μην τους δίνεται σημασία και μη συνεχίζεται μια συνομιλία υβριστικού περιεχομένου. Το Usenet μπορεί να σας ωφελήσει να μάθετε κάτι που δεν ξέρετε ή να ζητήσετε τη βοήθεια κάποιου.

1.4.4.2 Πώς Λειτουργεί το Usenet

Η λειτουργία του Usenet, όπως και όλων των υπηρεσιών του Διαδικτύου, βασίζεται σε ένα σύστημα προγραμμάτων και στην επικοινωνία ανάμεσα σε έναν «πελάτη» και έναν «διακομιστή». Το πρόγραμμα «πελάτης» (αναγνώστης νέων ή αναγνώστης συζητήσεων, «Newsreader») έρχεται σε επαφή με το διακομιστή (έναν υπολογιστή δηλαδή) και ζητά τις ομάδες συζήτησης και τα άρθρα που περιλαμβάνουν. Δεν υφίσταται κάποιο κεντρικό σύστημα που αποθηκεύει και διακινεί τα άρθρα. Υπάρχουν οι ονομαζόμενοι «διακομιστές νέων», οι οποίοι συνδέονται μεταξύ τους και ανταλλάσσουν τα μηνύματα. Η διαδικασία έχει ως εξής:

Χρησιμοποιείτε ένα πρόγραμμα νέων για να συντάξετε και να στείλετε το άρθρο σας στο διακομιστή νέων. Κάθε εταιρεία παροχής υπηρεσιών Internet (ISP) διαθέτει το δικό της διακομιστή νέων για τους συνδρομητές της. Αν δεν διαθέτει συνδρομή σε κάποια εταιρεία, μπορείτε να χρησιμοποιήσετε διακομιστές που προέρχονται δωρεάν σε διάφορες δικτυακές τοποθεσίες. Προσέξτε ότι το όλο σύστημα λειτουργεί ακριβώς όπως το ηλεκτρονικό ταχυδρομείο. Μόλις το πρόγραμμα νέων έρθει σε επαφή με το διακομιστή (ονομάζονται και NNTP διακομιστές), χρησιμοποιεί το πρωτόκολλο NNTP (Network News Transfer Protocol) και του μεταφέρει το άρθρο σας. Αυτός με τη σειρά του επικοινωνεί με έναν άλλο διακομιστή και παραδίδει ένα

αντίγραφο του άρθρου. Η διαδικασία συνεχίζεται και το μήνυμα σας κάνει το γύρο του κόσμου μέσα από τους διακομιστές νέων, στους οποίους, έχουν πρόσβαση εκατομμύρια χρήστες.

Οι διακομιστές νέων συνδέονται τις περισσότερες φορές με έναν ή δύο άλλους διακομιστές. Κάποιοι, όμως, λειτουργούν ως «σταθμοί» και συνδέονται ταυτόχρονα με πολλούς. Μόλις πληκτρολογήσετε και στείλετε ένα άρθρο, το πρόγραμμα θα έρθει σε επαφή με το διακομιστή νέων και θα το παραδώσει χρησιμοποιώντας το πρωτόκολλο NNTP. Ο διακομιστής, με τη σειρά του, θα παραδώσει ένα αντίγραφο σε έναν ή δύο άλλους και η ίδια διαδικασία συνεχίζεται μέχρι το άρθρο σας να κάνει το γύρο του κόσμου. Κατά τον ίδιο τρόπο ταξιδεύουν τα άρθρα από άλλους υπολογιστές στο δικό σας.

1.4.5 Telnet

Το Telnet είναι ένα εργαλείο που επιτρέπει σε κάποιον να συνδεθεί με έναν άλλον υπολογιστή στο Internet και στη συνέχεια, να το χρησιμοποιήσει σα να είχε συνδεθεί απευθείας με αυτό. Είναι όλα νόμιμα και κανονικά και δεν σημαίνει ότι αν μπείτε απλώς σε κάποια συσκευή που είναι συνδεδεμένη στο Internet θα μπλέξετε μαζί της ή ότι κάποιος άλλος θα μπορέσει να σβήσει ή να αλλάξει αρχεία στον υπολογιστή σας. Για να χρησιμοποιήσετε το Telnet προκειμένου να συνδεθείτε με ένα σύστημα, πρέπει να έχετε πληρώσει συνδρομή στο σύστημα αυτό.

Μέσω του Telnet, μπορούμε να συνδεθούμε με υπολογιστές του Internet σε ολόκληρο τον κόσμο και να εκμεταλλευόμαστε τις υπηρεσίες που προσφέρουν. Έτσι μπορούμε να χρησιμοποιούμε απομακρυσμένες βάσεις δεδομένων και άλλες πηγές πληροφόρησης, να αναζητήσουμε πληροφορίες σε βιβλιογραφικούς καταλόγους διαφόρων βιβλιοθηκών, κ.λ.π.

Ο αριθμός των υπολογιστών του Internet που προσφέρουν την υπηρεσία Telnet είναι πολύ μεγάλος και οι πληροφορίες που διατίθενται καλύπτουν όλους τους τομείς. Αρκετοί από τους υπολογιστές αυτούς περιέχουν on-line συστήματα βοηθείας με μενού που κάνουν τη χρήση τους πιο εύκολη. Κατά τη σύνδεση μας με έναν απομακρυσμένο υπολογιστή, μας ζητείται όνομα

χρήστη (login name) και συνθηματικό (password). Επομένως, θα πρέπει να έχουμε λογαριασμό (δηλαδή δικαίωμα πρόσβασης) στον υπολογιστή αυτό. Μερικές φορές για υπηρεσίες που διατίθενται δημόσια, μας υποδεικνύεται από τον απομακρυσμένο υπολογιστή κάποιο ειδικό login name (π.χ. guest) ώστε να μπορέσουμε να συνδεθούμε ακόμη κι αν διαθέτουμε λογαριασμό.

Δυστυχώς, το Telnet δεν είναι καθόλου γρήγορο. Αυτό μπορεί μερικές φορές να οφείλεται, στην πυκνή κυκλοφορία στο Internet ή στη φύση του συστήματος στο οποίο έχετε συνδεθεί.

1.4.6 Λίστες Ηλεκτρονικού Ταχυδρομείου (Mailing Lists)

Με τον όρο αυτό εννοούμε έναν κατάλογο διευθύνσεων e-mail, που χρησιμοποιείται για την ομαδική αποστολή μηνυμάτων – που αφορούν σε συγκεκριμένο θέμα- στα μέλη της. Η ιδιότητα του μέλους μιας λίστας σημαίνει αυτόματα και την αποδοχή της συμμετοχής στο συγκεκριμένο κατάλογο διευθύνσεων.

Αναλυτικότερα, θα μπορούσαμε να πούμε ότι τα mailing lists είναι μία ακόμη υπηρεσία με βάση το Internet που χρησιμοποιεί το e-mail για την αποστολή σχετικών με κάποιο συγκεκριμένο θέμα μηνυμάτων σε ένα γκρουπ συνδρομητών. Τα περισσότερα mailing lists είναι διαδραστικά, επιτρέπουν δηλαδή στους συνδρομητές τους να αποστέλλουν μηνύματα σε όλους τους υπόλοιπους συνδρομητές της λίστας, με σκοπό την ανταλλαγή ιδεών και απόψεων. Υπάρχουν βέβαια και κάποια mailing lists που έχουν π.χ. στόχο τη διανομή ενός Newsletter, οπότε μόνο ο διαχειριστής της λίστας έχει δικαίωμα να στείλει e-mail σε όλους τους συνδρομητές της. Το μέγεθος ενός mailing lists μπορεί να ποικίλει, με αποδεκτές από εκατοντάδες έως χιλιάδες συνδρομητές, ενώ υπάρχουν άπειρες τέτοιες λίστες με κάθε πιθανό και απίθανο θέμα. Υπάρχουν χιλιάδες ταχυδρομικοί κατάλογοι οι οποίοι καλύπτουν μια μεγάλη ποικιλία θεμάτων, από συνταγές μαγειρικής, μέχρι θέματα ιατρικής. Κάθε βδομάδα δημιουργούνται και καινούργιοι ηλεκτρονικοί κατάλογοι.

1.4.6.1 Πώς λειτουργούν οι ταχυδρομικοί κατάλογοι

Όταν ένας ταχυδρομικός κατάλογος λάβει ένα μήνυμα, ένα αντίγραφο του μηνύματος αυτού πηγαίνει σε όλα τα μέλη του ταχυδρομικού καταλόγου.

Οι περισσότεροι ταχυδρομικοί κατάλογοι μας επιτρέπουν να στέλνουμε και να λαμβάνουμε μηνύματα. Μερικοί άλλοι όμως μας επιτρέπουν μόνο να λαμβάνουμε μηνύματα, όχι και να στέλνουμε.

Εγγραφή σε Mailing Lists : Μπορούμε να γίνουμε συνδρομητές ενός ταχυδρομικού καταλόγου, όπως ακριβώς και σε μια εφημερίδα ή ένα περιοδικό. Αυτό μπορούμε να το κάνουμε στη διεύθυνση : http://www.list.com. Με την εγγραφή η ηλεκτρονική μας διεύθυνση προστίθεται στον ταχυδρομικό κατάλογο.

Ακύρωση εγγραφής : Αν δεν θέλουμε πια να λαμβάνουμε μηνύματα από ένα ταχυδρομικό κατάλογο, μπορούμε να ακυρώσουμε την εγγραφή μας όποτε θέλουμε. Με την ακύρωση της εγγραφής μας, διαγράφετε και η ηλεκτρονική μας διεύθυνση από τον κατάλογο.

Οι λίστες ηλεκτρονικού ταχυδρομείου είναι:

- Κλειστές, στις οποίες μπορούν να αποστείλουν μήνυμα μόνο εγγεγραμμένα μέλη,
- Κλειστές, στις οποίες μπορούν να αποστείλουν μήνυμα μόνο επιλεγμένοι χρήστες.

Παράλληλα δίνεται η δυνατότητα διατήρησης αρχείου με όλα τα μηνύματα τα οποία έχουν σταλεί στη λίστα. Τα αρχεία αυτά είναι κλειστά, η πρόσβαση στα οποία είναι εφικτή μόνο με τη χρήση κωδικού ασφαλείας. Σε κάθε μία από τις παραπάνω περιπτώσεις ισχύει ο κανονισμός λειτουργίας της υπηρεσίας.

Το Κέντρο Δικτύων συνιστά τη χρήση κλειστών λιστών ηλεκτρονικού ταχυδρομείου. Σε περίπτωση που επιθυμούμε να χρησιμοποιήσουμε την συγκεκριμένη υπηρεσία θα πρέπει να συμπληρώσουμε ηλεκτρονικά τη σχετική αίτηση, με την αποστολή της οποίας θα έχουμε αποδεχτεί και τους όρους του κανονισμού χρήσης της υπηρεσίας, που αναφέρονται σε αυτή. Μετά από δύο μέρες θα λάβουμε επιβεβαίωση της αίτησης.

1.4.7 Δικτυακά παιχνίδια (Entertainment Games)

Το Internet δεν είναι μόνο δουλειά, είναι και διασκέδαση. Γι' αυτό και υπάρχουν τα δικτυακά παιχνίδια γνωστά ως MYD, MOO, MUSH, κλπ.
Σε αυτά ο κάθε παίκτης συνδέεται στον εξυπηρετητή του παιχνιδιού, όπου παίρνει τον έλεγχο μιας εικονικής προσωπικότητας. Μπορεί να εξερευνήσει με άλλους παίχτες, να αντιμετωπίσει τα προβλήματα και τις δυσκολίες που εμφανίζονται, να τροποποιήσει το εικονικό περιβάλλον (π.χ. να δημιουργήσει νέα δωμάτια, κλπ.)

Βέβαια τα παιχνίδια του Internet δεν έχουν φτάσει ακόμα στα επίπεδα του PC ή ενός Sony PlayStation X. υπάρχει η δυνατότητα να μπει κάποιος στο Internet και να αρχίσει να παίζει αμέσως, χωρίς να χρειαστεί να ξοδέψει τίποτα. Όμως ανεξάρτητα από τι παιχνίδι παίζει, χρεώνεται το τηλεφώνημα.

1.4.8 Μηχανές Αναζήτησης (Search Engines)

Ένα από τα σημαντικότερα χαρακτηριστικά του Internet είναι η ευκολία που παρέχει στην είσοδο οποιασδήποτε πληροφορίας, επιτρέποντας στους χρήστες του να εισάγουν στοιχεία για κάθε θέμα. Τα στοιχεία αυτά είναι συνήθως ελεύθερα διαθέσιμα σε όλους τους χρήστες, καθιστώντας έτσι το Internet στο σύνολό του μία μοναδική πηγή πληροφόρησης και εύρεσης στοιχείων, που παρόμοιά της δεν υπήρξε ποτέ μέχρι τώρα στην πορεία της ανθρωπότητας. Η ραγδαία αύξηση της χρήσης του World Wide Web, αλλά και των υπόλοιπων υπηρεσιών του δικτύου, έδωσε στους χρήστες τη δυνατότητα να αποκτήσουν εύκολη πρόσβαση στην πληροφορία, αλλά και τη δυνατότητα παροχής στο δίκτυο όλων όσων αυτοί θεωρούν κατάλληλα. Ενώ όμως η πληθώρα πληροφοριών λογικά θα έπρεπε να είναι ευεργετική για τους χρήστες, οι οποίοι έχουν πλέον στη διάθεσή τους ένα τεράστιο όγκο στοιχείων, αυτή η ίδια πληθώρα προξενεί ένα σημαντικό πρόβλημα, που δεν είναι άλλο από το ότι οι χρήστες αδυνατούν τις περισσότερες φορές να εντοπίσουν τα σημεία εκείνα του δικτύου που περιέχουν τις πληροφορίες τις οποίες αυτοί χρειάζονται. Για παράδειγμα, έστω ότι κάποιος χρήστης αναζητεί πληροφορίες για ένα μουσικό συγκρότημα. Πιθανότατα, αρκετοί

χρήστες από όλο το Internet θα έχουν συγκεντρωμένες πληροφορίες για το συγκεκριμένο συγκρότημα σε διάφορες σελίδες του Web ή ενδεχομένως να υπάρχουν σχετικές πληροφορίες από δισκογραφικές εταιρείες κ.λ.π. Επίσης, είναι αρκετά πιθανό να έχουν τοποθετηθεί ορισμένα τραγούδια και φωτογραφίες του συγκροτήματος σε διάφορα FTP ή Gopher sites. Το πρόβλημα που προκύπτει για τον ενδιαφερόμενο χρήστη είναι πώς θα εντοπίσει τις πληροφορίες που αυτός χρειάζεται, πώς δηλαδή θα μάθει τις σελίδες και τα sites που περιέχουν αυτό που αναζητά.

Μολονότι όλον και κάποιον τρόπο μπορεί να σκεφτεί ένας χρήστης για να επιτύχει, κανένας τρόπος δεν μπορεί να συγκριθεί σε πληρότητα, ταχύτητα και αποτελεσματικότητα με την χρήση των περίφημων **μηχανών αναζήτησης** (search engines) του World Wide Web.

1.4.8.1 Ορισμοί

Σύνδεσμοι (links) : Ονομάζουμε link (σύνδεσμο) μια λέξη, μια φράση, μια φωτογραφία, ή ένα εικονίδιο που, πατώντας το με το ποντίκι, μας οδηγεί σε μια άλλη ιστοσελίδα του Δικτύου. Μερικές φορές δεν αλλάζουμε σελίδα, αλλά πατάμε ένα σύνδεσμο για να δούμε μια φωτογραφία, να ακούσουμε ένα τραγούδι ή για να μεταφέρουμε ένα πρόγραμμα στο σκληρό δίσκο.

Surfing: Πολύ συχνά ακούμε τον όρο surfing ή ελληνιστί-σερφάρισμα! Αναφέρεται στην κίνηση κάποιου από σελίδα σε σελίδα, χωρίς κάποιο προκαθορισμένο σχέδιο, ακολουθώντας συνδέσμους από την μια στην άλλη. Πολλοί το συγκρίνουν με το ζάπινγκ στη τηλεόραση.

Browsers: Browsers (φυλλομετρητής) είναι το πρόγραμμα που λειτουργεί σαν παράθυρο προς τον κόσμο. Με τη βοήθειά του ο χρήστης επισκέπτεται τις σελίδες του δικτύου, αποθηκεύει ή εκτυπώνει κείμενα και εικόνες, αποκτά πρόσβαση σε κάθε λογής υπηρεσίες. Μάλιστα οι μοντέρνοι browsers έρχονται πακέτο με χρήσιμα βοηθητικά προγράμματα, που επιτρέπουν την διαχείριση του e-mail, το εύκολο διάβασμα νέων, δυνατότητες συνομιλίας και βιντεοσυνεδρίασης κ.α. Το πιο μεγάλο μερίδιο

στην αγορά καταλαμβάνουν δυο προγράμματα: Ο Internet Explorer της Microsoft, και ο Navigator της Netscape.

Μηχανές Αναζήτησης (search engines): Για να λυθεί το πρόβλημα της αναζήτησης γνώσεων και πληροφοριών, μια νέα τεχνολογία κάτω από το γενικό όνομα μηχανές αναζήτησης. Πρόκειται για πανίσχυρα υπολογιστικά συστήματα, που χρησιμοποιούν τεράστιες ποσότητες μνήμης και συστοιχίες σκληρών δίσκων, για να αποθηκεύσουν πληροφορίες από οποιαδήποτε σελίδα υπάρχει στο Internet και επιτρέπεται η πρόσβαση σε αυτή. Διαθέτουν ένα ειδικό πρόγραμμα – ανιχνευτή που λέγεται spider (αράχνη) ή robot, που βγαίνει σε τακτά χρονικά διαστήματα στο δίκτυο και μαζεύει καινούργιο υλικό που ταξινομείται στα αρχεία της μηχανής. Το περιβάλλον επικοινωνίας που παρέχουν στον εξωτερικό κόσμο είναι εξαιρετικά λιτό. Ο χρήστης ρωτά για ένα συγκεκριμένο θέμα γράφοντας σε ένα πλαίσιο μερικές λέξεις – κλειδιά. Σε κλάσματα του δευτερολέπτου οι μηχανές, μέσω ενός μηχανισμού συσχετισμού λέξεων, αναζήτησης σε ευρετήρια και αξιολόγησης ιστοσελίδων, επιστρέφουν μια λίστα από σελίδες που έχουν σχέση με αυτές τις λέξεις.

Μεταμηχανές αναζήτησης: Οι μεταμηχανές είναι προγράμματα ή ιστοσελίδες που αξιοποιούν άλλες μηχανές αναζήτησης, ώστε να βρουν τη ζητούμενη πληροφορία. Η επιτυχία τους βασίζεται στο γεγονός ότι δεν χρησιμοποιούν μία μηχανή αναζήτησης αλλά πολλές ταυτόχρονα, από τις οποίες παίρνουν τα καλύτερα αποτελέσματα, τα φιλτράρουν, τα συγκεντρώνουν και τα παρουσιάζουν στο χρήστη. Πρέπει να τονίσουμε ότι οι μεταμηχανές δε διαθέτουν δική τους βάση δεδομένων ή Web Robot. Βασίζονται αποκλειστικά με τις μηχανές τις οποίες συνεργάζονται. Μειονεκτούν στο γεγονός ότι ορισμένες από αυτές δεν υποστηρίζουν τελεστές Boole και πολλές φορές δεν ανανεώνουν τις μηχανές αναζήτησης στις οποίες στηρίζονται.

Πύλες (portal): Γενικά, θα μπορούσαμε να περιγράψουμε μια πύλη ως ένα σύνολο ιστοσελίδων που «κρέμονται» πάνω σε μια κεντρική ιστοσελίδα, από την οποία μπορεί κανείς να ξεκινήσει την περιήγησή του στο Διαδίκτυο. Αποτελεί λοιπόν την είσοδο σε ένα πλήθος πληροφοριών, συνήθως πάνω σε καθορισμένες θεματικές ενότητες. Η διαφορά από μία ιστοσελίδα είναι ότι η πύλη έχει δική της βάση δεδομένων με εκατοντάδες ή και χιλιάδες ιστοσελίδες γύρω από διάφορα θέματα. Παράγει δικό της

περιεχόμενο, αν και δεν αποκλείεται να περιέχει δεσμούς (links) και σε άλλες πύλες ή μεμονωμένες ιστοσελίδες. Επομένως, η πύλη είναι κάτι παραπάνω από μία ιστοσελίδα.

Επιπλέον, αποτελεί ένα σύνολο προγραμμάτων και λειτουργιών που έχουν σκοπό να βοηθήσουν το χρήστη να βρει πληροφορίες. Επομένως, η πύλη είναι μια μηχανή αναζήτησης ; Μια πύλη περιλαμβάνει τη δική της μηχανή αναζήτησης αλλά δεν είναι μόνο μηχανή αναζήτησης.

Ο σκοπός μιας πύλης είναι να γίνει η αφετηρία της εξερεύνησης του χρήστη στο Internet. Κάθε πύλη θέλει να έχει τη δική της «κοινωνία» χρηστών, οι οποίοι θα τη θεωρούν τη πρώτη σελίδα που θα επισκεφθούν κατά την καθημερινή τους εξόρμηση στο διαδίκτυο. Για αυτόν ακριβώς τον λόγο προσφέρει υπηρεσίες ηλεκτρονικού ταχυδρομείου, ειδησεογραφία, χρηματιστήριο, δελτίο καιρού, δελτίο κίνησης στους δρόμους, γκρουπ συζητήσεων και πολλές άλλες λειτουργίες. Για τον ίδιο λόγο πάλι ο χρήστης μιας πύλης μπορεί να την διαμορφώσει έτσι, ώστε να δημιουργήσει ένα δικό του περιβάλλον αλληλεπίδρασης με αυτήν. Ο τελικός στόχος είναι η πύλη να μπορεί από μόνη της να καλύψει σχεδόν όλες τις ανάγκες ενός χρήστη στο Internet.

Γενικά οι πύλες χωρίζονται σε δύο μεγάλες κατηγορίες:

Τις κάθετες πύλες (vertical portals): Μια κάθετη πύλη παρέχει πληροφορίες συνήθως για ένα συγκεκριμένο θέμα και αποτελεί τις περισσότερες φορές την εξέλιξη μιας ιστοσελίδας. Γνωστότερες κάθετες πύλες του εξωτερικού:

MP3.com	www.mp3.com
NASA's Earth Sciences Portal	Sdcd.gsfc.nasa.gov/ESD/portal/
CNET.com	www.cnet.com

Τις οριζόντιες πύλες (horizontal portals) : Οι οριζόντιες πύλες δε σχετίζονται με συγκεκριμένα θέματα, αλλά παρέχουν γενικότερες πληροφορίες. Γνωστότερες οριζόντιες πύλες του εξωτερικού:

Yahoo	www.yahoo.com
altavista	www.altavista.com
AOL	www.aol.com

Οι κυριότερες πύλες στην Ελλάδα:

In.gr	www.in.gr
Lawnet.gr	www.lawnet.gr
Flash.gr	www.flash.gr

1.4.8.2 Πώς λειτουργούν οι μηχανές αναζήτησης

Το πρόγραμμα ανιχνευτής ψάχνει συνεχώς στο δίκτυο, ελέγχοντας όσες σελίδες βρει στο πέρασμά του. Από κάθε σελίδα ενδιαφέρεται να βρει τις λέξεις – κλειδιά που την αντιπροσωπεύουν περισσότερο. Όσο εξελίσσονται αυτές οι μέθοδοι φιλτραρίσματος κειμένου, τόσο οι μηχανές αναζήτησης γίνονται εξυπνότερες και τα αποτελέσματά τους πιο εύστοχα. Μόλις τελειώσει αυτή η διαδικασία, τα δεδομένα που αφορούν τη σελίδα, μαζί με

τον τίτλο και τη διεύθυνσή της, μπαίνουν σε ναι τεράστια βάση δεδομένων (database).

Να δούμε τώρα τα πράγματα από την πλευρά του χρήστη. Για να βρούμε σελίδες στο Internet για κάποιο θέμα που μας ενδιαφέρει, δεν έχουμε παρά να πάμε σε μια μηχανή αναζήτησης και να την τροφοδοτήσουμε με λέξεις που έχουν σχέση με αυτό. Μια τέτοια πρακτική λέγεται ελεύθερη αναζήτηση ή ψάξιμο με λέξεις κλειδιά (keyword search). Μπορούμε να δώσουμε όσες λέξεις θέλουμε και με οποιαδήποτε σειρά. Η μηχανή θα μας επιστρέψει συνδέσμους προς όλες τις σελίδες που πιστεύει ότι ταιριάζουν με την ερώτηση (query) που κάναμε, μαζί με τους τίτλους τους και άλλες χρήσιμες πληροφορίες.

1.4.8.3 Κατηγορίες μηχανών αναζήτησης

Ανάλογα με το εύρος ή το θέμα τους, οι μηχανές αναζήτησης διακρίνονται σε τέσσερις βασικές κατηγορίες:

Πλήρεις: διαβάζουν σελίδες από παντού, σε όλες σχεδόν τις γλώσσες. Είναι οι πιο χρήσιμες μηχανές και μπορούν να δώσουν απάντηση σε οποιαδήποτε ερώτηση.

Τοπικές: διαβάζουν σελίδες από μια συγκεκριμένη γεωγραφική περιοχή, και συνήθως υποστηρίζουν μια μόνο γλώσσα. Μπορούν να φανούν χρήσιμες σε περιπτώσεις που ψάχνουμε κάτι συγκεκριμένο από μία περιοχή. Υπάρχουν και μηχανές εξειδικευμένες στο Ελληνικό κομμάτι του δικτύου.

Θεματικές: Είναι περιορισμένες σε ένα αντικείμενο, όπως ιατρική, τέχνη, κλπ.

Αναφοράς: Είναι οι εγκυκλοπαίδειες, τα λεξικά και κάθε μηχανή που χρησιμοποιεί κάποιο υλικό αναφοράς σαν βάση. Δεν πρόκειται λοιπόν καθαρόαιμες μηχανές αναζήτησης, αλλά η λογική του ψαξίματος με λέξεις – κλειδιά είναι παρόμοια.

1.4.8.4 Οι γνωστότερες μηχανές και "μεταμηχανές" αναζήτησης

Google: Είναι η ισχυρότερη μηχανή αναζήτησης. Αναπτύχθηκε ταχύτατα τα τελευταία χρόνια και προς το παρόν έχει ξεφύγει αρκετά στην κούρσα των μηχανών αναζήτησης. Μάλιστα το 2000 τιμήθηκε με πολλά διεθνή βραβεία για τις καινοτομίες που εισήγαγε. Η μεγάλη διαφορά που χωρίζει το Google από τις άλλες μηχανές οφείλεται τόσο στην ποσότητα και την ποιότητα των αποτελεσμάτων, όσο και στην ταχύτητα στην επιστροφή της απάντησης. Για την ποσότητα φροντίζει το πρόγραμμα ανίχνευσης που χρησιμοποιεί, το Google Bot. Ούτε λίγο ούτε πολύ, εξετάζει και αξιολογεί πάνω από ένα δισεκατομμύριο ιστοσελίδες σε τακτά χρονικά διαστήματα. Η ταχύτητα του Google είναι παροιμιώδης. Οφείλεται σε ένα σύστημα διασύνδεσης ανάμεσα σε χιλιάδες υπολογιστές που συνεργάζονται για την εξαγωγή της απάντησης. Για όσους δεν έχουν γρήγορες συνδέσεις, είναι σημαντική η έλλειψη γραφικών και διαφημίσεων, που επιταχύνει κατά πολύ την έλευση των σελίδων του. Το κυρίαρχο θέμα βέβαια είναι η ποιότητα. Δύο είναι τα βασικά κριτήρια: α) το κατά πόσο οι σελίδες που προτείνει μια μηχανή αναζήτησης είναι σημαντικές, και β) κατά πόσο είναι αυτές που ζητάει ο χρήστης, είναι δηλαδή πάνω στο θέμα που ψάχνει.

Direct Hit: Βρίσκεται στο www.directhit.com. Για την ταξινόμηση των σελίδων που παρουσιάζει, εφαρμόζει μια ενδιαφέρουσα τεχνική. Αναλύει τη δραστηριότητα εκατομμυρίων χρηστών, όταν αυτοί ψάχνουν μέσω της συγκεκριμένης μηχανής αναζήτησης. Ελέγχει (ανωνύμως) ποιους συνδέσμους ακολουθούν μετά από κάθε ψάξιμο και πόση ώρα καταναλώνουν στο κάθε site που επισκέπτονται. Μ΄ αυτό το ιδιόμορφο γκάλοπ, οι σελίδες που συγκεντρώνουν την προτίμηση και το ενδιαφέρον των χρηστών, πριμοδοτούνται σε σχέση με τις υπόλοιπες και στο μέλλον εμφανίζονται νωρίτερα από τις υπόλοιπες.

Ask Jeeves: Βρίσκεται στο www.ask.com . Δουλεύει με μια τεχνολογία που λέγεται natural language query (ερώτηση φυσικής γλώσσας). Αυτή τη στιγμή είναι ιδιαίτερα χρήσιμη, απλά μπορείτε να παίξετε μαζί της ρωτώντας. Οι υπολογιστές θα δέχονται ερωτήσεις και εντολές σε φυσική γλώσσα και θα απαντούν με τον ίδιο τρόπο.

Fast Search: Βρίσκεται στο www.allthe web.com. Το μεγάλο πλεονέκτημα της Νορβηγικής αυτής μηχανής είναι η πολύ μεγάλη βάση δεδομένων που διαθέτει. Μέσα από μια εξαιρετικά λιτή εμφάνιση, εμφανίζει ταχύτατα μεγάλη ποσότητα αποτελεσμάτων. Είναι γεγονός ότι υστερεί σε ευστοχία, δηλαδή μπορεί τα πρώτα αποτελέσματα να είναι άσχετα με αυτό που ζητάτε, αλλά σε δύσκολα θέματα θα εμφανίσει πολλές σελίδες που δεν θα βρείτε αλλού.

Alta Vista : Βρίσκεται στο www.altavista.com. Είναι γρήγορη μηχανή με μεγάλη βάση δεδομένων. Η ποιότητα των αποτελεσμάτων της είναι από μέτρια ως πολύ καλή, ανάλογα με το θέμα, καθώς μαζεύει υλικό από πολλές πηγές και το ταξινομεί με ιδιαίτερα πολύπλοκους μεθόδους. Πρωτοπορεί στον τομές της μετάφρασης, καθώς δίνει τη δυνατότητα μετάφρασης των σελίδων που προτείνει σε πολλές γλώσσες.

IxQuick : Βρίσκεται στο www.ixquick.com. Είναι μεταμηχανή, πράγμα που σημαίνει ότι δεν έχει τα δικά της δεδομένα, αλλά παίζει το ρόλο του ενδιάμεσου, μεταφέροντας την ερώτηση του χρήστη σε ορισμένες μηχανές αναζήτησης και συλλέγοντας τα αποτελέσματα. Η συγκεκριμένη μεταμηχανή, κάνει τη ερώτηση σας σε 12 ισχυρές μηχανές αναζήτησης, παίρνει τις πρώτες απαντήσεις από την καθεμιά και τις συνδυάζει με κάποια πολύπλοκη λογική. Οι μεταμηχανές είναι χρήσιμες στην περίπτωση που έχουμε μια ερώτηση για κάποιο σχετικά άγνωστο θέμα και θέλουμε να ψάξουμε με τι μια σε πολλές μηχανές αναζήτησης, σίγουροι ότι οι σελίδες που θα βρεθούν θα είναι λίγες.

Copernic 2001: Είναι ένα πρόγραμμα μεταμηχανής το οποίο χρησιμοποιεί δέκα άλλες γνωστές μηχανές (Yahoo, AltaVista, Excite, και άλλες), προκειμένου να βρει απαντήσεις. Όταν εντοπίσει κάποια ιστοσελίδα που είναι κοινή σε όλες τις μηχανές, την προωθεί προς τα αποτελέσματά του.

Lycos: Βρίσκεται στο www.lycos.com. Είναι πολύ ισχυρός σε αναζήτηση μουσικής, φωτογραφιών και video. Επίσης έχει συγκεντρώσει στην αρχική του σελίδα αρκετές υπηρεσίες και πληροφοριακό υλικό, κυρίως για νέους. Δεν είναι τόσο εύστοχος σε αναζήτηση σπάνιων θεμάτων, καθώς αντλεί το υλικό του κυρίως από καταλόγους που έχουν φτιάξει ειδικοί του Internet πάνω σε δημοφιλή θέματα.

Search : Βρίσκεται στο www.search.com. Είναι από τα ισχυρότερα εργαλεία αναζήτησης εξειδικευμένων πληροφοριών. Έχει συγκεντρώσει εκατοντάδες μηχανές αναζήτησης και τις έχει χωρίσει σε κατηγορίες. Πατώντας σε κάποιο σύνδεσμο κάτω από τη γραμμή Specialize your search έχετε τη δυνατότητα να χρησιμοποιήσετε όλες τις μηχανές αναζήτησης που αντιστοιχούν στο θέμα που επιλέξατε.

Ελληνικές μηχανές αναζήτησης : Προς το παρόν, οι ελληνικές μηχανές αναζήτησης απέχουν πολλοί από τα διεθνή standards. Έχουμε περίπου 2 εκατομμύρια σελίδες και κάποιες βασικές υπηρεσίες on-line. Το βασικό πρόβλημα αυτή τη στιγμή στην κατασκευή και εξέλιξη των ελληνικών μηχανών, είναι ότι δεν υπάρχει η κατάλληλη τεχνογνωσία και οι όποιες προσπάθειες ξεκινούν κυριολεκτικά από το μηδέν. Στον πίνακα παρουσιάζονται οι κυριότερες ελληνικές μηχανές αναζήτησης.

Μηχανή	**Διεύθυνση**
Trinity	Find.in.gr
Trinity	www.pathfinder.gr
Pop	www.pop.gr
Anazitisis	www.anazitisis.gr
Greek Indexer	www.gr-indexer.gr

Trinity : Η πύλη .in.gr , που είναι το πιο δημοφιλές site στο ελληνικό Internet, διαθέτει μηχανή αναζήτησης στη σελίδα find.in.gr. Το πλαίσιο αναζήτησης υπάρχει επίσης και στην κεντρική σελίδα της πύλης στην διεύθυνση www.in.gr. Η μηχανή αυτή λέγεται trinity. Είναι η καλύτερα ενημερωμένη μηχανή, με μεγάλη βάση δεδομένων. Το σύστημα επιλογής προτεινόμενων σελίδων είναι μέτριο, άρα μην περιμένετε να βρείτε οπωσδήποτε στις 10 πρώτες σελίδες αυτό που θέλετε. Την ίδια μηχανή χρησιμοποιεί και η πύλη Pathfinder (www.pathfinder.gr). Η λογική που χρησιμοποιούμε είναι η ίδια με το Google και τις άλλες μηχανές.

1.4.8.5 Κατάλογοι

Όσο ισχυρές και να είναι οι μηχανές αναζήτησης, δεν μπορούν να φτάσουν ακόμη το επίπεδο της ανθρώπινης ευφυΐας στα θέματα της εκτίμησης της ποιότητας των ιστοσελίδων και το χωρισμό τους σε κατηγορίες. Σε αυτό το θέμα υπερτερούν οι θεματικοί κατάλογοι (subject directories). Οι κατάλογοι είναι συλλογές από επιλεγμένα sites, χωρισμένα σε κατηγορίες. Η επιλογή και η κατηγοριοποίηση γίνονται αφενός από ειδικούς της πληροφορικής που ταξινομούν και αξιολογούν τις σελίδες και αφετέρου από άτομα εξειδικευμένα στο κάθε θέμα ξεχωριστά (π.χ. καθηγητές ιστορίας). Βασικά κριτήρια επιλογής ενός site που θα μπει σε έναν κατάλογο είναι η πληρότητα, η ευκολία στη χρήση, η ποιότητα και ο μέσος ημερήσιος αριθμός επισκεπτών. Επομένως είναι λογικό η ποιότητα των sites που προτείνονται να είναι σαφώς βελτιωμένη σε σχέση με αυτή των μηχανών αναζήτησης. Επιπλέον, αρκετοί κατάλογοι συνοδεύουν κάθε site με μια συνοπτική περιγραφή.

Ο πιο πλήρης και πιο αξιόπιστος θεματικός κατάλογος στο Internet είναι το Yahoo. Η κεντρική σελίδα του Yahoo βρίσκεται στη διεύθυνση www.yahoo.com. Έχει επιπλέον πολλές χρήσιμες υπηρεσίες. Ξεκίνησε το 1994,συγκέντρωσε πολλές προτιμήσεις, καθώς εισήγαγε πολύ σημαντικές καινοτομίες και απλοποίησε την αναζήτηση των χρηστών.

ΚΕΦΑΛΑΙΟ 2

Το ηλεκτρονικό εμπόριο (e-commerce)

2.1 Ο ορισμός του ηλεκτρονικού εμπορίου

Η ανάγκη για ηλεκτρονικό εμπόριο προκύπτει από την απαίτηση των επιχειρήσεων και των κυβερνήσεων για καλύτερη χρήση της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών ώστε να βελτιωθούν οι σχέσεις αμφίδρομης επικοινωνίας με τους πελάτες πολίτες καταναλωτές, οι επιχειρηματικές διεργασίες και η ανταλλαγή πληροφοριών ενδοεπιχειρησιακά, αλλά και κυρίως μεταξύ των επιχειρήσεων. Πάντως η ουσιαστική επιδίωξη της κάθε επιχείρησης στον έντονα ανταγωνιστικό επιχειρηματικό στίβο της εποχής μας είναι η εξασφάλιση στρατηγικού πλεονεκτήματος. Η τεχνολογία και ειδικότερα το ηλεκτρονικό εμπόριο παρέχει ευέλικτες και ολοκληρωμένες λύσεις τοποθέτησης των επιχειρήσεων στις επιθυμητές αγορές (target markets) παρεμβαίνοντας ευεργετικά σε κάθε στάδιο της αλυσίδας αξίας τους (value chain). Το Internet ήταν αυτό που έδωσε μεγάλη ώθηση στην ανάπτυξη του ηλεκτρονικού εμπορίου. Έτσι σε πολλές περιπτώσεις βλέπουμε μικρές επιχειρήσεις ή νεοσύστατες να διευθύνουν τις επιχειρήσεις τους on-line, όπως ακριβώς και οι μεγαλύτεροι ανταγωνιστές τους. Με αυτόν τον τρόπο όλες οι επιχειρήσεις μεγάλες ή μικρές περνούν τα πλεονεκτήματα του Internet και προχωρούν στη μείωση του κόστους τους, με το να καταργούν ασύμφορα ιδιωτικά δίκτυα και ψηφιοποιώντας τις επιχειρήσεις τους σε όλους τους τομείς. Η κίνηση αυτή δεν είναι νέα, έχει ξεκινήσει εδώ και μια δεκαετία και συνεχίζει να αυξάνεται καθώς οι προσωπικοί υπολογιστές γίνονται καθιερωμένο εργαλείο κάθε επιχείρησης. Για τη δημιουργία του, σημαντικό πόλο έπαιξε η σπουδαία συνεργασία μεταξύ ψηφιακής πληροφόρησης, υπολογιστικών εφαρμογών και το Internet. Αυτή η συνεργασία έκανε δυνατή την ανάπτυξη του ηλεκτρονικού εμπορίου.

Πριν εξηγήσουμε το ηλεκτρονικό εμπόριο ας θυμηθούμε τι αποτελεί το παραδοσιακό εμπόριο. Το παραδοσιακό εμπόριο αποτελείται κυρίως από την πώληση ενός προϊόντος και την είσπραξη των χρημάτων. Η διαδικασία

της αγοραπωλησίας χωρίς το ηλεκτρονικό εμπόριο έχει περίπου ως εξής: Ο επιχειρηματίας πρέπει να ανακαλύψει τις ανάγκες της αγοράς, να σχεδιάσει την επιχείρησή του, να βρει προμηθευτές των προϊόντων ή των πρώτων υλών, να προσελκύσει πελάτες, να παρέχει τεχνική υποστήριξη, να πληρώσει φορολογία και προσωπικό. Οι καταναλωτές αντίθετα πρέπει να βρουν κάποια ανάγκη για οτιδήποτε έστω αν είναι υλικό προϊόν ή υπηρεσία ή πληροφορία. Μετά αυτοί πρέπει να βρουν πληροφορίες για αυτό που τους ενδιαφέρει να μάθουν πού το πουλάνε και να συγκρίνουν τις επιλογές που έχουν βρει (τιμή, υπηρεσία, υποστήριξη και φήμη), πριν αγοράσουν το προϊόν. Κάνοντας την πώληση είναι πιθανόν να ακολουθήσουν διαπραγματεύσεις για την τιμή, την ποσότητα και τον τρόπο παράδοσης. Και ο κύκλος δεν τελειώνει εκεί. Η τεχνική υποστήριξη προσθέτει περισσότερα βήματα στον κύκλο. Οι καταναλωτές παίρνουν ότι χρειάζονται για να κρατήσουν τα προϊόντα τους σε καλή κατάσταση, ενώ οι προμηθευτές προσπαθούν να μάθουν τι χρειάζεται περισσότερο η αγορά. Εντωμεταξύ τράπεζες και άλλοι οικονομικοί οργανισμοί κατευθύνουν τις μεταβιβάσεις μεταξύ αυτών των δύο (αγοραστών-προμηθευτών).

Αν κάποιος σκεφτεί όλες αυτές τις πράξεις και συναναστροφές θα καταλάβει ότι δεν είναι μια απλή αγοραπωλησία καθώς και ότι το ηλεκτρονικό εμπόριο δεν αποτελεί τη διοίκηση μιας επιχείρησης μέσα από δίκτυα, παρά από χαρτιά, τηλέφωνα, ταχυδρομεία, τρένα, αεροπλάνα, δρόμους καθώς και όλα τα μέσα μετακίνησης των προϊόντων και των πληροφοριών.

Το ηλεκτρονικό εμπόριο είναι ένα σύστημα που περιέχει όχι μόνα αυτές τις πράξεις που επικεντρώνονται στην αγορά και πώληση προϊόντων και υπηρεσιών που δημιουργούν κέρδος αλλά έχει να κάνει και με εκείνες τις συναλλαγές που υποστηρίζουν αυτό το κέρδος, όπως δίνοντας προσφορές πωλήσεων, δημιουργώντας ζήτηση για κάποια αγαθά, τεχνική υποστήριξη και επικοινωνία μεταξύ των συναλλασσόμενων. Το ηλεκτρονικό εμπόριο κτίζεται πάνω στα πλεονεκτήματα και στη δομή του παραδοσιακού ηλεκτρονικού εμπορίου με το να προσθέτει την ευκαμψία που προσφέρουν τα ηλεκτρονικά δίκτυα.

Με το να χειρίζόμαστε ψηφιακές πληροφορίες μέσα σε ηλεκτρονικά δίκτυα, το ηλεκτρονικό εμπόριο φέρνει μερικές νέες ευκαιρίες διευθύνσεις εμπορικών δραστηριοτήτων. Για παράδειγμα με τη χρησιμοποίηση

ψηφιακής πληροφορίας για τη διεξαγωγή εμπορικής δραστηριότητας, το ηλεκτρονικό εμπόριο κάνει ευκολότερη τη συνεργασία μεταξύ τμημάτων. Τα τμήματα αυτά μπορεί να είναι τμήματα ανταλλαγής πληροφοριών για τη δημιουργία στρατηγικής Marketing, συνεργαζόμενες εταιρείες που σχεδιάζουν και κατασκευάζουν νέα προϊόντα ή να προσφέρουν νέες υπηρεσίες.

Επίσης, το να διευθύνει κανείς εμπορικές δραστηριότητες σε ηλεκτρονικά δίκτυα αφαιρεί φυσικά εμπόδια. Για παράδειγμα, τα ηλεκτρονικά συστήματα είναι έτοιμα να εξυπηρετήσουν πελάτες 24 ώρες το 24ωρο και 7 ημέρες την εβδομάδα. Παραγγελίες προϊόντων και υπηρεσιών μπορούν να γίνουν δεκτές οποιαδήποτε στιγμή και από οπουδήποτε.

Το ηλεκτρονικό εμπόριο κάνει δυνατές νέες μορφές επιχειρήσεων καθώς επίσης και νέους τρόπους διοίκησης. Το Amazon.com για παράδειγμα είναι ένα βιβλιοπωλείο με έδρα στο Σιατλ. Αυτή η επιχείρηση δεν έχει κανένα φυσικό κτίριο (αποθήκες, γραφεία). Πουλάει όλα τα βιβλία μέσω Internet και τα αποστέλλει κατευθείαν μέσω του εκδότη και έτσι δεν χρειάζεται να κρατάει κανένα αρχείο πωλήσεων ή πελατών.

Ο ορισμός του ηλεκτρονικού εμπορίου δεν είναι στατικός. Ακόμα και αν η νέα τεχνολογία μας προσφέρει πάρα πολλές ικανότητες, αύριο κάτι νέο και καλύτερο μπορεί να εμφανιστεί. Με έναν απλό ορισμό, θα μπορούσαμε να πούμε πως ηλεκτρονικό εμπόριο είναι η αγοραπωλησία προϊόντων και υπηρεσιών μέσω του Internet. Βέβαια, εάν θέλουμε να είμαστε πιο σωστοί με τον όρο ηλεκτρονικό εμπόριο (e-commerce) εννοείται κάθε εμπορική συναλλαγή, η οποία εκτελείται αποκλειστικά σε ηλεκτρονικό επίπεδο, δηλαδή με τη χρήση ηλεκτρονικών υπολογιστών που συνδέονται μέσω τηλεφωνικών γραμμών. Για την πραγματοποίηση μιας τέτοιας συναλλαγής χρησιμοποιούνται πολύπλοκοι προγραμματιστικοί μηχανισμοί και το κατάλληλο λογισμικό το οποίο επιτρέπει την Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange – EDI) ανάμεσα στις δύο πλευρές (μεταξύ επιχειρήσεων αλλά και μεταξύ επιχειρήσεων και καταναλωτών) που εμπλέκονται στη συγκεκριμένη συναλλαγή. Με άλλα λόγια, η συγκεκριμένη μορφή συναλλαγής πραγματοποιείται μόνο μέσω υπολογιστών, παρακάμπτοντας τον ανθρώπινο παράγοντα και ελαχιστοποιώντας ταυτόχρονα την πιθανότητα λάθους και την κακόβουλη χρήση στοιχείων.

Διαφορά ηλεκτρονικών και παραδοσιακών επιχειρηματικών συναλλαγών

Ο κύκλος της συν/γής	Παραδοσιακός τρόπος	Ηλεκτρονικό εμπόριο
Πηγές πληροφοριών για το προϊόν	Περιοδικά, φυλλάδια, κατάλογοι	Web pages
Παραγγελία του προϊόντος	Γράμμα, ειδική φόρμα	e-mail
Τιμοκατάλογοι	Κατάλογοι	Online κατάλογοι
Έλεγχος διαθεσιμότητας του προϊόντος	Τηλέφωνο, fax	----------
Δημιουργία παραγγελίας	Έντυπη φόρμα	e-mail, web pages
Αποστολή-λήψη παραγγελίας	Ταχυδρομείο, fax	e-mail, EDI
Προτεραιότητα παραγγελιών	----------	Online βάση δεδομένων
Έλεγχος αποθεμάτων	Έντυπη φόρμα τηλεφ., Fax	Online βάση δεδομένων web pages
Προγραμματισμός παράδοσης	Έντυπη φόρμα	Online βάση δεδομένων e-mail
Τιμολόγηση	Έντυπη φόρμα	Online βάση δεδομένων
Παραλαβή προϊόντος	Μεταφορέας	----------
Γράμμα απολαβής παραγγελίας	Έντυπη φόρμα	e-mail
Αποστολή-λήψη τιμολογίου	Ταχυδρομείο	e-mail
Προγραμματισμός πληρωμής	Έντυπη φόρμα	Online βάση δεδομένων EDI
Αποστολή πληρωμής	Ταχυδρομείο	EDI

2.2 Κατηγορίες ηλεκτρονικού εμπορίου

Οι ηλεκτρονικές συναλλαγές (ανταλλαγές δεδομένων και χρηματικές συναλλαγές) υφίστανται κατά την εφαρμογή του ηλεκτρονικού εμπορίου. Οι ηλεκτρονικές συναλλαγές διακρίνονται σε πέντε κατηγορίες:

Επιχείρηση προς επιχείρηση (business to business – b2b): οι εφαρμογές αυτής της μορφής χρησιμοποιούν κυρίως την τεχνολογία της ηλεκτρονικής μεταβίβασης δεδομένων και στοχεύουν στην απλοποίηση των διαδικασιών των επιχειρήσεων, στον έλεγχο και τη μείωση του αποθέματος, στην αυτοματοποιημένη αντικατάσταση των προϊόντων κ.α. Απαραίτητη προϋπόθεση για την επιτυχία των εφαρμογών της κατηγορίας αυτής είναι η συνεργασία και ο συντονισμός των επιχειρήσεων (ακόμη και των ανταγωνιστικών). Οι κύριες εφαρμογές της κατηγορίας είναι οι εξής:

- Πρόγραμμα Συνεχούς Αναπλήρωσης (Continuous Replenishment Program – CPR).
- Ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange – EDI)
- Χρηματοοικονομικό EDI (Financial EDI)
- Ηλεκτρονική Μεταφορά Κεφαλαίου (Electronic Funds Transfer – EFT)
- Ανάπτυξη Κοινών Επιχειρηματικών Διαδικασιών μεταξύ επιχειρήσεων (Shared Business Processes)
- Ηλεκτρονική Διαπραγμάτευση (Electronic Negotiation)
- Μεσιτεία Πληροφοριών, Υπηρεσίες Εμπιστοσύνης (InfoBrockerage, Trust Services)
- Αγορές Τρίτου Φορέα (Third Party Marketplaces)

Επιχείρηση προς καταναλωτές (business to consumers –b2b): Οι περισσότερες εφαρμογές που υπάρχουν στο διαδίκτυο είναι προσανατολισμένες στον τελικό καταναλωτή. Οι επιχειρήσεις εκμεταλλευόμενες τα στρατηγικά οφέλη που προσφέρει το ηλεκτρονικό εμπόριο και ειδικότερα η παγκοσμιοποίηση της αγοράς μέσω της οικονομίας του Internet, δημιουργούν καινοτομικά προϊόντα και υπηρεσίες

τα οποία τα προωθούν στους καταναλωτές. Στην Ελλάδα, η αγορά B2C έχει μόλις αρχίσει να σχηματίζεται και θα απαιτηθεί αρκετός χρόνος για να φτάσει σε ένα ορισμένο επίπεδο ωριμότητας. Ακόμα και στις Η.Π.Α., όπου ο βαθμός διείσδυσης του Internet είναι υψηλός(πάνω από 50% το 2000), ένα μεγάλο ποσοστό του πληθυσμού δεν έχει πραγματοποιήσει ακόμα μια ηλεκτρονική συναλλαγή. Παρόλα αυτά, η προοπτική της αγοράς αυτής αναγνωρίζεται από πολλές εταιρείες συνεχίζουν να επενδύουν σε υποδομές ηλεκτρονικού εμπορίου. Οι εφαρμογές αυτής της κατηγορίας είναι:

- Υποστήριξη πελατών (πριν και μετά την πώληση) – Παροχή Προηγμένων Υπηρεσιών
- Ηλεκτρονική Δημοσιογραφία
- Ηλεκτρονικές Αγορές –Ηλεκτρονικά καταστήματα

Δημόσιοι φορείς προς πολίτες – καταναλωτές (government to consumers-g2c): Αφορά την παροχή υπηρεσιών. Μέσω του ηλεκτρονικού εμπορίου οι πολίτες – φορολογούμενοι συναλλάσσονται με τους δημόσιους φορείς για σκοπούς φορολογίας, για να προμηθευτούν τα απαραίτητα πιστοποιητικά ή βεβαιώσεις και για να εξασφαλίσουν τις απαραίτητες πληροφορίες που χρειάζονται. Η εύκολη πρόσβαση σε δημόσια έγγραφα και υπηρεσίες θα αλλάξει τον τρόπο που πολλοί πολίτες αντιμετωπίζουν τη δημόσια διοίκηση και την αποτελεσματικότητα λειτουργίας της. Όλο και περισσότερες κυβερνήσεις υιοθετούν τεχνολογίες Internet για να μειώσουν το κόστος λειτουργίας τους, να βελτιώσουν την παραγωγικότητά τους και να αυξήσουν την προσβασιμότητα των πολιτών σε πληροφορίες και υπηρεσίες on-line. Οι δημόσιοι οργανισμοί επίσης μπορούν με τη χρήση του ηλεκτρονικού εμπορίου να ενθαρρύνουν τη συμμετοχή των πολιτών στα κοινά.

Δημόσιοι φορείς προς επιχείρηση(government to business – g2b): Καλύπτει όλες τις συναλλαγές μεταξύ επιχειρήσεων και δημόσιων οργανισμών. Η αυτοματοποίηση των διαδικασιών διαγωνισμών, προμηθειών, εισπράξεων και πληρωμών του δημοσίου συμβάλλει σημαντικά στην εξοικονόμηση χρόνου, χρήματος καθώς και ανθρωποωρών, ενώ μπορεί να μειώσει σημαντικά τις γραφειοκρατικές διαδικασίες. Για παράδειγμα, στις Η.Π.Α. οι λεπτομέρειες για τις προμήθειες των προσεχών κυβερνήσεων, εκδίδονται στο Internet και οι ενδιαφερόμενες επιχειρήσεις εφαρμογές του ηλεκτρονικού εμπορίου στις οποίες πραγματοποιούνται

ανταποκρίνονται ηλεκτρονικά. Προς το παρόν, αυτή η κατηγορία είναι σε νηπιακό στάδιο, αλλά μπορεί να αναπτυχθεί ραγδαία όσο οι κυβερνήσεις χρησιμοποιούν τις δικές τους λειτουργίες για να προωθήσουν την αντίληψη τους για το ηλεκτρονικό εμπόριο. Οι συναλλαγές των επιχειρήσεων με τους δημόσιους φορείς αφορούν συνήθως τέσσερις περιπτώσεις:

- Φορολογία
- Εισαγωγές – Εξαγωγές μέσω τελωνείων
- Δημόσιες προμήθειες
- Προηγμένες ηλεκτρονικές υπηρεσίες

Καταναλωτές προς καταναλωτές (consumer to consumer – c2c): Αφορά, ουσιαστικά, τις συναλλαγές που πραγματοποιούνται μέσω των ηλεκτρονικών δημοπρασιών (e-auction). Οι ηλεκτρονικές δημοπρασίες είναι η χρησιμοποίηση του διαδικτύου για την παροχή και άντληση πληροφοριών και τη διενέργεια συναλλαγών σε πραγματικό χρόνο (real time). Ανταγωνιστικό τους πλεονέκτημα σε σύγκριση με τα e-shops είναι ότι μπορεί να βρείτε προϊόντα σε πολύ χαμηλές τιμές. Οι κυβερνοκαταναλωτές μπορούν να βρουν σπάνια και φθηνά μεταχειρισμένα αντικείμενα, ενώ με τη δύναμη της τεχνολογίας έχουν αναπτυχθεί μοντέλα δυναμικής τιμολόγησης, με τα οποία δίνεται η δυνατότητα αγοράς φθηνότερων καινούριων και επώνυμων προϊόντων.

2.2.1 Το κινητό ηλεκτρονικό εμπόριο (mobile-commerce)

Όπως έχει ήδη αναφερθεί, ως ηλεκτρονικό εμπόριο ορίζεται η διεκπεραίωση οικονομικών συναλλαγών με χρήση ηλεκτρονικών μέσων. Λόγω της ραγδαίας ανάπτυξης του εμπορίου στο Internet, το ηλεκτρονικό εμπόριο συχνά αναφέρεται σε αγορές από on-line καταστήματα του διαδικτύου, που είναι γνωστά ως δικτυακοί τόποι ηλεκτρονικού εμπορίου, εικονικά καταστήματα, ή καταστήματα του κυβερνοχώρου.

Παρόλα αυτά ο όρος ηλεκτρονικό εμπόριο δεν θα έπρεπε να συνδεθεί αποκλειστικά με την ύπαρξη μιας ιστοσελίδας όπου είναι δυνατή η

πραγματοποίηση αγορών. Περιλαμβάνει κάθε είδος ηλεκτρονικής επικοινωνίας μέσω της οποίας μπορεί ο πελάτης να αναζητήσει κάποιο προϊόν που τον ενδιαφέρει και να πραγματοποιήσει μια συναλλαγή.
Επιπλέον, λόγω της ταχύτατης ανάπτυξης της τεχνολογίας και των καλύτερων και αποδοτικότερων συστημάτων έγινε δυνατή η ασύρματη επικοινωνία πελατών που βρίσκονται σε κίνηση με τους δικτυακούς τόπους ακόμα και μέσω συσκευών που καταλαμβάνουν ελάχιστο χώρο και δεν αποτελούν βάρος για τον πελάτη όπως είναι οι συσκευές κινητής τηλεφωνίας.

Αυτή η έννοια της κίνησης περιλαμβάνεται στον ορισμό του όρου: κινητό ηλεκτρονικό εμπόριο (M-commerce) στο οποίο γίνεται χρήση ασύρματων συναλλαγών για την παροχή υπηρεσιών που στηρίζονται στην εκάστοτε θέση καθώς και στο συγκεκριμένο προφίλ χρηστών κινητών συσκευών υψηλής ταχύτητας και ασύρματών δικτύων ανά τον κόσμο. Η πραγματοποίηση συναλλαγών όπως κρατήσεις ξενοδοχείων, εισιτηρίων, αγοράς προϊόντων με χρήση κινητού τηλεφώνου ή άλλης συσκευής θα αποτελέσει τον κυρίαρχο τρόπο για την ολοκλήρωση όμοιων ενεργειών στην 3G εποχή.

2.3 Τα προϊόντα του Ηλεκτρονικού Εμπορίου

Οι εφαρμογές του ηλεκτρονικού εμπορίου παρέχουν τη δυνατότητα εύρεσης και ανάκτησης πληροφοριών, καθώς επίσης και συναλλαγής τεσσάρων τύπων προϊόντων: αγαθά, εργασίες, υπηρεσίες και άυλα αγαθά. Κάθε ένα από αυτά έχει ιδιαίτερα χαρακτηριστικά που καθιστούν χρήσιμη τη μελέτη τους, αφού η αντιμετώπισή τους σε μια εφαρμογή του ηλεκτρονικού εμπορίου πρέπει να γίνεται με προσαρμογή στα ιδιαίτερα χαρακτηριστικά τους.

Αγαθά : Πρόκειται για φυσικά αντικείμενα, που έχουν παραχθεί σύμφωνα με κάποιες προδιαγραφές που κατά κύριο λόγο τις ορίζει ο κατασκευαστής τους. Συνήθως συμπεριλαμβάνεται στην έννοιά τους και η

μεταφορά από τον τόπο παραγωγής στον τόπο πώλησης. Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν : χημικά, φαρμακευτικά προϊόντα, είδη ένδυσης, ανταλλακτικά κάθε είδους, οχήματα κλπ.

Εργασίες : Με τον όρο αυτό αναφερόμαστε σε εργασίες ανάπτυξης ή κατασκευής εφαρμογών και προϊόντων των οποίων όμως τις προδιαγραφές ορίζει ο πελάτης. Η δυνατότητα της άμεσης ηλεκτρονικής επικοινωνίας επιτρέπει όχι μόνο τη διαπραγμάτευση των προδιαγραφών αυτών αλλά και το διακανονισμό των πληρωμών , την παράδοση των παραγγελιών καθώς και άλλες δραστηριότητες που αποτελούν μέρος της συναλλαγής. Παραδείγματα αποτελούν τα προϊόντα λογισμικού, ηλεκτρικές/υδραυλικές εγκαταστάσεις, κατασκευές χώρων κλπ.

Υπηρεσίες : Η διάθεση και πώληση υπηρεσιών είναι συνήθως διαδικασίες αλληλοεξαρτώμενες. Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν δημόσιες, τουριστικές, χρηματοοικονομικές, υγείας, ψυχαγωγικές κλπ.

Άυλα αγαθά : Σε αυτήν την κατηγορία το κόστος των προϊόντων προσδιορίζεται από το περιεχόμενο και τη χρήση τους και όχι από το κόστος κατασκευής τους. Στα άυλα αγαθά υπάγονται και οι επιχειρηματικές διαδικασίες που αναφέρονται στην αναπαραγωγή – ανατύπωση ορισμένων προϊόντων. Σε αυτήν την κατηγορία τα προϊόντα είναι συνήθως αγαθά τα οποία είναι συνδεδεμένα με την έννοια της πνευματικής ιδιοκτησίας και των δικαιωμάτων χρήσης. Παραδείγματα αυτής της κατηγορίας περιλαμβάνουν τις κινηματογραφικές ταινίες, προϊόντα μουσικής, πακέτα λογισμικού, σχέδια διαφόρων ειδών, κλπ.

Πρέπει να σημειωθεί ότι οι παραπάνω κατηγορίες είναι πολύ γενικού περιεχομένου. Στην πράξη, ένα προϊόν μπορεί να προέλθει από τη συνένωση δύο ή περισσότερων από τις παραπάνω γενικές κατηγορίες: για παράδειγμα, ένα πακέτο λογισμικού είναι ένα προϊόν με στοιχεία άυλου αγαθού, ενώ αυτό μπορεί να συνοδεύεται από ένα συμβόλαιο συντήρησης κάτι που πρακτικά θεωρείται παροχή υπηρεσίας και ανήκει στην κατηγορία υπηρεσίες.

2.4 Το ζήτημα των πληρωμών

Με την εμφάνιση του ηλεκτρονικού εμπορίου οι ανάγκες για ευκολότερη ροή του χρήματος πολλαπλασιάστηκαν. Οι συμβατικές μέθοδοι πληρωμών και εισπράξεων δεν επαρκούν για το νέο τρόπο συναλλαγών, αγορών και πωλήσεων. Οι πραγματικές ηλεκτρονικές συναλλαγές πραγματοποιούνται με τη χρήση των: α) πιστωτικών καρτών, β) έξυπνων καρτών, γ) ηλεκτρονικού χρήματος, δ) ηλεκτρονικών επιταγών.

2.4.1 Πιστωτικές κάρτες (πλαστικό χρήμα) – credit cards

Προς το παρόν, οι πιστωτικές κάρτες, κυριαρχούν στους τρόπους πληρωμών μέσω Internet. Στατιστικές μελέτες αποδεικνύουν ότι το 90% των online συναλλαγών, που έγιναν μέσα στο 1996, πραγματοποιήθηκαν με χρήση πιστωτικών καρτών. Αν και υπάρχει μεγάλη ανησυχία όσον αφορά την ασφάλεια που παρέχουν οι πιστωτικές κάρτες σε on-line συναλλαγές, οι καταναλωτές δείχνουν να προτιμούν τη χρήση ενός τρόπου πληρωμών με τον οποίο είναι αρκετά εξοικειωμένοι.

Σε μια παραδοσιακή συναλλαγή με πιστωτική κάρτα, ο προμηθευτής καταγράφει τα στοιχεία της πιστωτικής κάρτας του πελάτη δημιουργώντας ένα έγγραφο συναλλαγής. Το εν λόγω έγγραφο υπογράφεται από τον αγοραστή και προωθείται, στη συνέχεια, στην τράπεζα για διεκπεραίωση. Στο τέλος η τράπεζα χρεοπιστώνει τους αντίστοιχους λογαριασμούς ενημερώνοντας τα εμπλεκόμενα μέρη για την συναλλαγή που έγινε.

Σε ένα μηχανισμό ηλεκτρονικής πληρωμής με χρήση πιστωτικής κάρτας, περιλαμβάνονται επιπλέον μηχανισμοί ασφαλείας (π.χ. έλεγχος ταυτότητας πελάτη και εμπόρου). Το γεγονός αυτό έχει οδηγήσει στην ύπαρξη μιας γκάμας συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες. Δύο από τα χαρακτηριστικά που προσδιορίζουν και διαφοροποιούν τα συστήματα αυτά είναι το επίπεδο της ασφάλειας των συναλλαγών και το

λογισμικό που απαιτείται από όλα τα εμπλεκόμενα μέρη (αγοραστής, προμηθευτής, τράπεζα).

Κατά τη διάρκεια μιας on-line συναλλαγής, τα στοιχεία της πιστωτικής κάρτας ενός αγοραστή μπορούν να μεταφερθούν με δύο τρόπους. Ο πρώτος θεωρείται μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο (ή την τράπεζα) σε μη κρυπτογραφημένη μορφή. Η μέθοδος αυτή κρίνεται ως μη ασφαλής γιατί κατά την μεταβίβαση των στοιχείων μπορεί να παρεισφρήσει κάποιος εισβολέας και να τροποποιήσει τα στοιχεία της συναλλαγής ή ακόμη και να τα υποκλέψει. Ο δεύτερος τρόπος θεωρείται πιο ασφαλής και προβλέπει την κρυπτογράφηση όλων των πληροφοριών που σχετίζονται με την πληρωμή πριν την αποστολή τους στον έμπορο (ή στην τράπεζα) μέσω του Internet.

Διεθνώς οι πιστωτικές κάρτες έχουν κυριαρχήσει στην αγορά και ήδη έχουν προχωρήσει σε νέες εξελιγμένες μορφές όπως οι κάρτες co-branded, affinity, smart cards, prepaid cards, με αποτέλεσμα στις αναπτυγμένες χώρες να αντιστοιχεί σε κάθε άτομο μία έως τρεις κάρτες. Στην Ελλάδα απέχουμε ακόμη από τα διεθνή πρότυπα. Ο αριθμός όμως των πιστωτικών καρτών παρουσιάζει μια αρκετά σημαντική άνοδο τελευταία, η οποία θα ενταθεί τα επόμενα χρόνια, κυρίως γιατί η είσοδος στην αγορά νέων προϊόντων ανεβάζει το βαθμό συναισθητοποίησης του κοινού ως προς το ότι υπάρχει ένας εναλλακτικός τρόπος συναλλαγών πέρα από τα μετρητά, που για πολύ κόσμο είναι η φυσική λύση.

Οι κάρτες μπορούν να χωριστούν σε τρεις κατηγορίες:

1. Στην κατηγορία των καρτών που *προπληρώνεται* το ποσό για το οποίο πρόκειται να γίνουν συναλλαγές.
2. Στην κατηγορία των καρτών που χρησιμοποιούνται για *αναλήψεις ή συναλλαγές με άμεση χρέωση* του τραπεζικού λογαριασμού του κατόχου.
3. Στην κατηγορία των καρτών που η *πληρωμή γίνεται μετά* από τις συναλλαγές.

2.4.2 Ηλεκτρονικό χρήμα (electronic money ή e-cash)

Η έννοια του e-cash χρησιμοποιείται αρκετά συχνά τελευταία και αποτελεί σύντμηση του αγγλικού όρου Electronic Cash. Ο όρος αυτός συναντάται και με άλλα ονόματα, όπως Net cash, Virtual Cash, Digital Cash κλπ. Όλα είναι στην ουσία παραλλαγές του ίδιου θέματος, αλλά η κεντρική ιδέα έχει ως εξής: πρόκειται για ηλεκτρονικές χρηματικές μονάδες που παρέχουν σε έναν χρήστη κάποια ηλεκτρονική τράπεζα, με αντίτιμο βέβαια «πραγματικά χρήματα». Με απλά λόγια, ο χρήστης καταβάλλει κάποιο χρηματικό ποσό και ο ηλεκτρονικός του λογαριασμός τροφοδοτείται με το αντίστοιχο «ηλεκτρονικό». Στη συνέχεις, αυτός έχει τη δυνατότητα να επισκεφθεί ένα οποιοδήποτε εμπορικό κέντρο και να πραγματοποιήσει τις αγορές του. Στη διάρκεια των δοσοληψιών το ηλεκτρονικό του απόθεμα ενημερώνεται διαρκώς, καθώς τα αποτελέσματα των εμπορικών του συναλλαγών καταχωρούνται σε μία ηλεκτρονική τράπεζα. Συνεπώς, τα «ψηφιακά» χρήματα μειώνονται, ενώ αντίστοιχα αυξάνονται εκείνα του πωλητή μέσω ενός αυτόματου μηχανισμού συναλλαγών.

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξόφλησης μικροποσών μέσω του Internet. Ένας τέτοιος μηχανισμός μπορεί να αποτελέσει το επόμενο βήμα στις εφαρμογές ηλεκτρονικών πληρωμών. Σε ένα σύστημα ψηφιακού χρήματος, το νόμισμα δεν είναι τίποτα άλλο παρά μια σειρά από ψηφία. Όπως στον πραγματικό κόσμο, έτσι και στον αντίστοιχο ηλεκτρονικό, οι μέθοδοι πληρωμών υπάγονται σε δύο ευρείες κατηγορίες: χρέωση και πίστωση. Στην πρώτη περίπτωση, συγκεντρώνουμε πρώτα τα χρήματα και έπειτα πληρώνουμε κάποιον λογαριασμό. Στη δεύτερη, πραγματοποιούμε κάποιες αγορές και καταβάλλουμε το ανάλογο χρηματικό ποσό αργότερα. Όπως οι έννοιες, λοιπόν, cash και credit συνυπάρχουν στον σημερινό πραγματικό επιχειρησιακό κόσμο, το ίδιο συμβαίνει και στον αντίστοιχο ψηφιακό. Με τον όρο electronic ή digital cash εννοείται το ηλεκτρονικό ισοδύναμο ενός π.χ. χαρτονομίσματος, με ονομασία έναν μοναδικό αναγνωριστικό αριθμό και το ποσό που αναπαριστά.

Ο όρος digital credit υποδηλώνει το ίδιο πιστωτικό σύστημα που ισχύει και στις κανονικές συναλλαγές. Η μόνη διαφορά έγκειται στην ενσωμάτωση ψηφιακών χρονομετρών και υπογραφών για λόγους καταχώρησης των συναλλαγών. Κατά την αγορά, δημιουργείται μία περιγραφή της συναλλαγής με τα ονόματα του λήπτη και αυτού που καταβάλλει το χρηματικό ποσό, την ημερομηνία και ώρα της συναλλαγής και το ποσό της

πληρωμής. Ο αγοραστής υπογράφει με το ιδιωτικό του κλειδί (κωδικό) το «έγγραφο» της δοσοληψίας και ο πωλητής στη συνέχεια, χρησιμοποιώντας ένα δημόσιο κλειδί, επιβεβαιώνει την πράξη της συναλλαγής και ενημερώνει το σύστημα εκκαθαρίσεων κάποιας ηλεκτρονικής τράπεζας.

Ένας χρήστης μπορεί να κάνει ανάληψη ψηφιακού χρήματος από μια τράπεζα μεταφέροντας το ποσό αυτό στον ηλεκτρονικό του υπολογιστή. Το ψηφιακό χρήμα που παραχωρείται από την τράπεζα σημαδεύεται κατάλληλα για λόγους εγκυρότητας και ασφαλείας. Σε περίπτωση αγοράς προϊόντων μέσω του Internet, ο αγοραστής αποστέλλει στον προμηθευτή το αντίτιμο σε ψηφιακό χρήμα. Ο τελευταίος με τη σειρά του, προωθεί στην τράπεζα τη ψηφιακή-ροή έλαβε προκειμένου να διερευνηθεί κατά πόσο η ροή αυτή αποτελεί έγκυρη χρηματο-ροή ή όχι.

Για να διασφαλιστεί ότι κάθε χρηματο-ροή (token) χρησιμοποιείται μόνο μια φορά, η τράπεζα καταγράφει τον σειριακό αριθμό κάθε token που ξοδεύεται. Αν ο σειριακός αριθμός του token υπάρχει ήδη στην βάση δεδομένων, τότε η τράπεζα έχει εντοπίσει κάποιον που προσπάθησε να χρησιμοποιήσει περισσότερες από μια φορές το token και θα πληροφορήσει τον έμπορο ότι αυτή η χρηματική μονάδα είναι άχρηστη.

2.4.3 Έξυπνες κάρτες (smart cards)

Αρκετά από τα σημερινά συστήματα βασίζονται στην τεχνολογία των έξυπνων καρτών. Οι κάρτες αυτές κατά μια έννοια είναι μια επέκταση των καρτών προ-πληρωμής (prepayment cards) αφού μπορούν να αποθηκεύσουν αξίες (χρήματα) για μελλοντική χρήση. Μία μορφή, η πιο γνωστή ίσως, ηλεκτρονικής κάρτας, η οποία χρησιμοποιείται ευρέως, είναι η τηλεφωνική. Αν και η χρήση της ενθαρρύνεται από την ανωνυμία που προσφέρει, δεν είναι δυνατή η συμπλήρωση και επαναχρησιμοποίησή της. Κάρτες οι οποίες επίσης θα μπορούσαν να συμπεριληφθούν σε αυτή την κατηγορία, είναι οι κάρτες υγείας, οι κάρτες οι οποίες χρησιμοποιούνται στην κινητή τηλεφωνία, οι κάρτες για έλεγχο προσβάσεως και αυθεντικότητας κτλ.

Μία τυπική έξυπνη κάρτα η οποία προορίζεται για χρήση στο Internet, διαθέτει ένα ενσωματωμένο chip μνήμης για αποθήκευση της ψηφιακής υπογραφής του χρήστη, αλλά και το ιδιωτικό του κλειδί. Μετά από την διαδικασία του login σε ένα δίκτυο το οποίο βασίζεται στο Internet, ζητείται από το χρήστη να εισάγει την κάρτα του σε μία συσκευή αναγνώσεως καρτών (card reader) και να πληκτρολογήσει τον προσωπικό αριθμό ταυτοποιήσεώς του (PIN). Μετά από αυτή τη διαδικασία, δίνεται πρόσβαση σε εξειδικευμένες βάσεις δεδομένων και υπηρεσίες όπως είναι το ηλεκτρονικό εμπόριο.

Είναι λοιπόν αυτονόητο, ότι τα συστήματα ασφαλείας του internet, που βασίζονται στην τεχνολογία των έξυπνων καρτών, προσφέρουν αρκετά πλεονεκτήματα αφού οι κάρτες είναι φορητές και προσφέρεται μεγαλύτερη ασφάλεια (πρέπει κανείς και να κατέχει την κάρτα, αλλά και να γνωρίζει το PIN). Αρκετές εταιρείες – και ιδιαίτερα οι τράπεζες –πειραματίζονται στην κατεύθυνση αυτή, για χρησιμοποίηση τέτοιων συστημάτων.

Οι έξυπνες κάρτες έχουν δύο κύρια προτερήματα απέναντι στις μαγνητικές κάρτες: α) μπορούν να αποθηκεύσουν 10-100 φορές περισσότερες πληροφορίες και β) κρατούν αυτές τις πληροφορίες πιο ανθεκτικές σε επιθέσεις και πιο ασφαλισμένες από τις μαγνητικές κάρτες. Επιπροσθέτως, σε συνδυασμό με κάποιες συσκευές, οι έξυπνες κάρτες μπορούν να εκτελούν σύνθετες πράξεις αποφάσεων περιλαμβάνοντας ρουτίνες που θα αποδεικνύουν την εγκυρότητα της κάρτας στο τερματικό και αντιστρόφως (αμοιβαία αυθεντικότητα που μπορεί να μειώσει τις διαρροές και τις απάτες). Τα βασικά όμως πλεονεκτήματα της έξυπνης κάρτας είναι ότι:

1. αυξάνει την ασφάλεια των δεδομένων
2. προσδίδει ελαστικότητα στις εφαρμογές και
3. παρέχει δυνατότητες εκτελέσεως ελέγχου εγκυρότητας offline.

Στην πράξη αυτά τα χαρακτηριστικά αλληλοσυνδέονται, αλλά το πιο σημαντικό από αυτά είναι ίσως το μεγάλο επίπεδο της ασφαλείας, που εναλλακτικές τεχνολογίες όπως οι μαγνητικές κάρτες και οι κάρτες μνήμης δεν μπορούν να εξασφαλίσουν. Αυτό κάνει τις έξυπνες κάρτες βιώσιμες σε εφαρμογές που διαχειρίζονται χρήματα, προσωπικά στοιχεία κτλ.

2.4.4 Ηλεκτρονικές επιταγές

Στις αρχές της δεκαετίας του 1970, οι τράπεζες άρχισαν να μελετούν διάφορους τρόπους με τους οποίους θα μείωναν το κόστος επεξεργασίας των επιταγών. Το αποτέλεσμα της έρευνας αυτής ήταν ο ηλεκτρονικός χειρισμός των πληρωμών. Σε έναν λογαριασμό όψεως μιας τράπεζας, ο δικαιούχος-εργοδότης στέλνει μια κατάσταση πληρωμών. Εν συνεχεία, η τράπεζα μεταφέρει τα χρήματα στους λογαριασμούς των τραπεζών των εργαζομένων, μέσω αυτοματοποιημένων συστημάτων συγκέντρωσης και διευθέτησης τραπεζικών λογαριασμών. Οι καταναλωτές χρησιμοποιούν απευθείας πληρωμή για να αντιμετωπίσουν δισεκατομμύρια συναλλαγές αξίας $13 τρις στα ιδιωτικά τους δίκτυα. Το κόστος για τις τράπεζες ήταν το μισό από αυτό που θα δαπανούσαν εάν χρησιμοποιείτο το παραδοσιακό-χειρονακτικό σύστημα επιταγών.

Μία έντυπη επιταγή είναι ουσιαστικά μια εντολή μεταφοράς κεφαλαίων από ένα λογαριασμό σε ένα άλλο. Η εντολή αυτή αποστέλλεται αρχικά στον αποδέκτη κεφαλαίων, ο οποίος με τη σειρά του παρουσιάζει την επιταγή στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό. Σήμερα, μία έντυπη επιταγή μπορεί να αντικατασταθεί από ένα ψηφιακά υπογεγραμμένο μήνυμα (electronic check) του Internet. Μία ηλεκτρονική επιταγή έχει όλα τα χαρακτηριστικά που διαθέτει μια έντυπη επιταγή και χρησιμοποιείται σαν ένα μήνυμα προς την τράπεζα του αποστολές για την μεταφορά κεφαλαίων από έναν λογαριασμό σε έναν άλλο.

Από άποψη ασφαλείας, η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη επιταγή. Και αυτό γιατί ο αποστολέας μπορεί να προστατεύσει τον εαυτό του από μια απάτη. Αυτό γίνεται με την κωδικοποίηση του αριθμού του λογαριασμού του με το δημόσιο κλειδί της τράπεζας, χωρίς έτσι να αποκαλύπτει τον αριθμό του λογαριασμού του στον έμπορο.

2.5 Ηλεκτρονικές τράπεζες

Η ραγδαία ανάπτυξη του Internet και του ηλεκτρονικού εμπορίου ήταν φυσικό να επεκταθεί και στις τράπεζες. Στη Ευρώπη, μεταξύ 2.400 περίπου τραπεζών, το 70% προσφέρει online τραπεζικές υπηρεσίες έναντι του 15% των τραπεζών που λειτουργούν στις Η.Π.Α. Στην Ελλάδα, οι ηλεκτρονικές τραπεζικές υπηρεσίες βρίσκονται σε πρώιμο στάδιο. Ωστόσο, οι προοπτικές είναι καλές, παρόλο το ότι μόνο το 3,6 του ελληνικού πληθυσμού κάνει χρήση του Internet (έρευνα OTEnet). Είναι αξιοσημείωτο ότι στο 10% περίπου των ελληνικών επιχειρήσεων που διαθέτουν δικές τους ιστοσελίδες, το 4,5% από αυτές αναφερόταν σε θέσεις (site) που προσέφεραν τραπεζικές και χρηματοοικονομικές υπηρεσίες.

2.5.1 Συναλλαγές μέσω ηλεκτρονικών τραπεζικών μεθόδων

1.***Η Διαδικτυακή Τραπεζική***: Διαδικτυακή Τραπεζική (Internet banking) είναι η χρησιμοποίηση του διαδικτύου για την παροχή και άντληση χρηματοπιστωτικών και χρηματοοικονομικών πληροφοριών και η διενέργεια τραπεζικών συναλλαγών σε πραγματικό χρόνο (real time).Οι τράπεζες δημιουργούν τη δική τους ιστοσελίδα (web site) στο Internet με στοιχεία που παρουσιάζουν την εικόνα τους στο κοινό και παρέχουν πληροφορίες για τα προσφερόμενα προϊόντα και τον τρόπο διενέργειας συναλλαγών όπως παρακολούθηση υπολοίπου λογαριασμού, μεταφορές κεφαλαίων από λογαριασμό σε λογαριασμό, εντολές εξόφλησης τιμολογίων ΔΕΚΟ και άλλων εταιρειών, εντολές πληρωμών με χρήση πιστωτικών καρτών κλπ. Πληροφορίες μπορεί να παρέχονται επίσης και για προϊόντα θυγατρικών εταιρειών και να πραγματοποιούνται συναλλαγές όπως τραπεζοασφάλειες, καταθέσεις, χορηγήσεις, αμοιβαία κεφάλαια κλπ. Αναμφισβήτητα πλεονεκτήματα του Internet banking είναι ότι ο πελάτης

εξοικονομεί χρόνο αφού δεν είναι αναγκασμένος να μεταβεί στην τράπεζά του και επί πλέον το κόστος των συναλλαγών είναι μικρότερο. Σήμερα, εκτιμάται ότι ένα 10% των πελατών πραγματοποιεί τραπεζικές συναλλαγές εξ αποστάσεως σε παγκόσμιο επίπεδο αλλά το ποσοστό αυτό αυξάνεται εντυπωσιακά από χρόνο σε χρόνο.

2.*Η Τραπεζική Ανοικτής Γραμμής*: Με τον όρο τραπεζικής ανοικτής γραμμής (online banking) νοείται η διενέργεια τραπεζικών πράξεων σε απευθείας σύνδεση με την επιχείρηση ή τον πελάτη μέσω του Internet. Διακρίνουμε δύο μοντέλα: α) των Η.Π.Α., που περιορίζεται σε ορισμένες μόνο τραπεζικές υπηρεσίες όπως καταθέσεις και αναλήψεις χωρίς μετρητά. Το κύριο πλεονέκτημα που προσφέρουν οι τράπεζες on-line των Η.Π.Α. είναι το υψηλό επιτόκιο στις καταθέσεις και η μικρή προμήθεια για αναλήψεις ποσών με επιταγή. Μειονέκτημα αποτελεί ότι δεν διαθέτουν συνήθως δίκτυο ATMs και οι πελάτες μπορούν να πληρώσουν έξοδα για κάθε επιταγή. β) της Ε.Ε. on-line τράπεζες οι οποίες μπορούν να διαθέτουν δίκτυο υποκαταστημάτων και ATMs ενώ προσφέρουν εκδόσεις για καταθετικά και δανειοδοτικά προϊόντα και άλλες υπηρεσίες όπως διενέργεια χρηματιστηριακών πράξεων και επενδύσεις σε τίτλους. Μερικές από αυτές παρέχουν ισχυρά κίνητρα για την προσέλκυση πελατείας όπως υψηλό επιτόκιο σε λογαριασμούς ταμιευτηρίου ή προθεσμίας ή τόκο σε λογαριασμούς όψεως, αν το επιτρέπει η ισχύουσα νομοθεσία, μη επιβάρυνση με μηνιαία χρέωση λόγω της κίνησης του λογαριασμού ή ειδικές προσφορές για τους πελάτες τους.

3. ***Η Τηλεφωνική Τραπεζική***: Η Τηλεφωνική Τραπεζική (telephone banking) είναι το πρώτο είδος διενέργειας συναλλαγών χωρίς μετάβαση στο κατάστημα που εμφανίστηκε διαχρονικά. Η σύνδεση της επιχείρησης με τον Η/Υ της τράπεζας επιτυγχάνεται μέσω τηλεφωνικής γραμμής και συσκευής διαμορφωτή / αποδιομορφωτή (modem) και της χρήσης κωδικού αριθμού. Η Alpha Bank ήταν η πρώτη τράπεζα στην Ελλάδα που εφάρμοσε αυτή την τεχνική, ακολούθησε η Citibank και κατόπιν άλλες τράπεζες. Οι υπηρεσίες που προσφέρονται είναι το υπόλοιπο λογαριασμού, μεταφορά κεφαλαίων από λογαριασμό σε λογαριασμό, εξόφληση υποχρεώσεων με χρέωση τραπεζικού λογαριασμού ενώ σε πιο εξελιγμένη μορφή μπορεί να

πραγματοποιηθούν και άλλες συναλλαγές λιανικής επενδυτικής μορφής. Πολλές τράπεζες χρησιμοποιούν ή τηλεφωνικά κέντρα ή τονικά ή φωνητικά τηλεφωνικά συστήματα. Αν και τα αυτόματα συστήματα αναγνώρισης φωνής λειτουργούν με μικρότερο κόστος από τα κέντρα με χειριστές-υπαλλήλους, εν τούτοις οι πελάτες φαίνεται να προτιμούν τα δεύτερα. Συναφής είναι και η τραπεζική μέσω κινητής τηλεφωνίας (GSM banking ή mobile banking).

4. ***Η Τηλεματική Τραπεζική***: Πιο γνωστή σαν Home Banking είναι η δεύτερη μορφή τραπεζικής εξ αποστάσεως που εμφανίστηκε ιστορικά. Η σύνδεση του πελάτη με τον Η/Υ της τράπεζας πραγματοποιείται με προσωπικό υπολογιστή και μισθωμένες τηλεπικοινωνιακές γραμμές και η πρόσβαση εξασφαλίζεται με έναν προσωπικό αριθμό ταυτοποίησης. Πέραν των υπηρεσιών της τηλεφωνικής τραπεζικής προσφέρονται και οι εξής πληροφορίες: άντληση πληροφοριών για τις τιμές συναλλάγματος, τα επιτόκια και τους λοιπούς όρους δανεισμού, χρηματιστηριακές τιμές, παρουσίαση των προσφερόμενων προϊόντων και υπηρεσιών της τράπεζας και διενέργεια συναλλαγών με χρέωση τραπεζικού λογαριασμού ή πιστωτικής κάρτας.

2.6 Ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange-EDI)

Ο συνδυασμός του EDI με την τεχνολογία του Bar Coding συντελεί στην αποτελεσματικότερη διακίνηση πληροφοριών σχετικά με τα προϊόντα, παρέχοντας τη δυνατότητα αυτοματοποίηση μη παραγωγικών διαδικασιών. Η τεχνολογία εξαλείφει τη χρήση του χαρτιού από τις επιχειρηματικές διαδικασίες που συντελούνται μέχρις ότου το προϊόν φτάσει στον τελικό το προορισμό. Ιδιαίτερη έμφαση δίνεται στη διαδικασία παραγγελιοδοσίας/παραγγελιοληψίας λόγω της ιδιαίτερης σημασίας της στο εμπορικό κύκλωμα.

Το EDI βασίζεται στη συμφωνία δύο ή περισσότερων εμπορικών εταίρων για τα έντυπα και τα δεδομένα που επιθυμούν να ανταλλάσσουν

ηλεκτρονικά μεταξύ τους. Για παράδειγμα, στην εταιρεία Α, ο χρήστης μέσω μιας εφαρμογής (π.χ. Word, Excel) εκτελεί μια εργασία (π.χ. έκδοση τιμολογίου πώλησης). Αυτή την εργασία ο χρήστης έχει τη δυνατότητα να την εκτυπώσει (παραστατικό) ή να μην αποθηκεύει σ' ένα αρχείο στον ηλεκτρονικό υπολογιστή της εταιρείας. Στη συνέχεια, χάρη στον «EDI μεταφραστή», η συγκεκριμένη εργασία μετασχηματίζεται αυτόματα σ' ένα κατάλληλο για ηλεκτρονική μετάδοση αρχείο και τοποθετείται σ' έναν ηλεκτρονικό φάκελο που περιέχει αναγνωριστικά σημεία για τον αποδέκτη και την ηλεκτρονική ταυτότητά του. Ο ηλεκτρονικός φάκελος μεταδίδεται σε ένα δίκτυο προστιθέμενης αξίας (value added network-VAN). Και τοποθετείται στο «γραμματοκιβώτιο» του αποδέκτη. Στην εταιρεία Β, ο χρήστης μπαίνει στο VAN με το μόντεμ του και παίρνει τα μηνύματά του από το «γραμματοκιβώτιό» του. Στη συνέχεια, πάλι χάρη στον «EDI μεταφραστή», το περιεχόμενο του ηλεκτρονικού φακέλου μεταφράζεται αυτόματα σε μορφή αναγνωρίσιμη από την εφαρμογή του χρήστη Β.

Το κόστος υιοθέτησης αλλά και χρησιμοποίησης ενός συστήματος EDI είναι αρκετά σημαντικό, όμως τα πλεονεκτήματα που εμφανίζονται είναι πάρα πολλά και ποικίλα. Ακόμη, σύμφωνα με τη διεθνή εμπειρία, το όφελος αυξάνεται εντυπωσιακά και υπερβαίνει κατά πολύ το κόστος με την επίτευξη της κρίσιμης μάζας χρηστών. Ως κρίσιμη μάζα χρηστών καλείται εκείνος ο αριθμός των συναλλασσόμενων μέσω EDI με τον οποίο επιτυγχάνεται η απόσβεση της αρχικής επένδυσης χάρη στο μεγάλο όγκο των συναλλαγών. Έτσι οι εφαρμογές EDI δεν αναπτύσσονται μεμονωμένα από τις διάφορες επιχειρήσεις αλλά στο πλαίσιο μιας ομάδας χρηστών, ώστε να επιτυγχάνεται η εκ των προτέρων ύπαρξη της κρίσιμης μάζας. Όταν η τεχνική αυτή εξαπλώνεται και χρησιμοποιείται όπως το τηλέφωνο ή το φαξ, τότε υπάρχει μεγιστοποίηση της ωφέλειας από τη χρήση του.

Σύμφωνα με τη διεθνή εμπειρία, τα αποτελέσματα από τη χρήση του EDI είναι τα εξής:

- Μείωση σφαλμάτων πληκτρολόγησης κατά 97%
- Καλύτερη εξυπηρέτηση πελατών κατά 76%
- Μείωση επαναπληκτρολογήσεων κειμένων κατά 73%
- Καλύτερη διαχείριση αποθεμάτων κατά 26%
- Ταχύτερη διαδικασία παραγωγής κατά 26%

- Μείωση αποθηκευτικού χώρου κατά 18%
- Μείωση εξόδων δημιουργίας και διαχείρισης εγγράφων κατά 16%

2.6.1 Χρηματοοικονομικό EDI (Financial EDI)

Το χρηματοοικονομικό EDI αποτελεί μια εξειδικευμένη περίπτωση του EDI, όπου ένας από τους δύο συναλλασσόμενους είναι Τράπεζα ή άλλο χρηματοπιστωτικό ίδρυμα. Η ηλεκτρονική επικοινωνία μεταξύ των επιχειρήσεων και των τραπεζών για την διεκπεραίωση πληρωμών αποτελεί μια από τις πλέον γοργά αναπτυσσόμενες τεχνολογίες ηλεκτρονικού εμπορίου.

Εφαρμογές αυτής της τεχνολογίας έχουν ήδη αναπτυχθεί για διεξαγωγή τραπεζικών συναλλαγών από το σπίτι καθώς και για την πληρωμή εμπορικών συναλλαγών (όπου πελάτης και προμηθευτής δίνουν αντίστοιχες οδηγίες στις τράπεζες με τις οποίες συναλλάσσονται για τη διευθέτηση λογαριασμών).

2.7 Πλεονεκτήματα του ηλεκτρονικού εμπορίου για τους προμηθευτές

Είναι δυνατό να απαριθμήσει κανείς έναν αριθμό δραστηριοτήτων που προσθέτουν αξία σε μια επιχείρηση μέσω του ηλεκτρονικού εμπορίου, όπως: μάρκετινγκ, πρόσβαση σε νέες αγορές, περιορισμός του άμεσου κόστους, ταχύτερη παράδοση προϊόντων, καλύτερη εξυπηρέτηση των πελατών, βελτίωση της δημόσιας εικόνας της επιχείρησης, εκμάθηση της νέας τεχνολογίας, νέες σχέσεις με τους πελάτες, νέες δυνατότητες προϊόντων και νέα λειτουργικά μοντέλα. Όλα αυτά τα πλεονεκτήματα μπορούν να χωριστούν σε τρεις μεγάλες κατηγορίες: βελτίωση, μετασχηματισμός και αλλαγή προτύπων. Στη συνέχεια θα εξετάσουμε τις τρεις αυτές κατηγορίες πλεονεκτημάτων.

2.7.1 Βελτίωση της λειτουργίας των επιχειρήσεων

Το ηλεκτρονικό εμπόριο επιτρέπει τη βελτίωση πολλών πλευρών της λειτουργίας μιας επιχείρησης, σε τομείς όπως: μάρκετινγκ, πρόσβαση σε νέες αγορές, περιορισμός του άμεσου κόστους, ταχύτερη παράδοση προϊόντων, καλύτερη εξυπηρέτηση των πελατών, βελτίωση της δημόσιας εικόνας της επιχείρησης :

Μάρκετινγκ:

Το ηλεκτρονικό εμπόριο μπορεί να βελτιώσει σε μεγάλο βαθμό την προώθηση των προϊόντων μέσα από την άμεση, πλούσια σε πληροφορίες και αμφίδρομη επικοινωνία με τους πελάτες.

Τα ψηφιακά δίκτυα επιτρέπουν στους πωλητές να προσφέρουν αναλυτικές πληροφορίες για τα προϊόντα τους μέσα από τη δημοσίευση οδηγών και καταλόγων. Το πλεονέκτημα της ηλεκτρονικής δημοσίευσης σε σύγκριση με τα παραδοσιακά μέσα διαφήμισης είναι ότι το περιεχόμενο μπορεί να είναι εξατομικευμένο και να καθορίζεται με βάση τους χειρισμούς του ίδιου του πελάτη (αλληλενεργό περιεχόμενο).

Επίσης οι πληροφορίες μπορούν να αλλάζουν συχνά και είναι διαθέσιμες όλο το 24-ωρο σε όλο τον πλανήτη, με την προϋπόθεση ότι ο πελάτης διαθέτει την κατάλληλη πρόσβαση στο δίκτυο.

Τα χαρακτηριστικά αυτά είναι πολύ σημαντικά σε ένα κόσμο όπου οι υποψήφιοι πελάτες βομβαρδίζονται με διαφημιστικά μηνύματα, τα περισσότερα από τα οποία δεν τους ενδιαφέρουν και απλά τους ενοχλούν.

Πρόσβαση σε νέες αγορές:

Χάρη στην παγκόσμια διάδοση των ψηφιακών δικτύων και τον αμφίδρομο χαρακτήρα της επικοινωνίας, το ηλεκτρονικό εμπόριο αντιπροσωπεύει ένα νέο κανάλι για την πώληση υπαρχόντων προϊόντων.
Αρκετοί υποστηρίζουν ότι το ηλεκτρονικό εμπόριο είναι κατάλληλο για δυο μορφές προϊόντων, υλικά προϊόντα (π.χ. αλεύρι ή βιβλία) και προϊόντα που μπορούν να παραδοθούν μέσω του δικτύου (π.χ. πληροφορίες ή λογισμικό).

Η άποψη αυτή είναι πολύ περιοριστική. Ένας πολύ μεγάλος αριθμός επιχειρήσεων δραστηριοποιείται στον τομέα των υπηρεσιών, και οι δυνατότητες χρήσης του ηλεκτρονικού εμπορίου από τις επιχειρήσεις αυτές είναι προφανείς. Για παράδειγμα, οι αεροπορικές εταιρίες δεν πωλούν υλικά αγαθά, ούτε αυτό που προσφέρουν μπορεί να παραδοθεί μέσα από το δίκτυο. Παρέχουν μια υπηρεσία. Μπορούν όμως να χρησιμοποιήσουν το ψηφιακό δίκτυο για την κράτηση θέσεων, την πώληση εισιτηρίων, και φυσικά για το μάρκετινγκ των υπηρεσιών τους.

Περιορισμός του άμεσου κόστους:

Η χρήση ενός ψηφιακού δικτύου για τη δημοσίευση και τη μετάδοση πληροφοριών σε ηλεκτρονική μορφή μπορεί να μειώσει το κόστος σε σύγκριση με την επικοινωνία και τη δημοσίευση σε έντυπη μορφή. Ακόμη, η χρήση ενός δημόσιου δικτύου, όπως το Internet, έχει πολύ μικρότερο κόστος από τη δημιουργία και τη συντήρηση ενός ιδιωτικού δικτύου.
Μερικοί τομείς όπου η μείωση του κόστους είναι άμεσα ορατή, είναι η ψηφιακή μετάδοση εγγράφων, η επικοινωνία μεταξύ τμημάτων της επιχείρησης και μεταξύ επιχείρησης και προμηθευτών, καθώς και η υποστήριξη των πελατών σε 24-ωρη βάση χωρίς την ανάγκη λειτουργίας ενός τηλεφωνικού κέντρου. Ένα πολύ καλό παράδειγμα πρόσθετης μείωσης του κόστους είναι η παράδοση προϊόντων σε ηλεκτρονική μορφή, όπως για παράδειγμα μια σύνθεση ενός γραφίστα ή μια έκθεση ενός συμβούλου επιχειρήσεων.

Ταχύτερη παράδοση προϊόντων:

Χάρη στην αμεσότητα της πρόσβασης στις νέες πληροφορίες, το ηλεκτρονικό εμπόριο επιτρέπει τη συντόμευση του χρόνου που απαιτείται για την παραγωγή και την παράδοση πληροφοριών και υπηρεσιών.

Αυτό είναι ιδιαίτερα σημαντικό σε κλάδους που εξαρτώνται από την έγκαιρη παράδοση κρίσιμων πληροφοριών, όπως τα μέσα ενημέρωσης και η χρηματιστηριακή αγορά. Ειδικά στα μέσα ενημέρωσης, το ψηφιακό δίκτυο είναι ένα χαρακτηριστικό παράδειγμα μαζικής παραγωγής εξατομικευμένων προϊόντων: οι ηλεκτρονικές εφημερίδες μπορούν να διαμορφώνουν το περιεχόμενό τους ανάλογα με τις προτιμήσεις που υποβάλλει κάθε

συνδρομητής, και να του στέλνουν μόνο τις πληροφορίες που τον ενδιαφέρουν, με αμεσότητα και ακρίβεια.

Καλύτερη εξυπηρέτηση των πελατών:

Το ηλεκτρονικό εμπόριο μπορεί να βελτιώσει σε πολύ μεγάλο βαθμό την εξυπηρέτηση των πελατών, αυτοματοποιώντας τη διαδικασία απάντησης στις πιο συχνές και συνηθισμένες ερωτήσεις, και επιτρέποντας έτσι στο ανθρώπινο δυναμικό της επιχείρησης να ασχοληθεί με τις περιπτώσεις που πραγματικά απαιτούν ιδιαίτερη προσοχή.

Η διαθεσιμότητα της υποστήριξης των πελατών σε 24-ωρη βάση και όλες τις ημέρες το χρόνου, είναι ένα πολύ ισχυρό ανταγωνιστικό εργαλείο. Παράλληλα, ένα μεγάλο μέρος της δραστηριότητας για την υποστήριξη των πελατών περνά στην ευθύνη των ίδιων των πελατών, που έχουν τη δυνατότητα να μελετήσουν τις ηλεκτρονικά δημοσιευμένες οδηγίες και προδιαγραφές των προϊόντων, ή να πάρουν αυτόματα απαντήσεις στις περισσότερες ερωτήσεις τους. Έτσι, μια σημαντική πηγή κόστους πρακτικά παύει να υπάρχει. Χάρη στην παγκόσμια πρόσβαση του δικτύου, μια μεγάλη επιχείρηση μπορεί με μικρό αριθμό προσωπικού να διατηρεί ένα μόνο κέντρο υποστήριξης με 24-ωρη δυνατότητα άμεσης απάντησης στα ερωτήματα εκείνα των πελατών, από όλο τον κόσμο, που δεν μπορούν να απαντηθούν αυτόματα από τη βάση δεδομένων του συστήματος.

Από την άλλη πλευρά, η προσφορά πληροφοριών και εκτεταμένης υποστήριξης στους πελάτες μέσα από το δίκτυο, επιτρέπει στην επιχείρηση να αντλεί πληροφορίες σχετικά με τα ενδιαφέροντα και τη συμπεριφορά των πελατών (π.χ. μελετώντας τις ερωτήσεις που υποβάλλονται από διαφορετικές ομάδες πελατών). Η γνώση αυτή είναι πολύτιμη και μπορεί να οδηγήσει στη βελτίωση προϊόντων ή στην ανάπτυξη νέων προϊόντων. Δυο γνωστές Αμερικανικές εταιρίες μεταφοράς δεμάτων, Federal Express (www.fedex.com) και UPS (www.ups.com) χρησιμοποιούν σε μεγάλο βαθμό αυτή την προσέγγιση.

Βελτίωση της δημόσιας εικόνας της επιχείρησης:

Το ηλεκτρονικό εμπόριο μπορεί να αποτελέσει ένα εξαιρετικά θετικό στοιχείο της δημόσιας εικόνας μιας επιχείρησης, ιδιαίτερα όταν η

επιχείρηση αυτή απευθύνεται σε τμήματα της αγοράς με ευνοϊκή στάση απέναντι στη νέα τεχνολογία.

Η δημόσια εικόνα (ή επωνυμία) είναι ένα από τα πολυτιμότερα άυλα κεφάλαια μιας επιχείρησης. Πολλές επιχειρήσεις επενδύουν τεράστια κεφάλαια για την καλλιέργεια και τη διατήρηση μιας ισχυρής επωνυμίας. Αυτό ισχύει κυρίως στις ανταγωνιστικές αγορές, όπου οι διαφορές μεταξύ των προϊόντων είναι βασικά μικρές και δεν επαρκούν για να κερδίσουν την προτίμηση των καταναλωτών. Το ηλεκτρονικό εμπόριο μπορεί να αποτελέσει ένα τρόπο για την ενίσχυση της δημόσιας εικόνας μιας επιχείρησης με πολύ μικρό σχετικό κόστος.

2.7.2 Μετασχηματισμός των επιχειρήσεων

Εκτός από τη βελτίωση των παραπάνω δραστηριοτήτων, το ηλεκτρονικό εμπόριο προσφέρει ευκαιρίες για μετασχηματισμό των επιχειρήσεων.

Εκμάθηση της νέας τεχνολογίας:

Η γρήγορη πρόοδος του ηλεκτρονικού εμπορίου θα υποχρεώσει πολλές επιχειρήσεις να προσαρμοστούν στη νέα τεχνολογία και να πειραματιστούν με τη χρήση νέων προϊόντων, υπηρεσιών και διαδικασιών.

Η επιχείρηση είναι ένας οργανισμός που πρέπει συνεχώς να μαθαίνει. Αυτό δεν ισχύει μόνο για την εξελισσόμενη τεχνολογία, αλλά και για το γενικότερο επιχειρηματικό περιβάλλον, στο οποίο περιλαμβάνονται οι συνθήκες της αγοράς, οι οργανωτικές δομές και η διακίνηση των προϊόντων. Στην πραγματικότητα η μάθηση στους τομείς αυτούς είναι πολύ δυσκολότερη από την εκμάθηση της χρήσης νέων τεχνολογικών εφαρμογών. Έτσι, η τεχνολογία του ηλεκτρονικού εμπορίου μπορεί να αποτελέσει την ώθηση για τη συνειδητοποίηση και την έγκαιρη προσαρμογή σε εξωτερικούς παράγοντες που υπερβαίνουν τις διαστάσεις του ψηφιακού δικτύου.

Νέες σχέσεις με τους πελάτες:

Το ηλεκτρονικό εμπόριο δημιουργεί ένα νέο τοπίο σχέσεων μεταξύ προμηθευτών και πελατών, με τη συχνή και άμεση επικοινωνία, την παροχή πλουσιότερων εξατομικευμένων πληροφοριών, και τη συλλογή στοιχείων για τις προτιμήσεις και τη συμπεριφορά των πελατών.
Η σχέση με τους πελάτες είναι ένα από τα πρώτα χαρακτηριστικά μιας επιχείρησης που αλλάζουν με την εφαρμογή του ηλεκτρονικού εμπορίου. Η εποχή που ο πελάτης έπρεπε να συμβιβαστεί με αυτά που διέθετε η επιχείρηση, έχει περάσει. Τώρα η επιχείρηση μπορεί να είναι πραγματικά ευαίσθητη στις ανάγκες και τις επιθυμίες των πελατών, και να προσαρμόζει την παραγωγή ή τα αποθέματά της στις διακυμάνσεις της ζήτησης, τις οποίες πληροφορείται άμεσα από τις ερωτήσεις των πελατών μέσω του δικτύου.

Πρόκειται για μια δραστηριότητα που προσθέτει αξία στο μάρκετινγκ της επιχείρησης. Ένας πελάτης που έχει συνηθίσει σε μια τέτοια ικανότητα ανταπόκρισης είναι δύσκολο να αλλάξει προμηθευτή, επειδή τότε θα πρέπει να περιμένει μέχρι ο νέος προμηθευτής να "μάθει τις συνήθειές του". Έτσι, η σχέση αυτή αυξάνει την αφοσίωση των πελατών.

2.7.3 Αλλαγή προτύπων

Οι βελτιώσεις και οι μετασχηματισμοί που είδαμε παραπάνω αφορούν μικρές ή μεγάλες αλλαγές μεμονωμένων δραστηριοτήτων μιας επιχείρησης. Η αλλαγή προτύπων αποτελεί μια εντελώς διαφορετική κλίμακα αλλαγών, που οδηγούν σε νέα προϊόντα και νέες λειτουργικές δομές.

Νέες δυνατότητες προϊόντων:

Η ροή και επεξεργασία των πληροφοριών, που γίνεται δυνατή χάρη στη φύση του ηλεκτρονικού εμπορίου, επιτρέπει τη σύλληψη νέων προϊόντων ή την εξειδίκευση υπαρχόντων προϊόντων με πρωτοποριακούς τρόπους.
Το ηλεκτρονικό εμπόριο δεν προσφέρει μόνο την ευκαιρία πώλησης των υπαρχόντων προϊόντων από ένα νέο κανάλι διανομής, αλλά και τη δυνατότητα δημιουργίας και βελτίωσης προϊόντων. Η μαζική παραγωγή

εξατομικευμένων προϊόντων είναι η μια πλευρά αυτής της δυνατότητας. Η δεύτερη είναι ότι ο πωλητής μπορεί να εμπλέξει τον αγοραστή πολύ νωρίς (μερικές φορές ακόμη και από το στάδιο του σχεδιασμού) στην αλυσίδα αξιών της επιχείρησης, με αποτέλεσμα την έγκαιρη προσαρμογή των υπαρχόντων προϊόντων και τη δημιουργία νέων προϊόντων σύμφωνα με τις ανάγκες και τις επιθυμίες των πελατών. Το κλειδί στη δραστηριότητα αυτή είναι η αυξημένη ροή πληροφοριών μεταξύ πωλητή και αγοραστή.

Νέα λειτουργικά μοντέλα:

Το ηλεκτρονικό εμπόριο, σε συνδυασμό με την αλλαγή των δομών της αγοράς, οδηγεί στην εμφάνιση νέων μοντέλων για τη λειτουργία επιχειρήσεων, που βασίζονται στην αφθονία των πληροφοριών και την άμεση διανομή τους στους πελάτες.

Το ηλεκτρονικό εμπόριο μπορεί να προσφέρει ευκαιρίες για την ανάπτυξη νέων προϊόντων, αλλά κυρίως μπορεί να οδηγήσει στην αναθεώρηση των μοντέλων που καθορίζουν τις επιχειρηματικές δραστηριότητες. Δεν υπάρχει ένα ενιαίο μοντέλο που να ισχύει για όλες τις επιχειρήσεις που εφαρμόζουν το ηλεκτρονικό εμπόριο. Αντίθετα, υπάρχει ένα διαφορετικό μοντέλο για κάθε τύπο επιχείρησης. Το κέντρο βάρους όλων αυτών των μοντέλων είναι ο νέος ρόλος των ενδιαμέσων. Σε πολλούς κλάδους θα εξαφανιστούν οι παραδοσιακοί μεσάζοντες, ενώ θα εμφανιστούν νέες μορφές ενδιαμέσων, ιδιαίτερα σε σχέση με την ψηφιακή υποδομή.

2.8 Πλεονεκτήματα του ηλεκτρονικού εμπορίου για τους πελάτες

Τα πλεονεκτήματα από την εφαρμογή του ηλεκτρονικού εμπορίου δεν βρίσκονται μόνο στην πλευρά των προμηθευτών. Υπάρχουν πέντε τουλάχιστον σαφή πλεονεκτήματα για τους πελάτες.

Χαμηλότερες τιμές προϊόντων:

Η μείωση των τιμών είναι ένα έμμεσο αποτέλεσμα του χαμηλότερου κόστους συναλλαγής. Σύμφωνα με τη θεωρία του κόστους συναλλαγών, για κάθε δραστηριότητα της αλυσίδας αξιών μια επιχείρηση πρέπει να αποφασίσει αν θα την αναθέσει σε εξωτερικό προμηθευτή ή αν θα την εκτελέσει η ίδια. Το κριτήριο της απόφασης αυτής είναι το σχετικό κόστος των δυο επιλογών.

Το ηλεκτρονικό εμπόριο επιτρέπει την απλοποίηση και την αυτοματοποίηση πολλών δραστηριοτήτων, ιδίως αυτών που αφορούν την επικοινωνία με πελάτες ή προμηθευτές. Έτσι, ο συνολικός κύκλος από τη σχεδίαση του προϊόντος ως την παράδοση στον τελικό καταναλωτή απλοποιείται, πολλά στάδια που περιλάμβαναν τη χρήση ενδιαμέσων καταργούνται ή ενοποιούνται, και το κόστος παραγωγής και διάθεσης των προϊόντων μειώνεται.

Αυξημένος ανταγωνισμός:

Το ηλεκτρονικό εμπόριο δεν γνωρίζει γεωγραφικά σύνορα. Ο καθένας μπορεί να δημιουργήσει μια "ιδεατή επιχείρηση", που μέσα από την ψηφιακή υποδομή θα είναι προσιτή σε όλο τον κόσμο. Οι τοπικοί προμηθευτές κάθε περιοχής παύουν να προστατεύονται από τη γεωγραφική απόσταση, με αποτέλεσμα μια αύξηση του ανταγωνισμού, που συμπιέζει τις τιμές σύμφωνα με τον νόμο της προσφοράς και της ζήτησης. Βέβαια η τιμή κάθε προϊόντος έχει ένα κατώτατο όριο, που εξαρτάται από το κόστος παραγωγής του. Αν οι τιμές έχουν ήδη πλησιάσει αρκετά αυτό το όριο, ο ανταγωνισμός μπορεί να ωθήσει τους πωλητές να προσφέρουν προϊόντα αυξημένης αξίας. Η πρόσθετη αξία μπορεί να έχει τη μορφή βελτιωμένης ποιότητας ή δωρεάν υπηρεσιών υποστήριξης.

Αυξημένη αγοραστική παραγωγικότητα:

Το μέτρο της παραγωγικότητας ενός αγοραστή είναι το κόστος και ο χρόνος που απαιτούνται για την επιλογή προμηθευτή-προϊόντος και τη λήψη της απόφασης αγοράς. Αν ο αγοραστής είναι μια επιχείρηση που παράγει προστιθέμενη αξία, η αύξηση της αγοραστικής παραγωγικότητας μεταφράζεται άμεσα σε μείωση του κόστους των δικών της προϊόντων ή υπηρεσιών. Το ηλεκτρονικό εμπόριο διευκολύνει σε μεγάλο βαθμό τη

διερεύνηση της αγοράς και τον εντοπισμό του κατάλληλου προϊόντος στην κατάλληλη τιμή σε συντομότερο χρόνο και με σχεδόν μηδενικό κόστος.

Καλύτερη διαχείριση των πληροφοριών:

Η απόφαση σχετικά την ανάθεση μιας δραστηριότητας σε εξωτερικό προμηθευτή ή την εκτέλεσή της από την ίδια την επιχείρηση καθορίζεται κυρίως από τις πληροφορίες που είναι διαθέσιμες. Η ψηφιακή υποδομή αυξάνει τρομακτικά τον όγκο αλλά και τη δυνατότητα οργάνωσης και χρήσης των πληροφοριών, επιτρέποντας έτσι την τεκμηρίωση παρόμοιων αποφάσεων με ακρίβεια και αξιοπιστία. Πολλά διοικητικά στελέχη βλέπουν ευνοϊκά την προοπτική αυτή και προσπαθούν να ενσωματώσουν τις ηλεκτρονικές επικοινωνίες στην καθημερινή τους δουλειά.

Καλύτερος έλεγχος αποθεμάτων:

Οι ηλεκτρονικές επικοινωνίες επιταχύνουν την ολοκλήρωση των συναλλαγών, αυξάνοντας έτσι την ευελιξία στις προμήθειες των επιχειρήσεων. Πολλές επιχειρήσεις αξιοποιούν τη δυνατότητα αυτή με την εφαρμογή του συστήματος JIT (Just-In-Time, "Την τελευταία στιγμή"), που μειώνει τα περιθώρια ανανέωσης των αποθεμάτων, περιορίζοντας έτσι σημαντικά το κόστος παραγωγής/διάθεσης των προϊόντων τους.

Στην πραγματικότητα ο μηδενισμός των αποθεμάτων δεν είναι κάτι εφικτό, και πάντοτε υπάρχει ανάγκη για ένα ελάχιστο απόθεμα ασφαλείας. Ο κρίσιμος παράγοντας, που επιτρέπει τον περιορισμό της ελάχιστης απαραίτητης ποσότητας αποθεμάτων, είναι ο χρόνος. Όσο λιγότερος χρόνος απαιτείται για την ολοκλήρωση μιας παραγγελίας, τόσο μικρότερο απόθεμα είναι υποχρεωμένη να κρατά μια επιχείρηση, ώστε να μην υπάρξει διακοπή στις δραστηριότητές της. Οι ηλεκτρονικές επικοινωνίες κάνουν δυνατή τη στιγμιαία επικοινωνία μεταξύ των τμημάτων μιας επιχείρησης και μεταξύ της επιχείρησης και των προμηθευτών της. Επίσης, η συνεχής παρακολούθηση των αποθεμάτων από το σύστημα μηχανογράφησης επιτρέπει την πραγματοποίηση προβλέψεων για το επίπεδο των αναγκών στο άμεσο μέλλον. Υπάρχει μάλιστα η δυνατότητα σύνδεσης των συστημάτων της επιχείρησης με αυτά του προμηθευτή, ώστε ο προμηθευτής να χρησιμοποιεί τις προβλέψεις για τον έλεγχο των δικών του αποθεμάτων και να καλύπτει αυτόματα (και έγκαιρα) τις ανάγκες της επιχείρησης.

ΚΕΦΑΛΑΙΟ 3

Τα προβλήματα και οι κίνδυνοι στις ηλεκτρονικές συναλλαγές

3.1 Γενικά

Στην αρχή της εμφάνισης των υπολογιστών, μερικές δεκαετίες πριν, τα θέματα ασφαλείας αφορούσαν μόνο στα μεγάλα υπολογιστικά δίκτυα. Όσο περνούσε όμως ο καιρός και ο υπολογιστής γινόταν προσιτός σε ολοένα περισσότερο κόσμο, το ζήτημα άρχισε να παίρνει άλλη τροπή. Με την εμφάνιση των Windows και ιδιαίτερα των Windows 95, στα μέσα της περασμένης δεκαετίας, ο προσωπικός υπολογιστής έγινε ένα ευρύ καταναλωτικό προϊόν. Ακόμη μεγαλύτερες αλλαγές επήλθαν με την έλευση του World Wide Web, καθώς το Internet έγινε απλούστερο, πιο εύκολο στη χρήση και πιο ελκυστικό, φέρνοντας όμως στο προσκήνιο και προβλήματα. Ξαφνικά το ζήτημα της ασφάλειας των δεδομένων δεν αφορούσε μόνο στα μεγάλα δίκτυα αλλά και στον απλό χρήστη, ο οποίος άρχισε να ασχολείται με τους ιούς.

Ανεξάρτητα από το επίπεδο της πολυπλοκότητάς τους, σε όλα τα ηλεκτρονικά συστήματα υπάρχουν συμφυείς κίνδυνοι. Οι κίνδυνοι αυτοί σχετίζονται καταρχήν με τα ίδια τα ηλεκτρονικά συστήματα (σχεδιασμός και ανάπτυξη, πολιτική και διαδικασίες λειτουργίας, εσωτερικοί έλεγχοι , συμμόρφωση με το υφιστάμενο νομικό και κανονιστικό πλαίσιο, διαδικασίες διαχείρισης συστημάτων, εξάρτηση από τρίτους υπεργολάβους κλπ). Πρόσθετοι κίνδυνοι είναι αυτοί των φυσικών καταστροφών, της επίθεσης κατά του συστήματος (παραβίαση ασφαλείας) και της αδυναμίας ανταπόκρισης ενός εκ των συμμετεχόντων στο σύστημα ηλεκτρονικών συναλλαγών.

Στατιστικά: Σύμφωνα με το Κέντρο Συντονισμού CERT (www.cert.org) ο αριθμός των περιστατικών παραβίασης ασφαλείας που έχουν εκδοθεί

μεταξύ 1998 και 2002 είναι 182.463. Ένα περιστατικό μπορεί να αφορά επίθεση σε πέραν του ενός κόμβου.

Σύμφωνα με έρευνα του Υπουργείου Εμπορίου της Βρετανίας (www.security-survey.gov.uk) το μέσο κόστος μιας σοβαρής ενέργειας hacking ξεπερνά για τον παθόντα τις 30.000 λίρες.

Σύμφωνα με το Υπουργείο Δικαιοσύνης των Η.Π.Α. (www.usdoj.gov), από το Μάρτιο του1998 ως το Φεβρουάριο του 2003, 60 υποθέσεις hacking έφτασαν στα αμερικάνικα δικαστήρια.

Σύμφωνα με έρευνα του FBI (www.fbi.gov) και του Computer Security Institute (www.gocsi.com), το 90% των εταιρειών που ερωτήθηκαν υπέστησαν επιθέσεις από hackers με συνολικές ζημιές 455 εκατ.δολαρίων.

3.2 Κίνδυνοι στα πληροφοριακά συστήματα

Ας δούμε πιο συνηθισμένους τρόπους που χρησιμοποιούνται σήμερα για επίθεση ή παράνομη πρόσβαση σε προσωπικούς Η/Υ:

3.2.1 Ιοί υπολογιστών

Οι ιοί είναι προγράμματα τα οποία εισβάλουν σε έναν υπολογιστή, συνήθως μέσω του Web και του ηλεκτρονικού ταχυδρομείου και σπανιότερα μέσω προγραμμάτων που τρέχουν από δισκέτες ή CD-ROM (που έχουν ληφθεί από άλλα μολυσμένα συστήματα). Μπορούν να προκαλέσουν ποικίλες ζημιές. Μπορούν να διαγράψουν αρχεία δεδομένων, να σβήσουν προγράμματα ή να καταστρέψουν οτιδήποτε στο σκληρό δίσκο του «μολυσμένου» μηχανήματος. Όμως, δεν είναι όλοι οι ιοί καταστρεπτικοί, διότι μερικοί απλώς εμφανίζουν ενοχλητικά μηνύματα.

Ο όρος «ιός» είναι αρκετά γενικός και απευθύνεται σε μια μεγάλη ποικιλία προγραμμάτων. Οι ιοί είναι γραμμένοι για καθορισμένα είδη υπολογιστών, όπως τα PCs ή τα Macs, επειδή τα αρχεία που προσβάλλουν τρέχουν μόνο σε ένα είδος υπολογιστή. Οι παραδοσιακοί ιοί προσκολλώνται

σε προγράμματα ή αρχεία δεδομένων, μολύνουν τον υπολογιστή, αυτοαναπαράγονται στο σκληρό δίσκο του συστήματος και καταστρέφουν τα δεδομένα, το σκληρό δίσκο ή τα αρχεία. Οι ιοί συνήθως προσβάλλουν τέσσερα τμήματα του υπολογιστή:

- Το σύστημα αρχείων-directories, το οποίο καταγράφει τις θέσεις όλων των αρχείων του υπολογιστή (και χωρίς αυτό ο υπολογιστής δεν λειτουργεί).
- Τα εκτελέσιμα αρχεία .
- Τις περιοχές εκκίνησης του συστήματος, οι οποίες χρειάζονται στην εκκίνηση του υπολογιστή.
- Τα αρχεία δεδομένων, αφού πρόσφατα έχουν γραφτεί ιοί που προσβάλλουν και αυτά τα αρχεία, όπως ορισμένοι ιοί που προσκολλώνται σε μακροεντολές ενός αρχείου δεδομένων του Microsoft Word και ενεργοποιούνται όταν εκτελεστεί η συγκεκριμένη μακροεντολή.

3.2.1.1 Τα είδη των ιών

Boot Sector Viruses: Είναι η πρώτη μορφή ιών. Εξαπλώθηκαν ιδιαίτερα την εποχή που η μεταφορά δεδομένων απαιτούσε τη χρήση δισκετών. Για να ενεργοποιηθεί ένας τέτοιος ιός, θα πρέπει να εκκινήσουμε το σύστημα με ένα αποθηκευτικό μέσο, το οποίο θα περιέχει μολυσμένο boot sector (ειδική περιοχή των αποθηκευτικών μέσων την οποία διαβάζει ο υπολογιστής πριν από οτιδήποτε άλλο). Ελάχιστα απειλούν σήμερα.

File Viruses: Πρόκειται για το πιο κοινό και γνωστό είδος ιού. Τα file viruses παραμένουν κρυμμένα στον κώδικα εκτελέσιμων αρχείων και ενεργοποιούνται όταν ο χρήστης ενεργοποιεί κάποιο από αυτά. Όταν ανοιχτεί το αρχείο, ο ιός εκτελείται άμεσα και στη συνέχεια εκτελείται και το κανονικό πρόγραμμα με αποτέλεσμα να μη γίνεται αντιληπτή από το χρήστη η ύπαρξη ιού. Στη συνέχεια ο ιός μπορεί να αντιγράψει τον εαυτό του και σε άλλα αρχεία του δίσκου ή στη μνήμη του υπολογιστή.

Macro Viruses: Τα macro viruses είναι μια ιδιαίτερη μορφή ιών, οι οποίοι προσβάλλουν αρχεία που περιέχουν ακολουθίες εντολών για συγκεκριμένα προγράμματα (μακροεντολές). Με την εκτέλεση μιας μακροεντολής μολυσμένου αρχείου μέσα από το κατάλληλο πρόγραμμα (π.χ. επεξεργαστές κειμένου ή φύλλα εργασίας), ο ιός ενεργοποιείται. Τα macro viruses βρίσκονται πολύ συχνά σε αρχεία MS-Word και MS-Excel, που είναι τα δύο πιο διαδεδομένα προγράμματα εφαρμογών γραφείου.

Προγράμματα «Δούρειοι Ίπποι» (Trojan Horse Programmes). Τα προγράμματα αυτά παρουσιάζονται συνήθως σε διάφορες ιστοσελίδες ως πολύ χρήσιμα και ενδιαφέροντα, με σκοπό να πείσουν το χρήστη να τα εγκαταστήσει στον Η/Υ του. Είναι προγράμματα που μεταμφιέζονται σε κανονικά, χρήσιμα προγράμματα, αλλά στην πραγματικότητα είναι ιοί, ενεργούν δηλαδή όπως ακριβώς ο Δούρειος Ίππος. Για παράδειγμα, ένα τέτοιο πρόγραμμα, ενώ παρουσιάζεται ως calculator με δυνατότητα μαθηματικών υπολογισμών, στην πραγματικότητα διαγράφει κάθε αρχείο του δίσκου. Τα πιο «δυνατά» από αυτά είναι ταυτόχρονα και backdoors, «πίσω πόρτες», που λειτουργούν ως κρυφές δίοδοι στο σύστημα. Ένα από τα πιο πρόσφατα και επικίνδυνα Trojans που λειτουργεί ως κατεξοχήν backdoor είναι το 'The Thing', το οποίο επιτρέπει στον εισβολέα να διαχειριστεί το σύστημα του ανυποψίαστου χρήστη από απομακρυσμένη τοποθεσία.

Exploits: Το exploit είναι ένα κομμάτι κώδικα σχεδιασμένο με τέτοιον τρόπο ώστε να παρακάμπτει ή να επιτίθεται στα συστήματα ασφαλείας κάποιου υπολογιστικού συστήματος. Τα exploits συνήθως εκμεταλλεύονται διάφορα αδύνατα σημεία των συστημάτων ασφαλείας, όπως μη ασφαλισμένες ρυθμίσεις συστήματος και buffer overflows. Τα exploits στοχεύουν συνήθως σε δίκτυα LAN και λιγότερο σε προσωπικούς υπολογιστές.

Worms: Τα worms είναι προγράμματα που έχουν σχεδιαστεί να προσβάλλουν δίκτυα όπως το Internet. Δεν κρύβονται σε κάποιο αρχείο. Είναι αυτόνομα αρχεία, τα οποία πολλαπλασιάζονται αδιακρίτως. Πιο συγκεκριμένα, ταξιδεύουν από τον ένα δικτυακό υπολογιστή στον άλλο, ενώ καθοδόν δημιουργούν αντίγραφα του εαυτού τους. Από τα πιο καταστροφικά «σκουλήκια» ήταν το Code Red και Code Red II.

Άλλες μορφές: Εκτός των προαναφερόμενων γενικών κατηγοριών, υπάρχουν και κάποιες επιμέρους κατηγορίες ανάλογα με τον τρόπο που δρουν, όπως τα Cluster Virus, τα Encrypted Virus, τα Memory-resident Virus και τα Polymorphic Virus.

3.2.2 Παρεμπόδιση υπηρεσίας (Dos-Denial Of Service)

Τα Dos (Denial Of Service-καμία σχέση με το ομώνυμο λειτουργικό σύστημα) attacks είναι εργαλεία επίθεσης σχεδιασμένα έτσι ώστε να απαγορεύουν σε χρήστες να έχουν πρόσβαση σε συγκεκριμένες πηγές του Δικτύου. Το Dos-Denial Of Service δεν συνιστά παράνομη πρόσβαση αλλά καθιστά τον Η/Υ μη λειτουργήσιμο είτε γιατί του επιβάλλεται η εκτέλεση κάποιας προβληματικής εντολής (π.χ. ping of death), είτε γιατί του αποστέλλεται τεράστιος όγκος πληροφοριών από το διαδίκτυο (γνωστό σαν 'flooding') και δεν μπορεί να ανταπεξέλθει στο φόρτο εργασίας που δημιουργείται.

Αυτή η μέθοδος χρησιμοποιείται από τους λιγότερο έμπειρους εισβολείς, οι οποίοι ουσιαστικά δεν ενδιαφέρονται να εισέλθουν σε ένα δίκτυο ή σύστημα, αλλά απλώς να προκαλέσουν την κατάρρευσή του λόγω υπερφόρτωσης. Γνωστά DOS attacks είναι τα winnuke, teardrop και synfloods.

3.2.3 Μη ενημερωμένες λογισμικές εφαρμογές και εκμετάλλευση λαθών του λογισμικού λειτουργικών συστημάτων

Δυστυχώς, δεν υπάρχει λογισμικό χωρίς λάθη (bugs). Έχει υπολογιστεί ότι κάθε 1.000 γραμμές κώδικα περιέχουν πάνω από 15 λάθη, ακόμη και ύστερα από εξαντλητικό έλεγχο, τα οποία είναι συνήθως «κρυμμένα» και μόνο με κατάλληλους συνδυασμούς εμφανίζονται.

Αυτές τις αδυναμίες εντοπίζουν και εκμεταλλεύονται διάφοροι για να εισβάλουν στον Η/Υ μας. Για εντοπισμό συγκεκριμένων γνωστών αδυναμιών σε διάφορα λογισμικά προγράμματα, οι 'hackers' έχουν δημιουργήσει εξειδικευμένα λογισμικά εργαλεία που αυτοματοποιούν την όλη διαδικασία.

3.2.4 Προσπάθεια υποκλοπής κωδικών, λογαριασμών χρηστών κλπ με συνεχή δοκιμή πιθανών συνδυασμών

Αφού ο εισβολέας αποκτήσει μια στοιχειώδη πρόσβαση σε ένα σύστημα, θα προσπαθήσει να «μαντέψει» τον κωδικό (password) ενός ισχυρού χρήστη (για παράδειγμα του διαχειριστή του δικτύου) ώστε να μπορέσει να αποκτήσει πλήρη έλεγχο.

3.2.5 Φυσικές και εσωτερικές επιθέσεις

Όσο και αν φαίνεται παράξενο, οι πιο συνήθεις τρόποι παραβίασης ενός δικτύου συστήματος γίνονται από μέσα από την ίδια την εταιρεία και στηρίζονται στην αμέλεια των χρηστών να τηρούν έστω και στοιχειώδη μέτρα ασφάλειας. Για παράδειγμα, πόσοι χρήστες φροντίζουν να έχουν έστω ένα κωδικό πρόσβασης στον υπολογιστή τους ή, αν έχουν, να φροντίζουν να μην είναι κάτι το προφανές, να τον αλλάζουν ανά τακτά χρονικά διαστήματα κλπ.

3.2.6 Κινητός κώδικας προγραμματισμού (Mobile code: Java/Javascript/activex)

Στην περίπτωση αυτή ο Η/Υ μας γίνεται μέσο για επίθεση σε άλλους Η/Υ, όπως για παράδειγμα στις γνωστές μαζικές επιθέσεις 'DDOS-

Distribute Denial Of Service Attacks'. Ο δράστης εγκαθιστά στον Η/Υ μας ένα πρόγραμμα 'Δούρειου Ίππου' ή εκμετάλλευσης κάποιας αδυναμίας μιας λογισμικής εφαρμογής. Το πρόγραμμα αυτό δέχεται εντολές από άλλα προγράμματα-διαχειριστές (handlers), που βρίσκονται σε άλλους Η/Υ στο διαδίκτυο. Σε συγκεκριμένο χρόνο οι δέκτες παίρνουν την εντολή να εξαπολύσουν μαζική επίθεση κατά συγκεκριμένων δικτύων. Ο Η/Υ μας δεν είναι αποδέκτης της επίθεσης αυτής αλλά χρησιμοποιείται μαζί με τη σύνδεσή μας στο διαδίκτυο για πραγματοποίηση επίθεσης σε άλλους υπολογιστές.

3.2.7 Spam και Hoaxes

Spam ή αν προτιμάτε ανεπιθύμητα e-mails. Υπήρξαν ένα από τα πρώτα δυσάρεστα φαινόμενα του δικτύου και ,όπως τα περισσότερα , χρησιμοποίησαν το ηλεκτρονικό ταχυδρομείο. Τελευταίες έρευνες φέρνουν τα ανεπιθύμητα μηνύματα να καταλαμβάνουν περισσότερο από το 40% των μηνυμάτων που στέλνονται καθημερινά δίνοντας στο spam διαστάσεις καταιγίδας. Ο μεγαλύτερος όγκος τους αναφέρεται σε διαφημίσεις για site με «ροζ» περιεχόμενο, ενώ το υπόλοιπο ποσοστό τους καταναλώνεται σε διαφημίσεις παντός είδους προϊόντων και υπηρεσιών, αλλά και σε ενημερωτικά newsletters και λίστες ηλεκτρονικού ταχυδρομείου. Στις δύο τελευταίες περιπτώσεις μάλιστα, πολύ συχνά οι αποστολείς καταφέρονται κατά του spam, προτρέποντας τους παραλήπτες, αν δεν θέλουν την αποστολή, να διαγραφούν από την όποια λίστα (στην πραγματικότητα αυτή η τακτική πιστοποιεί τις προθέσεις του αποστολέα καθώς και τη φύση του μηνύματος).

Εξίσου ενοχλητικά και διάσημα είναι και τα Hoaxes ή Urban Legends τα οποία συναντάμε με τη μορφή μηνύματος. Ο όρος Hoax χρησιμοποιείται στα Αγγλικά για να περιγράψει μια απάτη ή κάτι ψεύτικο, αν και ο όρος που ταιριάζει στα μηνύματα αυτά είναι το Urban Legend (Αστικός Θρύλος). Δημοφιλέστερη κατηγορία τους είναι τα προειδοποιητικά μηνύματα σχετικά με ιούς, ενώ για περισσότερη αξιοπιστία τα hoaxes πολύ συχνά υποστηρίζουν ότι αποτελούν μηνύματα με αποστολέα κάποιον μεγάλο

οργανισμό(π.χ. IBM, Microsoft, κλπ). Αν θελήσουμε να βρούμε το σήμα κατατεθέν τους, τότε χωρίς ιδιαίτερη δυσκολία θα πρέπει να το αναζητήσουμε στα μηνύματα που ζητούν προώθηση σε άλλους χρήστες. Στην τελευταία κατηγορία ανήκουν και τα λεγόμενα chain letters, τα οποία δηλώνουν ξεκάθαρα ότι ο κύριος λόγος ύπαρξής τους είναι να διακινηθούν σε όσο το δυνατόν περισσότερους χρήστες του δικτύου και υπόσχονται συνήθως τύχη και άλλα οφέλη σε όποιον τα προωθήσει.

3.2.8 Ψευδή ηλεκτρονικά μηνύματα (e-mail spoofing)

Η απάτη αυτή εμπίπτει στην κατηγορία της «Κοινωνικής Μηχανικής» (Social Engineering), που στηρίζεται στην παραπλάνηση ατόμων και πραγματοποιείται όταν ένα ηλεκτρονικό μήνυμα παρουσιάζεται ότι έχει σταλεί από συγκεκριμένο πρόσωπο ενώ στην πραγματικότητα έχει σταλεί από άλλο. Σκοπός της απάτης αυτής είναι να ξεγελαστεί ο παραλήπτης και να απαντήσει στο μήνυμα δίνοντας στοιχεία ή πληροφορίες που δεν θα έπρεπε.

3.2.9 Μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου (e-mail borne viruses)

Το e-mail, δυστυχώς, πρόκειται για μια ιδιαίτερα μη ασφαλή μέθοδο επικοινωνίας, η οποία είναι ευεπίφορη τόσο σε υποκλοπές όσο και σε παραποιήσεις. Οι ιοί καθώς και άλλοι κακόβουλοι κώδικες μεταφέρονται συχνά με μηνύματα ηλεκτρονικού ταχυδρομείου. Σε καμιά περίπτωση δεν πρέπει να ανοίγεται οποιοδήποτε αρχείο συνημμένο σε ηλεκτρονικό μήνυμα αν δεν επιβεβαιωθεί η πηγή του μηνύματος. Στην περίπτωση που το συνημμένο είναι πρόγραμμα που θα τρέξει στον Η/Υ σας, οπωσδήποτε πρέπει να ελεγχθεί και επιβεβαιωθεί ποιος έγραψε τον κώδικα. Ο ιός 'melissa' έχει αποδείξει έμπρακτα ότι δεν είναι αρκετό να αναγνωρίσουμε

τη διεύθυνση του αποστολέα για να εμπιστευθούμε το περιεχόμενο του μηνύματος.

Επιπρόσθετα, υπάρχουν ορισμένα είδη ιών που εκμεταλλεύονται τη δυνατότητα των Windows να κρύβουν τον τύπο των αρχείων ο οποίος καθορίζεται από τους τρεις χαρακτήρες στο τέλος του ονόματος του αρχείου. Έτσι, στέλνουν μηνύματα με φαινομενικά ακίνδυνα συνημμένα αρχεία με ονόματα όπως:

Love-Letter-For-You.txt	Timofonica.txt
MySis.avi	AnnaKournikova.jpg
QuickFlick.mpg	

Όμως στην πραγματικότητα, ο τύπος των αρχείων αυτών είναι:

Love-Letter-For-You.txt.vbs	Timofonica.txt.vbs
MySis.avi.exe	AnnaKournikova.jpg.vbs
QuickFlick.mpg.exe	

Λυγίζοντας στον πειρασμό και ανοίγοντας τα πιο πάνω συνημμένα αρχεία εκτελείται ο κώδικας του ιού και προσβάλλει τον υπολογιστή μας. Το πρώτο από τα πιο πάνω κακόβουλα προγράμματα ευθύνεται για το γνωστό ιό 'I LOVE YOU'.

3.2.10 Συστήματα διαχείρισης Η/Υ (Remote Administration Programmes)

Στην ομάδα αυτή περιλαμβάνονται κυρίως τρία προγράμματα, το Backorifice, το Netbus και το Subseven. Πρόκειται για προγράμματα που όταν οι δράστες επιτύχουν να εγκαταστήσουν στον Η/Υ μας (με λειτουργικό Windows), ξεγελώντας μας συνήθως με ένα από τους τρόπους που έχουν αναφερθεί πιο πάνω, μπορούν να θέσουν σε λεπτομερή παρακολούθηση τον Η/Υ μας μέχρι και να λάβουν τον πλήρη έλεγχο της λειτουργίας του από άλλον απομακρυσμένο Η/Υ συνδεδεμένο στο διαδίκτυο.

3.2.11 Παρακολούθηση δικτύου (Packet Sniffing)

Ειδικά προγράμματα, γνωστά σαν 'Packet Sniffers', έχουν τη δυνατότητα να παρακολουθούν την κίνηση ενός τοπικού δικτύου και να αναζητούν συγκεκριμένες πληροφορίες, όπως μυστικούς κωδικούς πρόσβασης. Αυτό σημαίνει ότι, έχοντας κερδίσει πρόσβαση σε έναν Η/Υ μέσα σε κάποιο τοπικό δίκτυο, υπάρχει η δυνατότητα παρακολούθησης της κίνησης όλων των Η/Υ του δικτύου και σε δεύτερη φάση την περαιτέρω εισχώρηση στους υπόλοιπους Η/Υ. Το πρόβλημα αυτό είναι εντονότερο σε περιοχές του εξωτερικού που παρέχεται σύνδεση με τα γνωστά 'cable-modems', μια και όλα τα σπίτια της περιοχής είναι συνδεδεμένα συνήθως στο ίδιο τοπικό δίκτυο.

3.3 Κίνδυνοι στις ηλεκτρονικές συναλλαγές

Το ηλεκτρονικό εμπόριο δεν στηρίζεται στα «κλειστά» τραπεζικά συστήματα αλλά στο Internet, που πρόκειται για έναν ιδιαίτερα μη ασφαλή τρόπο επικοινωνίας. Δεν υπόκεινται όλες οι ηλεκτρονικές συναλλαγές στον

ίδιο βαθμό κινδύνου. Όπως είναι λογικό, οι χρηματικές συναλλαγές είναι υψηλότερου κινδύνου από τις απλές ανταλλαγές δεδομένων.

Ας δούμε τα πιο συνηθισμένα προβλήματα και κινδύνους στις ηλεκτρονικές συναλλαγές:

3.3.1 Μη εγκεκριμένη πρόσβαση σε πληροφορίες (παράνομη εισβολή hacker)

Το ερώτημα το οποίο διατυπώνεται κυρίως από τους μη γνωρίζοντες, είναι από ποιον και γιατί φτιάχνονται οι ιοί, από ποιόν και γιατί πραγματοποιούνται επιθέσεις στα εταιρικά δίκτυα και στους δικτυακούς τόπους.

Η απάντηση και στα δύο ερωτήματα είναι δύσκολη, αν και η συνήθης είναι οι «hackers|» και οι «crackers». Οι πρώτοι είναι οι «ερασιτέχνες», με στόχο τους συνήθως μόνο δίκτυα με ισχυρά συστήματα ασφαλείας. Αν και δεν υπάρχει καθολική συμφωνία σχετικά με την ορολογία, οι crackers θεωρούνται hackers που διαπράττουν ηλεκτρονικά εγκλήματα με σκοπό το κέρδος, ενώ οι τελευταίοι οδηγούνται περισσότερο από μη ωφελιμιστικά κίνητρα και «σπάνε» συστήματα περισσότερο για να αποδείξουν τις ικανότητές τους παρά για να κερδίσουν χρήματα. Οι crackers χρησιμοποιούν περισσότερο εξελιγμένο εξοπλισμό και συνήθως επιτίθενται κατά ομάδες. Πάντως, αυτό δεν αποκλείει την πιθανότητα και οι δύο να προκαλέσουν εκτεταμένες ζημιές σε ένα δίκτυο. Κατά γενική εκτίμηση οι crackers είναι «δυνατότεροι» αλλά περισσότερο προβλέψιμοι, ενώ οι hackers είναι λιγότερο προβλέψιμοι αλλά ευκολότερα αντιμετωπίσιμοι.

3.3.2 Παράνομη παρακολούθηση (eavesdropping)

Η συλλογή πληροφοριών για αριθμούς καρτών, για ύψη ή/και αριθμούς λογαριασμών και σε μερικές περιπτώσεις για αυτό καθαυτό το γεγονός της πραγματοποιήσεως μιας συναλλαγής με κάποιον εμπορικό φορέα (

δημιουργία προφίλ αγοραστού, με ταυτόχρονη προσβολή της ιδιωτικότητάς του), είναι συχνές περιπτώσεις στο δίκτυο.

3.3.3 Τροποποίηση δεδομένων (data modification)

Η μεταβολή των στοιχείων μιας εμπορικής παραγγελίας, ή και η τροποποίηση κάποιων δεδομένων σε ηλεκτρονικές συναλλαγές (π.χ. του ονόματος του δικαιούχου σε κάποια επιταγή, ή του ποσού της επιταγής), είναι φαινόμενα που δεν εξαιρούνται από τις επιθέσεις στο Internet.

3.3.4 Έλλειψη τυποποίησης

Δεν έχει υιοθετηθεί μία κοινά αποδεκτή μέθοδος (ή πρότυπο) διεκπεραίωσης των ηλεκτρονικών συναλλαγών στο Internet, που επιτρέπει την επικοινωνία μεταξύ των διαφόρων τύπων λογισμικού των συναλλασσόμενων μερών. Η εξασφάλιση ή όχι αυτής της διαλειτουργικότητας θα καθορίσει και την μελλοντική πορεία των ηλεκτρονικών συστημάτων πληρωμών.

3.3.5 Διπλή κατανάλωση (double spending)

Από τη στιγμή που το ψηφιακό χρήμα είναι μια αφηρημένη έννοια, στην ουσία , bits ή μηνύματα που αποστέλλονται μέσω καλωδιώσεων και μαγνητικών μέσων, μια τεχνική που μπορεί να χρησιμοποιείται για να υπάρχουν πάντα αυτά τα χρήματα (κατά συνέπεια και τα πραγματικά σαν αναπαράσταση των ψηφιακών) στην κατοχή μας, είναι να αποστέλλονται (δηλ. να καταναλώνονται) τα ίδια κάθε φορά...μηνύματα! Αυτό όμως δεν γίνεται στο συμβατικό χρήμα, αφού το χαρτονόμισμα με τον συγκεκριμένο αριθμό σειράς που δόθηκε για αγορές, πέρασε πλέον στον δικαιούχο πωλητή και δεν είναι δυνατόν να καταναλωθεί εκ νέου από τον αγοραστή(χωρίς να πλαστογραφηθεί). Έτσι λοιπόν και η «διπλή κατανάλωση» των bits είναι

πλαστογραφία. Επομένως τίθεται η ανάγκη μοναδικής αναγνωρίσεως των μηνυμάτων που συνιστούν το «ψηφιακό χρήμα».

3.3.6 Κρυπτογράφηση των συναλλαγών

Στις παραδοσιακές συναλλαγές, τα στοιχεία των συναλλαγών, είτε το επιθυμούν οι συμβαλλόμενοι είτε όχι, είναι στη διάθεση των φορολογικών αρχών, με δεδομένο ότι ή δεν είναι δυνατή ή δε γίνεται κανενός είδους κρυπτογράφηση αυτών. Αντίθετα, στις ηλεκτρονικές συναλλαγές η κρυπτογράφηση (encryption) των στοιχείων είναι όχι μόνο δυνατή αλλά και απαραίτητη για την προστασία των συναλλασσόμενων. Έτσι όμως περιορίζεται και η πρόσβαση από τις φορολογικές αρχές. Θεωρητικά οι ιδιωτικές αρχές μπορούν να σπάσουν κάποιους από αυτούς τους κώδικες, αλλά σε πρακτικό επίπεδο κάτι τέτοιο είναι αδύνατο. Στο ηλεκτρονικό εμπόριο του μέλλοντος θα υπάρχουν δισεκατομμύρια κρυπτογραφημένων συναλλαγών, που θα χρησιμοποιούν δισεκατομμύρια κρυπτογραφικούς συνδυασμούς μέσα από δισεκατομμύρια εναλλακτικές ηλεκτρονικές οδούς.

3.3.7 Επιθέσεις στα πρωτόκολλα των συστημάτων ηλεκτρονικών πληρωμών

Όταν σχεδιάζεται μια λύση ασφαλείας, πρέπει να εστιάζεται μεγάλη προσοχή στην περιοχή όπου αναμένονται επιθέσεις εναντίον του συστήματος. Τα πρωτόκολλα των συστημάτων ηλεκτρονικών πληρωμών, είναι δυνατόν να δεχθούν επιθέσεις σε δύο επίπεδα : α) στο ίδιο πρωτόκολλο και β) στο κρυπτοσύστημα που το υποστηρίζει.

Αναφορικά με την πρώτη περίπτωση (επιθέσεις κατά του πρωτοκόλλου), θα πρέπει να επισημάνουμε ότι ακόμη και αν μια κρυπτογραφική τεχνική είναι ασφαλής, η μη ορθή της χρήση είναι δυνατόν να αποκαλύψει κάποιες ευπάθειες, αρκετές για να τις εκμεταλλευτεί ένας επίδοξος εισβολέας.

Πρόσφατα μηνύματα και εκμετάλλευση παλαιών (freshness and replay): ένα πρωτόκολλο μπορεί να δεχθεί επιθέσεις υπό την έννοια της εκμεταλλεύσεως υπαρχόντων μηνυμάτων τα οποία παλαιότερα ήταν νόμιμα, όχι όμως και στην «τωρινή» φάση (freshness). Το κλασσικό αντίμετρο είναι η εγγύηση ότι το μήνυμα ανήκει στην τρέχουσα συναλλαγή (είναι δηλ. πρόσφατο) και δεν αποτελεί τμήμα μιας παλαιότερης συναλλαγής (replay). Αυτό επιτυγχάνεται με μια τυχαία τιμή, που επιλέγεται από τον παραλήπτη του μηνύματος, και αποστέλλεται στην οντότητα που αυθεντικοποιείται (αποστολέας) για να την συμπεριλάβει στην απάντησή της. Οι τιμές αυτές δεν απαιτούν συγχρονισμό μεταξύ των δύο οντοτήτων και είναι σαφώς πολύ ανθεκτικές και διαδεδομένες στο σχεδιασμό του κρυπτογραφικού πρωτοκόλλου.

Ψευδο-τερματικό (fake-terminal): εκείνα τα πρωτόκολλα τα οποία εκτελούν αυθεντικοποίηση προς μία μόνο κατεύθυνση, είναι πολύ ευαίσθητα σε επιθέσεις ψευδο-τερματικών. Ένα κλασικό παράδειγμα αποτελούν τα ATMs τα οποία βρίσκονται «κάπου» για να αυθεντικοποιούν τον πελάτη ο οποίος χρησιμοποιεί το PIN της κάρτας του. Ο πελάτης δεν γνωρίζει φυσικά κατά πόσον αυτό το τερματικό είναι νόμιμο ή ψεύτικο (για συγκέντρωση των PINs των πελατών). Πάντως, η χρήση κάποιας έξυπνης κάρτας ή ενός ηλεκτρονικού πορτοφολιού, βοηθούν στο να αποφευχθεί αυτό το είδος επιθέσεων.

Στην δεύτερη περίπτωση (επιθέσεις κατά του κρυπτοσυστήματος), γίνονται επιθέσεις στο κρυπτοσύστημα το οποίο χρησιμοποιείται από το σύστημα πληρωμών.

Ευθεία επίθεση (Brute force attack): ένα είδος ευθείας επιθέσεως είναι η δοκιμή κάθε πιθανού κλειδιού, προκειμένου να «σπάσει» το σύστημα. Συμπερασματικά θα μπορούσαμε να πούμε ότι το πεδίο τιμών από το οποίο επιλέγονται τα κλειδιά είναι καθοριστικό, αφού αν δεν είναι αρκετά μεγάλο, το αποτέλεσμα θα είναι δυσάρεστο για το ίδιο το σύστημα. Ακόμη όμως και σε μεγάλα πεδία τιμών, μπορεί να εκδηλωθούν επιθέσεις και με τη χρήση «λεξικών» (dictionaries) που κατέχει ο εισβολέας για εύκολη ανίχνευση των PINs που επιλέγουν οι χρήστες (user-defined).

Κρυπτανάλυση (Cryptanalysis): θεωρείται πιο επιτηδευμένη μέθοδος επιθέσεως για να εκμεταλλευθεί οποιαδήποτε αδυναμία του κρυπτοσυστήματος. Πολλά κρυπτοσυστήματα δεν είναι αποδεδειγμένα

ασφαλή, αλλά βασίζονται στην εμπειρία με αποτέλεσμα να είναι επιρρεπή στα σφάλματα.

Σε κάθε περίπτωση πάντως, για να «σπάσει» μια απλή κάρτα απαιτείται υλικό(κάποιων εκατοντάδων ή χιλιάδων ευρώ) και αρκετή εμπειρία. Από την πλευρά των παρανομούντων (crackers) αυτό σημαίνει μία επένδυση για όλες τις παράνομες στο μέλλον ενέργειές τους. Από την πλευρά των παθόντων όμως, η ζημιά η οποία μπορεί να προκληθεί, εξαρτάται από τα μέτρα τα οποία ελήφθησαν προκειμένου να αποφευχθεί μια επίθεση στο σύστημά τους: όσο καλύτερη επένδυση στη λύση ασφαλείας τόσο λιγότερες οι πιθανότητες επιτυχημένης επιθέσεως εναντίον του. Για να γίνει πιο συγκεκριμένο αυτό, θα αναφερθούμε στην περίπτωση των τραπεζών, όπου θα πρέπει οπωσδήποτε να υπάρχει μηχανισμός ανιχνεύσεως και αποκαλύψεως της πηγής που προκαλεί παράνομες διακινήσεις κεφαλαίων (ειδικά σε σημαντικούς λογαριασμούς) χωρίς βέβαια αυτό να προσβάλλει την ανωνυμία και μη ανιχνευσιμότητα των εντίμων πληρωτών.

3.3.8 Κίνδυνοι στο e-banking

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο, η συχνότητά τους τα τελευταία χρόνια αυξάνεται μια και όλο και περισσότερες τράπεζες παρέχουν στους πελάτες τους on-line υπηρεσίες. Η αύξηση αυτή δεν είναι τεράστια, εντούτοις όμως αποτελεί ένα ανησυχητικό φαινόμενο μια και πολλοί θεωρούν τις οικονομικές πληροφορίες που τους αφορούν άκρως απόρρητες και διατηρούν μια επιφυλακτική στάση απέναντι σε διαδικασίες που τις καθιστούν ευάλωτες στο ευρύ κοινό, όπως είναι το e-banking.

Στοιχεία για το ηλεκτρονικό έγκλημα δεν κοινοποιούνται δημοσίως, αλλά υπολογίζεται ότι στις Η.Π.Α. χάνονται ετησίως περίπου 11 δισεκατομμύρια δολάρια από εταιρείες και καταναλωτές λόγω αυτής της μορφής εγκλήματος. Το μεγαλύτερο μέρος προέρχεται από οικονομικά ιδρύματα. Μάλιστα το μεγαλύτερο μέρος των ζημιών δεν προκύπτει από τις κλοπές χρημάτων, αλλά από έξοδα που κάνουν οι εταιρείες μετά από τέτοιου είδους

επιθέσεις, προκειμένου να διασφαλίσουν τα συστήματά τους ώστε να μην ξανασυμβούν.

Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους πάντως να επιτύχουν τους σκοπούς τους. Παρά τις οποιεσδήποτε τεχνικές αδυναμίες των συστημάτων για online banking, οι μεγαλύτεροι κίνδυνοι προέρχονται από τον ανθρώπινο παράγοντα. Έρευνες που έχουν γίνει από ειδικούς σε θέματα ασφαλείας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είχαν την εκούσια ή ακούσια βοήθεια και κάποιου που εργαζόταν στην τράπεζα.

Οι εισβολείς, πάντως, μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι άνθρωποι αυτοί αποτελούν τους πιο προκλητικούς στόχους, μια και δεν έχουν συνείδηση του μεγέθους της ζημιάς που μπορούν να κάνουν ανοίγοντας απλά μια επισύναψη στο ηλεκτρονικό τους ταχυδρομείο ή ακολουθώντας ένα link. Οι απλοί χρήστες πέφτουν πολύ εύκολα θύματα προγραμμάτων που υποτίθεται ότι κάνουν κάτι χρήσιμο για αυτούς, αλλά στην πραγματικότητα ανοίγουν «τρύπες» ασφαλείας στο σύστημα επιτρέποντας σε χάκερς να έχουν πρόσβαση σε αυτό.

Οι κλεμμένες πληροφορίες αποτελούν την πρώτη φάση μιας αρκετά επίπονης διαδικασίας η οποία μπορεί να διαρκέσει μέχρι και εβδομάδες, έτσι ώστε ο χάκερ να υποδυθεί κάποιον άλλο στο διαδίκτυο, η οποία όμως διευκολύνεται συνεχώς με καινούρια προγράμματα που κυκλοφορούν στην αγορά. Η εποχή που πολλές επιθέσεις θα γίνονται με αυτοματοποιημένο τρόπο δεν απέχει πολύ, σύμφωνα με αρκετούς ειδικούς.

Μια άλλη μέθοδος που τις περισσότερες φορές έχει αποτελέσματα δεν επικεντρώνεται στην τράπεζα ευθέως, αλλά σε μια από τις εταιρείες που συνεργάζονται με αυτήν προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με τους πελάτες της. Σε πολλές περιπτώσεις οι τράπεζες επιτρέπουν στις εταιρείες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, ο εισβολέας θα πρέπει να μελετήσει τον τρόπο με τον οποίο οι εταιρείες επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία κάνουν την κίνησή τους.

Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν στον τομέα του e-banking εσπευσμένα προκειμένου να διατηρήσουν τον ανταγωνισμό με τις μεγαλύτερες τράπεζες. Δυστυχώς όμως λόγω αυτής της βιασύνης, οι τράπεζες αφήνουν πολλές «τρύπες» στα συστήματά τους, κάτι που οι επίδοξοι εισβολείς εκμεταλλεύονται πολύ εύκολα.

3.4 Μέτρα προστασίας για τα πληροφοριακά συστήματα

Παρότι οι πιο πάνω κίνδυνοι δημιουργούν μια εικόνα πολύ αρνητική και δύσκολη να αντιμετωπιστεί, στην πραγματικότητα μπορούν να περιοριστούν σημαντικά, αρκεί να δοθεί η κατάλληλη σημασία στην ασφάλεια του Η/Υ μας και να ληφθούν συγκεκριμένα μέτρα. Τα μέτρα που παρουσιάζονται πιο κάτω είναι βασισμένα και στις εισηγήσεις που δίνονται από τον οργανισμό CERT, που ειδικεύεται σε θέματα ασφαλείας στο διαδίκτυο.

3.4.1 Πρόληψη: προγράμματα antivirus-λογισμικό προστασίας από τους ιούς (antivirus software)

Θα αναφερθούμε στα πιο γνωστά και εύχρηστα προγράμματα αντιμετώπισης των ιών σε όποια μορφή και αν επιχειρήσουν να εισβάλλουν στον υπολογιστή. Σκουλήκια, Δούρειοι Ίπποι και επίδοξοι hackers θα δυσκολευτούν αρκετά αν υπάρχει εγκατεστημένο ένα από τα παρακάτω προγράμματα, που θα είναι σωστά ρυθμισμένο και θα ανανεώνεται συχνά.

MCAFEE VIRUSSCAN: Ένα από τα πιο διάσημα και πιο παλαιά εργαλεία για την αντιμετώπιση των ιών. Το McAfee έχει φτάσει ήδη στην έκδοση 7.0 στην οποία και ενσωματώνει χαρακτηριστικά που δύσκολα θα βρούμε αλλού. Μεταξύ αυτών, ξεχωρίζουν η δυνατότητα ελέγχου και προστασίας από τους ιούς 'όταν πραγματοποιείται συγχρονισμός μεταξύ PC και PDA, αλλά και το εξυπηρετικότατο HAWK (Hostile Activity Watch Kernel) που

αναλαμβάνει να παρακολουθεί διαρκώς όλες τις δραστηριότητες του υπολογιστή και να ξεχωρίζει τις πιθανές «παρανομίες».

NORTON ANTIVIRUS: Ο άλλος διάσημος της κατηγορίας και αγαπημένος πολλών Ελλήνων χρηστών παρουσιάζεται πλήρως εξοπλισμένος και στην έκδοση για το 2003. Το πρόγραμμα, εκτός από την προστασία που παρέχει για όλα τα είδη των ιών που μεταδίδονται μέσω mail, φροντίζει πλέον και για την προστασία του χρήστη από τη χρήση δημοφιλών εφαρμογών όπως το MSN Messenger, το Yahoo IM αλλά και των υπολοίπων εφαρμογών instant messaging. Παράλληλα, όπως και το McAfee, το Norton Antivirus ενσωματώνεται με τον πιο εύχρηστο τρόπο στις εφαρμογές ηλεκτρονικού ταχυδρομείου καθώς και στις εφαρμογές του MS Office, ενώ διαθέτει και ιδιαίτερα εξυπηρετικό (αν και κάπως αργό) live update.

SOPHOS ANTIVIRUS: Το πρόγραμμα με την καλύτερη μηχανή αναζήτησης για ιούς και με το καλύτερο εταιρικό site για όλους τους χρήστες που θέλουν να ενημερωθούν. Εκτός όμως από αυτά, το πρόγραμμα προσφέρεται περισσότερο για εταιρική χρήση, καθώς πολλές από τις λειτουργίες του ευνοούνται από το δικτυακό περιβάλλον.

ETRUST EZ ARMOR SUITE: Αξιόπιστο και οικονομικό. Το Etrust διαθέτει όλα σχεδόν τα απαραίτητα χαρακτηριστικά στην πιο χαμηλή τιμή.

F-SECURE ANTIVIRUS: Το πιο απλό ίσως πρόγραμμα της κατηγορίας και από τα πιο αποτελεσματικά. Αυτή βέβαια η απλότητα έχει χαρακτηριστεί από πολλούς το αδύνατο σημείο του προγράμματος που παρόλα αυτά διατηρεί φανατικούς οπαδούς.

PANDA ANTIVIRUS PLATINUM: Από τα προγράμματα με τα πιο εύχρηστα interface, το οποίο μάλιστα προσφέρεται ιδιαίτερα και για την εκμάθησή του. Χαρακτηριστικό του επίσης είναι οι φωνητικές (για κάποιους ενοχλητικές) ειδοποιήσεις και το σχετικά αρνητικό του σημείο που οφείλεται στο ότι δεν έχει εξ ορισμού ενεργοποιημένη την επιλογή για live update.

ΑΓΟΡΑ ΛΟΓΙΣΜΙΚΟΥ

ΟΝΟΜΑΣΙΑ	**WEB SITE**	**ΔΙΑΘΕΣΗ ΣΤΗΝ**	**ΤΙΜΗ**
McAfee Virus Scan 7.0	www.MacAfee-at-home.com	Interaxon, TopNet	26-29 €
Norton Antivirus 2003	www.symantec.com	Orthology Consulting, Πουλιάδης	35-38.5 €
Kaspersky Antivirus	www.kaspersky.com	Online	50.5 €
Command Antivirus	www.commandsoftware.com	Online	19.95 €
Bit Defender ProEdition	www.bitdefender.com	TopNet	39 €
AVG 6.0	www.grisoft.com	Online	39.95 €
Etrust EZ Amor Suite	www.my-etrust.com	Online	19 €
F-Secure AntiVirus	www.f-secure.com	Enter Engineering	117 €
Sophos AntiVirus	www.sophos.com	Oktabit	164 €
Norman Virus Control 5.2	www.norman.com	Γεννάδιος	60 €
Panda AntiVirus Platinum	www.pandasecurity.com	Panda Software	45.5 €

3.4.2 Άγνωστα συνημμένα αρχεία και προγράμματα σε ηλεκτρονικά μηνύματα (attachments)

Οι ιοί αρέσκονται στο να δημιουργούν αυτομάτως πληθώρα ηλεκτρονικών διευθύνσεων από τη λίστα διευθύνσεων (e-mail address

book) ενός χρήστη που έχει μολυνθεί και να στέλνουν σε όλους τους φίλους και γνωστούς με τους οποίους αυτός επικοινωνεί. Το κείμενο που περιέχεται στο e-mail με το μολυσμένο attachment, πολλές φορές είναι γνώριμο στον παραλήπτη, οδηγώντας τον στο να ανοίξει το επισυναπτόμενο αρχείο χωρίς να υποψιαστεί τίποτα. Στις περισσότερες δε εγκαταστάσεις προγραμμάτων ηλεκτρονικού ταχυδρομείου, οι χρήστες έχουν το πρόγραμμα ρυθμισμένο έτσι που να εκτελεί τα attachments (αν είναι εκτελέσιμα αρχεία, δηλαδή προγράμματα) ή να εκκινεί τη σχετική εφαρμογή αν είναι αρχεία (π.χ. αν το attachment είναι ένα έγγραφο του MS Word, να εκκινεί το Word). Αυτή η λειτουργία είναι υπεύθυνη για τη μεγαλύτερη διακίνηση ιών, καθώς ο χρήστης δεν προλαβαίνει να ελέγξει αν το αρχείο που του έχει έρθει είναι μολυσμένο ή όχι. Βασική, λοιπόν, προφύλαξη είναι η απενεργοποίηση της συγκεκριμένης λειτουργίας, όσο κι αν κάτι τέτοιο μπορεί να είναι κάπως άβολο. Αξίζει να αναφερθεί εδώ ότι με τον τελευταίο τρόπο λειτουργούν οι ιοί τύπου Melissa, που δεν μεταφέρονται μέσα από εκτελέσιμα αρχεία, αλλά μέσα από αρχεία άλλων εφαρμογών (οι λεγόμενοι ιοί μακροεντολών που ενσωματώνονται σε ένα φύλλο εργασίας του Excel ή σε ένα έγγραφο του Word).

Προτού, λοιπόν, ανοίξουμε οποιοδήποτε αρχείο και προτού τρέξουμε οποιοδήποτε πρόγραμμα λαμβάνουμε συνημμένο σε μήνυμα ηλεκτρονικού ταχυδρομείου θα πρέπει να το εξετάζουμε με λεπτομέρεια, έστω και αν φαίνεται ότι προέρχεται από γνωστό πρόσωπο:

α) Ελέγχουμε το αρχείο με ένα ενημερωμένο (updated) πρόγραμμα προστασίας από ιούς.

β) Επιβεβαιώνουμε, αν είναι δυνατό, ότι ο φερόμενος ως αποστολέας πράγματι έχει στείλει το συνημμένο αρχείο ή πρόγραμμα.

γ) Δεν τρέχουμε προγράμματα που προέρχονται από άγνωστες πηγές (άτομα ή εταιρείες).

3.4.3 Έλεγχος με το πρόγραμμα Antivirus κάθε νέας δισκέτας ή CD πριν από τη χρήση

Παρά τη διάδοση των ιών μέσω ηλεκτρονικού ταχυδρομείου, και οι παραδοσιακοί τρόποι δεν υστερούν καθόλου σε αποτελεσματικότητα. Η μόλυνση από δισκέτα ή από cd δεν διαφέρει καθόλου σε συμπτώματα και η λύση είναι μία, δηλαδή ο έλεγχος κάθε δισκέτας και cd που πρόκειται να διαβάσει το μηχάνημα. Σύμφωνα με μελέτες ένα ποσοστό 25% των δισκετών και των cd με πειρατικό λογισμικό έχει μολυνθεί με ιούς.

3.4.4 Cookies και Web tracking

Ένα θεμελιώδες θέμα ασφαλείας συνίσταται στη διαφύλαξη του προσωπικού απορρήτου, το οποίο πλέον αποτελεί ένα ακανθώδες ζήτημα στο Internet. Ένας μεγάλος όγκος πληροφοριών μπορεί να συλλεχθεί σχετικά με τους χρήστες του δικτύου και πολλές φορές δεν είναι ξεκάθαρο ποιος ή με ποιο τρόπο θα χρησιμοποιήσει αυτές τις πληροφορίες. Συγκεκριμένα, δύο από τις σημαντικότερες τεχνολογίες που σχετίζονται με το θέμα είναι : α) τα cookies και β) το Web tracking.

Μέσω των Internet passports, διασφαλίζεται το προσωπικό απόρρητο του χρήστη, ενώ ταυτόχρονα επιτρέπεται στα Web sites να συλλέγουν πληροφορίες που χρειάζονται για να προσφέρουν εξειδικευμένες υπηρεσίες στους επισκέπτες τους. Η πιο κοινή χρήση των δεδομένων αυτών είναι η «διευκόλυνση» της εισόδου των χρηστών σε Web sites που ζητούν όνομα χρήστη και password.

Το cookie που βρίσκεται στο σκληρό δίσκο περιλαμβάνει το όνομα του χρήστη και τα password, με αποτέλεσμα να μη χρειάζεται να δηλώνονται κάθε φορά, αφού τα στέλνει στον server και ο χρήστης εισέρχεται στο site ελεύθερα. Τα cookies μπορεί να περιλαμβάνουν σχεδόν κάθε είδος πληροφοριών, όπως την τελευταία φορά που ένας χρήστης επισκέφθηκε κάποιο site, τα αγαπημένα του sites και άλλες παρόμοιες πληροφορίες. Μπορούν, επίσης, να χρησιμοποιηθούν για την παρακολούθηση των χρηστών όσο βρίσκονται σε κάποιο site και τη συλλογή πληροφοριών σχετικών με τις σελίδες που προτιμούν να επισκέπτονται.

Εκτός από τα cookies, υπάρχουν και άλλες μέθοδοι παρακολούθησης του τρόπου με τον οποίο οι χρήστες χρησιμοποιούν ένα Web site. Μία από αυτές προτείνει τη λεπτομερή εξέταση του ημερολογίου λειτουργίας του Web server. Η εξέταση αυτή επιτρέπει τον προσδιορισμό των δημοφιλέστερων σελίδων των sites που μόλις επισκέφτηκαν οι χρήστες, του αριθμού των σελίδων που διαβάζουν σε μία τυπική επίσκεψη και άλλων σχετικών πληροφοριών.

Άλλες μέθοδοι στηρίζονται στη χρήση ορισμένων προγραμμάτων λογισμικού, ονόματι sniffers, τα οποία εξετάζουν κάθε πακέτο που εισέρχεται ή εξέρχεται από ένα Web site.

Για τη διαφύλαξη του ιδιωτικού απορρήτου έχουν αναπτυχθεί αρκετές τεχνολογίες και πρότυπα. Σε αυτά περιλαμβάνονται τα Platform for Privacy Preferences (P3P), Internet Content and Exchange standard (ICE) και Open Profiling Standard (OPS). Οι τεχνολογίες αυτές ονομάζονται γενικά Internet passports. Τα Internet passports επιτρέπουν στους χρήστες να ελέγχουν ποιες προσωπικές πληροφορίες θα γίνουν διαθέσιμες στα Web sites, καθώς και τον τρόπο με τον οποίο αυτά θα τις χρησιμοποιήσουν. Επιτρέπουν, επίσης, στους χρήστες να ελέγχουν το είδος των πληροφοριών που θα συλλέξει το site κατά τη διάρκεια της πλοήγησής τους και το πώς θα τις χρησιμοποιήσει.

3.4.5 Εξειδικευμένο σύστημα προστασίας – Firewall

Είναι γεγονός ότι οι διάφοροι "hackers" αναζητούν αδιάκοπα τρόπους και μεθόδους προσβολής της ασφάλειας των υπολογιστών που είναι συνδεδεμένοι στο διαδίκτυο. Για το λόγο αυτό ενδείκνυται πάντοτε η χρήση εξειδικευμένου συστήματος προστασίας, γνωστού ως "firewall". Το σύστημα αυτό μπορεί να εγκατασταθεί στον Η/Υ σας ή να παρεμβληθεί μεταξύ του Η/Υ σας και του διαδικτύου και ελέγχει όλη την κίνηση από και προς το διαδίκτυο για τυχόν παράνομες επιθέσεις.

Τα firewalls αποτελούν συνδυασμούς hardware και software και συντίθεται χρησιμοποιώντας routers, servers και μια ποικιλία λογισμικού,

τοποθετούνται δε στο πιο εμπαθές σημείο μεταξύ του δικτύου και του Internet και μπορεί να είναι από απλά ως εξαιρετικά πολύπλοκα συστήματα. Υπάρχουν πολλά είδη firewalls, τα περισσότερα εκ των οποίων διαθέτουν κάποια κοινά χαρακτηριστικά. Ένα από τα απλούστερα είδη των firewalls χρησιμοποιεί την τεχνική του φιλτραρίσματος των πακέτων. Στην περίπτωση αυτή ένας router εξετάζει την επικεφαλίδα κάθε πακέτου δεδομένων που ταξιδεύει μεταξύ του Internet και του επιχειρησιακού δικτύου. Οι επικεφαλίδες αυτές διαθέτουν πληροφορίες όπως την IP διεύθυνση του αποστολέα και του παραλήπτη και το πρωτόκολλο που χρησιμοποιείται για την αποστολή. Βασιζόμενος σε αυτές τις πληροφορίες, ο router γνωρίζει το είδος της Internet υπηρεσίας που χρησιμοποιείται για την αποστολή των δεδομένων καθώς και την ταυτότητα του αποστολέα και του παραλήπτη των δεδομένων. Αφού διευκρινιστούν αυτές οι πληροφορίες ο router μπορεί να εμποδίσει την αποστολή ορισμένων πακέτων μεταξύ του Internet και του προσωπικού υπολογιστή. Για παράδειγμα, ο router θα μπορούσε να μπλοκάρει όλη την κίνηση εκτός του ηλεκτρονικού ταχυδρομείου. Επιπροσθέτως, θα μπορούσε να μπλοκάρει την κίνηση από και προς κάποιες ύποπτες τοποθεσίες ή από ορισμένους χρήστες. Οι proxy servers χρησιμοποιούνται αρκετά συχνά στα firewalls. Ένας proxy server είναι λογισμικό σε επίπεδο server, το οποίο τρέχει σε έναν host σε ένα firewall και παίζει το ρόλο του οχυρού.

Στην περίπτωση αυτή μόνο ο proxy server αλληλεπιδρά με το Internet (και όχι μεμονωμένα οι ανεξάρτητοι υπολογιστές του δικτύου) και ως εκ τούτου μπορούν να παρακολουθήσουν καλύτερα τα θέματα ασφαλείας. Είναι σαφώς ευκολότερο να κρατήσει ο χρήστης ασφαλή τον εν λόγω server παρά τους εκατοντάδες, σε ορισμένες περιπτώσεις, ανεξάρτητους υπολογιστές του δικτύου. Όταν κάποιος χρήστης του επιχειρησιακού δικτύου θέλει να έχει πρόσβαση σε έναν server στο Internet, στέλνει μια αίτηση από τον υπολογιστή του στον proxy server, εν συνεχεία ο proxy server έρχεται σε επαφή με τον server του Internet και τέλος, ο proxy server στέλνει τις πληροφορίες από τον Internet server στον υπολογιστή του επιχειρησιακού δικτύου. Συνεπώς, ο proxy server δρα ως ενδιάμεσος, προσφέροντας μεγαλύτερη ασφάλεια και καταγράφοντας όλη την κίνηση μεταξύ του Internet και του επιχειρησιακού δικτύου.

3.4.6 PGP

Το ασφαλέστερο και πιο διαδεδομένο πρόγραμμα για την προστασία της ηλεκτρονικής αλληλογραφίας μας ονομάζεται Pretty Good Privacy (PGP). Αναπτύχθηκε από τον Phil Zimmermann και σήμερα κυκλοφορεί σε δύο εκδόσεις, μία που διανέμεται ελεύθερα στο δίκτυο ως freeware και μια που διατίθεται εμπορικά από τη Network Associates, την εταιρεία που παράγει το γνωστό McAfee antivirus.

3.4.7 Έλεγχος του λογισμικού προς εγκατάσταση (ακόμα και από επίσημες πηγές)

Δεν πρέπει να φέρνουμε στον υπολογιστή μας προγράμματα αν δεν είναι από έμπιστες πηγές. Και όταν λέμε «έμπιστες πηγές» εννοούμε κεντρικά sites (τύπου TUCOWS) τα οποία έχουν σοβαρό λόγο να ελέγχουν τα προγράμματα που διαθέτουν ήτα ίδια τα sites των κατασκευαστών των προγραμμάτων. Οι πιθανότητες να είναι προσβεβλημένο από ιό είναι πολύ λιγότερες στο επίσημο site της εταιρείας. Σε κάθε περίπτωση όμως, θα πρέπει να ελέγχεται, όπου αυτό είναι δυνατό, και το λογισμικό από επίσημες πηγές (licensed CDs). Δεν είναι λίγες οι περιπτώσεις «επιδρομών» σε επίσημα sites μεγάλων εταιρειών. Επίσης, όπου υπάρχει ψηφιακή υπογραφή του λογισμικού, αν είναι δυνατόν ελέγχουμε την ψηφιακή υπογραφή του αντιγράφου με εκείνη που δίνει ο κατασκευαστής του λογισμικού.

3.5 Ασφάλεια συναλλαγών

Λόγω του αυξανόμενου ενδιαφέροντος επιχειρήσεων για την πραγματοποίηση παραγγελιών και πληρωμών μέσα από το δίκτυο, η ασφάλεια των συναλλαγών είναι σήμερα αντικείμενο έντονης συζήτησης. Βασική προϋπόθεση για την τελική επιτυχία του ηλεκτρονικού εμπορίου είναι η εμπιστοσύνη των πελατών στην αξιοπιστία και την προστασία των

συναλλαγών από κάθε κίνδυνο υποκλοπής ή παραποίησης. Πράγματι, η έλλειψη εμπιστοσύνης στην ασφάλεια δημόσιων δικτύων, όπως το Internet αποτελεί τον μεγαλύτερο φραγμό για μια μεγάλης κλίμακας αποδοχή του ηλεκτρονικού εμπορίου από τον κόσμο των επιχειρήσεων.

Η αβεβαιότητα σε θέματα ασφάλειας κάνει τους καταναλωτές να διστάζουν να δώσουν πληροφορίες πληρωμών, όπως αριθμούς πιστωτικών καρτών, μέσα από το Internet. Η αστική ευθύνη (πραγματική ή φανταστική) των προμηθευτών σε περίπτωση υποκλοπής τέτοιων πληροφοριών από "κατασκοπευτικά" προγράμματα που μπορούν να διεισδύσουν σε οποιονδήποτε ενδιάμεσο κόμβο του δικτύου, κάνει επίσης πολλές επιχειρήσεις απρόθυμες να προχωρήσουν στην πραγματοποίηση πωλήσεων μέσα από το Internet. Έτσι, τόσο για να μετριαστούν οι φόβοι προμηθευτών και πελατών, όσο και για να προστατευτούν αποτελεσματικά οι ευαίσθητες πληροφορίες που μεταδίδονται από δημόσια δίκτυα, έχει αυξηθεί το ενδιαφέρον για θέματα προστασίας των συναλλαγών, εξακρίβωσης της αυθεντικότητας των μηνυμάτων, αλλά και προστασίας της ανωνυμίας.

Τα κύρια προβλήματα ασφάλειας, που συνδέονται με το ηλεκτρονικό εμπόριο, είναι τα εξής:

Διακριτικότητα: Η δυνατότητα προστασίας των πληροφοριών από μη εξουσιοδοτημένους χρήστες.

Αυθεντικότητα: Η δυνατότητα επιβεβαίωσης της ταυτότητας των δυο πλευρών που επικοινωνούν.

Γνησιότητα: Η προστασία των πληροφοριών από παραποίηση κατά τη μετάδοση ή την αποθήκευση.

Διαθεσιμότητα: Η δυνατότητα πρόβλεψης του χρόνου κατά τον οποίο οι πληροφορίες και οι υπηρεσίες είναι (ή δεν είναι) διαθέσιμες.

Αποκλεισμός: Η δυνατότητα αποφυγής ανεπιθύμητων πληροφοριών ή ανεπιθύμητης επικοινωνίας.

Από τα προβλήματα αυτά, τα τρία πρώτα (διακριτικότητα, αυθεντικότητα και γνησιότητα) αποτελούν τα κύρια εμπόδια για την ευρύτερη διάδοση και αποδοχή του ηλεκτρονικού εμπορίου.

3.5.1 Διακριτικότητα των συναλλαγών

Μέχρι σήμερα δεν υπάρχει καμία πραγματική εγγύηση για το ότι τα μηνύματα που ανταλλάσσονται μέσα από το Internet δεν μπορούν να υποκλαπούν ή ακόμη και να παραποιηθούν από κάποιον που έχει πρόσβαση σε έναν ενδιάμεσο κόμβο της διαδρομής τους από τον αποστολέα ως τον παραλήπτη. Η απειλή αυτή ονομάζεται "μη εξουσιοδοτημένη παρακολούθηση του δικτύου" ή απλά "υποκλοπή πακέτων".

Η παράνομη υποκλοπή πληροφοριών από δίκτυα επικοινωνίας δεν είναι κάτι καινούριο, αλλά η φύση του Internet μεγεθύνει το πρόβλημα. Αν κάποιος αποκτήσει πρόσβαση σε κόμβο που ανήκει στις κεντρικές αρτηρίες του δικτύου, μπορεί να υποκλέψει σχεδόν κάθε επικοινωνία. Επίσης, ένας κόμβος μπορεί να υποκλέπτεται συγχρόνως από πολλούς, χωρίς αυτό να έχει ορατή επίπτωση στην απόδοση του κόμβου. Αν αυτό που θα υποκλαπεί είναι το κλειδί (password) πρόσβασης στο δίκτυο ενός χρήστη, οι επόμενες υποκλοπές μπορούν να γίνουν με νόμιμο τρόπο και με απεριόριστη πρόσβαση στις πληροφορίες του συγκεκριμένου χρήστη.

3.5.2 Απόρρητο των συναλλαγών

Το ηλεκτρονικό εμπόριο πρέπει να εξασφαλίζει το απόρρητο όλων των πληροφοριών που διακινούνται. Μετά την άφιξή τους στον κόμβο προορισμού οι πληροφορίες πρέπει να αφαιρούνται από το δημόσιο δίκτυο, αφήνοντας ίσως μόνο κάποια στοιχεία που αποδεικνύουν την πραγματοποίηση της μετάδοσης. Η αρχειοθέτηση των πληροφοριών από τον προμηθευτή πρέπει να γίνεται σε απόλυτα προστατευμένα συστήματα, και πρέπει να υπάρχει πρόβλεψη για την αυτόματη καταστροφή, σε περίπτωση έκτακτης ανάγκης, των μηνυμάτων που εκκρεμούν.

Το απόρρητο είναι ένας πολύ σημαντικός παράγοντας για συναλλαγές που περιλαμβάνουν ευαίσθητα Δεδομένα, όπως αριθμούς πιστωτικών καρτών, και θα γίνει ακόμη σημαντικότερος όταν αρχίσουν να κυκλοφορούν

στο δίκτυο πληροφορίες όπως στοιχεία εργαζομένων, αριθμοί κοινωνικής ασφάλισης, κτλ.

Τα δημόσια δίκτυα και οι ασύρματοι κόμβοι επιδεινώνουν το πρόβλημα της υποκλοπής των δεδομένων που μεταδίδονται. Η μόνη λύση για την προστασία του απορρήτου των μηνυμάτων είναι η κρυπτογράφησή τους, που διασφαλίζει το απόρρητο του περιεχομένου ακόμη και αν από τεχνική άποψη το μήνυμα υποκλαπεί.

3.5.3 Γνησιότητα των συναλλαγών

Για την πραγματοποίηση ηλεκτρονικών συναλλαγών απαιτείται επίσης η προστασία του περιεχομένου των μηνυμάτων από κάθε παραποίηση στη διαδρομή μεταξύ αποστολέα και παραλήπτη. Ο τρόπος κωδικοποίησης πρέπει να εξασφαλίζει ότι κανείς δεν μπορεί να προσθέσει, να αφαιρέσει ή να αλλάξει οτιδήποτε στο περιεχόμενο του μηνύματος κατά τη μετάδοση. Δεν πρέπει να είναι δυνατή η εξαπάτηση της μιας ή της άλλης πλευράς από κάποιον που μπόρεσε να παραποιήσει το μήνυμα σε έναν ενδιάμεσο κόμβο.

Ενώ η εμπιστευτικότητα της επικοινωνίας αφορά την προστασία του περιεχομένου από άτομα που δεν είναι εξουσιοδοτημένα να το γνωρίζουν, η γνησιότητα αφορά την προστασία του περιεχομένου των μηνυμάτων από κάθε τροποποίηση στη διάρκεια της μετάδοσης. Υπάρχουν διάφορες τεχνικές για την εξασφάλιση της γνησιότητας μηνυμάτων, όπως η αρίθμηση, η προσθήκη κωδικών ελέγχου, και διάφορες τεχνικές κρυπτογράφησης. Οι κωδικοί ελέγχου μπορούν να προστατεύουν το σύνολο του μηνύματος ή κάποια επιλεγμένα πεδία. Η αρίθμηση των μηνυμάτων επιτρέπει τη διατήρηση της αρχικής σειράς των μηνυμάτων και την ανίχνευση της απώλειας μηνυμάτων ή της παρεμβολής μη γνήσιων μηνυμάτων. Οι τεχνικές κρυπτογράφησης και αποκρυπτογράφησης μπορούν επίσης να ανιχνεύσουν τις μη εξουσιοδοτημένες αλλαγές στο περιεχόμενο ενός μηνύματος.

3.5.4 Κρυπτογράφηση

Οι ευαίσθητες πληροφορίες που κυκλοφορούν σε δημόσια δίκτυα μπορούν να προστατευτούν με την κρυπτογράφησή τους, δηλαδή με τη γραφή τους σε κάποιο σύστημα συμβόλων ακατανόητο για οποιονδήποτε τις υποκλέψει. Η κρυπτογράφηση ψηφιακών πληροφοριών γίνεται με την εφαρμογή κάποιων πολύπλοκων μαθηματικών πράξεων στο ψηφιακό περιεχόμενό τους. Στις πράξεις αυτές χρησιμοποιείται ένα "κλειδί", που είναι ένας πάρα πολύ μεγάλος αριθμός (αποθηκευμένος επίσης ψηφιακά). Η αντιστροφή της κρυπτογράφησης, δηλαδή η αποκρυπτογράφηση, γίνεται με κάποιες άλλες μαθηματικές πράξεις, στις οποίες πρέπει να χρησιμοποιηθεί το ίδιο ή κάποιο συμπληρωματικό "κλειδί".

Σήμερα υπάρχουν δυο κύριες μέθοδοι κρυπτογράφησης. Η παλιότερη χρησιμοποιεί για κρυπτογράφηση και αποκρυπτογράφηση το ίδιο κλειδί, που πρέπει να διατηρείται μυστικό. Η νεότερη χρησιμοποιεί ένα ζευγάρι από συμπληρωματικά κλειδιά, από τα οποία το ένα είναι μυστικό ενώ το άλλο είναι δημόσιο.

3.5.4.1 Κρυπτογράφηση με μυστικό κλειδί

Η κρυπτογράφηση με μυστικό κλειδί, που ονομάζεται επίσης συμμετρική κρυπτογράφηση, χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ενός μηνύματος. Αποστολέας και παραλήπτης πρέπει να έχουν το ίδιο μυστικό κλειδί για να μπορέσουν να επικοινωνήσουν.

Η κρυπτογράφηση με μυστικό κλειδί λειτουργεί ως εξής:

- Δυο επιχειρήσεις που πρέπει να επικοινωνήσουν μοιράζονται εκ των προτέρων ένα κοινό μυστικό κλειδί.
- Η πρώτη επιχείρηση κρυπτογραφεί το μήνυμα με το κοινό μυστικό κλειδί. Το μήνυμα μετατρέπεται σε μια σειρά από ακατανόητα σύμβολα.
- Το μήνυμα μεταδίδεται κανονικά στη δεύτερη επιχείρηση. Ακόμη και αν κάποιος το υποκλέψει δεν θα μπορέσει να το διαβάσει (εκτός αν έχει επίσης υποκλέψει το μυστικό κλειδί).

- Η δεύτερη επιχείρηση λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το κοινό μυστικό κλειδί.

Ένα σημαντικό πρόβλημα της μεθόδου αυτής είναι ότι το κλειδί πρέπει να είναι γνωστό στα δυο μέρη πριν ξεκινήσει η επικοινωνία. Επίσης, αν η πρώτη επιχείρηση θέλει να επικοινωνήσει με κάποια τρίτη θα πρέπει να χρησιμοποιήσει άλλο κλειδί, διαφορετικά η δεύτερη επιχείρηση θα είναι σε θέση να υποκλέψει την επικοινωνία (αφού γνωρίζει ήδη το κλειδί από την προηγούμενη επικοινωνία). Πρακτικά, για κάθε νέα επικοινωνία πρέπει να παράγεται ένα νέο κλειδί, που πρέπει να μεταδοθεί με κάποιον ασφαλή τρόπο, αλλά η επικοινωνία δεν μπορεί να είναι ασφαλής πριν από τη μετάδοση του κλειδιού - μια τυπική περίπτωση φαύλου κύκλου.

Η κρυπτογράφηση με μυστικό κλειδί χρησιμοποιεί τη μέθοδο DES που είναι ευρύτατα αποδεκτή.

3.5.4.2 Κρυπτογράφηση με δημόσιο κλειδί

Η κρυπτογράφηση με δημόσιο κλειδί, που ονομάζεται επίσης ασύμμετρη κρυπτογράφηση, αναπτύχθηκε (μεταξύ άλλων) ως λύση στο πρόβλημα της διανομής των κλειδιών κρυπτογράφησης, που δημιουργεί τον παραπάνω φαύλο κύκλο. Η μέθοδος αυτή χρησιμοποιεί δυο κλειδιά: ένα για την κρυπτογράφηση και ένα διαφορετικό για την αποκρυπτογράφηση. Τα δυο κλειδιά έχουν μια ιδιαίτερη μαθηματική σχέση μεταξύ τους, ώστε το καθένα από τα δυο να μπορεί να αποκρυπτογραφήσει μόνο πληροφορίες που έχουν κρυπτογραφηθεί με το άλλο. Η πρώτη μορφή κρυπτογράφησης με δημόσιο κλειδί (PKE - Public Key Encryption) είναι η μέθοδος PGP (Pretty Good Privacy) που αναπτύχθηκε από τον Robert Zimmerman. Η δημοσίευσή της προκάλεσε μια θύελλα αντιδράσεων, καθώς άνοιξε το "κουτί της Πανδώρας" στο πεδίο των συστημάτων ισχυρής κρυπτογράφησης, που μέχρι τότε ήταν αυστηρή αποκλειστικότητα των μυστικών υπηρεσιών.

Σε αντίθεση με την παλιότερη μέθοδο, η κρυπτογράφηση με δημόσιο κλειδί απαιτεί για την επικοινωνία δυο ζεύγη κλειδιών, ένα για κάθε πλευρά. Ένα από τα κλειδιά κάθε ζεύγους είναι μυστικό και ένα είναι δημόσιο,

δηλαδή μπορεί να μεταδοθεί στην άλλη πλευρά χωρίς κίνδυνο (στην πραγματικότητα όλα τα δημόσια κλειδιά θα μπορούσαν κυριολεκτικά να δημοσιευτούν σε μια μορφή τηλεφωνικού καταλόγου).
Η κρυπτογράφηση με δημόσιο κλειδί λειτουργεί ως εξής:

- Πριν από την έναρξη της επικοινωνίας κάθε πλευρά δίνει στην άλλη το δημόσιο κλειδί της.
- Η πρώτη επιχείρηση κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί της δεύτερης επιχείρησης. Το μήνυμα μετατρέπεται σε μια σειρά από ακατανόητα σύμβολα.
- Το μήνυμα μεταδίδεται κανονικά στη δεύτερη επιχείρηση. Ακόμη και αν κάποιος το υποκλέψει δεν θα μπορέσει να το διαβάσει (παρά μόνο αν γνωρίζει το μυστικό κλειδί της δεύτερης επιχείρησης).
- Η δεύτερη επιχείρηση λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το μυστικό της κλειδί. Το κλειδί αυτό είναι γνωστό μόνο στην ίδια (δεν υπάρχει ανάγκη να δοθεί σε κανέναν άλλο) και έτσι μόνο η δεύτερη επιχείρηση (παραλήπτης) μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί της.

3.5.5 Προβλήματα εξαγωγής της κρυπτογράφησης

Αρκετές κυβερνήσεις διατηρούν νομοθετικές ρυθμίσεις που απαγορεύουν την εισαγωγή ή την εξαγωγή συστημάτων κρυπτογράφησης. Για παράδειγμα οι Η.Π.Α. θέτουν περιορισμούς στην εξαγωγή συστημάτων κρυπτογράφησης, επειδή τα εντάσσουν στα πολεμικά υλικά. Γενικά η κυβέρνηση των Ηνωμένων Πολιτειών επιτρέπει την εξαγωγή κρυπτογράφησης στις εξής περιπτώσεις: όταν τα δεδομένα έχουν οικονομική φύση και η συναλλαγή γίνεται μεταξύ γνωστών τραπεζών, όταν το περιεχόμενο των δεδομένων είναι αυστηρά ορισμένο, όταν το μήκος των δεδομένων είναι περιορισμένο, και όταν η μέθοδος κρυπτογράφησης δεν μπορεί να χρησιμοποιηθεί εύκολα για άλλους σκοπούς. Η εξαγωγική νομοθεσία μπορεί να είναι εξαιρετικά πολύπλοκη, καθώς πρέπει να θεωρεί πολλαπλούς παράγοντες. Επιπλέον η τεχνολογία της κρυπτογράφησης είναι

ένα ταχύτατα εξελισσόμενο πεδίο και οι νόμοι πολλές φορές αλλάζουν. Ερωτήματα σχετικά με τη δυνατότητα εξαγωγής κάθε συγκεκριμένης εφαρμογής πρέπει να απευθύνονται στο αρμόδιο νομικό συμβούλιο.

Στην Ευρώπη τα κράτη μέλη της Ευρωπαϊκής Ένωσης έχουν διαφορετικούς νόμους σχετικά με τη διακίνηση κρυπτογραφημένων πληροφοριών. Μερικές χώρες (π.χ. Βρετανία και Φινλανδία) έχουν πολύ φιλελεύθερη νομοθεσία, ενώ άλλες (π.χ. Γαλλία) απαγορεύουν τη μετάδοση κρυπτογραφημένων πληροφοριών σε δημόσια δίκτυα. Ειδικά η Γαλλία όμως (μαζί με αρκετές άλλες χώρες) δείχνει να διαπιστώνει ότι θα πρέπει να εκσυγχρονίσει τη νομοθεσία της στο σημείο αυτό, για να μη βρεθεί σε οικονομικά μειονεκτική θέση. Παράλληλα η Ευρωπαϊκή Ένωση αναπτύσσει προτάσεις εναρμονισμού της νομοθεσίας των χωρών μελών, όχι μόνο στο πεδίο της κρυπτογράφησης αλλά και σε θέματα όπως ο φόρος προστιθέμενης αξίας, που θα ευνοήσουν τη διεθνοποίηση των συναλλαγών και την πρόοδο του ηλεκτρονικού εμπορίου.

3.5.6 Αυθεντικότητα: ψηφιακές υπογραφές

Από τη στιγμή που το περιεχόμενο του μηνύματος προστατεύεται, μένει να εξακριβωθεί η ταυτότητα του αποστολέα του μηνύματος. Ο αποστολέας μπορεί να συμπεριλάβει στο μήνυμα ένα κείμενο κωδικοποιημένο με το δικό του μυστικό κλειδί. Αν ο παραλήπτης μπορέσει να αποκρυπτογραφήσει το κομμάτι αυτό με το δημόσιο κλειδί του αποστολέα, θα βεβαιωθεί αυτόματα για την αυθεντικότητα της ταυτότητας του αποστολέα. Το ειδικό αυτό τμήμα του μηνύματος, που κωδικοποιείται με το μυστικό κλειδί του αποστολέα και μπορεί να αποκρυπτογραφηθεί μόνο με το δημόσιο κλειδί του, ονομάζεται ψηφιακή υπογραφή.

3.5.7 Πιστοποίηση της ταυτότητας

Η επιβεβαίωση της ταυτότητας του αποστολέα μπορεί να ενισχυθεί ακόμη περισσότερο με τη χρήση ειδικών ψηφιακών πιστοποιητικών, που μπορούν να ελεγχθούν πριν από την έναρξη της επικοινωνίας. Για παράδειγμα, πριν ξεκινήσει η επικοινωνία καθένα από τα δυο μέρη πρέπει να εξασφαλίσει ότι το δημόσιο κλειδί που του έχει δοθεί ανήκει πράγματι στο άλλο μέρος.

Η λύση στο πρόβλημα αυτό είναι να υπάρχει κάποιο αξιόπιστο τρίτο μέρος, συνήθως κάποιος οργανισμός, που μπορεί να εγγυηθεί την ταυτότητα των δυο συναλλασσόμενων. Ένας τέτοιος οργανισμός ονομάζεται Αρχή Πιστοποίησης (CA - Certificate Authority) και μπορεί να είναι μια τράπεζα, ένα επιμελητήριο, ή άλλος αντίστοιχος οργανισμός. Τα δυο μέρη μπορούν να εγγραφούν σε μια Αρχή Πιστοποίησης, η οποία δημιουργεί για το καθένα ένα ειδικό ψηφιακό μήνυμα που περιέχει το όνομα και το δημόσιο κλειδί του. Το μήνυμα αυτό, που ονομάζεται ψηφιακό πιστοποιητικό, δίνεται σε κάθε ενδιαφερόμενο, κρυπτογραφημένο με το γνωστό σε όλους δημόσιο κλειδί της Αρχής Πιστοποίησης. Έτσι, χρησιμοποιώντας ένα μόνο ευρύτατα γνωστό και αξιόπιστο δημόσιο κλειδί (αυτό της Αρχής Πιστοποίησης) καθένα από τα δυο μέρη μπορεί να εξακριβώσει πέρα από κάθε αμφιβολία την ταυτότητα του άλλου και να έχει μια ασφαλή επικοινωνία μαζί του.

Τα ψηφιακά πιστοποιητικά είναι η καρδιά των ασφαλών ηλεκτρονικών συναλλαγών. Μέσα από τη λειτουργία ενός αξιόπιστου οργανισμού πιστοποίησης γίνεται δυνατή η εξασφάλιση της αμοιβαίας εμπιστοσύνης μεταξύ των δυο μερών μιας συναλλαγής. Για παράδειγμα, ο οργανισμός πιστωτικών καρτών VISA εκδίδει ψηφιακά πιστοποιητικά για όλες τις τράπεζες που έχουν δικαίωμα να χορηγούν κάρτες VISA, οι οποίες με τη σειρά τους εκδίδουν ψηφιακά πιστοποιητικά για όλους τους κατόχους καρτών και για όλα τα καταστήματα που δέχονται κάρτες VISA. Τη στιγμή της συναλλαγής, το λογισμικό ελέγχει τη γνησιότητα των ψηφιακών πιστοποιητικών εμπόρου και πελάτη, και τότε μόνο επιτρέπει την έναρξη της επικοινωνίας.

Με απλά λόγια, τα ψηφιακά πιστοποιητικά κάνουν δυνατή την ασφαλή λειτουργία του ηλεκτρονικού εμπορίου. Το σύστημα SET σήμερα

προσφέρει ανάλογες δυνατότητες κρυπτογράφησης και πιστοποίησης για ασφαλείς συναλλαγές και πληρωμές μέσω του Internet.

3.5.8 Πρωτόκολλα ασφαλών συναλλαγών

3.5.8.1 Το πρωτόκολλο SET

Το πρωτόκολλο SET ρυθμίζει τη μετάδοση κρυπτογραφημένων πληροφοριών για πληρωμές από πιστωτικές κάρτες μέσω του δικτύου. Το πρωτόκολλο, που ανακοινώθηκε τον Φεβρουάριο του 1996 από τους δυο μεγαλύτερους οργανισμούς πιστωτικών καρτών, VISA και Mastercard, περιλαμβάνει μια σειρά από απλές τεχνικές προδιαγραφές για την προστασία πληρωμών με πιστωτικές κάρτες μέσα από το Internet και άλλα ανοικτά δίκτυα. Στην κοινοπραξία των επιχειρήσεων που ανέπτυξαν και στηρίζουν το πρωτόκολλο SET ανήκουν ονόματα όπως Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems και Verisign. Το πρωτόκολλο SET βασίζεται σε κρυπτογράφηση με δημόσιο κλειδί και τεχνολογία πιστοποίησης της εταιρίας RSA Data Security. Οι στόχοι της ασφάλειας πληρωμών είναι οι εξής: πιστοποίηση της ταυτότητας εμπόρων και πελατών, εξασφάλιση του απορρήτου των πληρωμών, προστασία των δεδομένων από παραποίηση ή πλαστογράφηση, και ακριβής ορισμός των αλγορίθμων και πρωτοκόλλων που θα χρησιμοποιούνται για αυτές τις υπηρεσίες ασφαλείας.

Ένα από τα πλεονεκτήματα του Internet είναι ότι επιτρέπει στους χρήστες να βρίσκουν πληροφορίες όλο το 24-ωρο και ανεξάρτητα από τη γεωγραφική απόσταση, το αντίτιμο όμως είναι ο αυξημένος κίνδυνος υποκλοπής και απάτης. Όταν ο "άλλος" με τον οποίο γίνεται μια συναλλαγή δεν είναι παρά ένα όνομα στην οθόνη του υπολογιστή, είναι πολύ δύσκολο να ελεγχθεί αν ο αριθμός λογαριασμού που δίνει είναι γνήσιος ή έγκυρος. Πώς μπορεί ένας έμπορος να αισθάνεται άνετα όταν πρέπει να δεχθεί έναν αριθμό πιστωτικής κάρτας χωρίς καμία άλλη επιβεβαίωση της ταυτότητας του αγοραστή; Όμοια, πώς μπορεί ο πελάτης να εμπιστευτεί έναν έμπορο που ποτέ στη ζωή του δεν έχει συναντήσει;

Ένας τρόπος για την αύξηση της ασφάλειας και της αμοιβαίας εμπιστοσύνης των δυο συναλλασσόμενων πλευρών είναι η πιστοποίηση της ταυτότητας αυτών που συναλλάσσονται. Πολλές επιχειρήσεις που δραστηριοποιούνται στον τομέα της υποστήριξης του ηλεκτρονικού εμπορίου προσπαθούν να υλοποιήσουν μεθόδους πιστοποίησης της ταυτότητας των χρηστών, που να είναι εύχρηστες, ασφαλείς, αξιόπιστες και να μπορούν να λειτουργήσουν με μεγάλο αριθμό χρηστών. Στο περιβάλλον ενός δημόσιου δικτύου πρέπει να υπάρχουν οργανισμοί πιστοποίησης, που να εγγυώνται την ταυτότητα των χρηστών που είναι εγγεγραμμένοι σε αυτούς. Η δυνατότητα πιστοποίησης της ταυτότητας παίζει κεντρικό ρόλο για την ασφάλεια των ηλεκτρονικών συναλλαγών.

Το πρωτόκολλο SET περιέχει ρυθμίσεις που καλύπτουν όλες τις ανάγκες ασφάλειας του ηλεκτρονικού εμπορίου:

- Απόρρητο των πληροφοριών.
- Ακεραιότητα των δεδομένων.
- Πιστοποίηση της ταυτότητας των πελατών.
- Πιστοποίηση της ταυτότητας του εμπόρου.
- Συμβατότητα.

Συνοπτικά, το πρωτόκολλο SET είναι ένα ενιαίο σύνολο όλων των απαραίτητων χαρακτηριστικών για την αύξηση του ενδιαφέροντος και της εμπιστοσύνης των επιχειρήσεων στο ηλεκτρονικό εμπόριο, ενώ υποστηρίζεται από τους μεγαλύτερους οικονομικούς και τεχνικούς οργανισμούς που συνδέονται με το ηλεκτρονικό εμπόριο.

Η έκδοση με αριθμό μηδέν (μια δοκιμαστική έκδοση) του πρωτοκόλλου SET είχε τεθεί σε λειτουργία στη διάρκεια του 1997 σε κλειστά δοκιμαστικά προγράμματα, ολοκληρώθηκαν πριν από το τέλος του 1997. Η πρώτη εμπορικά διαθέσιμη έκδοση (με δυνατότητα σύνδεσης στο τραπεζικό σύστημα) κυκλοφόρησε τον Φεβρουάριο του 1998.

3.5.8.2 Το πρωτόκολλο SSL

Το SSL πρωτόκολλο (Secure Socket Layer), εξασφαλίζει το δίαυλο μιας συναλλαγής μεταξύ τυπικά – ενός client και ενός server, διαχειριζόμενο το ίδιο την συναλλαγή. Η ασφάλεια αναπτύσσεται πλέον κάτω από το επίπεδο εφαρμογής και η εφαρμογή δεν απαιτείται να έχει κανέναν έλεγχο σε ό,τι αφορά τις υπηρεσίες που εφαρμόζονται σε μια συγκεκριμένη συναλλαγή. Όλες οι συναλλαγές είναι ασφαλείς με τον ίδιο τρόπο. Αυτή η λειτουργία (της εξασφαλίσεως του διαύλου επικοινωνίας) είναι γνωστή και σαν ασφάλεια βασισμένη στο δίαυλο και μπορεί να παράσχει τις εξής ευκολίες:

- Αυθεντικοποίηση των συναλλασσόμενων μερών (π.χ. ο client επιβεβαιώνεται ότι συναλλάσσεται με ένα νόμιμο σύστημα και αντιστρόφως)
- Προστασία και εξασφάλιση των δεδομένων που ανταλλάσσονται μεταξύ του client και του server (π.χ. για τήρηση εμπιστευτικότητας)
- Προστασία από επανάληψη (replay) της συναλλαγής
- Εξασφάλιση της ακεραιότητας των δεδομένων κατά τη διάρκεια της συναλλαγής

Μετά από όλα αυτά, θα μπορούσαμε να πούμε ότι το SSL διασφαλίζει το δίαυλο επικοινωνίας μεταξύ δύο οντοτήτων και δεν «βλέπει» μεμονωμένες συναλλαγές. Κατά συνέπεια εξασφαλίζει ιδιωτικότητα στο Internet και επιτρέπει στις client / server εφαρμογές να επικοινωνούν με τρόπο που να αποτρέπεται η παράνομη παρακολούθηση. Ο κάθε server έχει στην κατοχή του ένα ζεύγος ιδιωτικού / δημοσίου κλειδιού και μέσω αυτού αυθεντικοποιείται.

Το SSL απαιτεί ένα έμπιστο πρωτόκολλο μεταφοράς για αποστολή και λήψη δεδομένων. Είναι ένα πρωτόκολλο ανεξάρτητο του πρωτοκόλλου εφαρμογής υπό την έννοια ότι ένα πρωτόκολλο υψηλού επιπέδου μπορεί να βρίσκεται πάνω από το SSL και η όλη διαδικασία να λειτουργεί διαφανώς. Σε μία client / server WWW (World Wide Web) επικοινωνία, το πρωτόκολλο SSL μπορεί να αφήσει τον client να αυθεντικοποιήσει τον server, να αποφασίσει τον κρυπτογραφικό αλγόριθμο (ο οποίος υποστηρίζεται και από τον client και από τον server) και να εγκαθιδρύει ένα

κλειδί συνόδου για τη συγκεκριμένη συναλλαγή, πριν το πρωτόκολλο της εφαρμογής στείλει ή λάβει τα αρχικά bytes των δεδομένων.

Ο client στην προσπάθειά του να επιτύχει μια σύνδεση με το server, επιλέγει πάντα μια URL (Uniform Resourse Locator) η οποία δεν είναι τίποτα άλλο παρά μια διεύθυνση μιας Web σελίδας. Ο client πρέπει να γνωρίζει κατά πόσο ο server υποστηρίζει SSL ή όχι. Αυτό γίνεται αντιληπτό από τη μορφή αυτής της διευθύνσεως: αν αρχίζει με http:// , ο client γνωρίζει πως ο server δεν υποστηρίζει ή δεν απαιτεί SSL και αποστέλλει ένα απλό Connect για εγκαθίδρυση επικοινωνίας. Αν όμως η URL διεύθυνση αρχίζει με http://, ο client γνωρίζει πως ο server υποστηρίζει και απαιτεί SSL και αποστέλλει ένα SSL_Connect.

ΚΕΦΑΛΑΙΟ 4

ΣΥΜΠΕΡΑΣΜΑΤΑ

4.1 Η πραγματοποίηση συναλλαγών στο ηλεκτρονικό εμπόριο

Ένας απλός αλλά περιεκτικός ορισμός της «ηλεκτρονικής συναλλαγής» είναι ότι οποιαδήποτε μεταφορά δεδομένων με ηλεκτρονικό τρόπο αποτελεί ηλεκτρονική συναλλαγή. Οι ηλεκτρονικές συναλλαγές είναι οι ηλεκτρονικές ανταλλαγές δεδομένων και οι ηλεκτρονικές χρηματικές συναλλαγές.
Για την απόδοση μίας ολοκληρωμένης εικόνας σχετικά με την πραγματοποίηση συναλλαγών στο ηλεκτρονικό εμπόριο έπρεπε να απαντήσουμε αρχικά σε δύο βασικά ερωτήματα: α) που εμφανίζονται οι ηλεκτρονικές συναλλαγές και β) πως υλοποιούνται. Στη συνέχεια, ήταν κρίσιμο να υποδείξουμε τους κινδύνους που εμφανίζονται κατά την πραγματοποίηση των ηλεκτρονικών συναλλαγών αλλά και τα μέτρα προστασίας που υπάρχουν ώστε να εξασφαλίζεται η ασφάλεια αυτών.

Όσον αφορά το πρώτο ερώτημα, δηλαδή το που εμφανίζονται οι ηλεκτρονικές συναλλαγές, μπορούμε να πούμε ότι εμφανίζονται σε οποιοδήποτε περιβάλλον του ηλεκτρονικού εμπορίου συμμετέχουν επιχειρήσεις, δημόσιοι οργανισμοί και καταναλωτές. Αλλιώς, ηλεκτρονικές συναλλαγές πραγματοποιούνται όπου εφαρμόζεται το ηλεκτρονικό εμπόριο. Οι πιο συνηθισμένες εφαρμογές του ηλεκτρονικού εμπορίου ανάλογα με τα μέρη που εμπλέκονται σε μια ηλεκτρονική συναλλαγή αφορούν:

- δημόσιους φορείς προς επιχειρήσεις (government to business - g2b)
- δημόσιους φορείς προς πολίτες-καταναλωτές (government to consumers -g2c)
- επιχειρήσεις προς επιχειρήσεις (business to business - b2b)
- επιχειρήσεις προς καταναλωτές (business to consumers - b2c)
- καταναλωτές προς καταναλωτές (consumers to consumers-c2c)

Όσον αφορά το δεύτερο ερώτημα, δηλαδή το πως υλοποιούνται οι ηλεκτρονικές συναλλαγές, αναφερόμαστε στις τεχνολογίες τις μεθόδους και τα

μέσα που χρησιμοποιούνται για την πραγματοποίηση τους. Αναφέρουμε επιγραμματικά κάποια από αυτά:

- τη χρήση πιστωτικής κάρτας.
- τις έξυπνες κάρτες,
- το ηλεκτρονικό χρήμα.
- τις ηλεκτρονικές επιταγές
- τις ηλεκτρονικές τράπεζες

Με την εξάπλωση της χρήσης του ηλεκτρονικού εμπορίου και κατ' επέκταση την ολοένα αυξανόμενη χρήση των ηλεκτρονικών συστημάτων ανταλλαγής δεδομένων και χρηματικών πληρωμών, άρχισαν παράλληλα να αναπτύσσονται προβλήματα και να παρεισφύουν κίνδυνοι στα πληροφοριακά συστήματα και τις ηλεκτρονικές συναλλαγές. Κύριο παράδειγμα τρόπων που χρησιμοποιούνται για επίθεση ή παράνομη πρόσβαση σε προσωπικούς Η/Υ και πληροφοριακά συστήματα είναι οι ιοί, που είναι προγράμματα τα οποία εισβάλουν σε έναν υπολογιστή κυρίως μέσω του e-mail και μπορούν να προκαλέσουν ποικίλες ζημιές. Όσον αφορά τις ηλεκτρονικές συναλλαγές δεν υπόκεινται όλες στον ίδιο βαθμό κινδύνου, οι χρηματικές συναλλαγές είναι υψηλότερου κινδύνου από τις απλές ανταλλαγές δεδομένων. Από τα πιο συνηθισμένα προβλήματα και κινδύνους των ηλεκτρονικών συναλλαγών είναι το hacking ή μη εγκεκριμένη πρόσβαση σε πληροφορίες, καθώς και η παράνομη παρακολούθηση που έχει να κάνει με τη συλλογή πληροφοριών για αριθμούς καρτών, για ύψη ή/και αριθμούς λογαριασμών και σε μερικές περιπτώσεις για αυτό καθ' αυτό το γεγονός της πραγματοποιήσεως μιας συναλλαγής με κάποιον εμπορικό φορέα, κ.α.

Για την επιβίωση του ηλεκτρονικού εμπορίου έπρεπε να αναπτυχθούν μέτρα προστασίας τέτοια ώστε εξασφαλίζεται η ασφάλεια των ηλεκτρονικών υπολογιστών των χρηστών και των συναλλαγών που διεκπεραιώνουν μέσω αυτών. Το πιο σημαντικό μέτρο για την προστασία των υπολογιστών είναι τα προγράμματα antivirus-το λογισμικό προστασίας από τους ιούς με βάση και στις εισηγήσεις που δίνονται από τον οργανισμό CERT, που ειδικεύεται σε θέματα ασφάλειας στο διαδίκτυο. Σε σχέση με την ασφάλεια των συναλλαγών, μία λύση ασφαλείας, πρέπει να ικανοποιεί τις ακόλουθες θεμελιώδεις απαιτήσεις: *εμπιστευτικότητα μεταξύ* των

επικοινωνούντων, *αυθεντικοποίηση* για τα συναλλασσόμενα μέλη, *ακεραιότητα* των δεδομένων.

Σύμφωνα με όσα υποστηρίζουμε παραπάνω, οι καταναλωτικές αγορές online μάλλον δε θα γίνουν ποτέ τόσο δημοφιλείς όσο το παραδοσιακό εμπόριο. Αυτός όμως δεν είναι λόγος για να απογοητευόμαστε. Τα ηλεκτρονικά καταστήματα προσφέρονται για γρήγορες, άνετες και φθηνές αγορές όλο το 24ωρο και γι' αυτό αποκτούν σιγά σιγά το δικό τους πιστό κοινό. Πολλά ηλεκτρονικά καταστήματα προσπαθούν να κερδίσουν αυτό το κοινό με περίτεχνες πολιτικές marketing, ειδικές διαφημιστικές εκστρατείες και άλλα μεγαλόπνοα (και συνήθως πανάκριβα) σχέδια. Με βάση όμως τα όσα αναφέρθηκαν ήδη, ακόμα κι αν ο πελάτης «σαγηνεύτηκε» κάποτε από μια προσφορά, σπάνια θα επιστρέψει και πάλι στο ίδιο κατάστημα για να αγοράσει περισσότερα προϊόντα. (Τον «τράβηξε» η προσφορά και όχι το ίδιο το κατάστημα, η λειτουργία του οποίου δεν ταιριάζει συνήθως με την ψυχολογία και τον τρόπο ζωής του).

Στόχος, λοιπόν, των ηλεκτρονικών καταστημάτων δεν πρέπει να είναι απλώς η συγκέντρωση πελατών, αλλά η προσέλκυση ανθρώπων οι οποίοι είναι συνηθισμένοι στις online αγορές και έχουν πολλές πιθανότητες να ξαναγοράσουν με αυτόν τον τρόπο. Ένας καλός τρόπος για να επιτευχθεί κάτι τέτοιο είναι τα online κουπόνια. Σύμφωνα με πρόσφατη μελέτη του eMarketer, το 94% όσων χρησιμοποιούν online εκπτωτικά κουπόνια είναι άνθρωποι που έχουν ήδη αγοράσει άλλα προϊόντα από ηλεκτρονικά καταστήματα. Πρόκειται δηλαδή για καταναλωτές ήδη εθισμένους στη διαδικασία του ηλεκτρονικού εμπορίου που δεν φοβούνται τις online αγορές και είναι πάντα πρόθυμοι να αξιοποιήσουν μια καλή ευκαιρία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

1. «Ηλεκτρονικό Εμπόριο» (Β' έκδοση) Εκδόσεις Κλειδάριθμος
2. (Turban, Lee, King, Chung), «Ηλεκτρονικό Εμπόριο» Εκδόσεις Γκιούρδας
3. Κιουντούζης Ε., «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Ε. Μπένου, Αθήνα 1993
4. Φρυσήρας Κώστας, «Το Internet στην πράξη» Αθήνα 2001
5. Αλεξανδρής Ν., Κιουντούζης Ε., Τραπεζάνογλου Β., «Ασφάλεια Πληροφοριών-Τεχνικά-Νομικά-Κοινωνικά Θέματα», ΕΠΥ, Αθήνα 1995

Επιστημονικά Περιοδικά

1. RAM, τεύχος 31
2. ON, τεύχος 16
3. NET, τεύχος 19

Internet Addresses

1. www.enet.gr
2. www.geocities.com
3. www.go-online.gr
4. www.houseware.gr