Τ.Ε.Ι. ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ »

Σπουδαστές:
ΠΕΤΡΟΖΕΛΛΗΣ ΜΙΧΑΛΗΣ
ΔΡΙΒΑΣ ΠΑΝΑΓΙΩΤΗΣ
ΜΑΞΑΚΟΥΛΗ ΒΑΣΙΛΙΚΗ

Εποπτεύων Καθηγητής : ΜΠΑΚΑΛΗΣ ΑΡΗΣ

ΠΑΤΡΑ – 2013

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Ανέκαθεν οι επιχειρήσεις αναζητούσαν τρόπους για να προσελκύσουν νέους πελάτες και να αυξήσουν τις πωλήσεις τους. Από την άλλη μεριά οι καταναλωτές αναζητούσαν νέους τρόπους ώστε να μπορούν να αποκτούν πρόσβαση σε περισσότερα προϊόντα, εύκολα, χωρίς να χρειαστεί να προβούν σε πολλές μετακινήσεις και παράλληλα να έχουν και τις καλύτερες τιμές της αγοράς.

Αυτές τις ανάγκες και πολλές ακόμη, ήρθε να καλύψει η ανάπτυξη του ηλεκτρονικού εμπορίου το οποίο είναι και το κύριο θέμα της εργασίας αυτής. Η ιστορία του ηλεκτρονικού εμπορίου, εν συντομία, η ανάπτυξή του και η παρουσία του στον ελληνικό επιχειρηματικό χώρο, σε συνδυασμό με την εξέλιξη και την αποδοχή των νέων τεχνολογιών, αναπτύσσονται στις παραγράφους της εργασία.

Η παρούσα πτυχιακή εργασία συντάχτηκε από τους φοιτητές του Α.Τ.Ε.Ι Πάτρας, Πετροζέλη Μιχάλη , Δρίβα Παναγιώτη και Μαξακούλη Βασιλική υπό την επιμέλεια και επίβλεψη του καθηγητή μας Κ. Μπάκαλη Άρη. Το θέμα της πτυχιακής εργασίας «Ηλεκτρονικό Εμπόριο και ασφάλεια συναλλαγών » προτάθηκε από τον ίδιο τον Κ. Μπακάλη και εμείς προσπαθήσαμε να δώσουμε μια σφαιρική και κατά το δυνατόν πλήρης εικόνα του Ηλεκτρονικού Εμπορίου, καθώς και των κινδύνων που ελλοχεύουν στις συναλλαγές των χρηστών. Ακόμη στα κεφάλαια της εργασίας αναπτύσσεται η προσπάθεια των επιχειρήσεων να διασφαλίσουν τις συναλλαγές και να προστατεύσουν τους «πελάτες» τους αλλά και τις ίδιες τις επιχειρήσεις από κινδύνους ηλεκτρονικών επιθέσεων.

Οι πηγές, από όπου αντλήθηκαν οι πληροφορίες που χρησιμοποιήθηκαν για την συγγραφή αυτής της εργασίας, ήταν το διαδίκτυο, σε μεγαλύτερο ποσοστό, διάφορα συγγράμματα-βιβλία από οικονομολόγους σχετικούς με το θέμα, άρθρα από οικονομικές εφημερίδες και περιοδικά. Ακόμη χρησιμοποιήθηκαν αποτελέσματα στατιστικών ερευνών και στοιχεία από συνέδρια σχετικά με την αποδοχή την εξοικείωση και την χρήση του διαδικτύου στην Ελλάδα καθώς και την πρόθεση των ελληνικών επιχειρήσεων για ένταξη του ηλεκτρονικού εμπορίου στα «επιχειρηματικά όπλα» τους. Ακόμα παραθέτουμε, αυτούσιες, αρκετές απόψεις ειδικών και ανθρώπων που έχουν μεγάλη εμπειρία στο ηλεκτρονικό εμπόριο καθώς και αποσπάσματα οικονομοτεχνικών μελετών που βοηθούν στην εμβάθυνση του θέματος της εργασίας.

Στην προσπάθεια μας να εξηγήσουμε τι είναι το ηλεκτρονικό εμπόριο και πως εξήχθηκε δεν θα μπορούσαμε να παραλείψουμε μια εκτενή αναφορά στο διαδίκτυο και στις βασικές αρχές λειτουργίας του. Σίγουρα θα μπορούμε να γράψουμε περισσότερα πράγματα για αυτό αλλά θεωρήσαμε ότι θα ξέφευγε από το στόχο της εργασίας. Είναι δεδομένο ότι η βάση του Ηλεκτρονικού Εμπορίου είναι το διαδίκτυο και πάνω σε αυτό αναπτύχτηκαν όλες οι εφαρμογές του. Δόθηκε όμως μεγάλη βαρύτητα στην ασφάλεια του διαδικτύου και στο πως μπορούμε να προστατευτούμε από τις ηλεκτρονικές επιθέσεις αφού αυτές είναι και ο μεγαλύτερος κίνδυνος των συναλλαγών του Ηλεκτρονικού εμπορίου.

Τέλος θα θέλαμε να ευχαριστήσουμε τον καθηγητή μας Κ. Μπακάλη Άρη που μας ανάθεσε την εργασία αυτή και μας έδωσε την δυνατότητα να διευρύνουμε τις γνώσεις μας γύρο από το θέμα αλλά κυρίως για την εμπιστοσύνη που μου έδειξε, και την υπομονή που έκανε κατά τη διάρκεια υλοποίησης της πτυχιακής εργασίας. Η υλοποίηση αυτής της πτυχιακής μας έδωσε τη δυνατότητα για ομαδική εργασία ή οποία πολλές φορές έφερε αντικρουόμενες απόψεις στο προσκήνιο. Όμως το τελικό αποτέλεσμα είναι προϊόν ζύμωσης των απόψεων και των αντιλήψεων και των τριών φοιτητών, αφού η συνεργασία μεταξύ μας ήταν εποικοδομητική και άψογη.

1^{o} Κεφάλαιο
Ηλεκτρονικό Εμπόριο - Εισαγωγή

1.1 Ορισμός Ηλεκτρονικού Εμπορίου

Ο Σύνδεσμός Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδος (ΣΕΠΕ) ορίζει το Ηλεκτρονικό Εμπόριο ως εξής[1]:

«Το Ηλεκτρονικό Εμπόριο είναι μια νέα επιχειρηματική πρακτική. Σύγχρονες τεχνολογίες και μέθοδοι συνδυάζονται προκειμένου οι επιχειρήσεις να αυξήσουν την αξία τους να ελαχιστοποιήσουν τα κόστη τους και να μεγιστοποιηθεί η δυνατότητα προσέγγισης όσο το δυνατό περισσότερων πελατών.

Πολλοί όμως θεωρούν τον όρο Ηλεκτρονικό Εμπόριο (Electronic Commerce) ως αδόκιμο βασιζόμενοι στην άποψη ότι δεν υπάρχει τηλεοπτικό εμπόριο, ραδιοφωνικό εμπόριο ή ταχυδρομικό εμπόριο.

Στην κυριολεξία, ένα μέσο, το Internet, δίνει τη δυνατότητα στον έμπορο και στον καταναλωτή να έρθουν σε επαφή. Η συναλλαγή ολοκληρώνεται αν η προσφορά του εμπόρου είναι συμφέρουσα και έτσι έχουμε μια εμπορική συναλλαγή εξ' αποστάσεως.

Ουσιαστικά είναι μια ολοκληρωμένη συναλλαγή, μια εμπορική δραστηριότητα, χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες.

Για να μπορέσουμε όμως να κατανοήσουμε το Ηλεκτρονικό Εμπόριο (e-commerce) και τον τρόπο με τον οποίο αναπτύσσεται και υλοποιείται θα πρέπει να πούμε και δυο λόγια για το διαδίκτυο.

1.2 Το Διαδίκτυο

Το Internet (διαδίκτυο) αποτελεί τη βάση του Ηλεκτρονικού Εμπορείου και είναι αναπόσπαστο κομμάτι του ηλεκτρονικού επιχειρείν. Η εξέλιξη και η ανάπτυξη του είναι προφανές ότι παίζει πολύ σημαντικό ρόλο και αποτελεί προϋπόθεση για την υγιή ανάπτυξη του Ηλεκτρονικού Εμπορίου σε όλες του τις μορφές.

Το διαδίκτυο γεννήθηκε[2] πριν από 40 χρόνια περίπου (1969-70) σε μια προσπάθεια του Υπουργείου Αμύνης των Η.Π.Α να διασυνδέσει ένα δίκτυο υπολογιστών με το όνομα ARPAnet με διάφορα άλλα δορυφορικά δίκτυα. Στην πρώτη του υλοποίηση

[1] Επίσημη ιστοσελίδα ΣΕΠΕ: http://www.sepe.gr/default.aspx?pid=75&la=1
[2] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1

του το δίκτυο συνέδεσε 4 πανεπιστήμια των Η.Π.Α. Το 1971 είχαν συνδεθεί 23 κόμβοι και σιγά σιγά άρχισε να αναπτύσσεται προτού πάρει την σημερινή μορφή που γνωρίζουμε όλοι. Το διαδίκτυο μεγαλώνει και εξαπλώνεται με ρυθμούς που είναι τεράστιοι. Το 1989 είχε 80.000 κόμβους ενώ το 1992 χρειάστηκε να αναβαθμιστεί επειγόντως λόγω κορεσμού. Σήμερα οι χρήστες είναι πολλά εκατομμύρια αλλά ο αριθμός είναι ακόμα μικρός αν αναλογιστεί κανείς ότι ο πληθυσμός της γης είναι 5 δισεκατομμύρια καθώς και ότι η τεχνολογία θα αναπτύσσεται συνεχώς και σε χώρες που ήταν μέχρι πρότινος υποβαθμισμένες.

Η λειτουργία του διαδικτύου βασίζεται στην επιμέρους σύνδεση πολλών δικτύων. Το κάθε δίκτυο απαρτίζεται από 2 μέχρι και εκατοντάδες υπολογιστές, οι οποίοι γεωγραφικά βρίσκονται, συνήθως, σε απόσταση μερικών μέτρων έως και μερικών χιλιομέτρων ένας από τον άλλο. Κάθε υπολογιστής συνδέετε με έναν κεντρικό υπολογιστή (server) ο οποίος με τη σειρά του συνδέεται με κάποιον άλλο server με αποτέλεσμα να έχουμε τη δημιουργία ενός μεγάλου δικτύου. Η επικοινωνία μεταξύ των υπολογιστών γίνεται με τη βοήθεια του τηλεφωνικού δικτύου το οποίο παρέχει το υλικό του (καλώδια τηλεφωνικά κέντρα κτλ) και έτσι γίνεται δυνατή ή ανταλλαγή πληροφοριών και δεδομένων μεταξύ των υπολογιστών.

Το διαδίκτυο προσφέρει πολλές υπηρεσίες στους χρήστες του. Μερικές από τις υπηρεσίες αυτές είναι :

- Ο Παγκόσμιος Ιστός (World Wide Web –www)
- Το Ηλεκτρονικό ταχυδρομείο (e-mail)
- Μεταφορά Αρχείων (File Transferred Protocol – FTP)
- Ομάδες Συζητήσεων (Chat Rooms)

Ο Παγκόσμιος Ιστός είναι ίσως η πιο σημαντική υπηρεσία όσον αφορά το Ηλεκτρονικό εμπόριο, αφού πάνω του έχει δημιουργηθεί όλη η φιλοσοφία του. Τον Παγκόσμιο Ιστό θα μπορούσαμε να τον παρομοιάσουμε με ένα τεράστιο περιοδικό ποικίλης ύλης, μέσα στο οποίο μπορούμε ένα βρούμε τα πάντα. Καλύπτει όλη τη θεματολογία που μπορεί να φανταστεί κάποιος και συνεχώς εμπλουτίζεται με καινούριο υλικό.

Για να μπορέσουμε να πλοηγηθούμε στον Παγκόσμιο Ιστό χρειαζόμαστε ένα Φυλλομετρητη Ιστού. Ένα πρόγραμμα δηλαδή που μας δίνει τη δυνατότητα να αναζητήσουμε, να διαβάσουμε, να ταξιδέψουμε στον τεράστιο αυτό χώρο του Διαδικτύου. Τέτοιου είδους προγράμματα υπάρχουν πολλά και συνήθως τουλάχιστον

ένα βρίσκεται πάντα εγκαταστημένο σε κάθε υπολογιστή. Μερικά προγράμματα πλοήγησης στον Παγκόσμιο Ιστό είναι :

- Internet Explorer
- Firefox Mozilla
- Google Chrome
- Opera

Έτσι λοιπόν το διαδίκτυο σιγά σιγά γίνεται όλο και πιο δημοφιλές, εύχρηστο και αποδεκτό από όλο και περισσότερους ανθρώπους, οι οποίοι αναζητούν πληροφορίες, ενημερώνονται, αγοράζουν ή πωλούν πράγματα, επικοινωνούν με συνανθρώπους που βρίσκονται εκατοντάδες χιλιόμετρα μακριά και πολλά άλλα.

Πάνω σε αυτή την ραγδαία εξέλιξη του διαδικτύου και την μεγάλη αποδοχή και χρήση από ολοένα και περισσότερους ανθρώπους στηρίχτηκε και υλοποιήθηκε μια ιδέα η οποία ξεκινά από πολύ νωρίς, σε σχέση με την ηλικία του διαδικτύου.

1.3 Εξέλιξη Ηλεκτρονικού Εμπορίου (Ιστορική Αναδρομή [3])

Η εξέλιξη αυτού που σήμερα ονομάζουμε ηλεκτρονικό εμπόριο, από τις αρχές του 1970, όπου και πρωτχρησιμοποιήθηκε, σε ένα πρώιμο αρχικό και πολύ διαφορετικό από το σημερινό στάδιο, έχει ως εξής :

Δεκαετία του 1970

Αρχικά, το ηλεκτρονικό εμπόριο αναγνωρίστηκε ως η διευκόλυνση ηλεκτρονικών εμπορικών συναλλαγών, χρησιμοποιώντας τεχνολογίες όπως η ηλεκτρονική ανταλλαγή δεδομένων (EDI) και η ηλεκτρονική μεταφορά χρημάτων (EFT). Αυτές εισήχθησαν στα τέλη του 1970 επιτρέποντας στις επιχειρήσεις να στέλνουν εμπορικά φυλλάδια όπως, παραγγελίες αγοράς ή ηλεκτρονική έκδοση τιμολογίων.

Δεκαετία του 1980

Η ανάπτυξη και αποδοχή των πιστωτικών καρτών των αυτόματων τραπεζικών μηχανών και τηλεφωνικών καταθέσεων τη δεκαετία του 1980 είναι επίσης μορφές ηλεκτρονικού εμπορίου. Μία ακόμα μορφή του ήταν το σύστημα αεροπορικών κρατήσεων που τυποποιήθηκε από την εταιρία Sabre στις ΗΠΑ και την Travicom στο Ηνωμένο Βασίλειο. Οι τεχνολογίες ηλεκτρονικής επικοινωνίας που βασίζονται στην αρχιτεκτονική της ανταλλαγής μηνυμάτων (συστήματα EDI και ηλεκτρονικό ταχυδρομείο) αποκτούν σημαντική διάδοση. Πολλές δραστηριότητες, που παραδοσιακά διεκπεραιώνονταν με βασικό μέσο το χαρτί, μπορούν πλέον να γίνουν ταχύτερα και με μικρότερο κόστος. Οι συναλλαγές, που παλαιότερα απαιτούσαν έντυπα, όπως παραγγελίες αγοράς, συνοδευτικά έγγραφα και επιταγές πληρωμής,

[3] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ http://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%

μπορούν να γίνουν κατά ένα μέρος ή στο σύνολό τους ηλεκτρονικά - με δομημένο τρόπο χάρη στα συστήματα EDI ή μέσω του ηλεκτρονικού ταχυδρομείου.

Τέλη της δεκαετίας του 1980 - αρχές της δεκαετίας του 1990

Από το 1990 και έπειτα, το ηλεκτρονικό εμπόριο περιείχε επιπρόσθετα το σύστημα ενδοεπιχειρισιακού σχεδιασμού (ERP) ,την αναζήτηση και την αποθήκευση δεδομένων (data warehousing). Τα ηλεκτρονικά δίκτυα προσφέρουν μια νέα μορφή κοινωνικής επικοινωνίας, με δυνατότητες όπως ηλεκτρονικό ταχυδρομείο (e-mail), ηλεκτρονική διάσκεψη (conferencing) και ηλεκτρονική συνομιλία (IRC), ομάδες συζήτησης (newsgroups, forums), μεταφορά αρχείων (FTP) κτλ. Η πρόσβαση στο δίκτυο γίνεται φθηνότερη λόγω της διεθνούς απελευθέρωσης της αγοράς τηλεπικοινωνιών.

Μέσα της δεκαετίας του 1990

Η εμφάνιση του Παγκόσμιου Ιστού (WWW) στο Internet και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών (PC) που χρησιμοποιούν λειτουργικά συστήματα τύπου Windows, προσφέρουν μεγάλη ευκολία χρήσης λύνοντας το πρόβλημα της δημοσίευσης και της εύρεσης πληροφοριών στο Διαδίκτυο. Το ηλεκτρονικό εμπόριο γίνεται ένας πολύ φθηνότερος τρόπος για την πραγματοποίηση μεγάλου όγκου συναλλαγών, ενώ συγχρόνως διευκολύνει την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών δραστηριοτήτων, επιτρέποντας σε μικρές επιχειρήσεις να ανταγωνιστούν μεγαλύτερες, με πολύ ευνοϊκότερες προϋποθέσεις.

Τέλη της δεκαετίας του 1990

Η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και εξακρίβωσης της ταυτότητας του αποστολέα ηλεκτρονικών μηνυμάτων, καθώς και η σχετική προσαρμογή της νομοθεσίας στους τομείς των εισαγωγών-εξαγωγών και των επικοινωνιών, καθιστούν δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών.

Η εμφάνιση του internet και η ταχεία ανάπτυξη υπηρεσιών που βασίζονται στον παγκόσμιο ιστό (world wide web-www) έφερε γενική ευφορία τόσο στις επιχειρήσεις που δραστηριοποιούνται στο χώρο του internet, όσο και στον επιχειρηματικό κόσμο γενικότερα και αυτό γιατί τα διαφαινόμενα πλεονεκτήματα ήταν πολύ μεγάλα.

Σήμερα

Στις μέρες μας, το ηλεκτρονικό εμπόριο περιλαμβάνει τα πάντα, από την παραγγελία ψηφιακού περιεχομένου για άμεση διαδικτυακή κατανάλωση έως και την παραγγελία συμβατικών αγαθών και υπηρεσιών, αλλά και τις υπηρεσίες που διευκολύνουν άλλες μορφές ηλεκτρονικού εμπορίου. Σε ερευνητικό επίπεδο, μεγάλες εταιρίες και οικονομικά ιδρύματα χρησιμοποιούν το διαδίκτυο για να ανταλλάξουν χρηματοοικονομικά δεδομένα που υποβοηθούν εγχώριες και διεθνής εταιρίες. Η ακεραιότητα και η ασφάλεια των δεδομένων αποτελούν κρίσιμα ζητήματα του ηλεκτρονικού εμπορίου.

Ειδικά για το ηλεκτρονικό εμπόριο, η δυνατότητα να απευθυνθεί μια επιχείρηση στην παγκόσμια αγορά, να ξεφύγει από γεωγραφικούς περιορισμούς, να επεκταθεί χωρίς τεράστιες επενδύσεις και να αυξήσει τα κέρδη της ήταν πολύ ελκυστική.

Όσο όμως μεγάλες ήταν οι προσδοκίες για υλοποίηση επενδύσεων στο χώρο του διαδικτύου και για ανάπτυξη νέων επιχειρηματικών σχεδίων, η δημιουργία πολλών επιχειρήσεων που βασίζονταν στο διαδικτυακό εμπόριο, δεν έφερε και τόσο θετικά αποτελέσματα.

Σε καμία περίπτωση όμως αυτό δεν σημαίνει ότι όλες οι επιχειρήσεις απέτυχαν στην προσπάθειά τους να εφαρμόσουν το ηλεκτρονικό εμπόριο. Πάρα πολλά επιτυχημένα παραδείγματα από επιχειρήσεις, οι οποίες ερμήνευσαν σωστά τις αντιδράσεις των καταναλωτών, έκαναν επενδύσεις με γνώμονα τις ανάγκες αυτών και κατάφεραν να αποκομίσουν σημαντικά οφέλη από την εφαρμογή του ηλεκτρονικού εμπορίου.

Αρχικά, τα πρώτα προβλήματα που παρατηρήθηκαν, κατά την ανάπτυξη του ηλεκτρονικού εμπορίου δεν οδήγησαν στην κατάρρευση αυτού, αλλά σε επαναπροσδιορισμό των προσδοκιών και του τρόπου διεξαγωγής.

Οι λόγοι[4] που οδήγησαν την ανάπτυξη του ηλεκτρονικού εμπορίου στην αναπάντεχη αυτή εξέλιξη, εξηγούν γιατί οι καταναλωτές δεν ανταποκρίθηκαν όπως αναμενόταν και οι πωλήσεις μέσω του διαδικτύου ήταν πολύ λιγότερες από τις αναμενόμενες.

- οι επενδύσεις που απαιτήθηκαν ήταν μεγαλύτερες από τις αρχικά υπολογιζόμενες.
- η προσδοκία του εύκολου κέρδους στα πλαίσια της νέας οικονομίας οδήγησε επιχειρήσεις στην υλοποίηση επενδύσεων χωρίς σχεδιασμό και στρατηγική.
- Σε σχέση με το παραπάνω σημείο πρέπει να αναφέρουμε ότι δόθηκε ιδιαίτερη έμφαση στην τεχνολογία και τις τεχνικές δυνατότητες και πολύ λιγότερο στην επιχειρηματική διάσταση των προσπαθειών στο χώρο του ηλεκτρονικού εμπορίου.
- Οι καταναλωτές δεν «έτρεξαν» να αγοράσουν προϊόντα από ηλεκτρονικά καταστήματα.
- Μια επιχείρηση που ήταν γνωστή στην τοπική αγορά ήταν άγνωστη στην παγκόσμια αγορά του internet.
- Οι επιχειρήσεις που εφάρμοσαν επιτυχημένα το ηλεκτρονικό εμπόριο έως σήμερα φαίνετε ότι χρησιμοποίησαν τεχνολογία ως μέσο και όχι ως αυτοσκοπό, σε μια οργανωμένη σχεδιασμένη επιχειρηματική προσπάθεια η οποία δημιουργούσε κίνητρα και υπεραξία στους δικτυακούς καταναλωτές.

[4] Equal-Ανδρομέδα, Ηλεκτρονικό Επιχειρείν – Ηλεκτρονικό Εμπόριο, Επιστημονική Έρευνα – Συγγραφή : Χρύσα Πάτσα, Μάρτιος 2005

1.4 Πλεονεκτήματα του Ηλεκτρονικού Εμπορίου

Στο σημείο αυτό μπορούμε να αναφερθούμε στα πλεονεκτήματα του Ηλεκτρονικού Εμπορίου τα οποία καλό θα ήταν να τα χωρίσουμε σε δυο μεγάλες κατηγορίες:

1. Πλεονεκτήματα καταναλωτών
2. Πλεονεκτήματα επιχειρήσεων

Στην πρώτη κατηγορία αναφερόμαστε στο κέρδος που έχει ένας καταναλωτής ο οποίος θα χρησιμοποιήσει το Ηλεκτρονικό Εμπόριο. Έτσι λοιπόν έχουμε:

- **i.** Το ηλεκτρονικό εμπόριο παρέχει στους χρήστες του έναν μηχανισμό για την αγορά προϊόντων και υπηρεσιών ο οποίος λειτουργεί συνέχεια, 24 ώρες την ημέρα, και τα πάντα μπορούν να γίνουν από την άνετη πολυθρόνα τους , το γραφείο ή το σπίτι τους.
- **ii.** Το διαδίκτυο δεν περιορίζεται σε γεωγραφικά όρια, έτσι οι καταναλωτές έχουν τη δυνατότητα να επισκεφτούν, χωρίς καν να βγουν από το σπίτι τους, με περισσότερες εταιρείες και να συγκρίνουν προϊόντα, υπηρεσίες και τιμές.
- **iii.** Δίνει στους χρήστες τη δυνατότητα πρόσβασης σε ένα ευρύ φάσμα πληροφοριών και υπηρεσιών οι οποίες τους βοηθούν να πάρουν πιο σωστές αποφάσεις σχετικά με την αγορά προϊόντων.
- **iv.** Υπάρχει η δυνατότητα, ο χρήστης, να παρακολουθεί την κατάσταση στην οποία βρίσκεται η παραγγελία του. Μέσω του δικτυακού ιστοτόπου του ηλεκτρονικού καταστήματος ή μέσω ηλεκτρονικού ταχυδρομείου ή ακόμη μέσω γραπτών μηνυμάτων στο κινητό.
- **v.** Προϊόντα όπως λογισμικό, φωτογραφίες, μουσικά και video αρχεία δύναται να παραδοθούν άμεσα μέσω του διαδικτύου, χωρίς να χρειάζεται ή αποστολή με το συμβατικό ταχυδρομείο.
- **vi.** Υπάρχει η δυνατότητα άμεσης ενημέρωσης των πελατών για νέες προσφορές και προϊόντα μέσω ηλεκτρονικών μηνυμάτων.
- **vii.** Για να εξυπηρετείται ο πελάτης το ηλεκτρονικό κατάστημα χρησιμοποιεί ένα σύστημα καταγραφής των ενεργειών που ακολούθησε κατά την επίσκεψη του. Έτσι, την επόμενη φορά που θα το επισκεφτεί, θα του γίνονται προτάσεις για τα διάφορα προϊόντα, ανάλογα με τα ενδιαφέροντα και τις προηγούμενες αγορές του.

Παράλληλα με τους καταναλωτές οι επιχειρήσεις έχουν τα αρκετά ωφέλει από το Ηλεκτρονικό Εμπόριο που αλώστε ήταν και ο βασικός λόγος υλοποίησής του.

- **i.** Η επιχείρηση επεκτείνει τα γεωγραφικά όρια των πωλήσεων της, εισάγοντας την σε περιοχές που ήταν μη προσβάσιμες στο παρελθόν.
- **ii.** Με τη βοήθεια αυτοματοποιημένων επιχειρησιακών διαδικασιών το ηλεκτρονικό εμπόριο αυξάνει την ταχύτητα και την ακρίβεια, μειώνοντας

παράλληλα το κόστος, με την οποία οι διάφορες επιχειρήσεις ανταλλάσουν πληροφορίες.

iii. Απλοποιούνται οι δοσοληψίες και οι πληρωμές, αφού αρκεί η ηλεκτρονική καταβολή των χρημάτων από τον πελάτη μέσω πιστωτικών ή άλλων καρτών.

iv. Κάθε επιχείρηση ηλεκτρονικού εμπορείου αυξάνει τις γνώσεις σχετικά με τις προτιμήσεις των παλετών της καθώς υπάρχει δυνατότητα καταγραφής και αποτίμησης των ιδιαίτερων αναγκών τους.

2ο Κεφάλαιο
Ηλεκτρονικό Εμπόριο – Είδη & Τεχνικές

2.1 Η Λειτουργία του Ηλεκτρονικού Εμπορίου

Η λειτουργία του Ηλεκτρονικού εμπορίου είναι απλή και βασίζετε στην δημιουργία μιας ιστοσελίδας (site) στην οποία οι επιχειρήσεις προβάλλουν τα προϊόντα τους. Είναι ουσιαστικά ένα είδος on-line καταλόγου με όλα τα προϊόντα τους, τα χαρακτηριστικά τους και βέβαια τις αντίστοιχες τιμές τους. Κάθε πελάτης έχει στη διάθεσή του ένα «καλάθι αγορών» στο οποίο «τοποθετεί» τα προϊόντα που επιθυμεί να αγοράσει. Μόλις ολοκληρώσει την ηλεκτρονική του βόλτα στο συγκεκριμένο site, δίνει την τελική παραγγελία η οποία και εκτελείται αυτόματα.

Η πληρωμή των αγαθών, όπως και οι παραγγελίες, γίνεται και αυτή ηλεκτρονικά, μέσω κάποιας πιστωτικής (ή προπληρωμένης) κάρτας του καταναλωτή. Εκτός από την πληρωμή με κάρτα υπάρχει και η δυνατότητα πληρωμής με αντικαταβολή, η οποία γίνεται μόλις ο πελάτης παραλάβει το προϊόν που έχει παραγγείλλει από το ηλεκτρονικό κατάστημα.

Η επιλογή του τρόπου πληρωμής είναι συνάρτηση των δυνατοτήτων που δίνει το εκάστοτε ηλεκτρονικό κατάστημα και της επιθυμίας του πελάτη. Για να προσελκύσουν περισσότερους πελάτες τα ηλεκτρονικά καταστήματα φροντίζουν να δίνουν περισσότερους τρόπους πληρωμής στους πελάτες τους ώστε να καλύπτουν όλες τις πιθανές επιθυμίες.

2.2 Τεχνολογίες Ηλεκτρονικού Εμπορίου

Μπορούμε να χρησιμοποιήσουμε μια πυραμίδα για να ταξινομήσουμε τις υποδομές που χρειάζεται το ηλεκτρονικό εμπόριο για να υλοποιηθεί. Στην βάση της πυραμίδας τοποθετούμε την Τηλεπικοινωνιακή Υποδομή την οποία αναπτύξαμε παραπάνω. Στην συνέχεια, πάνω ακριβώς από την υποδομή, τοποθετούμε τις Τεχνολογίες τους Ηλεκτρονικού Εμπορίου. Αμέσως μετά τις Εφαρμογές του και τέλος τις Τεχνικές και Στρατηγικές Διεπιχειρησιακής Ολοκλήρωσης.

Οι τεχνολογίες του ηλεκτρονικού εμπορίου αναπτύχθηκαν και εξελίσσονται με το πέρασμα των χρόνων σε συνάρτηση πάντα με τις ανάγκες της επιχείρησης αλλά και τις δυνατότητες του Διαδικτύου. Οι περισσότερες τεχνολογίες χρησιμοποιούνται εδώ και αρκετά χρόνια, έχοντας κερδίσει πολλές επιχειρήσεις οι οποίες τις χρησιμοποιούν.

Παράλληλα η ανάγκη για τη δημιουργία παγκόσμιων προτύπων και τεχνολογιών, δημιούργησε μια ομαδοποίηση των αναγκών των επιχειρήσεων με στόχο τη βελτίωση των παροχών αλλά και του τρόπου λειτουργίας του Ηλεκτρονικού Εμπορίου.

Στην συνέχεια θα αναπτύξουμε μερικές από τις τεχνολογίες που χρησιμοποιεί το Ηλεκτρονικό Εμπόριο και θα δούμε πόσο συνέβαλαν στην ομαλή και ασφαλή λειτουργία του.

I. Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI - Electronic Data Interchange)

Η Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI) είναι μία τυπική μορφή ανταλλαγής επιχειρησιακών δεδομένων. Δημιουργήθηκε στις αρχές της δεκαετίας του '70 και επιτρέπει, κυρίως σε μεγάλους οργανισμούς, να ανταλλάσουν πληροφορίες κάθε είδους μέσα από μεγάλα ιδιωτικά δίκτυα.

Κάθε μήνυμα EDI αποτελείται από μια ομάδα από σύμβολα πληροφοριών, καθένα από τα οποία αντιπροσωπεύει ένα μοναδικό στοιχείο, όπως την τιμή, τον αριθμό μοντέλου του προϊόντος κ.ο.κ. Οι ομάδες αυτές είναι χωρισμένες με οριοθέτες. Μια ομάδα συμβόλων ονομάζεται τμήμα δεδομένων. Κάθε τμήμα δεδομένων πλαισιώνεται από μία κεφαλίδα και ένα επίμετρο και αποτελεί τη μονάδα μεταφοράς EDI. Αυτές λοιπόν οι μονάδες μεταφοράς ανταλλάσσονται μεταξύ των επιχειρήσεων, οι οποίες αναφέρονται ως εμπορικοί εταίροι, μέσω ιδιωτικών δικτύων κυρίως.

Εικόνα 2.1. ***Ηλεκτρονική Ανταλλαγή Δεδομένων*** (EDI)

Τα μηνύματα EDI συνήθως κρυπτογραφούνται για λόγους ασφαλείας αφού περιέχουν σημαντικά δεδομένα των εταίρων. Παράλληλα το EDI είναι μια μορφή ηλεκτρονικού εμπορίου που περιλαμβάνει επίσης ηλεκτρονικό ταχυδρομείο και φαξ.

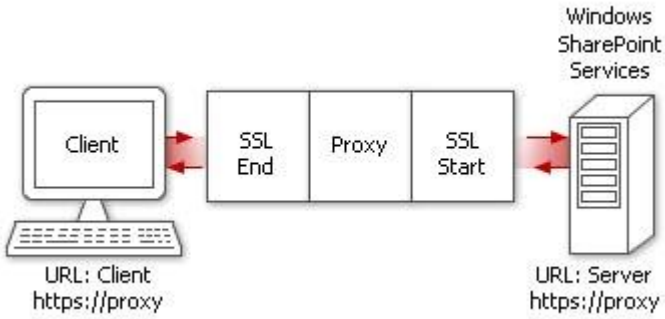
Τα πρότυπα που χρησιμοποιούνται σε παγκόσμιο επίπεδο προέρχονται από τον Οργανισμό Ηνωμένων Εθνών και καλύπτουν ένα ευρύ φάσμα επικοινωνιακών αναγκών των εμπορικών εταιριών. Το πρότυπο αυτό είναι το EDIFACT (EDI For Administration, Commerce and Transportation).

Η Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI) παρουσιάζει αρκετά πλεονεκτήματα όπως για παράδειγμα την μείωση της γραφικής εργασίας και παράλληλα της ανθρώπινης παρέμβασης η οποία έχει σαν αποτέλεσμα τη γρηγορότερη και λιγότερο επιρρεπής σε λάθη επεξεργασία. Υπάρχει καλύτερη αντιμετώπιση προβλημάτων και προσφέρονται καλύτερες υπηρεσίες προς τους πελάτες. Έτσι επιτυγχάνεται αύξηση του πελατολογίου αλλά και των προμηθευτών.
Ακόμη υπάρχει δυνατότητα για αυτοματοποιημένη διαχείριση αποθηκών ώστε να υπάρχει καλύτερη οργάνωση και ενημέρωση των προϊόντων.
Τέλος, ένα ακόμη πλεονέκτημα της EDI είναι ή ενίσχυση των τακτικών συναλλαγών οι οποίες πλέον γίνονται πιο εύκολες.

Σον αντίποδα τώρα των πλεονεκτημάτων υπάρχουν και κάποια αρνητικά στοιχεία τα οποία όμως δεν εμπόδισαν την εξέλιξη του. Για παράδειγμα η πολύπλοκη και δαπανηρή υλοποίηση των δικτύων όπως η χρήση ακριβών υλικών για τα Value Added Networks (VANs), είναι ένας ανασταλτικός παράγοντας για τη χρήση τους.
Ακόμη πολλές φορές η ύπαρξη δύο διαφορετικών EDI προτύπων καθιστά προβληματική τη συνεργασία μεταξύ αμερικάνικων και ευρωπαϊκών εταιρειών.

II. Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)[5]

Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από τη Netscape το 1996 και αποτέλεσε τη βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.



Εικόνα 2.2. **Μεταφορά δεδομένων με πρωτόκολλο** SSL

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών)

[5] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ : http://el.wikipedia.org/wiki/SSL

εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

III. Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)[6]

Η τεχνολογία SET αναπτύχθηκε για την εξακρίβωση και γνησιότητας ταυτότητας μεταξύ εμπόρων και καταναλωτών πριν από μία ηλεκτρονική συναλλαγή. Συγκεκριμένα παρέχει εμπιστευτικότητα και ακεραιότητα των κρίσιμων μεταδιδόμενων πληροφοριών αλλά και πιστοποίηση ότι ο έμπορος μπορεί να δέχεται συναλλαγές με πιστωτική κάρτα μέσω συνεργασίας από κάποιο οικονομικό οργανισμό αλλά και πιστοποίηση ότι ο κάτοχος της κάρτας είναι πραγματικά ο νόμιμος και γνήσιος χρήστης του λογαριασμού. Το SET δημιουργήθηκε από τη Visa και τη MasterCard.

IV. Ραβδωτός κώδικας (Barcode)[7]

Ραβδωτός Κώδικας ή γραμμωτός κώδικας η ραβδοκώδικας ονομάζεται η εφαρμογή οπτικής αναγνώρισης, η οποία αποτελείται από ένα σύνολο παράλληλων ανισόπαχων γραμμών και η οποία περιέχει πληροφορίες που αφορούν στο προϊόν στο οποίο αναγράφεται.

Συγκεκριμένα, οι γραμμές αντιστοιχούν στην περιγραφή και τα χαρακτηριστικά του προϊόντος, την ημερομηνία λήξης την τιμή, αλλά και το απόθεμα που υπάρχει σε μια αποθήκη κ.ά.

Η ανάπτυξη της τεχνολογίας του γραμμωτού κώδικα ξεκίνησε στις αρχές της δεκαετίας του 1960, με σκοπό να εξυπηρετήσει την πληρωμή προϊόντων στα καταστήματα τροφίμων. Οι πρώτες εφαρμογές σε βιομηχανικό περιβάλλον εμφανίστηκαν στα τέλη της ίδιας δεκαετίας σε μεγάλες αυτοκινητοβιομηχανίες, για τον περιορισμό του κόστους εργασίας που σχετιζόταν με την παραγωγή. Εκτεταμένη χρήση παρουσιάστηκε μετά την ανάπτυξη των πρώτων προτύπων (λόγω των πιέσεων των αρκετών πλέον χρηστών - προμηθευτών, υποκατασκευαστών των μεγάλων βιομηχανιών) στα τέλη της δεκαετίας του 1970. Κατά τη δεκαετία του 1980 υπήρξε αλματώδης ανάπτυξη του εξοπλισμού, κατ' επέκταση και των τρόπων χρήσης της τεχνολογίας γραμμωτού κώδικα.

---

[6] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ : http://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA

[7] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ http://el.wikipedia.org/wiki/%CE%A1%CE%B1%CE%B2%CE%B4%CF%

Εικόνα 2.3. **Ραβδωτός ή Γραμμωτός Κώδικας**

Η τεχνολογία του ραβδωτού κώδικα αποτελεί κομμάτι της μεγάλης οικογένειας των τεχνολογιών αυτόματης αναγνώρισης (Auto ID Technologies). Αποτελεί ένα σύγχρονο εργαλείο, με την βοήθεια του οποίου γίνεται πιο ομαλή, εύκολη και λειτουργική η διακίνηση και διαχείριση προϊόντων και υπηρεσιών.

Η ανάπτυξη της τεχνολογίας του γραμμωτού κώδικα ξεκίνησε στις αρχές της δεκαετίας του 1960, με σκοπό να εξυπηρετήσει την πληρωμή προϊόντων στα καταστήματα τροφίμων. Οι πρώτες εφαρμογές σε βιομηχανικό περιβάλλον εμφανίστηκαν στα τέλη της ίδιας δεκαετίας σε μεγάλες αυτοκινητοβιομηχανίες, για τον περιορισμό του κόστους εργασίας που σχετιζόταν με την παραγωγή. Εκτεταμένη χρήση παρουσιάστηκε μετά την ανάπτυξη των πρώτων προτύπων (λόγω των πιέσεων των αρκετών πλέον χρηστών - προμηθευτών, υποκατασκευαστών των μεγάλων βιομηχανιών) στα τέλη της δεκαετίας του 1970. Κατά τη δεκαετία του 1980 υπήρξε αλματώδης ανάπτυξη του εξοπλισμού, κατ' επέκταση και των τρόπων χρήσης της τεχνολογίας γραμμωτού κώδικα.

V. Έξυπνες κάρτες (Smart Cards)[8]

Έξυπνη κάρτα (smart card) είναι μια κάρτα, η οποία μοιάζει πολύ εξωτερικά με τη γνωστή πιστωτική κάρτα. Εσωτερικά, όμως, διαφέρει σημαντικά από αυτήν. Η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία (magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη.

Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της.

[8] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ http://el.wikipedia.org/wiki/%CE%88%CE%BE%CF%85%CF%80%CE%B

Εικόνα 2.4. **Δομή Έξυπνης Κάρτας**

Η βασική διαφορά των δύο τύπων καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη: Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα.

Εικόνα 2.5. ***Αναγνώστης Έξυπνης Κάρτας*** (Smart Card Reader)

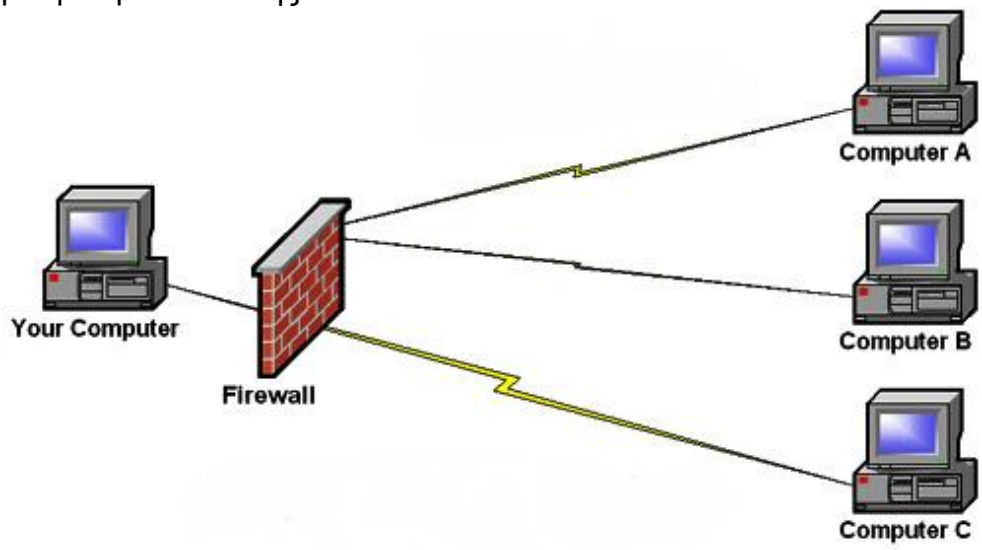
Οι έξυπνες κάρτες αποτελούν εξέλιξη των καρτών μαγνητικής λωρίδας με τη διαφορά ότι μπορούν να αποθηκεύσουν μεγάλη ποσότητα δεδομένων ενώ παράλληλα παρέχουν δυνατότητες κρυπτογράφησης και χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια των περιεχομένων τους.

Η έξυπνη κάρτα χρησιμοποιείται κυρίως στις εξής εφαρμογές:

- Τραπεζικές συναλλαγές (συσκευές ΑΤΜ, πιστωτικές κάρτες, κάρτες ανάληψης κτλ.)
- Συναλλαγές με υπηρεσίες κοινής ωφέλειας (π.χ. ΙΚΑ , ΟΓΑ , ΕΟΠΥΥ).
- Δορυφορικοί δέκτες (για την λήψη συνδρομητικών καναλιών)
- Συστήματα ασφαλείας υπολογιστών
- Συστήματα απαγόρευσης πρόσβασης σε μη εξουσιοδοτημένο προσωπικό.
- Κινητή τηλεφωνία
- Αυτόματα μηχανήματα πώλησης αγαθών.

VI. Πιστοποίηση και ασφάλεια[9]

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης , ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης.



Εικόνα 2.6. **Λειτουργία** Firewall

[9] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ http://el.wikipedia.org/wiki/Firewall

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά.

VII. Extranet

Extranet είναι ένα δίκτυο με ελεγχόμενη πρόσβαση που χρησιμοποιεί την τεχνολογία του Διαδικτύου για να μοιραστεί δημόσιες πληροφορίες/δεδομένα αλλά να κρατά ασφαλή τις ιδιωτικές πληροφορίες/δεδομένα. Συνήθως το extranet είναι μέρος ενός μεγαλύτερου ενδοδικτύου.

Εικόνα 2.7. **Ταξινόμηση Δικτύων**

Χρησιμοποιεί και αυτό κάποιον φυλλομετρητή σελίδων (browser) όπως και το Internet και συνήθως είναι μια απλή, ασφαλής περιοχή ανταλλαγής εγγράφων που είναι πολύ μεγάλα για να αποσταλούν με email ή ένας χώρος όπου η εργασία μπορεί να παρακολουθείται και να εγκρίνεται από απόσταση.

VIII. CMS (Σύστημα Διαχείρισης Περιεχομένου)[10]

Τα Συστήματα Διαχείρισης Περιεχομένου (ΣΔΠ, Content Management Systems, CMS) είναι διαδικτυακές εφαρμογές που επιτρέπουν την online τροποποίηση του περιεχομένου ενός δικτυακού τόπου.
Οι διαχειριστές, οι οποίοι δεν χρειάζεται να είναι εξειδικευμένοι, μέσω του διαδικτύου ενημερώνουν το περιεχόμενο στο ΣΔΠ, το οποίο είναι εγκατεστημένο σ' ένα διακομιστή. Οι αλλαγές αυτές γίνονται αυτόματα διαθέσιμες πάλι μέσω του διαδικτύου, σε όλους τους επισκέπτες και χρήστες του δικτυακού τόπου.
Παρόλο που η δημιουργία του συστήματος απαιτεί σημαντικό κεφάλαιο από την επιχείρηση, μπορεί να αποτελέσει σημαντικό και απαραίτητο εργαλείο για την εύκολη και άμεση ενημέρωση του ηλεκτρονικού καταστήματος της.

IX. CRM (Customer Relationship Management)

Το CRM (Customer Relationship Management) είναι μια επιχειρηματική στρατηγική, που στοχεύει στην μεγιστοποίηση των εσόδων και των κερδών, και στην αύξηση της ικανοποίησης των πελατών. Η «φιλοσοφία» CRM υποστηρίζει τεχνολογίες που

[10] Πηγή : ΒΙΚΙΠΑΙΔΕΙΑ http://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%

συγκεντρώνουν και αποθηκεύουν δεδομένα για τους προμηθευτές, τους πελάτες, τους συνεργάτες αλλά και τις εσωτερικές διαδικασίες μιας επιχείρησης.
Το CRM χαρακτηρίζεται ως πελατοκεντρικό και στόχος του είναι η διαχρονική πώληση και η εξυπηρέτηση πελατών, οι οποίοι είναι πιστοί στα προϊόντα και τις υπηρεσίες, μέσα από ένα συγκεκριμένο σύστημα διαχείρισης.

Το CRM μπορεί να χωριστεί σε δύο βασικούς τύπους.[11]

- Το Operational CRM το οποίο παρέχει front-office υποστήριξη στις Πωλήσεις, το Marketing και την Εξυπηρέτηση Πελατών. Όλες οι κινήσεις κάποιου πελάτη καταγράφονται στο «ιστορικό επαφών» του συγκεκριμένου πελάτη, δίνοντας έτσι τη δυνατότητα στο προσωπικό μιας επιχείρησης να μπορεί να καλέσει δεδομένα από μια βάση, όποτε αυτό είναι απαραίτητο. Το μεγαλύτερο πλεονέκτημα είναι πως κάθε πελάτης μπορεί να έρχεται σε επαφή με πολλά διαφορετικά άτομα της επιχείρησης, χωρίς να χρειάζεται να εξηγεί κάθε φορά όλο το ιστορικό των ενεργειών που έχουν γίνει. Το Operational CRM μαζεύει δεδομένα για τους πελάτες μιας επιχείρησης, ώστε:
    - Να διαχειρίζονται ευκολότερα οι προωθητικές ενέργειες (καμπάνιες)
    - Να αυτοματοποιούνται πολλές λειτουργίες Marketing
    - Αυτοματοποίηση των Πωλήσεων και της Παραγγελιοληψίας
- Analytical CRM το οποίο συνιστά την λογική συνέχεια του Operational CRM. Κάθε επιχείρηση η οποία έχει υλοποιήσει Operational CRM, ενημερώνει και εμπλουτίζει μια βάση δεδομένων με σκοπό την καθημερινή καταγραφή, την αυτοματοποίηση των διαδικασιών και την διαχείριση των σχέσεων με τους πελάτες. Στην συνέχεια το τμήμα Marketing της επιχείρησης καλείται να αναλύσει με τη βοήθεια των εργαλείων του Analytical CRM και να βγάλει χρήσιμα συμπεράσματα. Το Analytical CRM πραγματοποιεί:
    - Στοχευμένες καμπάνιες marketing
    - Εξειδικευμένες καμπάνιες marketing, με σκοπό το cross-selling και το up-selling
    - Ανάλυση της συμπεριφοράς των πελατών, ώστε να υποστηριχθεί η διαδικασία λήψεις αποφάσεων σχετικά με τα προϊόντα και τις προσφερόμενες υπηρεσίες
    - Ανάλυση κερδοφορίας (γενικότερα, αλλά και ανά πελάτη)

Ø Η Ελληνική Αγορά CRM

Σε έρευνα που πραγματοποίησε το Ebusinessforum[12] διαπιστώθηκε ότι οι Έλληνες επαγγελματίες θεωρούν πολύ σημαντικό θέμα, για την επιχείρηση τους, να

[11] Πηγή : Περιοδικό ΕΠΙΧΕΙΡΕΙΝ: http://epixeirein.gr/2008/04/04/crm-epixeirisi/
[12] Το Ebusinessforum (www.ebusinessforum.gr) είναι ένας μόνιμος μηχανισμός διαβούλευσης της Πολιτείας με την επιχειρηματική και ακαδημαϊκή κοινότητα με σκοπό την επεξεργασία θέσεων και προτάσεων που προάγουν την ηλεκτρονική επιχειρηματικότητα στην Ελλάδα, καθώς και τη διάδοση του ηλεκτρονικού επιχειρείν στις ελληνικές επιχειρήσεις. Στο Forum συμμετέχουν στελέχη από όλους τους επιχειρηματικούς κλάδους με έμφαση

υιοθετήσει την CRM προσέγγιση. Παραθέτουμε παρακάτω την καρτέλα που παρουσιάζει τα αποτελέσματα της έρευνας στην ερώτηση «Που χρησιμοποιείτε το CRM»

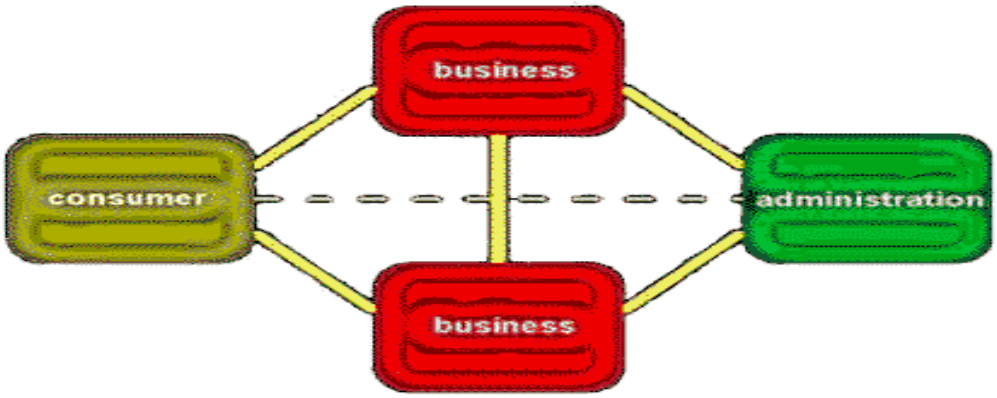
	Ποσοστό %
Καταγραφή Παραπόνων Πελατών	33,8
Καταγραφή Προτιμήσεων Πελατών	30,9
Επικοινωνία με Πελάτες (direct marketing και αποστολή φυλλαδίων)	30,9
Υλοποίηση Προγραμμάτων Πιστότητας	20,6
Παρακολούθηση Αποτελεσματικότητας Πωλητών	33,8
Προσαρμογή Προϊόντων σε απαιτήσεις μεμονωμένων Πελατών	20,6
Καθορισμός Τιμολογιακής Πολιτικής Προϊόντων	25,0
Σχεδιασμός Νέων Προϊόντων	26,5
Λήψη Στρατηγικών Αποφάσεων Marketing	29,5
Παρακολούθηση Κερδοφορίας Προγραμμάτων Πιστότητας	20,6
Παρακολούθηση όγκου πωλήσεων ανά πελάτη / τμήμα πελατών	29,4
Σχεδιασμός επικοινωνιακής στρατηγικής	22,1
Cross Selling	27,9

Εικόνα 2.8. **Χρήση του** CRM **στις ελληνικές επιχειρήσεις**

στον κλάδο Πληροφορικής και Τηλεπικοινωνιών, από Πανεπιστημιακά και Ερευνητικά Ιδρύματα, από τον Δημόσιο τομέα καθώς και εκπρόσωποι των κοινωνικών εταίρων και των καταναλωτών.

2.3 Τα Είδη του Ηλεκτρονικού Εμπορίου

Στο ηλεκτρονικό εμπόριο μπορούμε να διακρίνουμε 4 εμφανείς κατηγορίες οι οποίες διαμορφώνονται ανάλογα με το ποια είναι τα συναλλασσόμενα μέρη. Οι κατηγορίες αυτές είναι:



Εικόνα 2.9. **Σχέση Επιχείρηση – Πελάτης – Διαχειριστής Διαδικτύου**

- Ηλεκτρονικό εμπόριο Επιχείρησης προς Καταναλωτή (Business to Costumer-B2C)
- Ηλεκτρονικό εμπόριο Επιχείρησης προς Επιχείρηση (Business to Business-B2B)
- Ηλεκτρονικό εμπόριο Επιχείρησης προς Δημόσια διοίκηση (Business to Government-B2G)
- Ηλεκτρονικό εμπόριο Καταναλωτή προς Δημόσια διοίκηση (Costumer to Government-B2G)

- **Ηλεκτρονικό εμπόριο Επιχείρησης προς Καταναλωτή (B2C)**

Η κατηγορία επιχείρηση προς καταναλωτή ουσιαστικά αντιστοιχεί στο ηλεκτρονικό λιανικό εμπόριο. Εκεί ανήκουν όλες οι εφαρμογές ηλεκτρονικού εμπορίου, οι οποίες αναπτύσσονται με στόχο την απευθείας πώληση προϊόντων στους τελικούς καταναλωτές.

Η κατηγορία αυτή εξαπλώθηκε πολύ γρήγορα με την ανάπτυξη του παγκόσμιου ιστού (Word Wide Web) και των τεχνολογιών ασφαλούς πληρωμής μέσω διαδικτύου. Πλέον υπάρχουν «εμπορικά κέντρα» σε όλο το διαδίκτυο , προσφέροντας κάθε είδους καταναλωτικών αγαθών, από τρόφιμα και είδη πρώτης ανάγκης μέχρι αυτοκίνητα και σκάφη.

- **Ηλεκτρονικό εμπόριο Επιχείρησης προς Επιχείρηση (B2B)**

Το ηλεκτρονικό εμπόριο αυτής της μορφής, όπως μαρτυρά και το όνομα B2B, αφορά την διενέργεια ηλεκτρονικών εμπορικών συναλλαγών μεταξύ επιχειρήσεων και αφορά κυρίως πωλήσεις χονδρικής και αγορά προμηθειών.

Για παράδειγμα μια Εταιρία μπορεί να χρησιμοποιεί ένα δίκτυο παραγγελίας, για τους προμηθευτές της, λαμβάνοντας τιμολόγια αλλά και κάνοντας πληρωμές. Η κατηγορία «Επιχείρηση προς Επιχείρηση» (B2B) λειτουργεί εδώ και αρκετά χρόνια χρησιμοποιώντας συγκεκριμένα τη τεχνολογία της Ηλεκτρονικής Ανταλλαγής Εγγράφων (Electronic data interchange-EDI).

Το τελευταίο διάστημα έχει αρχίσει να αναπτύσσεται ιδιαίτερα Μια άλλη μορφή ηλεκτρονικού εμπορίου της κατηγορίας επιχείρηση προς επιχείρηση με τον όρο ηλεκτρονικές αγορές B2B (B2B Marketplaces).

- **Ηλεκτρονικό εμπόριο Επιχειρήσεις προς Δημόσια διοίκηση και Καταναλωτή προς Δημόσια διοίκηση (B2G)**

Οι κατηγορίες αυτές καλύπτουν συναλλαγές ανάμεσα σε εταιρείες ή ιδιώτες και φορείς της δημόσιας διοίκησης.

Έτσι μπορεί ένα υπουργείο ή μια δημόσια υπηρεσία να δημοσιεύσει τυχών προμήθειες που μπορεί να χρειαστεί στο διαδίκτυο και οι εταιρείες μπορούν να ανταποκριθούν ηλεκτρονικά.

Ήδη στα πλαίσια του επιχειρησιακού προγράμματος κοινωνία της πληροφορίας προγραμματίζεται να αναπτυχθούν πολλές εφαρμογές οι οποίες θα εξυπηρετούν τις συναλλαγές των πολιτών αλλά με φορείς της δημόσιας διοίκησης.

Σε αυτή την κατηγορία εφαρμογών ανήκει και το πρόγραμμα TAXIS το οποίο λειτουργεί τα τελευταία χρόνια στην Ελλάδα και μέσω του οποίου μπορεί να γίνει υποβολή φορολογικών δηλώσεων, δηλώσεων Φ.Π.Α κ.λπ.

2.4 Σύγκριση – Αξιολόγηση

Δεδομένου ότι οι πιο βασικές και περισσότερο ανεπτυγμένες κατηγορίες του Ηλεκτρονικού Εμπορίου θεωρούνται το ηλεκτρονικό εμπόριο επιχείρησης προς επιχείρησης και το εμπόριο επιχείρησης προς καταναλωτή μπορούμε να κάνουμε μια σύγκριση μεταξύ τους.

Το ηλεκτρονικό εμπόριο επιχείρησης προς καταναλωτή (B2C)

Οι εφαρμογές που αναπτύσσονται στην κατηγορία B2C έχουν την μορφή ηλεκτρονικών καταστημάτων στα οποία έχει πρόσβαση ο κάθε χρήστης του διαδικτύου με σκοπό να δει και τελικά να αγοράσει προϊόντα.

Παράλληλα προσομοιώνει το λιανικό εμπόριο και εφαρμόζεται από επιχειρήσεις οι οποίες θέλουν να πωλήσουν τα προϊόντα και τις υπηρεσίες τους, απευθείας στους τελικούς καταναλωτές.

Το ηλεκτρονικό κατάστημα δεν «γνωρίζει» τον κάθε «ηλεκτρονικό» πελάτη δεδομένου ότι αυτός μπορεί να είναι κάθε χρήστης το internet. Η συνολική αξία των ηλεκτρονικών συναλλαγών της κατηγορίας B2C είναι μικρότερη από ότι στην κατηγορία B2B.

Το ηλεκτρονικό εμπόριο επιχείρησης προς επιχειρήσεις (B2B)

Μοιάζει με το χονδρικό εμπόριο και πραγματοποιείται μεταξύ 2 επιχειρήσεων του προμηθευτή και του αγοραστή. Ουσιαστικά εφαρμόζεται από κάποιες επιχειρήσεις που θέλουν να πουλήσουν τα προϊόντα που παράγουν ή εμπορεύονται σε άλλες επιχειρήσεις.

Όσες επιχειρήσεις συμμετέχουν σε μια τέτοιου είδους ηλεκτρονική αγορά έχουν τη δυνατότητα να «γνωρίσουν» καλύτερα η μία την άλλη, αφού όλες είναι συνήθως μέλη μιας συγκεκριμένης αγοράς.

Εδώ οι ποσότητες των αγαθών που διακινούνται είναι πολύ μεγαλύτερες, συνήθως, από αυτές της κατηγορίας B2C.

Οι τρόποι επικοινωνίας και οι μέθοδοι παρουσίασης και παραγγελίας κάποιου προϊόντος είναι παρόμοιοι αφού χρησιμοποιούνται ανάλογες πλατφόρμες και εφαρμογές. Στην περίπτωση του B2B όμως υπάρχουν επιπλέον δυνατότητες στις εφαρμογές λόγω ,κυρίως, του μεγάλου όγκου παραγγελιών.

Βέβαια υπάρχει πάντα και η δυνατότητα μια επιχείρηση να εφαρμόσει και τους δυο τύπους ηλεκτρονικού εμπορίου (B2B & B2C), ανάλογα με τον κλάδο στον οποίο δραστηριοποιείται και τον τύπο της.

Για παράδειγμα μπορεί μια επιχείρηση που πουλά τα προϊόντα της απευθείας σε καταναλωτές, έχοντας αναπτύξει μια πλατφόρμα μέσω internet (εφαρμογή του B2C ηλεκτρονικό εμπόριο). Παράλληλα μπορεί να προμηθεύεται τις πρώτες ύλες ή άλλα προϊόντα, συμμετέχοντας σε μια ηλεκτρονική αγορά (εφαρμογή B2B ηλεκτρονικό εμπόριο)

2.5 Άλλα είδη Ηλεκτρονικού Εμπορίου[13]

Εκτός από τα προαναφερθέντα είδη του ηλεκτρονικού εμπορίου υπάρχουν και οι παρακάτω κατηγορίες οι οποίες δεν είναι τόσο διαδεδομένες αλλά είναι εξίσου σημαντικές :

[13] **Πηγή:** Εισαγωγή στις Νέες Τεχνολογίες και το Ηλεκτρονικό Εμπόριο – Ελευθέριος Παπαθανασίου (Καθηγητής Επιχειρηματικής Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών)

- **Μη επιχειρησιακό Ηλεκτρονικό Εμπόριο (Nonbusiness e-commerce)**

Πολλοί οργανισμοί, όπως για παράδειγμα τα εκπαιδευτικά ιδρύματα, μη κερδοσκοπικοί οργανισμοί, θρησκευτικές, κοινωνικές και πολιτιστικές οργανώσεις και διάφορες υπηρεσίες του δημόσιου τομέα έχουν πρόσφατα αρχίσει να χρησιμοποιούν διάφορους τύπους Ηλεκτρονικού Εμπορίου. Στόχος τους είναι η μείωση των τα εξόδων τους, η βελτίωση των λειτουργιών τους και η καλύτερη εξυπηρέτηση των μελών τους.

- **Ενδοεπιχειρησιακό Ηλεκτρονικό Εμπόριο (Intrabusiness EC).**

Η κατηγορία αυτή αναφέρεται σε εσωτερικές επιχειρησιακές διεργασίες, που συνήθως εκτελούνται μέσω Intranet (Ενδοδίκτυα). Περιλαμβάνονται ανταλλαγές αγαθών, υπηρεσιών και πληροφοριών. Παραδείγματα συναλλαγών είναι η μαζική πώληση προϊόντων σε εργαζομένους, η τηλεκπαίδευση, η ψυχαγωγία και άλλα.

3ο Κεφάλαιο
Το Ηλεκτρονικό Εμπόριο στην Ελλάδα

3.1 Χρήση του Ιντερνετ στην Ελλάδα

Η Γενική Γραμματεία Εθνικής Στατιστικής Υπηρεσίας της Ελλάδος[14] εκπόνησε έρευνα η οποία αφορά τη χρήση τεχνολογιών πληροφορικής και επικοινωνίας από τα νοικοκυριά το έτος 2006 και ειδικότερα το ηλεκτρονικό εμπόριο. Η Έρευνα διενεργήθηκε σε ολόκληρη τη Χώρα, σε τελικό δείγμα 4.896 ιδιωτικών νοικοκυριών και σε ισάριθμα μέλη αυτών, με κριτήριο την ύπαρξη ενός, τουλάχιστον, μέλους ηλικίας 16 – 74 ετών σε κάθε νοικοκυριό. Περίοδος αναφοράς της Έρευνας είναι το Α' τρίμηνο του 2006.

Με την Έρευνα αυτή συγκεντρώνονται αναλυτικές πληροφορίες που αφορούν στην πρόσβαση των νοικοκυριών σε επιλεγμένες τεχνολογίες πληροφόρησης και επικοινωνίας, π.χ. ηλεκτρονικό υπολογιστή, κινητό τηλέφωνο, ψηφιακή τηλεόραση, διαδίκτυο κλπ. Ακόμη, συγκεντρώνονται ατομικές πληροφορίες, οι οποίες παρέχονται από το άτομο που έχει προεπιλεγεί και αφορούν στη χρήση ηλεκτρονικού υπολογιστή, στην πρόσβαση στο διαδίκτυο (συναλλαγές με δημόσιες υπηρεσίες μέσω διαδικτύου, εμπορικές συναλλαγές στο διαδίκτυο κλπ.) και στις e-δεξιότητες. Η Έρευνα πραγματοποιήθηκε για πρώτη φορά στη Χώρα μας το 2002 και τα αποτελέσματά της είναι πλήρως εναρμονισμένα με τα στοιχεία των υπόλοιπων κρατών μελών της ΕΕ που διενεργούν την έρευνα, αφού αυτή πραγματοποιείται με κοινά αποδεκτό ερωτηματολόγιο.

Τα αποτελέσματα που προκύπτουν από την έρευνα αναφέρουν ότι :

- το 28,9% του συνολικού πληθυσμού της χώρας είχε πρόσβαση στο διαδίκτυο κατά το Α′ τρίμηνο του έτους,

- 35,0% του πληθυσμού που έκανε οποτεδήποτε χρήση του διαδικτύου

Βλέπουμε λοιπόν ότι μεγάλο ποσοστό των Ελλήνων κάνει χρήση του διαδικτύου και γνωρίζει την ύπαρξη και την λειτουργία του.

Αύξηση το 2011

Σε νεότερη έρευνα της Εθνικής Στατιστικής Υπηρεσίας Ελλάδος[15], η οποία πραγματοποιήθηκε στις αρχές του 2011, παρουσιάζετε μια σημαντική άνοδος στη χρήση του ηλεκτρονικού υπολογιστή αλλά και του διαδικτύου.

[14] Ελληνική Στατιστική Αρχή (ΕΛ.ΣΤΑΤ.) www.statistics.gr

[15] **Πηγή:** ΕΛ.ΣΤΑΤ (Στατιστικά Θέματα: Τεχνολογία - Κοινωνία Πληροφορίας) http://www.statistics.gr/portal/page/portal/ESYE/PAGE-themes?p_param=A190

Στο Α' τρίμηνο του 2011 το ποσοστό των ατόμων που έκανα χρήση του διαδικτύου (περιστασιακά) ανέρχεται στο 51,7%. Ενώ το ποσοστό των ατόμων που απλά χρησιμοποίησαν τον ηλεκτρονικό υπολογιστή ήταν 54,3%.

Η χρήση του διαδικτύου ή του ηλεκτρονικού υπολογιστή μπορεί να έχει γίνει από διάφορους χώρους όπως οικια, εργασία, χώροι εκπαίδευσης, φιλικά σπίτια, ξενοδοχεία, internet café κτλ.

Οι κυριότεροι λόγοι χρήσης διαδικτύου (πλοήγησης) είναι:

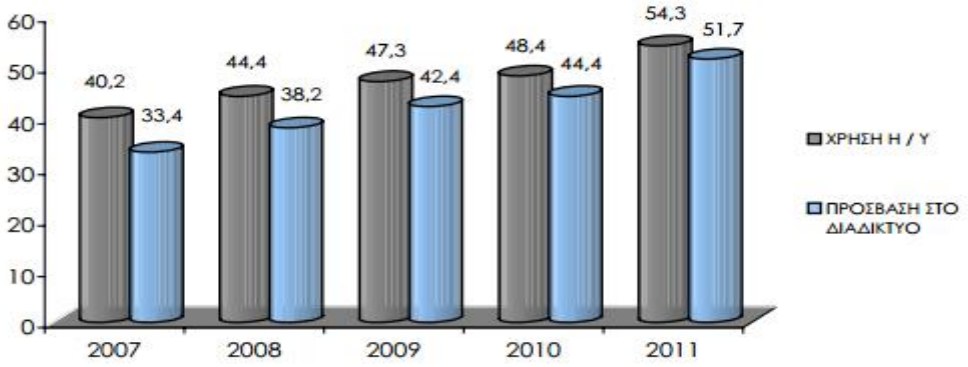
- Αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες. (77,8%)
- Αναζήτηση ή λήψη ηλεκτρονικών μηνυμάτων. (72,9%)
- Αναζήτηση πληροφοριών για ταξίδια και καταλύματα. (58,1%)
- Ανάγνωση πάσης φύσεως πληροφοριών με σκοπό τη γνώση. (54,9%)
- Ανάγνωση εφημερίδων και περιοδικών. (50.0%)
- Αποστολή μηνυμάτων σε chat sites, blogs, σε ομάδες συζήτησης (My Space, Facebook), συμμετοχή σε forums, ανταλλαγή γραπτών μηνυμάτων σε πραγματικό χρόνο (Messenger, Skype κ.α.). (42,3%)

Σημαντικό γεγονός αποτελεί ότι οι ηλιακή ομάδα 18-24 ετών επέλεξε σε ποσοστό 64% τον τελευταίο λόγο.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν και οι λόγοι για τους οποίους κάποια νοικοκυριά δεν έχουν Ίντερνετ στο σπίτι.

Τα τελευταία 5 χρόνια (2007-2011) υπάρχει ραγδαία αύξηση η οποία ανέρχεται σε 35,1% για χρήση του ηλεκτρονικού υπολογιστή και 54,8% για πρόσβαση στο διαδίκτυο.

Στο παρακάτω διάγραμμα παρουσιάζεται η αύξηση αυτή :



Εικόνα 3.1. **Χρήση ηλεκτρονικού υπολογιστή και πρόσβαση στο διαδίκτυο**: ***Α*' τρίμηνο** 2007-2011 (% **των ατόμων**)

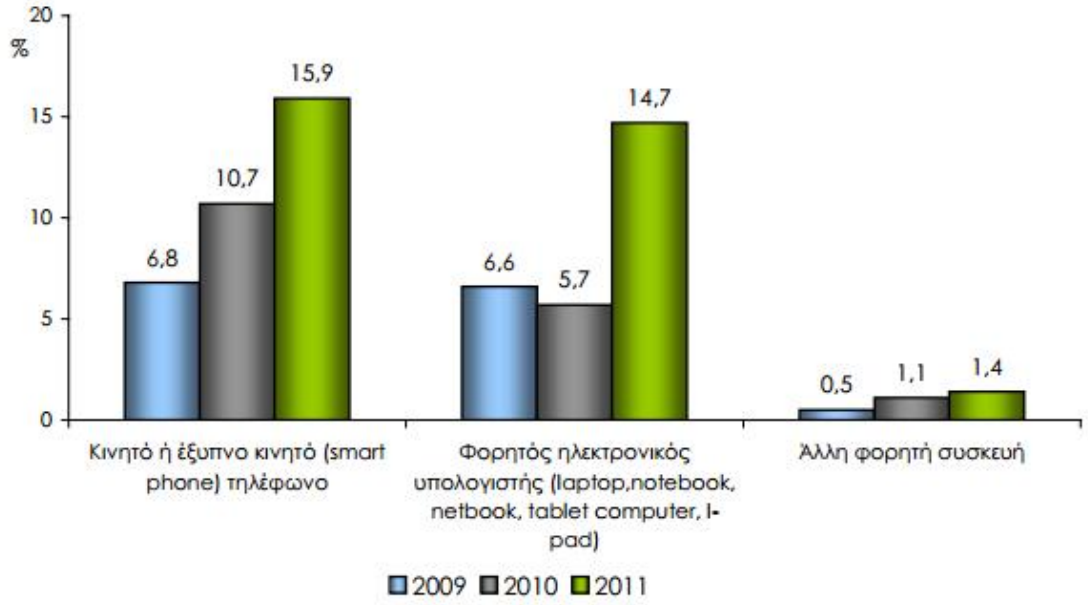
3.2 Το Ηλεκτρονικό Εμπόριο στην Ελλάδα

Η παραπάνω έρευνες της ΕΛ.ΣΤΑΤ επιβεβαιώνουν ότι το Ηλεκτρονικό Εμπόριο στην Ελλάδα αναπτύσσεται, αλλά με πιο αργούς ρυθμούς σε σχέση με τα υπόλοιπα ανεπτυγμένα Ευρωπαϊκά κράτη. Αυτό βέβαια είναι κάτι που δεν πρέπει να μας παραξενεύει διότι είναι γνωστό ότι σαν λαός έχουμε πιο αργούς ρυθμούς αφομοίωσης και ενστερνισμού των νέων τεχνολογιών και του internet.

Στην πενταετία 2007-2011, οι ηλεκτρονικοί καταναλωτές στην Ελλάδα παρουσίασαν αύξηση και πενταπλασιάστηκαν. Παράλληλα οι τάσεις, των ελλήνων χρηστών, για το μέλλον προβλέπονται αυξητικές. Έτσι μπορούμε να πούμε ότι το ηλεκτρονικό εμπόριο, στην Ελλάδα, έχει φύγει από την φάση της αποδοχής και βρίσκεται στην φάση της ωρίμανσης.

Ακόμη μελετώντας δεδομένα από έρευνες που έχουν πραγματοποιήσει, τα τελευταία χρόνια, εταιρείες κινητής τηλεφωνίας βλέπουμε ότι πάνω από το 50% του ενεργού πληθυσμού της χώρας κατέχει κινητό τηλέφωνο. Μεγάλο ποσοστό των κατόχων χρησιμοποιούν κινητά τελευταίας τεχνολογία (smart phones) μέσω των οποίων μπορούν να έχουν πρόσβαση στο internet αλλά και σε διάφορες εφαρμογές και υπηρεσίες.

Στο παρακάτω διάγραμμα βλέπουμε την αύξηση που παρουσιάζεται στη χρήση του διαδικτύου με πρόσβαση από κινητή συσκευή.



Εικόνα 3.2. **Πρόσβαση στο διαδίκτυο από κινητή συσκευή ανά είδος κινητής συσκευής**: ***Α*' τρίμηνο** 2009-2011

Η έρευνα έγινε από την ΕΛ.ΣΤΑΤ[16] και αφορούσε τη χρήση τεχνολογιών πληροφόρησης και επικοινωνίας για το έτος 2011.

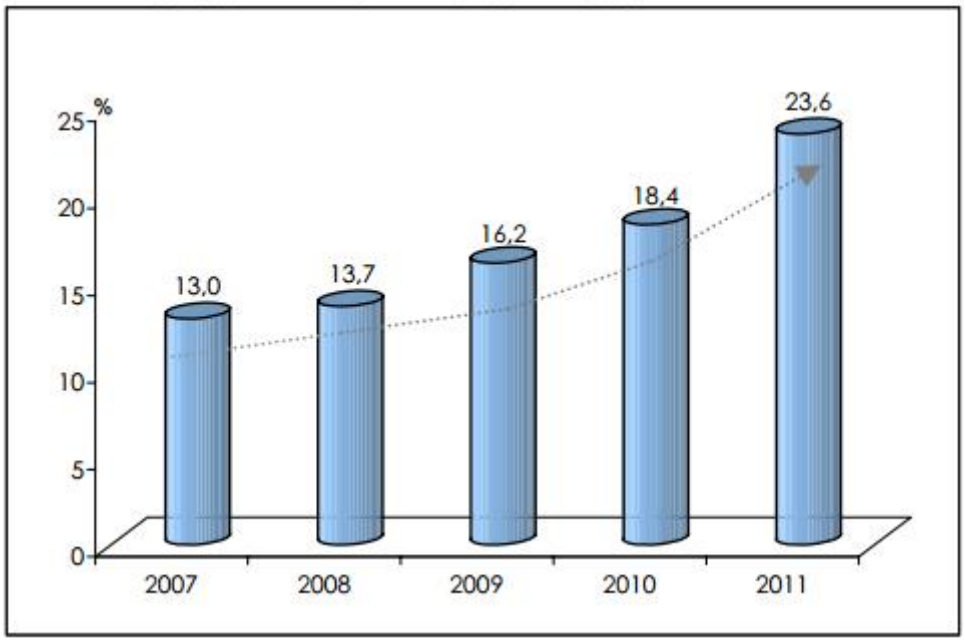
Σε ότι αφορά τις ελληνικές επιχειρήσεις και την χρήση του internet από αυτές παρατηρείται μια σταδιακή εξάπλωση του Ηλεκτρονικού Εμπορίου προς δύο κατευθύνσεις:

I. Επιχειρήσεις που ήδη υπάρχουν χρησιμοποιούν το Internet κυρίως για προώθηση των προϊόντων / υπηρεσιών τους.

II. Νέες επιχειρήσεις που δημιουργούνται στα πρότυπα των αντίστοιχων διεθνών οργανισμών με στόχο την πώληση προϊόντων ή υπηρεσιών.

Σε έρευνα του Οικονομικού Πανεπιστημίου Αθηνών[17] διαπιστώθηκε ότι το 30% των επιχειρήσεων προβάλλουν το προφίλ τους κάποιες γενικές πληροφορίες για περαιτέρω επικοινωνία, χωρίς όμως δυνατότητες για υποστήριξη πολύπλοκων εφαρμογών. Υπάρχουν όμως και αρκετές ελληνικές επιχειρήσεις που δραστηριοποιούνται στο διαδίκτυο και είτε έχουν αναπτύξει δυνατότητες on-line λήψης παραγγελιών είτε έχουν εφαρμογές για on-line πληρωμές.

Η σχέση των χρηστών (εν δυνάμει πελατών) και των επιχειρήσεων που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο παρουσιάζετε στο παρακάτω διάγραμμα που παρουσιάστηκε σε στατιστική έρευνα της ΕΛ.ΣΤΑΤ για το έτος 2011.



Εικόνα 3.3. **Ηλεκτρονικό Εμπόριο**: ***Α'*** **Τρίμηνο** 2007-2011

[16] **Πηγή**: ΕΛ.ΣΤΑΤ (Τεχνολογία-Κοινωνία Πληροφορίας > Χρήση Τεχνολογιών Πληροφόρησης και Επικοινωνίας από τα Νοικοκυριά - Συγκ. 2011)

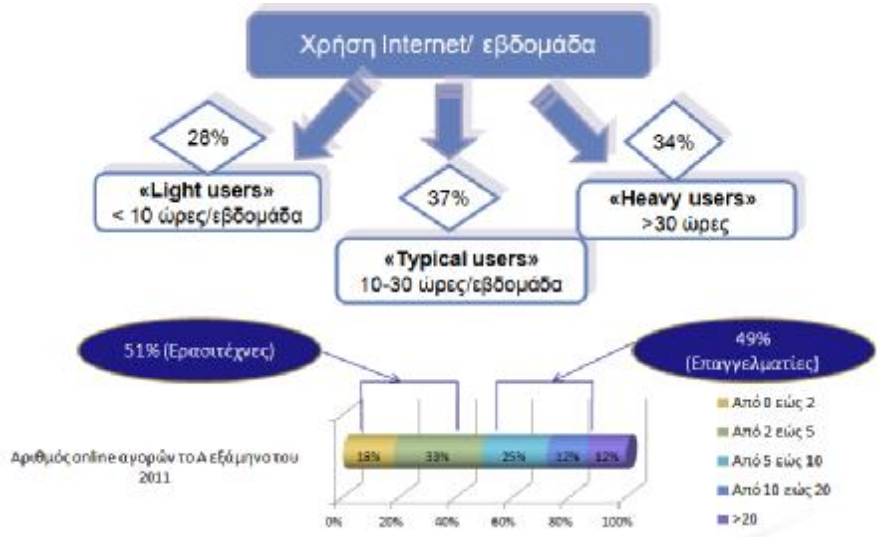
[17] **Πηγή :** Οικονομικό Πανεπιστήμιο Αθηνών (Εργαστήριο Επιχειρηματικής Πληροφορικής BILab) www.bclab.aueb.gr/

Παρατηρούμε λοιπόν ότι το ποσοστό των χρηστών του διαδικτύου που πραγματοποίησαν ηλεκτρονικές αγορές κατά το Α' τρίμηνο του 2011 ανέρχεται στο 23,6%. Σε σχέση με το αντίστοιχο ποσοστό του 2010 υπάρχει μια αύξηση της τάξης του 28,3% η οποία δηλώνει την σχετικά γρήγορη αποδοχή του ηλεκτρονικού εμπορίου από τους Έλληνες χρήστες τα τελευταία 2 χρόνια.

Μια ακόμη έρευνα , που μας δίνει το προφίλ του Έλληνα χρήστη του internet, είναι η τελευταία έρευνα από το εργαστήριο Ηλεκτρονικού Εμπορίου του Οικονομικού Πανεπιστημίου Αθηνών (ELTRUN)[18], για την καταγραφή της συνολικής αγοράς B-C ηλεκτρονικού εμπορίου και την συμπεριφορά των Ελλήνων on-line καταναλωτών.

Παρά τις σταθεροποιητικής τάσεις το Β' Εξάμηνο, οι συνολικές αγορές για προϊόντα και υπηρεσίες των Ελλήνων καταναλωτών διακυμάνθηκαν το 2011 στα € 1,7 δισ σημειώνοντας αύξηση 30% σε σχέση με το 2010. Αυτή την στιγμή 1,5 εκ. on-line Έλληνες καταναλωτές αγοράζουν κατά μέσο όρο 14-15 φορές / χρόνο από το Internet, ξοδεύοντας € 1.150 / χρόνο εκ των οποίων τα 2/3 κατευθύνονται σε Ελληνικά sites.

Η ετήσια συχνότητα και αξία αγορών των Ελλήνων on-line καταναλωτών είναι πλέον αντίστοιχη των Ευρωπαϊκών μέσων όρων.



Εικόνα 3.4. **Χρήση** Internet

Έτσι λοιπόν φτάνουμε στο συμπέρασμα ότι ο τυπικός Έλληνας on-line καταναλωτής είναι ένας σοβαρός χρήστης του Internet. Χαρακτηριστικά το 70% των χρηστών του internet, χρησιμοποιεί το ψηφιακό αυτό μέσο πάνω από 10 ώρες την εβδομάδα. Ακόμη θεωρείται «επαγγελματίας» αγοραστής αφού το 50%, των χρηστών, κάνει τουλάχιστον 2 on-line αγορές τον μήνα.

[18]**Πηγή**: Οικονομικό Πανεπιστήμιου Αθηνών Εργαστήριο Ηλεκτρονικού Εμπορίου και Ηλεκτρονικού Επιχειρείν (ELTRUN) http://www.eltrun.gr

3.3 Ηλεκτρονικό Εμπόριο στην Ελλάδα - Νομικό Πλαίσιο

Παράλληλα με την ανάπτυξη του ηλεκτρονικού εμπορίου και την άνοδο των ηλεκτρονικών αγορών δημιουργήθηκε η ανάγκη να θεσπιστούν μία σειρά από νέα νομοθετικά μέτρα τόσο για την προστασία του καταναλωτή όσο και του προμηθευτή.

Παραθέτουμε παρακάτω τις ποιο βασικές αρχές και τις σημαντικότερες νομοθετικές διατάξεις οι οποίες αφορούν το ηλεκτρονικό εμπόριο, όπως αναφέρονται αυτές στην ιστοσελίδα Αρχής Προστασίας Προσωπικών Δεδομένων[19] αλλά και άλλων σχετικών σελίδων[20].

- Ο Ν. 2251/94, για την "Προστασία Καταναλωτών", στο άρθρο 4, ρυθμίζει τις συμβάσεις από απόσταση. Εδώ εμπίπτει και το ηλεκτρονικό εμπόριο.
- Ο Ν. 2472/97 αναφέρεται στην προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και ο Ν. 2174/99 στην προστασία δεδομένων προσωπικού χαρακτήρα, στον τηλεπικοινωνιακό τομέα.
- Το πρόσφατο Προεδρικό Διάταγμα 150/2001, Φ.Ε.Κ. Α' 125, για τις ηλεκτρονικές υπογραφές, κάνει εμφανή την προσπάθεια της πολιτείας να προσφέρει μια σωστή βάση νομοθετικών πλαισίων.
- Το Προεδρικό Διάταγμα 131/2003, για το ηλεκτρονικό εμπόριο δίνει έμφαση στην εξώδικη επίλυση διαφορών, στη συνεργασία των κρατών - μελών της Ευρωπαϊκής Ένωσης, για την επίλυση των προβλημάτων των Καταναλωτών, στη θέσπιση κανόνων δεοντολογίας, με υποχρεωτική ισχύ, για τους αποδέκτες τους, στην ευθύνη των ενδιάμεσων, στη σύναψη των ηλεκτρονικών συμβάσεων, στις πληροφορίες, που πρέπει να παρέχονται στις εμπορικές επικοινωνίες (διαφημιστικά, χορηγίες, προσφορές κ.λπ.), στον τόπο εγκατάστασης των φορέων παροχής υπηρεσιών.
- Οι Καταναλωτές, όταν αγοράζουμε από χώρες, εκτός της Ευρωπαϊκής Ένωσης, πριν προβούμε σε οποιαδήποτε αγορά, πρέπει να αναζητήσουμε τις πληροφορίες, που διαθέτει ο έμπορος στο ηλεκτρονικό του κατάστημα και αφορούν το νομοθετικό κανονιστικό πλαίσιο, που θα διέπει τις αγορές μας.
- Η Σύμβαση των Βρυξελλών προβλέπει ότι, σε περίπτωση διαφοράς, που θα προκύψει με αλλοδαπό έμπορο ή εταιρία, ο Καταναλωτής, για τις χώρες μέλη της Ευρωπαϊκής Ένωσης, μπορεί να απευθυνθεί στο δικαστήριο του τόπου κατοικίας του. Το δε Δίκαιο, που θα εφαρμοστεί από το δικαστήριο, καθορίζεται από τη Σύμβαση της Ρώμης και, στις περισσότερες περιπτώσεις, είναι το Δίκαιο της χώρας του Καταναλωτή, καθώς, επίσης και οι Οδηγίες, για την προστασία του Καταναλωτή.
- Σύμφωνα με την οδηγία για το ηλεκτρονικό εμπόριο, εφαρμοστέο δίκαιο, όσον αφορά την παροχή προϊόντων και υπηρεσιών στο internet (εξαιρούνται οι συμβάσεις με Καταναλωτές), είναι η νομοθεσία του τόπου, όπου είναι εγκατεστημένος ο φορέας παροχής υπηρεσιών της κοινωνίας της πληροφορίας.

[19] **Πηγή** : http://www.dpa.gr (Αρχή Προστασίας Προσωπικών Δεδομένων)

[20] **Πηγή**: http://www.emporiko-oplostasio.com/elektroniko-emporio/electroniko-emporio-nomothesia.html (Περιοδικό Εμπορικό Οπλοστάσιο)

Έτσι λοιπόν οι καταναλωτές αλλά και οι έμποροι προστατεύονται και προστατεύουν τα προϊόντα τους δίνοντας μια αίσθηση ασφάλειας η οποία είναι απαραίτητη αφού στις δικτυακές συναλλαγές δεν υπάρχει ούτε η προσωπική επαφή του πελάτη-αγοραστή αλλά ούτε και η επαφή του αγοραστή με το προϊόν το ίδιο.

4ο Κεφάλαιο
Ανάλυση των Μοντέλων B2C και B2B

4.1 Επιχείρησης προς Καταναλωτή (Business to Costumer-B2C)

Το μοντέλο B2C είναι ίσως η πιο κλασσική μορφή ηλεκτρονικού εμπορίου, αλλά όχι και η πιο διαδεδομένη. Είναι είδος του εμπορίου που χαρακτηρίζεται ως πελατοκεντρικό, πραγματοποιείται δηλαδή μεταξύ των επιχειρήσεων και μεμονωμένων καταναλωτών. Θα μπορούσε να χαρακτηριστεί ως το ηλεκτρονικό ανάλογο των καθημερινών συναλλαγών στην αγορά προϊόντων αλλά και υπηρεσιών. Κάθε επιχείρηση που δραστηριοποιείται στο διαδίκτυο δημιουργεί έναν διαδικτυακό τόπο (site) στον οποίο παρουσιάζει τα προϊόντα της ή τις υπηρεσίες που παρέχει. Το site αυτό καλείται ηλεκτρονικό κατάστημα (e-shop).

Το ηλεκτρονικό κατάστημα συνήθως αποτελείται από ιστοσελίδες στις οποίες η επιχείρηση παρουσιάζει τα προϊόντα ή τις υπηρεσίες της. Η δομή της κάθε ιστοσελίδας είναι απλή και χωρισμένη σε κατηγορίες ώστε ο πελάτης-επισκέπτης να έχει εύκολη και άνετη πρόσβαση σε όλα τα προϊόντα. Ο πελάτης-επισκέπτης μπορεί να περιηγηθεί στις ιστοσελίδες του καταστήματος, να δει τα προϊόντα της επιχείρησης ή τις υπηρεσίες που παρέχει αυτή, και να επιλέξει με βάση τις επιθυμίες ή τις ανάγκες του. Να κάνει τις αγορές του και στο τέλος πληρώσει το αντίτιμο πάλι μέσω διαδικτύου χωρίς καν να βγει απ' το σπίτι του.

Σχετικά με τις πληρωμές να αναφέρουμε ότι συνήθως πραγματοποιούνται μέσω πιστωτικών καρτών, ή συστημάτων SET (Secure Electronic Transactions), αλλά και με την μέθοδο της αντικαταβολής μόλις ο πελάτης παραλάβει το προϊόν. Η παράδοση της παραγγελίας γίνεται είτε μέσω κλασικού ταχυδρομείου (ή courier) αν το προϊόν είναι κάποιο αντικείμενο ή γίνεται ηλεκτρονική αποστολή σε περιπτώσεις που η παραγγελία αφορά ηλεκτρονικό υλικό.

Τα προϊόντα που μπορεί κάποιος να βρει και να αγοράσει μέσο του εμπορίου B2C είναι πάρα πολλά και θα μπορούσαμε να πούμε ότι ελάχιστα δεν ανήκουν, προς το παρόν, στο μεγάλο κατάλογο του B2C εμπορίου.

Μεγάλη προτίμηση δείχνουν οι καταναλωτές σε προϊόντα όπως βιβλία, CD, ταινίες DVD, είδη ένδυσης και υπόδησης, αθλητικά είδη αλλά και ηλεκτρονικά παιχνίδια, ηλεκτρικές συσκευές κ.τλ. Ακόμη και είδη διατροφής, φαρμακευτικά σκευάσματα, και κοσμήματα βρίσκονται στις προτιμήσεις των αγοραστών του διαδικτύου.

Πέρα όμως από τα προϊόντα, οι αγοραστές του διαδικτύου, δείχνουν μεγάλη προτίμηση και στις υπηρεσίες. Ταξιδιωτικές υπηρεσίες όπως κρατήσεις σε ξενοδοχεία, αεροπορικά εισιτήρια, κ.α είναι πρώτα στις προτιμήσεις τους. Τραπεζικά προϊόντα όπως μετοχές, οικονομικές υπηρεσίες, ασφάλειες, διάφορες συνδρομές σε υπηρεσίες τηλεπικοινωνιακών προϊόντων αλλά και πληρωμές λογαριασμών.

Χαρακτηριστικά παραθέτουμε τα αποτελέσματα έρευνας που διεξήγαγε το ELTRUN[21]. Η έρευνα «Ηλεκτρονικό Εμπόριο 2010» της Εθνικής Στατιστικής Αρχής που έγινε με τη μέθοδο της τρισταδιακής στρωματοποιημένης δειγματοληψίας (επιφάνεια, νοικοκυριό, άτομο ηλικίας 16-74 ετών) σε 6.000 νοικοκυριά σε όλη την Ελλάδα και τα αποτελέσματα φαίνονται στον παρακάτω πίνακα:

ΑΓΑΘΑ – ΥΠΗΡΕΣΙΕΣ	% του συνολικού αριθμού αγορών
Ηλεκτρονικές συσκευές (βιντεοκάμερες, φωτογραφικές μηχανές, κινητά τηλέφωνα, τηλεόρασεις, DVDs κλπ.)	28,5
Ταξιδιωτικές υπηρεσίες (εισιτήρια, ενοικίαση αυτοκινήτου κλπ.)	27,8
Είδη ένδυσης και υπόδησης – αθλητικά είδη	24,5
Εξαρτήματα και περιφερειακός εξοπλισμός (hardware) ηλεκτρονικού υπολογιστή	24,1
Διαμονή σε καταλύματα (ξενοδοχεία, δωμάτια, διαμερίσματα κλπ.)	23,3
Βιβλία (σε ηλεκτρονική ή μη μορφή), περιοδικά, εφημερίδες	20,5
Εισιτήρια για εκδηλώσεις (συναυλίες, θεατρικές παραστάσεις, κινηματογράφο κλπ.)	20,1
Λογισμικό για ηλεκτρονικό υπολογιστή (εξαιρουμένων computer games και video games) και αναβαθμίσεις αυτού	16,2
Οικιακά είδη (έπιπλα, παιχνίδια, είδη τέχνης, ηλεκτρικές οικιακές συσκευές κλπ.)	14,5
Άλλα (κοσμήματα, πληροφορίες από βάσεις δεδομένων κλπ.)	9,4
Ταινίες, μουσική (DVDs, CDs, βιντεοκασέτες κλπ.)	9,1
Παιχνίδια για ηλεκτρονικό υπολογιστή και παιχνιδομηχανές και αναβαθμίσεις αυτών	5,8
Υλικό ηλεκτρονικής εκμάθησης	5,4
Υπηρεσίες τηλεπικοινωνιών (συνδρομές συνδρομητικής τηλεόρασης –Nova–, συνδρομές ευρυζωνικής σύνδεσης, λογαριασμοί κινητού ή σταθερού τηλεφώνου, καταβολή χρημάτων σε προπληρωμένη τηλεφωνική κάρτα κλπ.)	4,4
Είδη διατροφής – είδη παντοπωλείου	2,3
Φάρμακα	2,2
Μετοχές, οικονομικές υπηρεσίες, ασφάλειες (κάθε είδους)	1,9

Εικόνα 4.1. ***Αγαθά-Υπηρεσίες που αγοράστηκαν από το*** Internet
Απρίλιος 2009 – ***Μάρτιος*** 2010

[21] **Πηγή:** http://www.eltrun.gr/ (Οικονομικό Πανεπιστήμιο Αθηνών- Εργαστήριο Ηλεκτρονικού Εμπορίου (ELTRUN))

4.2 Επιχείρησης προς Επιχείρηση (Business to Business-B2B)

Ένα μεγάλο ποσοστό των συναλλαγών του Internet πραγματοποιούνται, σύμφωνα με έρευνες, μεταξύ των επιχειρήσεων. Μια επιχείρηση μπορεί να χρησιμοποιεί το ηλεκτρονικό εμπόριο για να προμηθευτεί πρώτες ύλες ή άλλα προϊόντα από άλλες επιχειρήσεις. Ο τρόπος αυτός του ηλεκτρονικού εμπορίου, το γνωστό B2B, είναι περισσότερο διαδεδομένος στην Αμερική και σε άλλες Ευρωπαϊκές χώρες, στην Ελλάδα όμως τα πράγματα κινούνται πιο αργά.

Η χρήση του B2B ηλεκτρονικού εμπορίου εμπεριέχει και άλλες δυνατότητες μεταξύ των επιχειρήσεων οι οποίες πραγματοποιούνται μέσα από δικτυακές πλατφόρμες. Η αναζήτηση νέου προμηθευτή ή κάποιου νέου προϊόντος για προώθηση είναι μερικοί ακόμα λόγοι για μια επιχείρηση για να χρησιμοποιήσει το B2B ηλεκτρονικό εμπόριο.

Η διαδικασία βέβαια είναι αρκετά πιο περίπλοκη, από τις διαδικασίες που θα ακολουθήσει ένας απλός χρήστης για να κάνει μια αγορά μέσο internet, καθώς το επίπεδο ασφαλείας που προσφέρεται είναι πολύ υψηλό, ενώ στις περισσότερες περιπτώσεις απαιτείται και η «εμπλοκή» ενός χρηματοπιστωτικού οργανισμού, ο οποίος θα αναλάβει την πιστοποίηση των συναλλασσομένων πλευρών. Άλλωστε μιλάμε για συναλλαγές που μπορεί να αρχίζουν από δεκάδες χιλιάδες ευρώ και να φτάνουν μέχρι και εκατομμύρια.

Αξίζει να σημειωθεί πάντως, ότι δεν είναι η πρώτη φορά που οι εταιρείες προσπαθούν να συνδυάσουν τη χρήση των τηλεπικοινωνιακών δικτύων με εκείνη των συστημάτων πληροφορικής για να μειώσουν το κόστος στην προμηθευτική τους αλυσίδα. Στις αρχές της δεκαετίας του '90 αρκετές εταιρείες έσπευσαν να εκμεταλλευτούν τις δυνατότητες των συστημάτων EDI (Electronic Data Interchange), τα οποία επέτρεπαν την ηλεκτρονική ανταλλαγή εγγράφων, μειώνοντας κατ'αυτόν τον τρόπο το κόστος αλλά και το χρόνο που απαιτείται για μια συναλλαγή. Όμως, το διαδίκτυο θεωρείται και είναι ένα αρκετά πιο εύχρηστο μέσο, ενώ δεν απαιτεί τεράστιες επενδύσεις σε υλικοτεχνική υποδομή.

4.3 Η Πορεία της Ελληνικής B2B Αγοράς

Η πορεία της Ελληνικής αγοράς B2B μπορεί να χαρακτηριστεί ως ανοδική. Βέβαια οι αρχικές προβλέψεις δεν ανταποκρίνονται στη σημερινή εικόνα, και αυτό φαίνεται μέσα από τις αναλύσεις και τις δηλώσει ανθρώπων που γνωρίζουν και παρακολουθούν το ηλεκτρονικό εμπόριο εκ των έσω. Παραθέτουμε παρακάτω μερικές από αυτές σημειώνοντας ότι σε γενικές γραμμές το σύνολο των ελληνικών επιχειρήσεων, που δραστηριοποιούνται στο χώρο του ηλεκτρονικού εμπορίου, δηλώνει περισσότερο ικανοποιημένο από την πορεία του.

Σε σχετικό άρθρο του στο Newsletter της cosmoONE Hellas MarketSite (Φεβρουάριος 2004) ο κος Χρήστος Λεμονής[22], διευθυντής marketing και επικοινωνίας της cosmoONE, αναφέρει ότι ορισμένοι μεγάλοι οργανισμοί στην Ελλάδα έχουν αρχίσει να υλοποιούν συστήματα Ηλεκτρονικών προμηθειών. Ήδη κάποιοι έχουν ξεπεράσει τις αναπόφευκτες 'παιδικές ασθένειες' και έχουν αρχίσει να ξεχνούν πως ήταν πριν η κατάσταση και οι τότε διαδικασίες.

Οι ηλεκτρονικές Δημοπρασίες δεν αποτελούν πλέον κάτι εξωτικό και για πολλούς από τους συμμετέχοντες είναι κάτι 'κοινό'. Πέραν του σχεδιασμού και της υλοποίησης συγκεκριμένων έργων, αναμφισβήτητα τα τελευταία δύο χρόνια έχει γίνει πολλή δουλειά από τους παρόχους υπηρεσιών και τεχνολογίας ηλεκτρονικού εμπορίου B2B, και προς την κατεύθυνση 'εκπαίδευσης' της αγοράς και προς την κατεύθυνση ενημέρωσης των κυβερνητικών (υπουργείων και ΔΕΚΟ) και μη οργανισμών (ΣΕΠΕ).

Από την άλλη πλευρά, ο κ. Πέτρος Αγγελάκης[23], γενικός διευθυντής της Business Exchanges, τονίζει ότι το B2B εμπόριο και οι σχετικές με αυτό εφαρμογές αποτελούν σήμερα το μόνο χώρο, στο ευρύτερο πεδίο του Internet, που παρουσιάζει σταθερή αύξηση και συνεχή ενδυνάμωση. 'Κάτω απ' αυτό το πρίσμα, οι αρχικές μας προβλέψεις και το επιχειρηματικό μας μοντέλο μπορούμε να πούμε ότι κάθε άλλο παρά διαψεύσθηκαν. Σίγουρα η ταχύτητα αποδοχής δεν είναι αυτή που πριν τριάμισι χρόνια εκτιμούσε η ελληνική και η παγκόσμια αγορά αλλά, αν παρατηρήσουμε προσεχτικά, θα δούμε ότι οι πάροχοι B2B υπηρεσιών, με σωστό σχεδιασμό και σωστές μετοχικές και οργανωτικές βάσεις, αντιμετωπίζουν τις προκλήσεις πολύ πιο ομαλά και με καλύτερα αποτελέσματα, επιτυγχάνοντας την αύξηση του αριθμού των συναλλασσομένων επιχειρήσεων αλλά και του όγκου αγορών που ηλεκτρονικο-ποιείται.

Σε παρόμοιο πλαίσιο κινείται και ο κ. Αντώνης Σαρόπουλος[24], γενικός διευθυντής της E-construction που έχει δημιουργήσει την ηλεκτρονική αγορά b2bconstuct.gr. Ο κ. Σαρόπουλος υποστηρίζει ότι η μέχρι σήμερα πορεία των ελληνικών b2b marketplaces χαρακτηρίζεται από μια συνεχή ανάπτυξη, τόσο στον τομέα των συμμετεχόντων όσο και στο ύψος των συναλλαγών που πραγματοποιούν. Παρ' όλα

[22] Διευθυντής marketing (cosmoONE) - http://www.cosmo-one.gr/nl_archive/2004/feb2004.htm
[23] Γενικός διευθυντής (Business Exchanges) - http://www.be24.gr/beinfo/index.do
[24] Γενικός διευθυντής (E-construction) - http://www.b2bconstruct.gr/company/companyprofile

αυτά, η εξέλιξη δεν υπήρξε αυτή που αναμενόταν τόσο για την ελληνική όσο και την παγκόσμια πραγματικότητα.

Γενικά μπορούμε να πούμε ότι, στα ελληνικά marketplaces παρατηρούμε ένα μικρό αλλά σταθερό ρυθμό ανάπτυξης, πράγμα το οποίο βοήθησε στην επιβίωσή τους κατά την διάρκεια των πρώτων ετών λειτουργίας. Με αργούς αλλά σταθερούς ρυθμούς, λοιπόν, αναπτύσσεται στην Ελλάδα το ηλεκτρονικό εμπόριο B2B και ενώ το ενθαρρυντικό της υπόθεσης είναι ότι ολοένα και περισσότερες εταιρίες τολμούν και αναπτύσσουν την εμπορική τους δραστηριότητα μέσα από τέτοιου είδους εφαρμογές.

5ο Κεφάλαιο
Ηλεκτρονικές Πληρωμές (E - payments)

5.1 Εισαγωγή[25]

Μεγάλο κεφάλαιο στην ανάπτυξη του ηλεκτρονικού εμπορίου είναι οι ηλεκτρονικές πληρωμές. Η δυνατότητα, δηλαδή, του πελάτη να μπορεί να εξοφλήσει κάποια οφειλή του κάνοντας χρήση των ηλεκτρονικών μέσων και των δικτυακών εφαρμογών που του παρέχει η εκάστοτε επιχείρηση.

Στην πιο γενική του μορφή, ο όρος ηλεκτρονικές πληρωμές (electronic payments) περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις οι οποίες εκτελούνται με την μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας[26]. Είναι από σημαντικότερους τομείς του ηλεκτρονικού εμπορίου, που σχετίζεται άμεσα με την ασφάλεια αλλά και την ευκολία του. Αν και υπάρχει διαρκής εξέλιξη αυτού του τρόπου πληρωμής, με τις διάφορες εταιρείες που ασχολούνται με τον τομέα των ηλεκτρονικών συναλλαγών να, ρίχνουν το βάρους τους στην ασφάλεια των συναλλαγών αλλά και στην ευκολία χρήσης του, μπορούμε να πραγματοποιήσουμε μια αρχική διάκριση των ηλεκτρονικών πληρωμών σε αυτές που:

- στηρίζονται στην μεταφορά αξίας και
- σε αυτές που στηρίζονται στην μεταφορά πληροφοριών[27].

Στην πρώτη κατηγορία, πραγματοποιείται η μεταφορά χρηματικών ποσών μέσω των συστημάτων ηλεκτρονικών πληρωμών. Αντίθετα, στην δεύτερη κατηγορία αυτό που μεταφέρεται μεταξύ των συναλλασσομένων μερών είναι πληροφορίες αφενός για την συναλλαγή και αφετέρου για τους τραπεζικούς λογαριασμούς των εμπλεκομένων. Η χρηματική συναλλαγή λαμβάνει χώρα είτε off-line είτε με την χρήση ιδιόκτητων ηλεκτρονικών δικτύων χρηματοπιστωτικών ιδρυμάτων ή εταιρειών. Σήμερα, ο κύριος όγκος των ηλεκτρονικών πληρωμών διεκπεραιώνεται μέσω συστημάτων ηλεκτρονικών πληρωμών που στηρίζονται στην μεταφορά πληροφοριών.

Ένας δεύτερος, πιο διαδεδομένος τρόπος ταξινόμησης των ηλεκτρονικών πληρωμών μπορεί να γίνει με βάση τη τεχνολογία που χρησιμοποιεί ένα ηλεκτρονικό δίκτυο διανομής. Έτσι, οι συναλλαγές μπορούν να πραγματοποιηθούν:

- **Μέσω τηλεφώνου**. Οι πληρωμές μέσω του τηλεφωνικού δικτύου αποτελούν μια καινούρια μορφή ηλεκτρονικών πληρωμών. Στόχος είναι η εκμετάλλευση της υπάρχουσας τεχνικής υποδομής αλλά και της σημαντικής διείσδυσης που έχει το τηλέφωνο ως τεχνολογία σε όλα τα κοινωνικά στρώματα. Πολλές επιχειρήσεις, τράπεζες αλλά και οι δημόσιες υπηρεσίες επιτρέπουν την

[25] **Πηγή**: Soramäki, K. & Hanssens, B. (2003). E-payments: What are they and what makes them different?. Διαθέσιμο στο www.e-pso.info.
[26] **Πηγή:** e-Business forum (Ε΄ Κύκλος Εργασιών: Ομάδα Εργασίας Ε3). Αθήνα Ιανουάριος 2004
[27] **Πηγή:** Goldfinger, C. (1999). Secure electronic payments on the Internet. Διαθέσιμο στο www.gefma.com.

εξόφληση λογαριασμών μέσω τηλεφώνου με αποτέλεσμα αυτά τα συστήματα ηλεκτρονικών πληρωμών να κερδίζουν σημαντικά την εμπιστοσύνη του καταναλωτικού κοινού.

- **Μέσω διαδικτύου (Internet**). Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η άνθηση του ηλεκτρονικού επιχειρείν καθιστά ιδιαίτερα σημαντική την ύπαρξη συστημάτων ηλεκτρονικών πληρωμών που χρησιμοποιούν το διαδίκτυο ως κανάλι διανομής. Επιπλέον, η εύκολη πρόσβαση στο διαδίκτυο από την πλειοψηφία του καταναλωτικού κοινού καθιστούν τα εν λόγω συστήματα ηλεκτρονικών πληρωμών ιδιαίτερα δημοφιλή στις μέρες μας. Οι πληρωμές μέσω διαδικτύου μπορούν να χωριστούν σε 2 υποκατηγορίες :
  - Token based systems
  - Notational based systems
- **Μέσω κινητής τηλεφωνίας (m-payments).** Η ανάπτυξη τεχνολογιών όπως το WAP επιτρέπουν την εκτέλεση βασικών χρηματικών συναλλαγών από κινητές και ασύρματες συσκευές ανεξαρτήτως χώρου και χρόνου. Πρόκειται για ένα μέσο πιο αυτόνομο ενώ η ευρεία αποδοχή και χρήση του από το καταναλωτικό κοινό το καθιστούν ιδιαίτερα δημοφιλή λύση συχνά ανταγωνιστική των πληρωμών μέσω διαδικτύου.

Παρακάτω παραθέτουμε έναν πίνακα στον οποίο έχουμε ομαδοποιήσει - κατηγοριοποιήσει τα συστήματα ηλεκτρονικών πληρωμών :

Token systems	**Electronic cash**		**DigiCash**	**DigiCash**
			Millicent	Digital Equipment
	Electronic purse systems		CAFI	ESPRIT
			MONDEX	Nat West,
Notational systems	Electronic payment orders transferred over the nets		NetBill	Carnegie Mellon
			NetCheque	University of California
	Credit card billing over the nets	Encrypted credit cards	CyberCash	CyberCash
			SET	VISA, MASTERCARD
		Third-party authorisation	First Virtual	First Vistual Holdings, Inc
	Smart-card based notational systems		FSTC e-	FSTC inc

5.2 Συστήματα Ηλεκτρονικών Πληρωμών[28]

Μέχρι σήμερα έχει υπολογιστεί ότι υπάρχουν διεθνώς τουλάχιστον 150 διαφορετικά συστήματα ηλεκτρονικών πληρωμών[29] που υποστηρίζουν συναλλαγές στο διαδίκτυο. Ο αριθμός αυτός αυξάνεται δε διαρκώς ως αποτέλεσμα των νέων τεχνολογικών λύσεων που κατά καιρούς εμφανίζονται αλλά και της προσπάθειας πολλών νέων παικτών να αποκτήσουν ρόλο μεσολαβητή στο κύκλωμα πληρωμών μέσω διαδικτύου.

Ένα δεύτερο πρόβλημα σε κάθε συστηματική προσπάθεια ταξινόμησης των συστημάτων ηλεκτρονικών πληρωμών μέσω διαδικτύου είναι η τάση σύνδεσης του συνόλου των ηλεκτρονικών πληρωμών με τις αγοραπωλησίες στο διαδίκτυο. Αν και η ανάπτυξη του διαδικτύου επέτρεψε τη ανάπτυξη συστημάτων όπως το E-cash ή το CyberCash που διεκπεραιώνουν τις ηλεκτρονικές συναλλαγές μέσω του διαδικτύου, το μεγαλύτερο μέρος των συναλλαγών που σχετίζονται με αγορές στο διαδίκτυο δεν διεκπεραιώνεται μέσω αυτού.

Για παράδειγμα, οι πιστωτικές κάρτες που αποτελούν το βασικό μέσο πληρωμής στο διαδίκτυο, χρησιμοποιούν το διαδίκτυο μόνο στα αρχικά στάδια της συναλλαγής όταν ο καταναλωτής αποστέλλει τα στοιχεία του στον έμπορο. Στην συνέχεια η συναλλαγή ολοκληρώνεται μέσω των ιδιόκτητων δικτύων των εταιρειών πιστωτικών καρτών.

Επιπλέον υπάρχουν συστήματα ηλεκτρονικών πληρωμών όπως το SWIFT που λειτουργούν πολύ πριν εμφανιστεί το διαδίκτυο. Επομένως είναι σαφές ότι δεν υπάρχει πλήρης αντιστοιχία μεταξύ των συστημάτων ηλεκτρονικών πληρωμών, εν γένη, και των συστημάτων που χρησιμοποιούν το διαδίκτυο ως βασικό κανάλι διανομής.

5.3 Παραδοσιακά Συστήματα Προσαρμοσμένα στο Διαδίκτυο

Στην κατηγορία αυτή ανήκουν συστήματα πληρωμών τα οποία προϋπήρχαν της εμφάνισης του Διαδικτύου. Η διαδεδομένη χρήση τους αλλά και η σιγουριά που προσέφεραν στους καταναλωτές κατέστησαν τα μέσα αυτά ιδιαίτερα δημοφιλή και στο διαδίκτυο. Επιπλέον η χρήση τους δεν απαιτούσε ιδιαίτερη επένδυση ούτε από την πλευρά των εταιρειών που δραστηριοποιούνταν στο διαδίκτυο με αποτέλεσμα να κυριαρχήσουν τουλάχιστον στα αρχικά στάδια του ηλεκτρονικού εμπορίου. Τα συστήματα αυτά απαιτούν την ύπαρξη τραπεζικών λογαριασμών από τους καταναλωτές με αποτέλεσμα ένα μέρος των συναλλαγών να πρέπει να εκκαθαριστεί εκτός του διαδικτύου. Ειδικότερα, τα συστήματα αυτά είναι:

Πιστωτικές κάρτες: Οι πιστωτικές κάρτες επιτρέπουν στους καταναλωτές την πραγματοποίηση συναλλαγών μέχρι ενός προκαθορισμένου ποσού. Το ποσό των

[28] **Πηγή:** e-Business forum (Ε΄ Κύκλος Εργασιών: Ομάδα Εργασίας Ε3). Αθήνα Ιανουάριος 2004

[29] **Πηγή :** Peirce, M. (2001). Payment mechanisms designed for the Internet. Διαθέσιμο στο http://ganges.cse.tcd.ie/meperice.

συναλλαγών που έχουν πραγματοποιηθεί μέσω της κάρτας εκκαθαρίζεται στο τέλος κάθε ημερολογιακού μήνα είτε πλήρως είτε μερικώς οπότε το υπόλοιπο θεωρείται ως πίστωση του εκδοτικού οργανισμού προς τον κάτοχο. Οι πιστωτικές κάρτες έχουν τύχει ευρείας χρήσης στο διαδίκτυο επειδή διαθέτουν σημαντικά πλεονεκτήματα έναντι των εναλλακτικών μεθόδων πληρωμής[30]. Κατ' αρχήν είναι διεθνώς γνωστές και αποδεκτές από τους εμπόρους. Η χρήση τους στο διαδίκτυο δεν διαφέρει σημαντικά από τον τρόπο που χρησιμοποιούνταν μέχρι τώρα στις συναλλαγές στον φυσικό κόσμο[31]. Επιπλέον, η σημαντική διάδοση των πιστωτικών καρτών και στις παραδοσιακές συναλλαγές έχει συντελέσει στην δημιουργία μιας ιδιαίτερα αποτελεσματικής υποδομής για την εκκαθάριση των πληρωμών η οποία μάλιστα επιτρέπει και την πραγματοποίηση διεθνών συναλλαγών. Αυτό έχει σαν αποτέλεσμα την πραγματοποίηση συναλλαγών στο διαδίκτυο χωρίς σημαντικές επενδύσεις από την πλευρά των εμπόρων αλλά και χωρίς αλλαγή στην συμπεριφορά των καταναλωτών.

Στα πρώτα στάδια του ηλεκτρονικού εμπορίου, οι καταναλωτές απλά έστελναν τον αριθμό της πιστωτικής τους κάρτας και την ημερομηνία λήξης στους εμπόρους με την μορφή απλού μηνύματος χωρίς κρυπτογράφηση. Σύντομα όμως αυτός ο τρόπος χρήσης της πιστωτικής κάρτας στο διαδίκτυο εγκαταλείφθηκε καθώς το μήνυμα ήταν πολύ εύκολο να υποκλαπεί με αποτέλεσμα να παρατηρηθούν κρούσματα απάτης με πιστωτικές κάρτες. Προκειμένου να λυθούν τα προβλήματα απάτης οι οργανισμοί πιστωτικών καρτών προχώρησαν στην δημιουργία προτύπων όπως το SET (Secure Electronic Transaction) που ήταν πρωτοβουλία της VISA και της MASTERCARD. Τα πρότυπα αυτά ενίσχυσαν σημαντικά την ασφάλεια των συναλλαγών στο διαδίκτυο μέσω πιστωτικής κάρτας δεν έτυχαν όμως ευρείας αποδοχής από το καταναλωτικό κοινό.

Μεταφορά ποσών επί πιστώσει: Σε αυτό το σύστημα πληρωμών ο καταναλωτής δίνει εντολή στην τράπεζα του να μεταφέρει χρηματικά ποσά ανάλογα της πληρωμής που θέλει να πραγματοποιήσει στον λογαριασμό του εμπόρου[32]. Αυτή η μέθοδος πληρωμής υποστηρίζεται σημαντικά από τις τράπεζες στα πλαίσια των εφαρμογών ηλεκτρονικής τραπεζικής που προσφέρουν στους πελάτες τους. Ειδικά για συναλλαγές στο διαδίκτυο οι πελάτες μπορούν να επιλέξουν την μεταφορά ποσών επί πιστώσει ως την επιθυμητή μέθοδο πληρωμής και απλά να αποδεχθούν τον λογαριασμό που θα εμφανιστεί στην οθόνη τους. Εφόσον ο πελάτης αποδέχεται την συναλλαγή μεταφέρεται στον δικτυακό τόπο της τράπεζας όπου ολοκληρώνει την συναλλαγή του και κατόπιν επιστρέφει στο ηλεκτρονικό κατάστημα στο οποία βρισκόταν.
Το συγκεκριμένο σύστημα πληρωμών προϋποθέτει την ύπαρξη συμφωνίας μεταξύ της τράπεζας και του εμπόρου. Επιπλέον ο πελάτης πρέπει να χρησιμοποιεί τις υπηρεσίες ηλεκτρονικής τραπεζικής που του προσφέρει η τράπεζα του. Σύμφωνα με μελέτη της Ευρωπαϊκής Κεντρικής Τράπεζας13, τα εν λόγω συστήματα ηλεκτρονικών

[30] **Πηγή**: European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective. Issue Paper available at www.ecb.int
[31] **Πηγή:** Turban, E.; Lee, J.; King, D. & Chung, H. M. (xxx). Electronic commerce: A managerial perspective. International Edition.
[32] **Πηγή:** European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective.

πληρωμών λειτουργούν προς το παρόν σε αυστηρά εθνικά πλαίσια με αποτέλεσμα να μην είναι βολικά για διεθνείς συναλλαγές.

Πάγιες εντολές: πρόκειται για προεγκριμένα χρεωστικά ποσά από τον τραπεζικό λογαριασμό του πελάτη που εκχωρούνται στον δικαιούχο. Οι πάγιες εντολές χρησιμοποιούνται συνήθως για επαναλαμβανόμενες πληρωμές όπως αυτές για λογαριασμούς ΔΕΚΟ ή για εφάπαξ πληρωμές όταν δεν υπάρχει άμεση επαφή μεταξύ εμπόρου και αγοραστή. Στις πάγιες εντολές, ο δικαιούχος αποστέλλει στον οφειλέτη ένα ειδικό έντυπο το οποίο ο τελευταίος συμπληρώνει αναγνωρίζοντας κατ' αυτό τον τρόπο την οφειλή του
δικαιούχου. Στην συνέχεια ο τελευταίος προωθεί το ειδικό έντυπο στην συμβεβλημένη τράπεζα για την ολοκλήρωση της συναλλαγής.

Οι πάγιες εντολές χρησιμοποιούνται και για πληρωμές στο Διαδίκτυο. Στην περίπτωση αυτή όλη η ανωτέρω διαδικασία γίνεται ηλεκτρονικά και ομοιάζει αρκετά στις πληρωμές στο διαδίκτυο με τη χρήση πιστωτικής κάρτας. Η βασικά διαφορά έγκειται στο γεγονός ότι ο οφειλέτης αποστέλλει το νούμερο του τραπεζικού του λογαριασμού και όχι αυτό της πιστωτικής του κάρτας.

Χρεωστικές κάρτες: το εν λόγω σύστημα ηλεκτρονικών πληρωμών αποτελεί μια παραλλαγή των πάγιων εντολών όπου οι απαιτούμενες για τη συναλλαγή πληροφορίες περιέχονται σε ειδικά κάρτα με μαγνητική ταινία ή μικροεπεξεργαστή. Για την πραγματοποίηση συναλλαγών απαιτείται η ύπαρξη ειδικού τερματικού το οποίο θα επαληθεύει την εγκυρότητα των πληροφοριών που είναι αποθηκευμένες στην κάρτα και θα ελέγχει αν αυτή βρίσκεται σε ισχύ. Η διαδικασία πληρωμής είναι ακριβώς ίδια με αυτή των παγίων εντολών με τη διαφορά ότι οι απαιτούμενες πληροφορίες είναι αποθηκευμένες στην κάρτα με αποτέλεσμα η συναλλαγή να είναι ασφαλέστερη. Ο κάτοχος της κάρτας πρέπει να διαθέτει ειδικό μηχάνημα υποδοχής συνδεδεμένο με τον υπολογιστή του που σημαίνει βέβαια ότι απαιτείται επιπλέον εξοπλισμός για τη χρήση της. Εντούτοις, το ειδικό αυτό μηχάνημα συχνά εκχωρείται στον πελάτη από την ίδια την τράπεζα.

Το βασικό μειονέκτημα των χρεωστικών καρτών είναι ότι από την σκοπιά του πελάτη δεν είναι σαφή τα πλεονεκτήματα τους έναντι των πιστωτικών καρτών[33]. Ειδικά στις συναλλαγές στο διαδίκτυο, οι χρεωστικές κάρτες προσφέρουν μικρότερη προστασία έναντι των πιστωτικών σε περιπτώσεις που τα αντικείμενα που αγοράστηκαν δεν παραδίδονται ή είναι ελαττωματικά. Από την πλευρά των εμπόρων πάντως οι χρεωστικές κάρτες είναι προτιμότερες καθώς δεν επιβαρύνουν με προμήθεια των έμπορων. Επιπλέον, στην επιχειρηματικές συναλλαγές μέσω

[33] **Πηγή** : Turban, E.; Lee, J.; King, D. & Chung, H. M. (2003). Electronic commerce: A managerial perspective. International Edition, Upper Saddle River: Prentice Hall, pp. 289.

διαδικτύου (B2B) οι χρεωστικές κάρτες μπορεί να αποδειχθούν φθηνότερη λύση ακριβώς για τον ίδιο λόγο.

Ηλεκτρονικές επιταγές: Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών. Μια επιταγή είναι μια γραπτή εντολή από τον εκδότη προς τον αποδέκτη που είναι συνήθως τράπεζα με την οποία ο εκδότης απαιτεί από τον αποδέκτη την καταβολή ενός συγκεκριμένου ποσού είτε στον εκδότη είτε σε τρίτο πρόσωπο που ορίζεται από αυτόν. Οι ηλεκτρονικές επιταγές ακολουθούν κατά βάση τον ίδιο κανόνα με τη διαφορά ότι η επιταγή είναι σε ηλεκτρονική μορφή15. Επιπλέον, καθώς ο εκδότης πρέπει να υπογράψει την επιταγή προκειμένου να είναι έγκυρη στις ηλεκτρονικές επιταγές χρησιμοποιείται η ψηφιακή υπογραφή προκειμένου να ολοκληρωθεί η διαδικασία16. Στην χρήση ηλεκτρονικών υπογραφών εντοπίζονται και τα περισσότερα προβλήματα που συναντά στην διάδοση του το συγκεκριμένο σύστημα πληρωμής. Η χρήση κρυπτογραφικών μεθόδων αλλά και η τεχνολογία που απαιτείται για να υποστηρίξει τις ηλεκτρονικές υπογραφές έχουν μέχρι τώρα δημιουργήσει αρκετά εμπόδια στην χρήση των ηλεκτρονικών επιταγών τα οποία και θα αναλυθούν σε επόμενη ενότητα.

5.4 Καινοτόμα Συστήματα πληρωμών Μέσω Internet[34]

Στην κατηγορία αυτή υπάρχουν συστήματα πληρωμών τα οποία κάνουν χρήση καινοτομικών τεχνολογιών που μέχρι πρόσφατα δεν ήταν διαθέσιμες για την διεξαγωγή πληρωμών. Επιπλέον, πολλά από τα συστήματα αυτά είναι προσαρμοσμένα στις τρέχουσες τάσεις του ηλεκτρονικού εμπορίου και προσπαθούν να ικανοποιήσουν τις καταναλωτικές τάσεις που φαίνεται να διαμορφώνονται στο διαδίκτυο όπως η αγορά άϋλων αγαθών μικρής αξίας κ.α. Μερικά από τα συστήματα αυτά όπως οι έξυπνες κάρτες αρχίζουν να χρησιμοποιούνται και στον φυσικό κόσμο ενώ άλλα είναι σχεδιασμένα αποκλειστικά για χρήση στο διαδίκτυο.

Ειδικότερα τα συστήματα αυτά είναι:

Σχήματα ηλεκτρονικού χρήματος: Ως ηλεκτρονικό χρήμα, η Ευρωπαϊκή Κεντρική Τράπεζα ορίζει «την αποθήκευση χρηματικής αξίας σε ψηφιακή μορφή μέσω μιας συσκευής που μπορεί να χρησιμοποιηθεί ευρέως για την πραγματοποίηση πληρωμών σε δίκτυα χωρίς την χρήση τραπεζικών λογαριασμών. Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο υπόθεμα. Ενώ τα δίκτυα θα είναι είτε ανοικτά δηλαδή θα επιτρέπουν την άμεση μεταφορά χρημάτων μεταξύ υποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται από συγκεκριμένο τραπεζικό λογαριασμό αποκλειστικά»[35]. Είναι επομένως εμφανές ότι το ηλεκτρονικό χρήμα έχει ανάλογες ιδιότητες με τα κοινά τραπεζογραμμάτια.

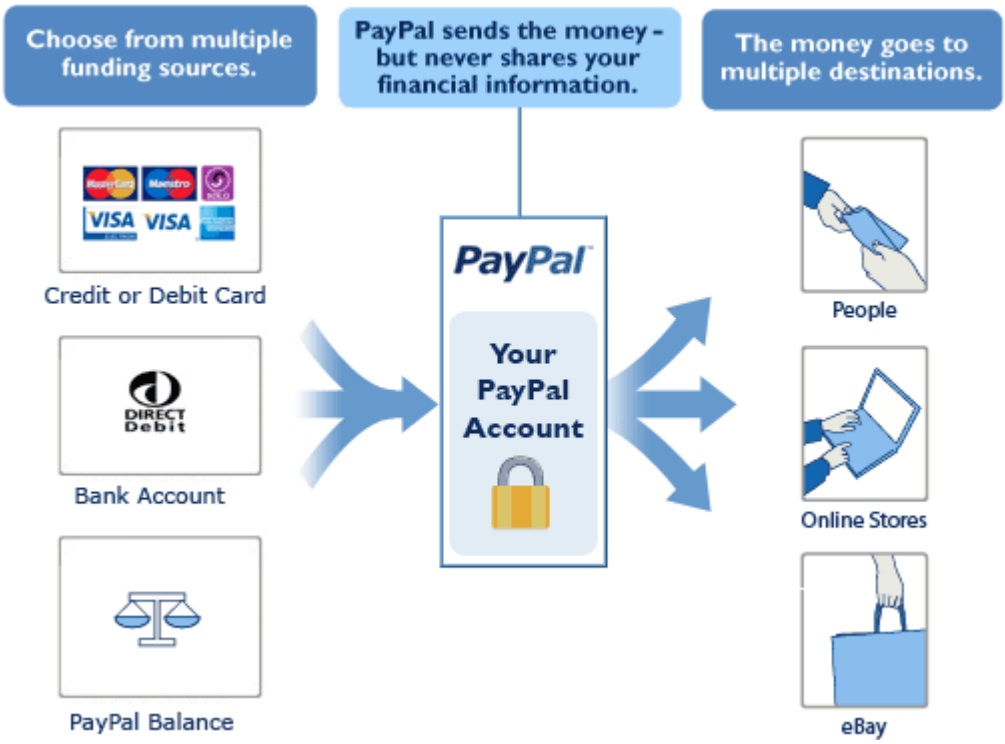
Προπληρωμένες κάρτες: πρόκειται για κάρτες που είναι δυνατόν να αγοραστούν από περίπτερα ή καταστήματα και περιέχουν μονάδες ανάλογα με την τιμή αγοράς

[34] **Πηγή:** e-Business forum (Ε΄ Κύκλος Εργασιών: Ομάδα Εργασίας Ε3). Αθήνα Ιανουάριος 2004
[35] **Πηγή:** Turban, E.; Lee, J.; King, D. & Chung, H. M. (2003). Electronic commerce: A managerial perspective. International Edition.

τους. Η κάρτα περιέχει ένα κωδικό που αποκαλύπτεται αφού αφαιρεθεί η ειδική επίστρωση από τον κάτοχο της. Οι λογαριασμοί με τα προπληρωμένα ποσά είναι αποθηκευμένοι σε ένα ειδικό διακομιστή και έτσι δεν απαιτείται αποθήκευση του ποσού στον υπολογιστή του χρήστη ή σε έξυπνη κάρτα.

Οι προπληρωμένες κάρτες χρησιμοποιούνται κυρίως για την διεκπεραίωση συναλλαγών μικρής αξίας στο διαδίκτυο. Επιπλέον έχουν το πλεονέκτημα ότι προστατεύουν την ανωνυμία του κατόχου καθώς δεν απαιτείται προεγγραφή σε κάποιο τρίτο μέρος ή χρήση τραπεζικού λογαριασμού.

PayPal[36] **:** είναι ο πιο διάσημος τρόπος συναλλαγών παγκοσμίως. Το Paypal πολύ γρήγορα αποδείχθηκε ως το πιο αξιόπιστο μέσο συναλλαγών στο διαδίκτυο. Πλέον οι περισσότερες επιχειρήσεις δέχονται πληρωμές μέσω Paypal καθώς έτσι διασφαλίζεται και ο έμπορος αλλά και ο πελάτης.



Εικόνα 5.1. **Πληρωμή μέσω** PayPal

Ποιος ο ρόλος του Paypal; Όταν κάποιος θέλει να κάνει μια αγορά μέσω internet πρέπει τις περισσότερες φορές η εταιρεία να πληρωθεί αμέσως και μετά να γίνει η αποστολή του προϊόντος. Για να πληρωθεί η εταιρεία όμως πρέπει να μεταφερθούν χρήματα από τον λογαριασμό μας ή από την πιστωτική μας κάρτα στον λογαριασμό της εταιρείας. Είναι φυσικό όμως να ανησυχούμε πολύ όταν δίνουμε διαδικτυακά σε κάποιον που ποτέ δεν έχουμε δει, στοιχεία είτε της πιστωτικής μας είτε του τραπεζικού μας λογαριασμού. Αυτό το κενό έρχεται να καλύψει το Paypal. Το PayPal έχει τα παρακάτω πλεονεκτήματα σε σχέση με τις άλλες μεθόδους πληρωμής μέσω interntet.

[36] **Πηγή:** http://www.ergasiaonline.gr/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD -paypal/

- Είναι γρήγορο, καθώς οι πληρωμές γίνονται άμεσα.
- Οι πληροφορίες για την πιστωτική σας κάρτα ή τον τραπεζικό σας λογαριασμό είναι αποθηκευμένες ασφαλώς στους servers του Paypal και ΔΕΝ δημοσιοποιούνται στον πωλητή, ο οποίος παραλαμβάνει μόνο τα χρήματα για την αγορά σας, χωρίς ποτέ να μαθαίνει κάτι άλλο για εσάς.
- Όλες οι σελίδες του Paypal είναι ισχυρά κρυπτογραφημένες, χωρίς το ενδεχόμενο υποκλοπής των προσωπικών ή οικονομικών σας στοιχείων.
- Είναι εύκολο, καθώς ο καθένας μπορεί να στείλει χρήματα με το πάτημα μερικών κουμπιών. Συνήθως το μόνο που απαιτείται είναι η χρήση ενός και μόνο password.
- Το Paypal συνεχώς επιλέγει και αξιολογεί την συνεργασία με κάποιο ηλεκτρονικό κατάστημα, αυξάνοντας έτσι την αξιοπιστία του πωλητή.
- Δεν κοστίζει καθόλου στους πελάτες, δηλαδή η αποστολή χρημάτων είναι εντελώς δωρεάν.

Pay Safe : Ένας άλλος τρόπος ασφαλούς πληρωμής στο διαδίκτυο είναι οι κάρτες Pay Safe, οι οποίες κερδίζουν όλο και περισσότερο την εμπιστοσύνη των χρηστών.

Η χρήσης τους είναι πολύ απλή και ξεκινά με την αγορά μιας κάρτας (ουσιαστικά είναι ένα χαρτάκι που έχει έναν 16ψήφιο αριθμό). Η κάρτα περιέχει συγκεκριμένο ποσό χρημάτων που είναι το ακριβές αντίτιμο που έχουμε καταβάλει για να την αγοράσουμε.

Εικόνα 5.2. **Πληρωμή μέσω** PaySafe

Για να πληρώσουμε για την αγορά κάποιου προϊόντος αρκεί να δώσουμε στη σελίδα του προμηθευτή μας τον 16ψήφιο κωδικό και η συναλλαγή έχει ολοκληρωθεί. Η κάρτα μας αμέσως χάνει την αξία της και το ποσό μεταβιβάζεται στον προμηθευτή.

Η κάρτα αυτή είναι πολύ εύκολο να αποκτηθεί από κάποιον αφού πωλείται σε πάρα πολλά σημεία (περίπτερα, ψιλικατζίδικα, super market κ.α) και δεν χρειάζεται να κάνουμε καμία εγγραφή με τα στοιχεία μας πουθενά. Είναι λοιπόν ουσιαστικά μια ανώνυμη πληρωμή. Αυτό βέβαια εξαρτάται και από την ιστοσελίδα που θα κάνουμε την αγορά η οποία μπορεί να μας ζητήσει στοιχεία, όχι για ταυτοποίηση, αλλά για επιβεβαίωση της συναλλαγής.

Ένα αρνητικό χαρακτηριστικό της κάρτας Pay Safe είναι ότι το ποσό της συναλλαγής είναι λίγο περιορισμένο και ανέρχεται στα 100€ (παίζει ρόλο και η χώρα που προμηθευόμαστε την κάρτα). Σε περίπτωση όμως που υπάρχει ανάγκη για μεταφορά μεγαλύτερου ποσού ο χρήστης μπορεί να χρησιμοποιήσει περισσότερες κάρτες.

Μπορεί να είναι λίγο κουραστικό να πρέπει να εισάγεις ένα σωρό αριθμούς αν θέλεις να κάνεις μία μεγάλη κατάθεση αλλά από την άλλη είναι ο μοναδικός τρόπος ο οποίος μπορεί να προσφέρει τέλεια ανωνυμία και προστασία των συναλλαγών μας.

5.5 To E-banking

Ο όρος e-banking ή ηλεκτρονική τραπεζική περιλαμβάνεις όλες τις υπηρεσίες που παρέχουν οι τράπεζες μέσω του Διαδικτύου, χωρίς δηλαδή τη φυσική παρουσία του πελάτη. Πως τώρα αυτός ο όρος συνδέεται με τις επιχειρήσεις και τους χρήστες του ηλεκτρονικού εμπορίου ;

Η σχέση των επιχειρήσεων με τις τράπεζες προσαρμόζεται πλέον στους ρυθμούς με τους οποίους εργάζεται η σύγχρονη, παγκοσμιοποιημένη και συνεχώς ανταγωνιστικότερη οικονομία. Συνεχής λειτουργία επί 24 ώρες και για τις 7 ημέρες της εβδομάδας, με παράλληλη εντυπωσιακή μείωση του χρόνου εκτέλεσης των εντολών με το συνεπακόλουθο περιορισμό του κόστους.

Αντίστοιχα οι χρήστες αναζητούν πιο εύκολους και γρήγορους τρόπους για να ολοκληρώσουν τις συναλλαγές τους και οι τράπεζες με την σειρά σους προσφέρουν αυτούς τους τρόπους ως δέλεαρ για να προσελκύσουν περισσότερους πλάτες.

Ανάλογα με τις παρεχόμενες υπηρεσίες το e-banking διακρίνεται σε λιανική ηλεκτρονική τραπεζική, αν απευθύνεται σε ιδιώτες, και σε χονδρική ηλεκτρονική τραπεζική όταν απευθύνεται σε επιχειρήσεις.

Στην Ελλάδα τώρα, σύμφωνα με τις πρόσφατη έρευνα που διεξήγαγε το e¬business forum[37] για την εισαγωγή του internet και της πληροφορικής στη λειτουργία της ελληνικής επιχείρησης, προέκυψε ότι μόλις το 28% των ελληνικών επιχειρήσεων που χρησιμοποιούν internet λαμβάνουν σήμερα υπηρεσίες e-banking. Αντίθετα, διεθνώς το web banking αναδεικνύεται ως ένα από τα ισχυρότερα κίνητρα για την αρχική ηλεκτρονική ενεργοποίηση των επιχειρήσεων.

Πάντως οι Ελληνικές Τράπεζες φαίνεται πως είναι έτοιμες να εξυπηρετήσουν τους Έλληνες καταναλωτές και τις ελληνικές επιχειρήσεις με μεγάλο πλήθος υπηρεσιών. Σύμφωνα με έρευνα που πραγματοποίησε το Οικονομικό Πανεπιστήμιο Αθηνών[38] οι ελληνικές τράπεζες είναι εφάμιλλες των Ευρωπαίων ανταγωνιστών τους όσον αφορά στην παρουσία τους στο Διαδίκτυο. Το έργο είχε ως αντικείμενο την αξιολόγηση των ιστοσελίδων των ελληνικών τραπεζών σε σύγκριση με τις αντίστοιχες ευρωπαϊκές. Το συμπέρασμα ήταν ότι η παρουσία τους είναι ισάξια, καθώς οι ελληνικές τράπεζες εισχώρησαν στο E-banking αργότερα, με αποτέλεσμα να έχουν πρόσβαση σε τελειότερη τεχνολογία και τεχνογνωσία.

Οι σημαντικότερες online υπηρεσίες που προσφέρονται από τις ελληνικές τράπεζες είναι :

- Ενημέρωση (υπόλοιπα λογαριασμών, κινήσεις)
- Πληρωμή λογαριασμών (πιστωτικές κάρτες, ΔΕΚΟ, κινητή τηλεφωνία)
- Πληρωμή ΦΠΑ (αν έχει υποβληθεί σχετική αίτηση μέσω Internet-Taxisnet)
- Πληρωμή ασφαλιστικών ταμείων (ΙΚΑ, ΤΕΒΕ)
- Μισθοδοσία
- Μεταφορές χρημάτων σε λογαριασμούς τρίτων στην ίδια ή άλλη τράπεζα (πχ πληρωμή προμηθευτών, εμβάσματα)
- Αιτήσεις τραπεζικών προϊόντων (κάρτες, δάνεια, καρνέ επιταγών)
- Χρηματιστηριακές συναλλαγές

Τα οφέλη που αποκομίζουν οι χρήστες είναι :

- Μείωση λειτουργικού κόστους:
- Μείωση λειτουργικών εξόδων
- Μείωση προμηθειών
- Ελαχιστοποίηση κινδύνου απωλειών χρημάτων
- Εξοικονόμηση χρόνου
- Δεν απομακρύνεστε από το σπίτι ή το γραφείο
- Δεν περιμένετε σε χρονοβόρες ουρές

[37] **Πηγή:** Ebusinessforum - www.ebusinessforum.gr
[38] **Πηγή:** http://www.eltrun.gr/ (Οικονομικό Πανεπιστήμιο Αθηνών- Εργαστήριο Ηλεκτρονικού Εμπορίου

- Ø Ευελιξία. Εκτελείτε τις συναλλαγές σας από οποιοδήποτε χώρο όλο το 24ωρο 7 ημέρες την εβδομάδα.

5.6 Κίνδυνοι του E-banking

Οι ηλεκτρονικές επιθέσεις δεν είναι νέο φαινόμενο, στατιστικά στοιχεία αποδεικνύουν ότι η συχνότητά τους τα τελευταία χρόνια αυξάνεται κυρίως. Η αύξηση αυτή μπορεί να μην είναι τεράστια, παρόλα αυτά όμως αποτελεί ανησυχητικό φαινόμενο αφού οι οικονομικές πληροφορίες που διακινούνται είναι άκρως απόρρητες και προσωπικές.

Ο δικηγόρος και καθηγητής του ΤΕΙ Μεσολογγίου Κος Χρήστος Τσουραμάνης[39] στο βιβλίο του «Η (αν)ανασφαλής Όψη του Διαδικτύου» αναφέρει ότι ειδικοί σε θέματα ασφάλειας έχουν υπολογίσει ότι μια τράπεζα μπορεί να ξοδέψει μέχρι και 1 εκατομμύριο δολάρια σε εξοπλισμό και συμβούλους ασφάλειας προκειμένου να διορθώσει τις ατέλειες και να κλείσει τις «τρύπες» στο σύστημά της. Το πρόβλημα πάντως δεν προβάλλεται στις πλήρεις του διαστάσεις για ευνόητους λόγους. Οι μεγαλύτερες και εντυπωσιακότερες επιθέσεις είναι αυτές φτάνουν στο φως της δημοσιότητας, οι υπόλοιπες και περισσότερες, κρατούνται κρυφές.

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 ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είχαν την εκούσια ή ακούσια βοήθεια και κάποιου που εργαζόταν στην τράπεζα.

Και χωρίς τη βοήθεια εκ των έσω, πάντως, οι εισβολείς 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» ασφάλειας στο σύστημα επιτρέποντας σε χάκερς, να έχουν πρόσβαση σε αυτό.

Εν κατακλείδι λοιπόν μπορούμε να πούμε ότι οι κίνδυνοι για επιθέσεις σε δίκτυα τραπεζών και σε συναλλαγές μέσω διαδικτύου είναι υπαρκτοί και έχουν προκαλέσει την απώλεια σημαντικών χρηματικών ποσών από χρήστες ή τράπεζες. Όμως η προσπάθεια για ασφαλείς συναλλαγές στο διαδίκτυο είναι συνεχής και όλοι οι φορείς κάνουν μεγάλες προσπάθειες για την αποφυγή οποιασδήποτε ηλεκτρονικής επίθεσης.

[39] **Πηγή:** Η (αν)ανασφαλής Όψη του Διαδικτύου . Χρ. Τσουραμάνης, Αθήνα Σεπτέμβριος 2005

5.7 Περιπτώσεις Ηλεκτρονικών Επιθέσεων

Παρακάτω παραθέτουμε μερικές από τις πιο σημαντικές επιθέσεις σε τράπεζες όπως αυτές καταγράφηκαν από ηλεκτρονικό περιοδικό Frontline[40].

Citibank (1994)

Ο Ρώσος χάκερ Βλαντιμίρ Λέβιν απέσπασε πόσο από λογαριασμούς της Citibank που υπολογίστηκε ότι ανερχόταν στα 10 εκατομμύρια δολάρια. Απέκτησε πρόσβαση στα δίκτυα της τράπεζας από την Αγία Πετρούπολη στη Ρωσία. Όταν συνελήφθη από την Σκότλαντ Γιαρντ και το FBI, παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς και passwords από πελάτες της τράπεζας και μετέφερε ποσά στο λογαριασμό του. Το 1998, ένα δικαστήριο στις Η.Π.Α. τον καταδίκασε σε 3 χρόνια κάθειρξη. Η τράπεζα ανέκτησε όλο το ποσό εκτός από 400.000 δολάρια.

ABN AMRO (Σεπτέμβριος 2000)

Ένα ολλανδικό τηλεοπτικό πρόγραμμα αποκάλυψε πως χάκερς, έκλεβαν σημαντικές πληροφορίες των πελατών της Ολλανδικής αυτής πολυεθνικής τράπεζας. Οι χάκερς έστελναν στους πελάτες της τράπεζας μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προέρχονταν από την τράπεζα (spoof). Τα mails αυτά εγκαθιστούσαν στους υπολογιστές των πελατών προγράμματα τα οποία επέτρεπαν στους χάκερς να έχουν πρόσβαση σε κρίσιμες πληροφορίες των λογαριασμών τους και με αυτόν τον τρόπο να μεταφέρουν χρήματα από αυτούς. Η τράπεζα διένειμε καινούριες εκδόσεις του λογισμικού της.

E*Trade (Σεπτέμβριος 2000)

Η εταιρεία παραδέχτηκε πως ο δικτυακός της τόπος είχε ένα τρωτό σημείο από όπου κάποιος χάκερ θα μπορούσε να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα. Ο προγραμματιστής που το ανακάλυψε δήλωσε πως ένας χάκερ εκμεταλλευόμενος το πρόβλημα αυτό, θα μπορούσε να αποκτήσει τον κωδικό και το username κάθε χρήστη.

Charles Schwab (Δεκέμβριος 2000)

Η Charles Schwab είναι η μεγαλύτερη online χρηματιστηριακή εταιρεία στις Η.Π.Α. Ο δικτυακός τόπος της εταιρείας έδινε τη δυνατότητα σε χάκερς να έχουν πρόσβαση σε όλους τους λογαριασμούς των πελατών της. Μάλιστα, όσο ο πελάτης ήταν συνδεδεμένος στο σύστημα, ο χάκερ μπορούσε να αγοράσει και να πουλήσει μετοχές από το λογαριασμό του.

Nara Bank, Western Union, Central National Bank κ.α. (Απρίλιος 2001)

[40] **Πηγή:** http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html

Αμερικανοί εισαγγελείς κατηγόρησαν δύο Ρώσους για ηλεκτρονικά εγκλήματα που σχετίζονταν με μια σειρά επιθέσεων σε δίκτυα τραπεζών και άλλων εταιρειών. Οι δύο χάκερς, εισέβαλαν στα συστήματα των εταιρειών, έκλεψαν πολύτιμες πληροφορίες και κατόπιν εμφανίζονταν στις εταιρείες ως σύμβουλοι ασφάλειας και προσέφεραν τις υπηρεσίες τους για διορθωθούν τα σφάλματα.

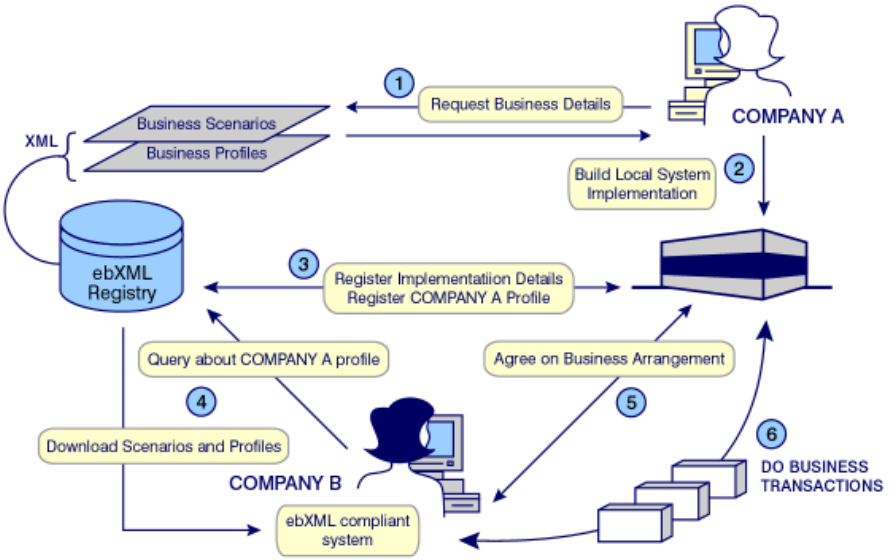
6ο Κεφάλαιο
Νέες Στρατηγικές και Τεχνολογίες

6.1 Electronic Business XML[41]

Το ebXML είναι ένα καινούριο πρότυπο για το παγκόσμιο ηλεκτρονικό εμπόριο. Είναι ένα σύνολο από προδιαγραφές που καθιστούν δυνατόν σε επιχειρήσεις από όλο τον κόσμο, οποιουδήποτε μεγέθους, οποιασδήποτε γεωγραφικής περιοχής να συνάπτουν συνεργασίες μέσω του διαδικτύου. Με την χρήση του ebXML, οι εταιρίες θα έχουν μία σταθερή μέθοδο για να ανταλλάσσουν μηνύματα, να συνάπτουν επιχειρηματικές σχέσεις, να μεταδίδουν δεδομένα με κοινά αποδεκτούς όρους και να ορίζουν και καταγράφουν επιχειρηματικές διαδικασίες.

Το ebXML βασίζεται στην γλώσσα XML (Extensible Markup Language) και προσφέρει ένα πλαίσιο εργασίας το οποίο σκοπεύει να μετατραπεί σε ένα παγκόσμιο standard, κάτω από την κηδεμονία του UN/CEFACT, ενός από τα τέσσερα μεγαλύτερα νομικά σώματα στον κόσμο.

Μέχρι τώρα, η υπάρχουσα τεχνολογία για να ανταλλάσσουν δεδομένα οι περισσότερες επιχειρήσεις ήταν το EDI, το οποιο είχε σημαντική προσφορά στην παραγωγικότητα και στον έλεγχο των αποθηκών. Ωστόσο οι περισσότερες εταιρείες θεωρούσαν το EDI ακριβό και δύσκολο στην εκτέλεσή του. Το ebXML χρησιμοποιώντας τις οικονομικές κλίμακες που παρουσιάζονται στο Διαδίκτυο, ξεπερνάει αυτά τα εμπόδια. Εκτός από B2B, το ebXML υποστηρίζει μηνύματα και υπηρεσίες B2C. Ωστόσο για τις B2C συναλλαγές, οι προδιαγραφές ορίζουν μόνο την αρχιτεκτονική από την πλευρά της επιχείρησης, και όχι του καταναλωτή.



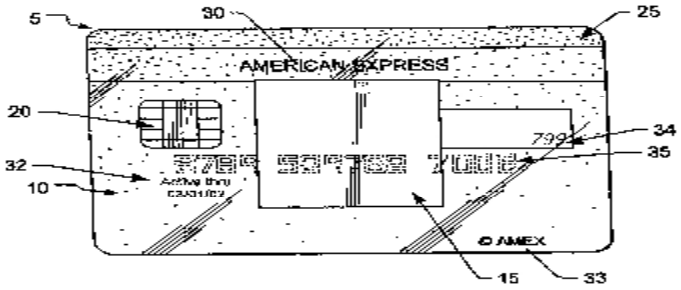
Εικόνα 6.1. **Παράδειγμα χρήσης του** Electronic Business XML

[41] **Πηγή:** Βικιπαίδεια http://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%C

6.2 Finread[42]

Οι χρεωστικές και πιστωτικές κάρτες βρίσκονται εδώ και πάρα πολλά χρόνια στην κυκλοφορία και όπως είναι φυσικό, δεν σχεδιάστηκαν για να συμβαδίσει η λειτουργία τους με το Internet. Εν έτη 2000, οι απάτες με πιστωτικές κάρτες ήταν στο σύνολό τους εκατοντάδες εκατομμυρίων Ευρώ και το 2001, ανέβηκε κατά ένα μνημειώδες 50%.

Σε αντίδραση σε αυτό το πρόβλημα, μια ομάδα από Ευρωπαίους συνεργάτες, χρηματοδοτούμενο από την ΕΕ, ξεκίνησαν ένα project με όνομα «Ολοκληρωμένο Κύκλωμα Ανάγνωσης Κάρτας Οικονομικών Συναλλαγών» (Financial Transactional Integrated Circuit Card Reader - FINREAD). Είναι η πρώτη φορά που επτά Ευρωπαϊκές κατασκευαστικές εταιρείες πιστωτικών καρτών ένωσαν τις δυνάμεις τους για να αντιμετωπίσουν το καταναλωτικό αυτό έγκλημα



Εικόνα 6.2. **Πιστωτική κάρτα**. (20 – **Έξυπνο τσιπάκι**)

Από την έναρξη του FINREAD, καθιερώθηκε ένα σύνολο από τεχνικές προδιαγραφές για ένα νέο είδος έξυπνων αναγνωστών καρτών, με αποτελέσματα στην τεχνολογία Ολοκληρωμένων Κυκλωμάτων (IC) για ασφαλείς πληρωμές από το Διαδίκτυο. Στις αρχικές μέρες οι πιστωτικές κάρτες είχαν απλά μια μαγνητική λωρίδα, αλλά τώρα τουάχιστον το 50% των καρτών είναι βασισμένο σε τσιπάκια. Ο κυριότερος λόγος είναι το Internet, το οποίο εξελίσσεται σε μία από τις βασικότερες πιθανές αιτίες για την βαρυσήμαντη αύξηση στις τραπεζικές απάτες.

Για επιτυχή αποτελέσματα ήταν αναγκαία η χρήση προδιαγραφών ανοικτού κώδικα. Έτσι, οι σχεδιαστές έξυπνων καρτών είχαν ελεύθερη πρόσβαση στις προδιαγραφές, διασφαλίζοντας στο FINREAD την περαιτέρω ανάπτυξη ενός παγκόσμιου συνδέσμου σε Η/Υ αναγνώστη καρτών. Η τεχνολογία πίσω από την έξυπνη κάρτα, σε συνδυασμό με τον αναγνώστη καρτών, επιτρέπει σε έναν απομακρυσμένο διακομιστή να κατεβάζει, διαμέσου του FINREAD και μιας πολύ ασφαλούς οδού, ένα μικρό applet το οποίο αναλαμβάνει όλες τις ευαίσθητες λειτουργίες (π.χ. πληκτρολόγηση PIN, προβολή ευαίσθητων δεδομένων, πρόσβαση στην έξυπνη κάρτα κτλ), τα οποία συνήθως γίνονταν συνήθως σε ανασφαλής Η/Υ.

[42] **Πηγή:** ICT Results : http://cordis.europa.eu/ictresults/index.cfm? section= home&tpl= article& BrowsingType=Features&ID

Πολλές απόπειρες είχαν γίνει με σκοπό την ανακάλυψη μιας κοινής αρχιτεκτονικής, η οποία θα παρείχε ένα ασφαλές interface για τους αναγνώστες καρτών ολοκληρωμένων κυκλωμάτων. Ωστόσο οι περισσότερες από αυτές πιθανές λύσεις βασίζονται στη χρήση των ιδιαιτεροτήτων που παρέχονται από τους κατασκευαστές. Αυτό δεν αποτελεί πρόβλημα για τον αναγνώστη καρτών FINREAD επειδή όταν συνδέεται με έναν Η/Υ, είναι σε θέση να διαχειρίζεται όλους τους τύπους πληρωμών και άλλων τύπων καρτών σε μία μόνο φυσική μονάδα. Το ίδιο applet θα τρέχει σε κάθε συμβατό με το FINREAD αναγνώστη, ανεξάρτητα από τον κατασκευαστή.

Ο FINREAD αναγνώστης επίσης έχει την δυνατότητα να αλλάζει από την ασφαλή κατάσταση (default), στην διαφανή κατάσταση για μη-ευαίσθητα ή μη-συμβατά FINREAD applets. Επιπρόσθετα πλεονεκτήματα είναι η εμπιστοσύνη του ιδιοκτήτη της κάρτας σε σχέση με τις αγορές μέσω Internet, ασφαλείς πληρωμές μέσω τραπεζών και ασφαλείς πληρωμές λιανικής μέσω ανοικτών δικτύων.

Εικόνα 6.3. ***Αναγνώστης*** FINREAD

Μάλιστα, στις 11 Οκτωβρίου του 2004, ένα σύνολο από 20 χώρες-μέλη του πρότυπου ISO (International Organisation for Standardization) έδωσαν την έγκρισή τους στο FINREAD, ώστε αυτό να γίνει ένα νέο Αντικείμενο Εργασίας για την έκδοση τεχνικών προδιαγραφών για μια ασφαλή και διαδραστική συσκευή συναλλαγών IC κάρτας.

6.3 E-CRM[43]

Η έλευση του Internet άλλαξε δραστικά την κατάσταση και κατέστησε το CRM (Customer Relationship Management) ως electronic-CRM ή e-CRM. Το χαμηλό κόστος επικοινωνίας του Internet επιτρέπει στις επιχειρήσεις να συλλέγουν και να επεξεργάζονται σε πολύ μικρό χρόνο, μεγάλο όγκο δεδομένων πωλήσεων, ανεξαρτήτως της γεωγραφικής περιοχής στην οποία πραγματοποιούνται οι συναλλαγές.

Πλέον κανείς δεν θεωρεί μεθοδολογίες CRM, χωρίς τη χρήση της νέας τεχνολογίας της τηλεπληροφορικής. Το Internet προσφέρεται για την ενσωμάτωση διαδικασιών CRM, εφόσον όμως υπάρχει η απαραίτητη υποδομή σε μια επιχείρηση. Κατά κανόνα

[43] **Πηγή:** Βικιπαίδεια http://en.wikipedia.org/wiki/ECRM

το CRM μπορεί ν' αξιοποιηθεί από τις επιχειρήσεις εκείνες που διαθέτουν κάποιου είδους μηχανογράφηση και στους υπολογιστές τους υπάρχουν αποθηκευμένα τα στοιχεία των πελατών τους.

Κάποια από τα κυριότερα πλεονεκτήματα του CRM και του E-CRM είναι :

- Εντοπισμός σημαντικότερων πελατών
- Αύξηση των ποσών που διαθέτουν για καταναλωτικές δαπάνες
- Στόχευση της εμπορικής επικοινωνίας
- Περιορισμός των απωλειών στην καταναλωτική βάση
- Δημιουργία πιστού αγοραστικού κοινού

Η μεγάλη υπόσχεση του CRM είναι η δυνατότητα ανταπόκρισης στις εξατομικευμένες ανάγκες των πελατών με μία συστηματοποιημένη μεθοδολογία. Η νέα τεχνολογία και η εξέλιξη του λογισμικού των ηλεκτρονικών υπολογιστών επιτρέπουν τον προγραμματισμό και την ενεργοποίηση επαφών με τους πελάτες, με βάση την ίδια την αγοραστική συμπεριφορά και τις συνήθειες τους, τις οποίες μπορούμε να γνωρίζουμε σε αρκετά μεγάλο βάθος.

6.4 RF (E-CRM) ID[44]

Το RFID (Radio Frequency Identification), είναι μία διαρκώς αναπτυσσόμενη τεχνολογία, που χρησιμοποιεί ραδιοσυχνότητες για την αναγνώριση προϊόντων και την μετάδοση πληροφοριών μέσα στην εφοδιαστική αλυσίδα και αποτελεί ένα βασικό φορέα δεδομένων που συμπληρώνει το σύνολο των προτύπων EANUCC σε σημαντικά πεδία εφαρμογών όπως:

- Τη Διαχείριση των «επιστρεφομένων - κενών» και των μονάδων logistics προς επαναχρησιμοποίηση
- Τις διαδικασίες logistics, συμπεριλαμβανομένης της παρακολούθησης και του εντοπισμού των ευπαθών και αλλοιουμένων ειδών
- Τον Ηλεκτρονικό Έλεγχο Προϊόντων για προγράμματα αντικλεπτικής προστασίας

Η βασική ιδέα είναι αρκετά απλή: ενσωματώνουμε μικρούς ραδιοφωνικούς πομπούς οπουδήποτε υπάρχει για κάτι αναγκαιότητα ανάγνωσης, σάρωσης, εναποθήκευσης ή ελέγχου. Όταν το RFID tag είναι ενεργοποιημένο από μία συσκευή ανάγνωσης, μεταδίδει πληροφορίες από το chip σε ένα κεντρικό υπολογιστικό σύστημα. Περίπου δύο kilobytes πληροφορίας, μπορούν να αποθηκευθούν σε ένα και μόνο chip.

[44] **Πηγή:** ICT Results : http://cordis.europa.eu/ictresults/index.cfm? section= home&tpl= article& BrowsingType=Features&ID=

Οι επιστήμονες προβλέπουν τη διεύρυνση της χρήσης του RFID μέσα στην επόμενη δεκαετία. Ήδη η Mastercard δοκιμάζει αυτή την τεχνολογία, σε 15.000 Αμερικανούς πελάτες της. Ωστόσο, στην προοπτική αυτή αντιδρούν οργανώσεις για τα πολιτικά δικαιώματα και άλλοι επιστήμονες, που υποστηρίζουν ότι, οι καταναλωτές θα γίνουν ευάλωτοι στις κλοπές.

Εφαρμογές του RFID :

Το RFID θα φέρει μεγάλες αλλαγές στις διαδικασίες διαχείρισης του αποθέματος στην εφοδαστική αλυσίδα. Οι αλλαγές αυτές με τη σειρά τους θα φέρουν μεγάλες απαιτήσεις από την υποδομή της επιχείρησης για την σωστή διαχείριση του όγκου των δεδομένων. Ακόμη, το κόστος υλοποίησης μιας λύσης RFID έχει μειωθεί δραματικά και εξακολουθεί να μειώνεται. Σύμφωνα πάντως με ένα πολύ πρόσφατο δελτίο τύπου, η διείσδυση του RFID προβλέπεται να γίνει γρηγορότερα από το αναμενόμενο.

Οι εφαρμογές των ετικεττών RFID είναι ατελείωτες. Μερικά παραδείγματα είναι : ασφαλής πρόσβαση σε ευαίσθητους χώρους και δεδομένα, πρόληψη απάτης για πωλητές, παρακολούθηση αποθήκης, δεδομένα αποστολής και συλλογή δεδομένων παραγωγικής διαδικασίας για κατασκευαστές. Το πιο σημαντικό όμως είναι ότι το RFID αναμένεται να εξελιχθεί σε έναν από τους πιο κρίσιμους παράγοντες για την επίτευξη του Real Time Enterprise (Εγχειρήματα σε Πραγματικό Χρόνο).
METRO Group

Η METRO Group - η τρίτη μεγαλύτερη εταιρία λιανικού εμπορίου παγκοσμίως και πρωτοπόρος στη εγκατάσταση συστημάτων RFID - και η Intermec Technologies Corporation ανήγγειλαν την επιτυχή ολοκλήρωση της εφαρμογής συστήματος RFID στο μεγαλύτερο και πιο πολυάσχολο κέντρο διανομής της METPO στην Unna της Γερμανίας. Το κέντρο διανομής είναι εξοπλισμένο με αναγνώστες Intermec IF5 Intelligent RFID και ετικέτες (tags) RFID της Intermec. Η «λύση» περιλαμβάνει την εγκατάσταση ετικετών σε περισσότερες από 50.000 παλέτες. Πιο αξιοσημείωτο γεγονός από αυτό αποτελεί το ποσοστό επιτυχούς ανάγνωσης ετικετών που αγγίζει το 99% καθώς και η πλήρης συμμόρφωση του συστήματος με τα πρότυπα του ETSI για λειτουργία στην Ευρώπη.

7ο Κεφάλαιο
Ασφάλεια Ηλεκτρονικών Συναλλαγών

7.1 Εισαγωγή

Σε κάθε δίκτυο η επικοινωνία μεταξύ των χρηστών κρύβει κινδύνους όσον αφορά την επικοινωνία τους και την ανταλλαγή δεδομένων. Οι κίνδυνοι αυτοί πολλαπλασιάζονται και γίνονται υψίστης σημασία όταν αναφερόμαστε στο διαδίκτυο (Internet) και όταν τα δεδομένα που ανταλλάσσονται είναι υψίστης σημασίας (προσωπικά, οικονομικά). Προκειμένου να εστιάσουμε στους κινδύνους που απειλούν τις ηλεκτρονικές συναλλαγές καλό είναι να ορισθεί τι είναι κίνδυνος.

«Κίνδυνος[45] *λοιπόν, είναι κάθε απειλή που σκοπό έχει να βλάψει την ακεραιότητα των ηλεκτρονικών συναλλαγών και να εκμεταλλευτεί οποιαδήποτε πληροφορία, που μπορεί να αποκομίσει παραβιάζοντας την ιδιωτικότητά τους.»*

Οι κίνδυνοι λοιπόν που ελλοχεύουν κατά τη διάρκεια των ηλεκτρονικών συναλλαγών είναι:

- **Η υποκλοπή δεδομένων**, δηλαδή η αποκάλυψη πληροφοριών. Το γεγονός αυτό, συμβαίνει όταν ο χρήστης καταφέρνει να υποκλέψει δεδομένα που μεταδίδονται σε μια διαδικτυακή επικοινωνία.

    - **Ενδεχόμενη ζημία:** Η παράνομη υποκλοπή μπορεί να προξενήσει βλάβη, τόσο ως παραβίαση ιδιωτικής ζωής των ατόμων όσο και ως μέσω εκμετάλλευση των δεδομένων που έχουν υποκλαπεί, όπως συναισθηματικών ή στοιχείων από πιστωτικές κάρτες για εμπορικό κέρδος ή δολιοφθορά.

- **Η καταστροφή / μαζική αλλοίωση δεδομένων**, δηλαδή όταν ο χρήστης τροποποιεί ή πλαστογραφεί δεδομένα, καθώς και όταν εισάγει παραποιημένα και πλαστά δεδομένα σε μεταδιδόμενα μηνύματα.

- **Οι απάτες (ψεύτικες συναλλαγές)** , η περίπτωση όπου κάποιος έχει μπει στο σύστημα κάποιου ηλεκτρονικού καταστήματος και έχει γράψει στοιχεία για ανύπαρκτες συναλλαγές ή τροποποιεί τη διεύθυνση παράδοσης κάποιας παραγγελίας, με σκοπό το προϊόν να πάει αλλού.

---

45 **Πηγή** : Αρσένης Πασχόπουλος & Παναγιώτης Σκαλτσάς, Ηλεκτρονικό Εμπόριο 2η Έκδοση, Εκδόσεις: Κλειδάριθμος, Αθήνα 2001

- **Η άρνηση εξυπηρέτησης**, όταν ένας χρήστης ενεργεί με σκοπό να αποτρέψει τη διάθεση πόρων και υπηρεσιών προς νόμιμους χρήστες. Στα δικτυακά περιβάλλοντα, είναι συνηθισμένη η παρεμπόδιση της μετάδοση πληροφοριών, είτε με τη μετατροπή τους, είτε με τη καθυστέρηση τους. Επιπλέον, η κατανάλωση, κλοπή και καταστροφή των πόρων είναι και αυτά παραδείγματα κινδύνων αυτού του είδους, δηλαδή τις ρωγμές διαθεσιμότητας.

    - **Ενδεχόμενη ζημία:** Είναι επιθέσεις που έχουν σαν στόχο να προκαλέσουν προβλήματα στη λειτουργία του συστήματος ή του δικτύου που πλήττουν ώστε να το εμποδίσουν να προσφέρει τις υπηρεσίες για τις οποίες είναι προορισμένο στους νόμους χρήστες του.

- **Η μεταμφίεση**, όταν ένας χρήστης υποκρίνεται ότι είναι κάποιος άλλος προκειμένου να έχει εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες ή δυσχέρειες σε οργανισμό.
    - **Ενδεχόμενη ζημία:** Η παραπλάνηση ατόμων φορέων, είναι επιζήμια κατά διαφορετικούς τρόπους. Οι πελάτες ενδέχεται να «φορτώσουν» κακόβουλο λογισμικό, από δικτυακό τόπο που παρουσιάζεται ως έμπιστη πηγή. Ενδέχεται να δοθούν εμπιστευτικές πληροφορίες λάθος άτομα. Η παραπλάνηση, είναι δυνατόν να οδηγήσει σε άρνηση αναγνώρισης ηλεκτρονικών συμβάσεων και άλλα. Η μεγαλύτερη ίσως ζημιά είναι το γεγονός, ότι η έλλειψη επαλήθευσης ταυτότητας αποτρέπει δυνητική πελατεία.

- **Η κατάχρηση**, δηλαδή η χρήση πληροφοριακών αγαθών αλλά και των υπολοίπων πόρων για διαφορετικούς σκοπούς από τους προκαθορισμένους, γεγονός που προκαλεί άρνηση εξυπηρέτησης, αύξηση κόστους λειτουργίας και δυσφήμηση.

- **Μη εξουσιοδοτημένη** πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών (hacking , cracking) . Η μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή ή σε ένα δίκτυο υπολογιστών πραγματοποιείται συνήθως κακόβουλα με την πρόθεση αντιγραφής, τροποποίησης ή καταστροφής δεδομένων (παρείσφρηση) .

    - **Ενδεχόμενη ζημία**: ενώ η εξουσιοδοτημένη παρείσφρηση αρχίζει ως μια διαδικασία παρενόχλησης, αναδεικνύει τα τρωτά σημεία των δικτύων πληροφοριών και παρακινεί άτομα με εγκληματική ή δόλια πρόθεση να εκμεταλλευτούν αυτές τις αδυναμίες.

- **Τα Spyware**, είναι μικρά προγράμματα που μπαίνουν στον ηλεκτρονικ υπολογιστή χωρίς να το καταλαβαίνουμε και στέλνουν πληροφορίες στον

αποστολέα τους σχετικά με το λειτουργικό μας σύστημα, τις ιστοσελίδες που επισκεπτόμαστε, το εάν χρησιμοποιούμε το διαδίκτυο για αγορές κ.λπ.

- **Οι Dialers**, είναι προγράμματα που χρησιμοποιούν την τηλεφωνική γραμμή για να καλέσουν τηλέφωνο έναν αριθμό, που δημιουργεί υψηλότερα κόστη (για παράδειγμα 090), ώστε να πληρωθεί η εταιρία για τις υπηρεσίες που προσφέρει από εμάς.

- **Το Phising**, με τον όρο phising δεν χαρακτηρίζεται κάποιο πρόγραμμα, αλλά η προσπάθεια ορισμένων να εκμαιεύσουν κρίσιμα δεδομένα (όπως είναι οι αριθμοί πιστωτικών καρτών, password κ.τ.λ.), προσποιούμενοι ότι είναι κάποιος φορέας, που το υποψήφιο θύμα τους εμπιστεύεται (Τράπεζες, εταιρείες τηλεφωνίας κ.τ.λ.)

- **Τα αυτόνομα κακόβουλα προγράμματα**[46], όπως οι Ιοί, τα Σκουλήκια και οι Δούρειοι Ίπποι (Trojan horses). Τα συγκεκριμένα αποτελούν την μεγαλύτερη απειλή.

  - Ένας ιός υπολογιστών είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό.
  - Ο δούρειος ίππος (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.

  - Ένα σκουλήκι υπολογιστή (computer worm) είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη.

46 Πηγή : ΒικιΠαίδεια

7.2 Λόγοι Ανασφάλειας στο Διαδίκτυο

Γιατί όμως υπάρχουν τόσοι πολλοί κίνδυνοι κατά τη χρήση του διαδικτύου; Το διαδίκτυο, όπως είναι γνωστό αποτελεί το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων, όχι κατά ανάγκη ίδιας τεχνολογίας, που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε όλη την Γη. Είναι λοιπόν αντιληπτό, ότι είναι πολύ δύσκολο να αντιμετωπιστεί ολικά από άποψη ασφάλειας, εξαιτίας της ετερογένειάς που το χαρακτηρίζει.

Βέβαια πολύ σημαντικό είναι το γεγονός ότι οι μηχανισμοί που στηρίζουν την λειτουργικότητα του σχεδιάστηκαν με σκοπό την βελτιστοποίηση των δυνατοτήτων διασύνδεσης ετερογενών δικτύων και εκμετάλλευσης πόρων-πληροφοριών και όχι για να παρέχουν ασφάλεια.

Συμπερασματικά, η ασφάλεια επιτυγχάνεται ως πρόσθετο χαρακτηριστικό του δικτυακού σχεδίου και όχι ως κομμάτι του.

Οι λόγοι που τρέπουν το διαδίκτυο ανασφαλές είναι[47] :

- **Η ετερογένεια των δικτύων** που διασυνδέει, με δεδομένο το απέραντο μέγεθος του, έχει σαν συνέπεια : Οι διαδικασίες που διασφαλίζουν ένα σύστημα σε ένα τέτοιο περιβάλλον, να απαιτούν έναν μεγάλο αριθμό περίπλοκων ρυθμίσεων και διαμορφώσεων.

- Η εύκολη και απεριόριστη πρόσβαση που παρέχει σε εκατομμύρια χρήστες, το τρέπει πιο ευάλωτο από κάθε άλλο δίκτυο. Είναι στόχος πολλών επιθέσεων από επίδοξους εισβολείς. Αυτοί ποικίλουν, από εφήβους, βανδάλους, ηλεκτρονικούς εγκληματίες και άλλους με σκοπό να διεισδύσουν στα συστήματα.

- Η μη ύπαρξη συνολικής πολιτικής ελέγχου προσπέλασης. Δεν υπάρχει κατάλληλη υποδομή στους υπάρχοντες κόμβους, εξαιτίας άγνοιας, κόστους και άλλων λόγων, με αποτέλεσμα να υπάρχει μεγάλος κίνδυνος από την ευρέως ανοικτή σύνδεσή τους στο διαδίκτυο.

- Η φύση των πρωτοκόλλων TCP/IP και των περισσότερων υπηρεσιών που υποστηρίζουν, δεν μπορούν να εκμηδενίσουν τους κινδύνους ασφάλειας (HCFA,1998). Το γεγονός ότι δεν επιτρέπονται τα πακέτα των δεδομένων, να περνούν από μία σειρά απρόβλεπτων ενδιάμεσων υπολογιστών και επιμέρους δικτύων μέχρι να φθάσουν στον τελικό προορισμό τους, δίνει την δυνατότητα σε ένα τρίτο μέρος να παρέμβει με διαφόρους τρόπους στην επικοινωνία των δύο νόμιμων μερών. Επιδέξιοι εισβολείς μπορούν σχετικά εύκολα να παραβιάσουν την ασφάλεια των TCP/IP υπηρεσιών, με δεδομένο και ότι η πλειοψηφία των δεδομένων που διακινούνται είναι σε μη κρυπτογραφημένη μορφή.

47 **Πηγή** : Dr. Ravindra K. Ahuja - Professor in Industrial and Systems Engineering University of Florida

- Η αυξημένη πολυπλοκότητα διαδικασιών, περιορίζει το αίσθημα εμπιστοσύνης, μιας και όσο πιο δυσνόητο είναι κάτι τόσο μεγαλύτερη είναι η δυσπιστία που επικρατεί γι' αυτό.

- Η αύξηση στον αριθμό διαύλων επικοινωνίας, σημαίνει ταυτόχρονα αύξηση των πιθανών σημείων επίθεσης, όποτε υπάρχει αναγκαιότητα για μεγαλύτερη και κατάλληλη οχύρωσή τους.

- Η ασάφεια όσον αφορά τα όρια του δικτύων που εν υπάρχουν στο διαδίκτυο, καθώς και οι διακρίσεις των τμημάτων ενός οργανισμού. Κάθε κόμβος πρέπει να είναι ικανός να αντιδράσει σωστά στην παρουσία ενός νέου και μη έμπιστου κόμβου[48] . Βεβαίως είναι πολύ πιθανό ένας κόμβος να ανήκει σε περισσότερα από ένα δίκτυα, οπότε να μην έχουμε σαφή εικόνα των νόμιμων χρηστών του.

- Η δυνατότητα ανωνυμίας ενός χρήστη, απαιτεί πολύ ισχυρούς μηχανισμούς πιστοποίησης, διαφορετικούς από αυτούς που πιστοποιούν ανθρώπους στα υπολογιστικά συστήματα.

- Η ύπαρξη αδυναμίας ελέγχου δρομολόγησης των δεδομένων, που διακινούνται σε κάθε δίκτυο και κατ' επέκταση στο διαδίκτυο.

Είναι προφανές ότι είναι αρκετοί οι λόγοι που μας κάνουν να αισθανόμαστε ανασφάλεια στο διαδίκτυο, οπότε είναι φυσικό να λειτουργούμε με δυσπιστία μέσα σε αυτό, δηλαδή να μην απολαμβάνουμε στο έπακρο την ηλεκτρονική εξυπηρέτηση που μας παρέχεται.

Το αίσθημα της ανασφάλειας μεγιστοποιείται εξαιτίας και των κινδύνων που εν υπάρχουν και τους αντιμετωπίζουμε από την χρήση του. Προκειμένου λοιπόν να διασφαλιστούν οι σύγχρονες επιχειρήσεις, δηλαδή τα δίκτυα τους να εξασφαλιστούν από την οποιαδήποτε σύνδεση τους με το διαδίκτυο, θέτουν κάποιες γενικές απαιτήσεις ώστε να μην είναι ευάλωτες σε οποιονδήποτε έχει σκοπό να σφετεριστεί την παρουσία τους.

7.3 Γενικές Απαιτήσεις για την Ασφάλεια Δικτύων

Η προστασία ενός δικτύου το οποίο συνδέεται και με το Internet είναι ένα θέμα που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις και οργανισμοί. Οι γενικές απαιτήσεις ασφάλειας δικτύων και συστημάτων πληροφοριών μπορούν να διατυπωθούν με τα εξής τέσσερα, αλληλένδετα χαρακτηριστικά:

Διαθεσιμότητα:

Με τον όρο διαθεσιμότητα εννοούμε ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν, παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις.

48 **Πηγή** : Norman Fenton - Professor of Risk Information Management at Queen Mary London university

Επαλήθευση ταυτότητας:

Επιβεβαίωση της δηλούμενης ταυτότητας φορέων ή χρηστών. Για την επαλήθευση ταυτότητας, απαιτούνται κατάλληλες μέθοδοι για διάφορες εφαρμογές και υπηρεσίες, όπως είναι η ηλεκτρονική σύναψη σύμβασης, ο έλεγχος της πρόσβασης σε ορισμένα δεδομένα και υπηρεσίες (π.χ. για τους τηλεργαζόμενους) και η επαλήθευση ιστοθέσεων (π.χ. για διαδικτυακές τράπεζες).

Πρέπει επίσης να περιλαμβάνεται η δυνατότητα ανωνυμίας, δεδομένου ότι πολλές υπηρεσίες δεν χρειάζονται την ταυτότητα του χρήστη, αλλά μόνο αξιόπιστη επιβεβαίωση ορισμένων κριτηρίων (των καλουμένων "ανώνυμων διαπιστευτηρίων"), όπως η φερεγγυότητα.

Ακεραιότητα:

Επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί, παραληφθεί, ή αποθηκευθεί, είναι πλήρη και δεν έχουν υποστεί αλλοίωση.

Τήρηση του απορρήτου:

Προστασία επικοινωνιών ή αποθηκευμένων δεδομένων έναντι υποκλοπής και ανάγνωσης από μη εξουσιοδοτημένα άτομα. Απαιτείται ιδιαίτερα για τη μετάδοση ευαίσθητων δεδομένων και είναι μία από τις απαιτήσεις, που ανταποκρίνεται στο μέλημα προστασίας της ιδιωτικής ζωής των χρηστών δικτύων επικοινωνιών.

8^{o} Κεφάλαιο
Προστασία και Αξιοπιστία στις Ηλεκτρονικές Συναλλαγές

8.1 Εισαγωγή

Ο σκοπός οποιασδήποτε λύσης ασφαλείας, είναι να εμποδίσει οποιονδήποτε να κλέψει, να καταστρέψει ή κατ' άλλο τρόπο να φθάσει σε ευαίσθητες πληροφορίες. Η ασφάλεια μιας εταιρείας είναι πραγματικά διπλής όψης: εμπιστευτικές πληροφορίες και ακεραιότητα. Με άλλα λόγια ένα σύστημα ασφαλείας χρησιμεύει για να εμποδίσουμε κάποιον που επιτίθεται να αποσπάσει ή να καταστρέψει τα δεδομένα που ενυπάρχουν σε ένα δίκτυο και να σταματήσει κάποιον, που επιτίθεται προκειμένου να προσβάλει τη υπόληψη της εταιρίας.

Σύμφωνα με την έρευνα των CERT/FBI[49], οι πιο πολλοί οργανισμοί στηρίζονται σε πολλαπλές τεχνολογίες για να εξασφαλίσουν τα δίκτυα τους. Οι τεχνολογίες καταφέρνουν να διασπαστούν σε δυο βασικές κατηγορίες:

- Αυτές που είναι κατασκευασμένες έτσι, ώστε να εξασφαλίζουν την επικοινωνία μέσω του δικτύου και
- αυτές που είναι κατασκευασμένες ώστε να προφυλάσσουν τους διακομιστές και τους χρήστες επάνω στο δίκτυο.

Το ηλεκτρονικό εμπόριο όλων των τύπων στηρίζεται στη σημασία της εμπιστοσύνης μεταξύ του καταναλωτή και του ιστοχώρου τον οποίο επισκέπτεται. Έτσι λοιπόν παραθέτουμε τις πιθανές λύσεις που θα προστατέψουν τους χρήστες από οποιαδήποτε απειλή.

8.2 Ψηφιακά Πιστοποιητικά[50]

Ο βασικός ρόλος ενός ψηφιακού πιστοποιητικού είναι να επιβεβαιώνουν ότι ο ιδιοκτήτης ενός δημόσιου ή ιδιωτικού κλειδιού είναι αυτός που λέει ότι είναι. Ένα ψηφιακό πιστοποιητικό περιλαμβάνει πληροφορίες όπως είναι τα στοιχεία δημόσιου κλειδιού, η περίοδος ισχύος του πιστοποιητικού, έναν υπογεγραμμένο κατατεμαχισμό των δεδομένων του πιστοποιητικού (δηλαδή κατατεμαχισμένα περιεχόμενα του πιστοποιητικού υπογεγραμμένα με το ιδιωτικό κλειδί της αρχής πιστοποίησης) και το όνομα του ιδιοκτήτη.

Πιστοποιητικά χρησιμοποιούνται για πιστοποίηση της αυθεντικότητας ατόμων (προσωπικά πιστοποιητικά), εταιρειών λογισμικού (πιστοποιητικά εκδοτών λογισμικού) και ιστοθέσεων (πιστοποιητικά ιστοθέσεων). Υπάρχουν πολλές αρχές πιστοποίησης με γνωστότερη τη VeriSign. Εταιρείες όπως η Microsoft προσφέρουν

[49] Τμήμα του FBI που διεξάγει έρευνες για το ηλεκτρονικό έγκλημα. (CERT -Certified Products Listing)
[50] **Πηγή :** ΕΕΤΤ – Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

συστήματα, τα οποία επιτρέπουν σε εταιρείες να εκδίδουν τα δικά τους ιδιωτικά, εσωτερικά πιστοποιητικά (Turban & co., 2004).

8.3 Πιστοποίηση Αυθεντικότητας[51]

Η ασφάλεια των πληροφοριών προϋποθέτει να επιβεβαιώνονται τα έγκυρα μέρη μιας δοσοληψίας, να προσδιορίζονται οι λειτουργίες που μπορούν να κάνουν, και οι λειτουργίες τους να οριοθετούνται μόνο σε εκείνες που είναι βασική προϋπόθεση για έναρξη και ολοκλήρωση της δοσοληψίας.

Αυτό μπορεί να κατορθωθεί με ένα σύστημα πιστοποίησης της αυθεντικότητας. Τα συστήματα πιστοποίησης αυθεντικότητας έχουν πέντε κύρια μέρη:

i. να υπάρχει ένα διακριτικό χαρακτηριστικό, που διαφοροποιεί το άτομο από τους άλλους,
ii. να υπάρχει ένας μηχανισμός διαφοροποίησης, που να επιβεβαιώνει την ύπαρξη του χαρακτηριστικού διαφοροποίησης,
iii. ένα άτομο ή μια ομάδα να πιστοποιείται ως προς την αυθεντικότητα του,
iv. να χρησιμοποιείται ένας ιδιοκτήτης, που είναι αρμόδιος για το σύστημα και
v. να υφίσταται ένας μηχανισμός ελέγχουν προσπέλασης, που να οριοθετεί τις ενέργειες οι οποίες μπορούν να πραγματοποιηθούν από το άτομο ή την ομάδα του οποίου πιστοποιείται η αυθεντικότητα.

Σε ένα σύστημα πιστοποίησης αυθεντικότητας, τα χαρακτηριστικά διαφοροποίησης μπορούν να στηριχθούν σε κάτι που γνωρίζει κάποιος (όπως κωδικούς πρόσβασης), σε κάτι που έχει (όπως ένα αδειοδοτικό) ή σε κάτι που είναι (όπως δακτυλικό αποτύπωμα). Κατά παράδοση, τα συστήματα πιστοποίησης αυθεντικότητας εξαρτώνται από κωδικούς πρόσβασης.

Σημαντική ασφάλεια πετυχαίνεται συσχετίζοντας κάτι που γνωρίζει κάποιος με κάτι που κατέχει, μια τεχνική που ονομάζεται διπαραγοντική πιστοποίηση αυθεντικότητας. Τα αδειοδοτικά θεωρούνται ως κάτι που έχει κάποιος και έχουν ποικίλα μεγέθη, σχήματα και μορφές. Τα παθητικά αδειοδοτικά είναι συσκευές αποθήκευσης που περιλαμβάνουν ένα απόρρητο κωδικό. Με τα παθητικά αδειοδοτικά, ο χρήστης βάζει το αδειοδοτικό μέσα από ένα σύστημα ανάγνωσης, που είναι ενωμένο σε ένα σταθμό εργασίας ή σε ένα προσωπικό υπολογιστή και μετά βάζει τον κωδικό πρόσβασης του, για να έχει τη δυνατότητα να προσπελάσει το δίκτυο.
Τα ενεργητικά αδειοδοτικά είναι μερικές αυτόνομες ηλεκτρονικές συσκευές, που δημιουργούν κωδικούς πρόσβασης μιας χρήσης. Στην συγκεκριμένη περίπτωση, ο χρήστης βάζει ένα PIN στο αδειοδοτικό, το αδειοδοτικό δημιουργεί έναν κωδικό

[51] **Πηγή** : ΕΕΤΤ – Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

πρόσβασης που είναι έγκυρος για μια μόνο είσοδο και έπειτα ο χρήστης εισχωρεί στο σύστημα, χρησιμοποιώντας τον κωδικό πρόσβασης μιας φοράς.

8.4 Το Δημόσιο Κλειδί[52]

Η αιχμή της τεχνολογίας για πιστοποίηση της αυθεντικότητας είναι η υποδομή δημόσιου κλειδιού (PKI - Public key infrastructure). Σε αυτό το ενδεχόμενο, αυτό το οποίο «έχει» κάποιο άτομο είναι ένα πιστοποιητικό και όχι ένα αδειοδοτικό. Η PKI έχει θεωρηθεί ως ο θεμέλιος λίθος για ασφαλή συστήματα ηλεκτρονικών πληρωμών.

Ασχολείται με τις πρακτικές, τα τεχνικά συστατικά και την υποδομή που χρειάζονται για να έχει την δυνατότητα να χρησιμοποιήσει κρυπτογράφηση ψηφιακών πιστοποιητικών, δημόσιου κλειδιού και ψηφιακών υπογραφών με μία εφαρμογή δικτύου. Επιπλέον η PKI είναι το θεμέλιο πολλών εφαρμογών δικτύου, που περιέχουν εφαρμογές SCM, ΕΙΔ, ασφαλούς ηλεκτρονικού ταχυδρομείου και ενδοδικτύου.

8.5 Ψηφιακές Υπογραφές[53]

Οι ψηφιακές υπογραφές στηρίζονται στα δημόσια κλειδιά. Έχουν τη δυνατότητα να χρησιμοποιούνται για την πιστοποίηση αυθεντικότητας της ταυτότητας του αποστολέα ενός εγγράφου ή ενός μηνύματος. Επιπλέον, έχουν τη δυνατότητα να χρησιμοποιούνται για να επαληθεύσουν ότι τα αρχικά περιεχόμενα ενός εγγράφου ή ενός ηλεκτρονικού μηνύματος δεν έχουν τροποποιηθεί .

Για παράδειγμα αν κάποιος επιθυμεί να αποστείλει το σχέδιο μιας οικονομικής σύμβασης, μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου και θέλει να επιβεβαιώσει στην εταιρεία που πρόκειται να συνεργαστεί ότι τα περιεχόμενα του σχεδίου δεν έχουν διαφοροποιηθεί κατά τη διάρκεια του «ταξιδιού τους» και ότι αυτός είναι ο πραγματικός αποστολέας πρέπει να ακολουθήσει τα παρακάτω βήματα:

i. Ο αποστολέας φτιάχνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που περιλαμβάνει τη σύμβαση.
ii. Με τη χρήση ενός ειδικού λογισμικού, στο μήνυμα, που παράγει μια ειδική σύνοψη του μηνύματος, μετατρεμμένη σε μία αλληλουχία χαρακτήρων, που ονομάζεται σύνοψη μηνύματος.

[52] **Πηγή** : ΕΕΤΤ – Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html
[53] **Πηγή :** Βικιπαίδεια: http://el.wikipedia.org/wiki/Ψηφιακή_Υπογραφή

iii. Ο αποστολέας κάνει χρήση του ιδιωτικού κλειδί του για να κρυπτογραφήσει τον κατατεμαχισμό. Αυτή είναι η ψηφιακή υπογραφή του την οποία κανείς άλλος δεν έχει δυνατότητα να βρει, διότι αυτή εξαρτάται στο ιδιωτικό του κλειδί.

iv. Ο αποστολέας κρυπτογραφεί το αρχικό μήνυμα και την ψηφιακή του υπογραφή, με τη χρήση το δημόσιο κλειδί του αποδέκτη. Αυτός είναι ο ψηφιακός του φάκελος.

v. Ο αποστολέας στέλνει με μήνυμα ηλεκτρονικού ταχυδρομείου τον ψηφιακό φάκελο στον αποδέκτη.

vi. Όταν τον λάβει, ο δέκτης χρησιμοποιεί το ιδιωτικό κλειδί του για να αποκρυπτογραφήσει τα περιεχόμενα του ψηφιακού φακέλου. Αυτό δημιουργεί ένα αντίγραφο του e-mail και της ψηφιακής υπογραφής του αποστολέα.

vii. Ο παραλήπτης κάνει χρήση του δημόσιου κλειδί του αποστολέα για νααποκρυπτογραφήσει την ψηφιακή υπογραφή, δημιουργώντας ένα αντίγραφο της πρώτης σύνοψης του μηνύματος.

viii. Χρησιμοποιώντας την ίδια συνάρτηση κατατεμαχισμού που χρησιμοποιήθηκε στο δεύτερο βήμα, ο παραλήπτης παράγει μια σύνοψη μηνύματος, από το αποκρυπτογραφημένο μήνυμα.

ix. Ο παραλήπτης κάνει σύγκριση σε αυτήν την σύνοψη με την πρώτη.

x. Αν οι δύο συνόψεις ταιριάζουν, ο δέκτης βγάζει συμπέρασμα ότι το μήνυμα είναι γνήσιο.

8.6 Ασφάλεια και WAP[54]

Όλο και περισσότεροι συνδρομητές κινητής τηλεφωνίας κάνουν χρήση των υπηρεσιών του πρωτοκόλλου WAP για αυτό το λόγο η ανάγκη για μία ασφαλή ασύρματη επικοινωνία διαρκώς μεγαλώνει. Παρακάτω αναλύεται το μοντέλο ασφάλειας του WAP (Wireless Application Protocol) και ο μηχανισμός του Ασύρματου Ασφαλούς Επιπέδου Μεταφοράς (Wireless Transport Layer Security, WTLS), που προσφέρει ένα ασφαλές περιβάλλον για τις ασύρματες συναλλαγές δια μέσου του internet.

Το μοντέλο ασφάλειας του WAP χωρίζεται τρία τμήματα. Ουσιαστικά η πύλη WAP είναι η ένωση μεταξύ των πρωτοκόλλων SSL και WTLS. Το SSL είχε δημιουργηθεί για ενσύρματα περιβάλλοντα με υψηλές ικανότητες υπολογιστικής ισχύς και εύρους ζώνης. Αντιθέτως, οι ασύρματες επικοινωνίες δούλευαν με αργούς ρυθμούς και οι συσκευές κινητής τηλεφωνίας είχαν πολύ λίγες δυνατότητες επεξεργασίας κρυπτογραφημένων δεδομένων.

Για την αντιμετώπιση αυτών των δυσκολιών, το πρωτόκολλο WTLS είναι έτσι κατασκευασμένο με τέτοιο τρόπο ώστε να επεξεργάζεται ταχυτέρα τους αλγορίθμους κρυπτογράφησης και να δίνει τη δυνατότητα μεγαλύτερου βαθμού συμπίεσης

[54] **Πηγή:** Βικιπαίδεια**:** http://en.wikipedia.org/wiki/WAP

δεδομένων. Το μοντέλο ασφαλείας του WAP που χρησιμοποιείται συνήθως προϋποθέτει ισχυρή σχέση μεταξύ στις εταιρίες κινητής τηλεφωνίας και τους τελικούς Web servers. Το WAP Forum έχοντας αποδεχτεί το δεδομένο ότι η αγορά για ασύρματες δικτυακές εφαρμογές διαρκώς μεγαλώνει, έχει αρχίσει να μελετά πιο ευέλικτες λύσεις, όπως είναι η χρήση των Ασύρματων Μονάδων Ταυτότητας (Wireless Identity Modules, WIMs).

Τα WIMs θα προφυλάσσουν τις συναλλαγές μέσω internet με την κρυπτογράφηση και τις ψηφιακές υπογραφές. Οι προδιαγραφές των WIMs εμφανίστηκαν αρχικά στην έκδοση 1.2 του πρωτοκόλλου WAP με στόχο την απομάκρυνση των λειτουργιών ασφαλείας από την ίδια την συσκευή κινητής τηλεφωνίας σε κάποιον άλλο μηχανισμό, όπως είναι οι έξυπνες κάρτες.

9ο Κεφάλαιο
Κρυπτογραφία[55]

9.1 Κρυπτογραφία[56]

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet.

Από την στιγμή, που άρχισαν να μεταφέρονται πληροφορίες, ξεκίνησε η ιδέα της κρυπτογράφησης ή του κώδικα για να ασφαλιστούν τα μηνύματα. Αν το μήνυμα είναι γραμμένο σε κώδικα, είναι ασφαλές ακόμα και αν υποκλαπεί. Με άλλα λόγια, η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων.

Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών, χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

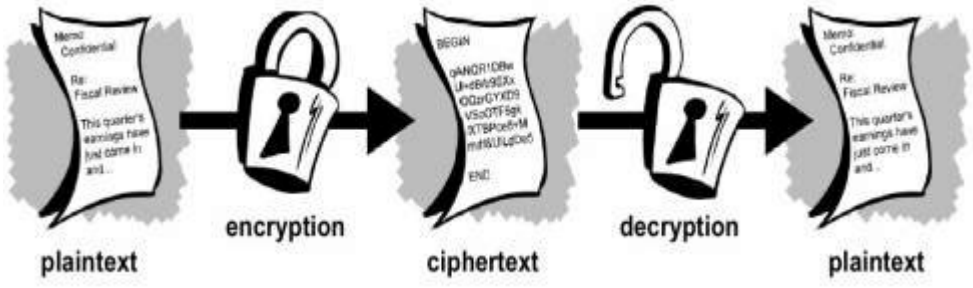
Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο

[55] Το κεφάλαιο αυτό βασίστηκε στις παρακάτω πηγές :
1. Βικιπαίδεια : http://el.wikipedia.org/wiki/Κρυπτογραφία,
2. Βιβλίο : Κρυπτογραφία και ασφάλεια δικτύων - William Stallings (Εκ. ΙΩΝ-2011)
3. Εργαστήριο Πληροφορικής (ΑΤΕΙ Λαμίας – Καθ. Λιμνιώτης Κών/νος)
4. http://www.efarmoges.gr/store/gr/articles/kryptografisi_8.shtml

[56] **Πηγή :** Βικιπαίδεια : http://el.wikipedia.org/wiki/Κρυπτογραφία,

απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Όλα τα συστήματα κρυπτογράφησης όσο περίπλοκα και αν είναι βασίζονται σε τέσσερα βασικά μέρη, όπως απεικονίζονται στο παρακάτω διάγραμμα:



Εικόνα 9.1 **Κρυπτογράφηση** - ***Αποκρυπτογράφηση***

1. Απλό κείμενο (plaintext). Αποτελεί το αρχικό μήνυμα που δημιουργεί ο χρήστης, το οποίο μπορεί να είναι όχι μόνο κείμενο, αλλά και video, ήχος ή οποιοσδήποτε άλλος τύπος αρχείου.

2. Κρυπτογραφημένο κείμενο (chipertext). Είναι το αρχικό απλό κείμενο το οποίο όμως είναι τροποποιημένο με τέτοιο τρόπο ώστε να μην μπορεί να διαβαστεί από τρίτους.

3. Κρυπτογραφικός αλγόριθμος (cryptographic algorithm). Είναι μία μαθηματική λειτουργία, που μετατρέπει το απλό κείμενο σε κρυπτογραφημένο και αντίστροφα.

4. Κλειδί (key). Ένα μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει και να αποκρυπτογραφήσει το μήνυμα. Κάθε κλειδί μετασχηματίζει το ίδιο απλό κείμενο σε διαφορετικό κρυπτογραφημένο κείμενο και μόνο οι κάτοχοι των κλειδιών μπορούν να διαβάσουν το κρυπτογραφημένο κείμενο.

Το βασικό χαρακτηριστικό των κρυπτογραφικών συστημάτων είναι ότι η ασφάλεια του συστήματος βασίζεται ολοκληρωτικά στη μυστικότητα του κλειδιού αποκρυπτογράφησης, καθώς εάν κάποιος λάβει το κρυπτογραφημένο κείμενο δεν μπορεί να το μετατρέψει στην αρχική του μορφή, εφόσον δεν είναι ο κάτοχος του κλειδιού αποκρυπτογράφησης.

Ο βαθμός απόκρυψης του μηνύματος προσδιορίζεται από το μήκος του κλειδιού. Ένα κλειδί μήκους 40 bits έχει περισσότερους από 1012 δυνατούς κώδικες, Το μήκος αυτό δεν είναι αρκετά ισχυρό, για να παρέχει υψηλή ασφάλεια μεταφοράς δεδομένων.

Το σύνηθες μήκος που χρησιμοποιείται κυρίως για κρυπτογράφηση δεδομένων είναι αυτό των 128 bits , που σημαίνει 1038 πιθανούς κώδικες, περισσότερους από τον

αριθμό των μορίων του νερού σε όλους τους ωκεανούς του πλανήτη. Είναι λοιπόν αντιληπτό πόσο δύσκολο είναι να βρεθεί ένας τέτοιος κώδικας, σχεδόν απίθανο.

9.2 Μέθοδοι Κρυπτογράφησης

Οι μέθοδοι κρυπτογράφησης είναι οι εξής τρεις :

- Συμμετρική Κρυπτογράφηση.
- Ασύμμετρη Κρυπτογράφηση.
- Κρυπτογράφηση Δημοσίου Κλειδιού (PKI).

9.2.1 Συμμετρική Κρυπτογράφηση[57]

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, πιο συγκεκριμένα ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα.

Έτσι κατά συνέπεια, το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού, για αυτό το λόγο απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται, αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

Εικόνα 9.2 . **Συμμετρική κρυπτογράφηση**

[57] **Πηγή:** Βικιπαίδεια : http://el.wikipedia.org/wiki/Κρυπτογραφία

Μερικοί αλγόριθμοι που ανήκουν στην κατηγορία της Συμμετρικής Κρυπτογράφησης είναι:

Data Encryption Standard (DES). Το DES αναπτύχθηκε κατά την δεκαετία του 70 και σήμερα χρησιμοποιείται ευρέως. Το μήκος του κλειδιού που χρησιμοποιεί είναι 56 bits και θεωρείται μικρό για την επίτευξη υψηλής προστασίας ανταλλασσόμενων μηνυμάτων από επιθέσεις. Το DES κρυπτογραφεί τα δεδομένα σε διακριτά μπλοκ των 64 bits και συχνά χρησιμοποιείται σε συνδυασμό με μία άλλη μέθοδο που ονομάζεται cipherblock chaining (CBC). Ο συνδυασμός αυτών των δύο μεθόδων έχει σαν αποτέλεσμα η κρυπτογράφηση καθενός μπλοκ να εξαρτάται από το περιεχόμενο του προηγούμενου αυξάνοντας με αυτόν τον τρόπο την ασφάλεια των κρυπτογραφημένων μηνυμάτων.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη αυτός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology). Δημιουργήθηκε για να προστατέψει αυτός δικτυακές υπηρεσίες που παρέχονταν από το Project Athena και βασίζεται στο μοντέλο διανομής κλειδιών (key distribution model) των Needham και Schoeder.

Triple DES, DESX, GDES, RDES. Οι αλγόριθμοι αυτοί, αποτελούν παραλλαγές του DES και μειώνουν τον κίνδυνο αποκρυπτογράφησης από εισβολείς, χρησιμοποιώντας μεγαλύτερου μήκους κλειδιά. Συγκεκριμένα, το Triple DES κρυπτογραφεί τα μηνύματα με τρία μυστικά κλειδιά στη σειρά, φθάνοντας το μήκος του κλειδιού στα 112 bits.

RC2, RC4, RC5. Οι αλγόριθμοι αυτοί αναπτύχθηκαν από την RSA Security Inc. Και χρησιμοποιούν κλειδιά με διάφορα μήκη που φθάνουν έως τα 2048 bits. Παρουσιάζουν ιδιαίτερο ενδιαφέρον, καθώς χρησιμοποιούνται για την κρυπτογράφηση / αποκρυπτογράφηση μηνυμάτων που μεταδίδονται στο διαδίκτυο.

International Data Encryption algorithm (IDEA). Ο αλγόριθμος αυτός είναι ιδιαίτερα διαδεδομένος στην Ευρώπη και χρησιμοποιεί μήκος κλειδιού 128 bits. Ο IDEA αποτελεί την καρδιά πολλών λογισμικών κρυπτογράφησης ηλεκτρονικών μηνυμάτων.

Οι συμμετρικοί αλγόριθμοι παρουσιάζουν αρκετά προβλήματα, κατά την επικοινωνία πελάτη και διακομιστή μέσω του διαδικτύου, επειδή απαιτείται η ανταλλαγή κλειδιών πριν την δρομολόγηση αυτής της επικοινωνίας. Αυτή, η ανταλλαγή κρυπτογραφημένων μηνυμάτων μεταξύ όλων των πελατών και του διακομιστή, προϋποθέτει την χρήση ίδιου κλειδιού, με συνέπεια να μην παραμένει για αρκετό καιρό μυστικό, λόγω αυτής της αυξημένης διάδοσής του και κρίνεται απαραίτητη η πάρα πολύ συχνή αλλαγή του.

9.2.2 Ασύμμετρη Κρυπτογράφηση[58]

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Εικόνα 9.3 . ***Ασύμμετρη κρυπτογράφηση***

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά. Κάθε χρήστης, λοιπόν έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική και δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα.

Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

[58] **Πηγή**: Βικιπαίδεια : http://el.wikipedia.org/wiki/Κρυπτογραφία

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

Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ότι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής. Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνο που γνωρίζει την ιδιωτική κλείδα.

Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα.

Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

10ο Κεφάλαιο
Πρωτόκολλα και Πιστοποιητικά Ασφάλειας Δικτύου

10.1 Ασφάλεια Internet Πρωτοκόλλου (IPSec)[59]

Η ασφάλεια του Internet πρωτοκόλλου ή IPSec είναι η βάση για την ασφάλεια των ηλεκτρονικών συναλλαγών, γιατί ο χειρισμός τους γίνεται σε επίπεδο πρωτοκόλλου. Το πρωτόκολλο αυτό διαβεβαιώνει ότι είναι ασφαλείς οι συναλλαγές από και προς τον Web διακομιστή μας.

Για παράδειγμα, αν κάποιος συνδεθεί στη Web τοποθεσία μας και προσπαθήσει να στείλει μία παραγγελία, το IPSec είναι η ασφάλεια που εφαρμόζεται σε αυτήν την συναλλαγή, βεβαιώνει λοιπόν ότι φθάνει αμετάβλητη, αδιάβαστη και προερχόμενη από το άτομο που ισχυρίζεται ότι την στέλνει.

Με άλλα λόγια, το IPSec λειτουργεί κλείνοντας το πακέτο των πληροφοριών το οποίο αποστέλλεται, σε ένα άλλο πακέτο, πριν σταλεί μέσω Διαδικτύου. Στον παραλήπτη, το πακέτο αποκωδικοποιείται και διαβάζεται από μία συσκευή που έχει καθορίσει ο αποστολέας.

Το IPSec, αποτελείται από τρεις διαφορετικούς μηχανισμούς ασφάλειας :

- την επικεφαλίδα ελέγχου ταυτότητας,
- το ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας και
- το κλειδί διαχείρισης

Επικεφαλίδα ελέγχου ταυτότητας (authentication header) : Το AH επικεντρώνεται στον έλεγχο ταυτότητας των ατόμων που στέλνουν τις πληροφορίες και βεβαιώνεται ότι δεν έχουν αλλοιωθεί στην διαδρομή. Το AH μπαίνει μετά την IP επικεφαλίδα, αλλά πριν από τις άλλες πληροφορίες που πρόκειται να πιστοποιηθούν.

Ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας (encapsulating security payload-ESP) : Το ESP πιστοποιεί επίσης την ταυτότητα του χρήστη, αλλά υποστηρίζει και την κρυπτογράφηση των δεδομένων. Υπάρχουν διαφορετικά επίπεδα ESP που μπορούν να προσαρμοστούν για κάθε κατάσταση. Στη χρήση του AH και του ESP, ο αποστολέας και ο παραλήπτης θα πρέπει να συμφωνήσουν σε ένα κλειδί κρυπτογράφησης, ένα κλειδί αποκρυπτογράφησης, μία μέθοδο ελέγχου ταυτότητας. Γενικά το ESP εφαρμόζεται πρώτα στο επίπεδο μεταφοράς για να προετοιμαστεί η αποστολή ενός μηνύματος. Μετά προστίθεται το AH στην κορυφή, ώστε το πρώτο πράγμα που θα διαβαστεί από τον παραλήπτη να είναι αυτό.

---

[59] **Πηγή** : 1. Βιβλίο : Κρυπτογραφία και ασφάλεια δικτύων - William Stallings (Εκ. ΙΩΝ-2011)
2. ΑΤΕΙ Λαμίας – Σχολή Τεχνολογικών Εφαρμογών – Τμήμα Πληροφορικής και Τεχνολογίας Υπολογιστών – Μάθημα Σχεδίαση εικονικών Δικτύων -Καθ. Λιμνιώτης Κών/νος

Πρωτόκολλο Διαχείρισης Κλειδιού Internet (Internet Key Management Protocol) : Το πρωτόκολλο αυτό αποτελεί τον πυρήνα του IPSec. Ο μηχανισμός αυτός επιτρέπει να ανταλλάσσουν δύο μέρη τα δημόσια κλειδιά τους και να διαμορφώνουν μία ασφαλή σύνοδο. Αφού γίνει η ανταλλαγή των δημόσιων κλειδιών, ορίζεται ένα προσδιοριστικό συνόδου. Το προσδιοριστικό αυτό, αποτελεί τον ορισμό της Διαδικτυακής σχέσης που μοιράζονται δύο μέρη. Για παράδειγμα, ένα προσδιοριστικό συνόδου πιστοποιεί το άτομο με το οποίο συνδιαλεγόμαστε και μετά επιτρέπει την εκτέλεση ορισμένων εντολών που μπορεί να έχουμε διαμορφώσει γι' αυτήν την σχέση.

Υπάρχουν δύο διαφορετικοί τρόποι που μπορούν να ανταλλαγούν τα κλειδιά μεταξύ δύο διαφορετικών μερών. Ο πρώτος είναι η μη αυτόματη ανταλλαγή. Αυτή η μέθοδος απαιτεί να δίνουν οι χρήστες μη αυτόματα το κλειδί που θέλουν να χρησιμοποιήσουν για να επικοινωνούν, μαζί με τα κλειδιά όλων των άλλων που σκοπεύουν να επικοινωνήσουν μαζί τους. Αν και αυτή η μέθοδος είναι πολύ χρονοβόρα, είναι η πιο ευρέως χρησιμοποιούμενη.

Η άλλη μέθοδος, στην οποία ανταλλάσσονται τα κλειδιά, αναφέρεται ως ISAKMP. Αυτό το εργαλείο διαχείρισης κλειδιών δεν ορίζει κλειδιά συνόδου, αλλά όταν χρησιμοποιείται με διαφορετικά κλειδιά πιστοποίησης, μπορεί να χρησιμοποιηθεί για να ορισθεί μία σύνδεση και να ανταλλαγούν κλειδιά, χωρίς να πρέπει να προσθέσουν οι χρήστες κάθε ένα ξεχωριστά. Αν και το ISAKMP είναι πιο περίπλοκο, εξοικονομεί πολύ χρόνο και επίσης είναι ασφαλές.

10.2 Γιατί είναι Απαραίτητο το IPSec;

Το IPSec είναι όπως και το PKI στο τρόπο που ορίζει την εμπιστοσύνη μεταξύ δύο διαφορετικών πλευρών. Σαν καθολική βάση, αυτό προσφέρει τις σημαντικές λειτουργίες ασφάλειας για διαδικτυακές συναλλαγές .

Εμπιστοσύνη : Βεβαιώνει ότι όλες οι συναλλαγές είναι εμπιστευτικές, με τον ίδιο τρόπο που κάνει και το PKI. Η λειτουργία ESP κρυπτογραφεί τα πακέτα πριν σταλούν μέσω διαδικτύου. Αφού κρυπτογραφηθεί η συναλλαγή, μπορεί να αποκρυπτογραφηθεί από τον Web διακομιστή. Έτσι, ακόμα και αν οι πληροφορίες υποκλαπούν, δεν θα μπορέσουν να αποκρυπτογραφηθούν.

Ακεραιότητα : Ο παραλήπτης, σε αυτή τη περίπτωση ο Web διακομιστής, μπορεί επίσης να βεβαιωθεί ότι τα δεδομένα δεν έχουν αλλαχθεί ή υποκλαπεί με κάποιον τρόπο. Επειδή η συναλλαγή κρυπτογραφείται πριν σταλεί, θα αποκρυπτογραφηθεί αν το μήνυμα δεν αλλοιωθεί. Έτσι, αν υπάρχει κάποια αλλαγή στο μήνυμα, δεν θα μεταφραστεί σε αναγνωρίσιμο υλικό όταν φθάσει στον Web διακομιστή.
Το IPSec έχει επίσης μία λειτουργία που παρέχει επίσης αυτή την λειτουργία, προσκολλώντας τον εαυτό του στα κρυπτογραφημένα δεδομένα. Αν υπάρχει πρόβλημα με την επικεφαλίδα πιστοποίησης, σημαίνει ότι τα δεδομένα θα μπορούσαν να έχουν αλλαχθεί.

Έλεγχος ταυτότητας : Ο παραλήπτης μπορεί επίσης να πιστοποιήσει την πηγή από την οποία προέρχονται τα πακέτα, εξαιτίας των πληροφοριών που παρέχονται από την επικεφαλίδα. Ο έλεγχος αυτός αποτελεί έναν από τους πιο σημαντικούς ελέγχους. Το γεγονός αυτό είναι προφανές, αν αναλογιστούμε ότι δεν έχει σημασία πόσο αυστηροί είναι οι έλεγχοι που εμποδίζουν την υποκλοπή μηνυμάτων, όταν δεν γνωρίζουμε την ταυτότητα του αποστολέα.

10.3 Πλεονεκτήματα του IPSec - Διαφορές από το PKI

Τα προφανή πλεονεκτήματα του, είναι ότι οι ηλεκτρονικές συναλλαγές κερδίζουν σε εμπιστοσύνη, ακεραιότητα και υπάρχει έλεγχος ταυτότητας χρηστών. Ωστόσο, η απλότητα είναι το μεγαλύτερο πλεονέκτημα που κερδίζει την κάθε εταιρία επιλέγοντας το από άλλα μέτρα ασφάλειας.

Επειδή αυτό είναι ολοκληρωμένο σε επίπεδο υποδομής, δεν υπάρχουν αλλαγές στις εφαρμογές ή στους προσωπικούς υπολόγισες που λειτουργούν σε ιδιωτικό δίκτυο. Η διαμόρφωση αυτή εξοικονομεί πολύ χρόνο και χρήματα. Επειδή ακόμα αυτό δεν χρησιμοποιείται σε ατομικό επίπεδο, δεν απαιτεί εκπαίδευση όλων των χρηστών, αφού δεν το αντιμετωπίζουν καθόλου. Ακόμη παρέχει την δυνατότητα σε άτομα που δεν βρίσκονται στα γραφεία τους, να χρησιμοποιούν σημαντικές, αλλά εμπιστευτικές πληροφορίες.

Δημιουργεί λοιπόν μία θαυμάσια λύση για απομακρυσμένους χρήστες, που μπορούν να δημιουργήσουν ένα τούνελ προς το ιδιωτικό δίκτυο χρησιμοποιώντας το

πρωτόκολλο αυτό μέσω του διαδικτύου. Αυτό μειώνει το κόστος των ιδιωτικών γραμμών και την ανησυχία σχετικά με τα μέτρα ασφάλειας για τους απομακρυσμένους χρήστες

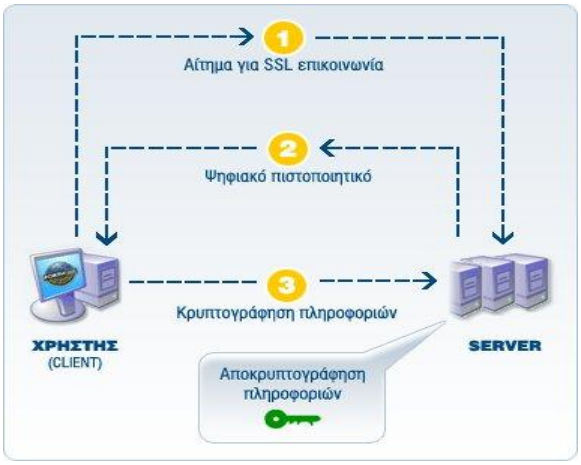
Αν και το IPSec ακούγεται πολύ παρόμοιο με το PKI, υπάρχει μία πολύ βασική διαφορά. Τα άλλα μέτρα ασφάλειας συναλλαγών που έχουμε δει λειτουργούν σε επίπεδο εφαρμογής, ενώ το IPSec λειτουργεί σε επίπεδο πρωτοκόλλου. Αυτό το κάνει ευκολότερο στη χρήση, μιας και οι εφαρμογές των δύο πλευρών που επικοινωνούν δεν χρειάζεται να είναι συμβατές.

Επιπλέον αυτό επιτρέπει στους χρήστες να πιστοποιούν και να επικοινωνούν μέσω μίας σύνδεσης, αντί να επικοινωνούν με μηνύματα. Το PKI είναι θαυμάσιο μέτρο ασφάλειας για μηνύματα ηλεκτρονικού ταχυδρομείου, ενώ το IPSec είναι καταλληλότερο για χρήση στο διαδίκτυο.

10.4 Secure Sockets Layer (SSL)[60]

Το SSL είναι ένα Internet socket-layer communication interface που επιτρέπει την ασφαλή επικοινωνία αγοραστή και πωλητή. Τα Πιστοποιητικά Ασφαλείας δικτυακών τόπων χρησιμοποιούν τη τεχνολογία SSL (Secure Socket Layer). Το SSL, είναι σήμερα το παγκόσμιο standard στο Διαδίκτυο και προσφέρει στον ηλεκτρονικό επισκέπτη του web site, κρυπτογραφημένη SSL επικοινωνία.

Είναι εύκολο να αναγνωρίσετε πότε πρόκειται να πραγματοποιήσετε μία κρυπτογραφημένη SSL επικοινωνία, από το μικρό χρυσό λουκέτο που θα εμφανιστεί στο κάτω δεξί μερος του browser σας και αυτόματα θα μεταφερθείτε σε ηλεκτρονική διεύθυνση της μορφής https:// .Η τεχνολογία αυτή έχει αναπτυχθεί από την Netscape Communications Corporation και λειτουργεί ως εξής:



Εικόνα 10.1. Secure Sockets Layer (SSL)

[60] **Πηγή**: ΑΤΕΙ Λαμίας – Σχολή Τεχνολογικών Εφαρμογών – Τμήμα Πληροφορικής και Τεχνολογίας Υπολογιστών – Μάθημα Σχεδίαση εικονικών Δικτύων -Καθ. Λιμνιώτης Κών/νος

I. Με το SSL, ο υπολογιστής του χρήστη, μέσω του οποίου πρόκειται να πραγματοποιηθεί κρυπτογραφημένη SSL επικοινωνία, στέλνει το αίτημα του στον διακομιστή, ο οποίος κάνει χρήση ψηφιακού πιστοποιητικού ασφαλείας και φιλοξενεί τον δικτυακό τόπο, με το οποίο πρόκειται να πραγματοποιηθεί η ηλεκτρονική συναλλαγή.

II. Ο διακομιστής στέλνει:

a. το πιστοποιητικό ασφαλείας στον υπολογιστή του χρήστη και του επιβεβαιώνει πως έχει επισκεφτεί την σωστή σελίδα και

b. το δημόσιο κλειδί του (κωδικός).

III. Ο υπολογιστής του χρήστη, χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει απόρρητες πληροφορίες (για παράδειγμα τον αριθμό της πιστωτικής του κάρτας). Στη συνέχεια, οι πληροφορίες αυτές αποστέλλονται στον διακομιστή που χρησιμοποιεί το ιδιωτικό του κλειδί για να τις αποκρυπτογραφήσει.

Με το SSL, ο αγοραστής υποβάλει μια "αίτηση" αγοράς μέσω του διαδικτύου. Ο πωλητής, του αποστέλλει τότε ένα δημόσιο κλειδί, που ο υπολογιστής του αγοραστή το χρησιμοποιεί για να κρυπτογραφήσει απόρρητες πληροφορίες (συνήθως τον αριθμό της πιστωτικής του κάρτας).

Στη συνέχεια οι πληροφορίες αυτές αποστέλλονται στον πωλητή που χρησιμοποιεί το ιδιωτικό του κλειδί για να τις αποκρυπτογραφήσει. Η όλη διαδικασία γίνεται αυτόματα χωρίς μεσολάβηση του αγοραστή και έτσι είναι πιο γρήγορη και ταυτόχρονα πιο εύκολη αφού ο αγοραστής δεν χρειάζεται να έχει ειδικές γνώσεις.

Μια άλλη εφαρμογή του SSL είναι ο Secure Courier που έχει και αυτός αναπτυχθεί από την Netscape Communications Corp. Ο Secure Courier χρησιμοποιείται για να μεταφέρονται "ευαίσθητες" πληροφορίες μεταξύ επιχειρήσεων ή άλλων οργανισμών και προβλέπεται να χρησιμοποιηθεί για την μεταφορά πληροφοριών μεταξύ των επιχειρήσεων και των Τραπεζών που εξοφλούν τις πιστωτικές κάρτες.

Η συλλογιστική είναι πως χάρη στο SC, (που δημιουργήθηκε με βάση τις προδιαγραφές που έχουν ορίσει οι εταιρείες Mastercard και Visa για τις ηλεκτρονικές συναλλαγές) μια εταιρεία δεν θα μπορεί να έχει πρόσβαση στα οικονομικά στοιχεία του πελάτη της (αριθμός της πιστωτικής κάρτας του, ημερομηνία λήξης, όνομα κτλ.). Έτσι δεν θα έχει και την ευκαιρία να τα χρησιμοποιήσει για παράνομους σκοπούς. Οι πληροφορίες αυτές θα μεταφέρονται απ' ευθείας από τον πελάτη στην Τράπεζα χωρίς μεσολάβηση κανενός τρίτου.

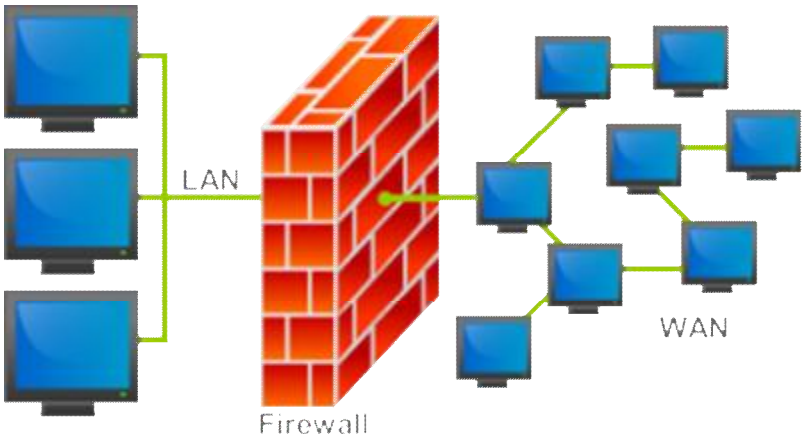
Χαρακτηριστική είναι η περίπτωση της PC Gifts and Flowers που δραστηριοποιείται τόσο στην Prodigy όσο και στο World -Wide Web. Το 1994 οι πωλήσεις της στην Prodigy ήταν 4 εκατομμύρια δολάρια (έγιναν 150.000 παραγγελίες). Το ίδιο χρονικό διάστημα από το World Wide Web site της εταιρείας έγιναν κατά μέσω όρο μόνο 200 πωλήσεις το μήνα παρά τον ασύγκριτα μεγαλύτερο πληθυσμό του δικτύου (Internet World, Ιούνιος, 1995).

Ο λόγος για την διαφορά αυτή πιστεύεται πως είναι η μεγαλύτερη εμπιστοσύνη που έχουν οι συνδρομητές της Prodigy για την ασφάλεια των συναλλαγών μέσω αυτής. Αυτός είναι και ο λόγος που προβλέπεται πως η υποστήριξη που παρέχουν στο Secure Sockets Layer (SSL) δύο εταιρείες με το μέγεθος και την προϊστορία των Mastercard και Visa, θα αυξήσει την εμπιστοσύνη των χρηστών του Internet στις συναλλαγές μέσω αυτού και θα αυξήσει δραματικά τις συναλλαγές.

10.5 Firewalls[61]

Το firewall, που μπορεί να αποδοθεί στα ελληνικά με τον όρο πύρινο τείχος προστασίας ή και ηλεκτρονική πύλη ασφαλείας, είναι ένα πρόγραμμα-τείχος που σε γενικές γραμμές έχει τη δυνατότητα να εμποδίσει τους ιούς (viruses) και τα προγράμματα τύπου spyware να εγκατασταθούν στον υπολογιστή μας. Αποτελεί μια πολύ καλή λύση προστασίας που μπορεί να χρησιμοποιηθεί τόσο από μεγάλες εταιρείες που διαθέτουν εκτεταμένο δίκτυο υπολογιστών όσο και από απλούς χρήστες που έχουν σύνδεση στο Internet τύπου dialup ή ADSL.

Ένα firewall μπορεί να ελέγξει την κίνηση (traffic) των πακέτων του Internet από και προς τον υπολογιστή μας. Μπορεί να εντοπίσει τις πιθανές επιθέσεις στον υπολογιστή μας, να αναλύσει την κίνηση και τα αρχεία που ανταλλάσσονται, να διακρίνει τις ύποπτες δραστηριότητες και να εμποδίσει την ολοκλήρωσή τους.



Εικόνα 10.2. **Τυπική Διάταξη** Firewall

Ένα firewall προστατεύει ένα δίκτυο από κάποιο άλλο δίκτυο, υποβάλλοντας τα διερχόμενα πακέτα πληροφοριών (εισερχόμενα και εξερχόμενα) σε μια σειρά από ελέγχους και λαμβάνει την απόφαση να τα αφήσει να διέλθουν ή να τα εμποδίσει, ανάλογα με το αν περνούν κάποια τεστ ή όχι. Στην ουσία πρόκειται για έναν ελεγκτή κυκλοφορίας δεδομένων στο Internet.

Μπορεί επίσης να ελέγξει τα προγράμματα που είναι εγκατεστημένα στον ίδιο τον υπολογιστή μας και συνδέονται στο Internet και τα οποία στέλνουν προς τα έξω

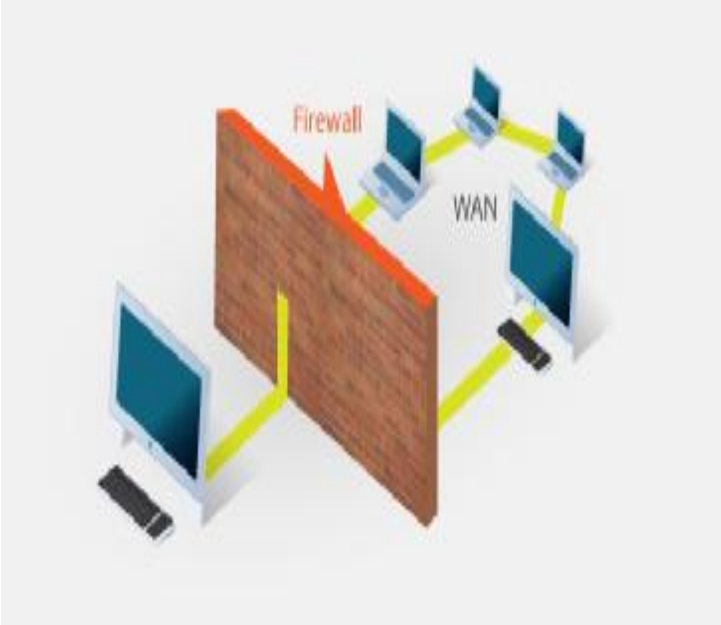
[61] **Πηγές :** 1. http://el.wikipedia.org/wiki/Firewall
2. Κέντρο ΠΛΗ.ΝΕ.Τ Φλώρινας http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html

ευαίσθητα προσωπικά μας δεδομένα ή αφήνουν ανοικτή μια κερκόπορτα (backdoor) για να μπορούν οι πιθανοί hackers να ελέγξουν τον υπολογιστή μας. Ένα firewall μπορεί να κρατήσει κλειστές αυτές τις πόρτες και να μας ενημερώνει για κάθε ύποπτη κίνηση.

Η κάθε σοβαρή εταιρεία και ο κάθε οργανισμός που έχει συναλλαγές μέσω Internet, οφείλει να εφαρμόσει μια πολιτική ασφαλείας (security policy) και την καρδιά αυτής της πολιτικής ασφαλείας αποτελεί το firewall. Θα πρέπει να έχουμε υπόψη μας ότι για να μπορεί να θεωρηθεί μια εφαρμογή firewall ως πετυχημένη, θα πρέπει να μπορεί να ελέγχει και τις εσωτερικές αιτήσεις εφαρμογών και υπηρεσιών που γίνονται για πρόσβαση στο Internet και όχι μόνο αυτές που γίνονται από έξω προς τα μέσα.

Ένα firewall μπορεί να είναι ένα μηχάνημα (συσκευή) ή και ένα πρόγραμμα (εφαρμογή) υπολογιστή, το οποίο χρησιμοποιείται για να επιβάλλει συγκεκριμένους κανόνες επικοινωνίας και ανταλλαγής πληροφοριών ανάμεσα σε δύο δίκτυα υπολογιστών. Το firewall παρεμβάλλεται ανάμεσα σε δύο διαφορετικά δίκτυα υπολογιστών και φιλτράρει τα διακινούμενα πακέτα πληροφοριών.

Το firewall κατά τη λειτουργία του (φιλτράρισμα) λαμβάνει υπόψη του ένα σύνολο από κανόνες (κριτήρια) που ορίζονται από τον χρήστη (διαχειριστή του firewall) και με βάση αυτούς τους κανόνες επιτρέπει ή απορρίπτει την κυκλοφορία (διακίνηση) των δεδομένων ανάμεσα στα δύο δίκτυα υπολογιστών.



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

Ενώ τα προγράμματα anti-virus, anti-trojan, anti-spam κοκ έχουν συγκεκριμένο αντικείμενο απασχόλησης και μας προστατεύουν από πολύ συγκεκριμένες απειλές, ένα firewall μπορεί να μας προστατεύσει από κάθε είδους απειλή όσον αφορά τη σχέση του υπολογιστή μας ή του δικτύου μας με τον έξω κόσμο.

Θα πρέπει να έχουμε υπόψη μας ότι αν αποφασίσουμε να εγκαταστήσουμε ένα firewall και δεν το ρυθμίσουμε ώστε να λειτουργεί σωστά και αποδοτικά, τότε το πιθανότερο είναι να κάνει ζημιά και να μειώσει την απόδοση και την ευελιξία του υπολογιστή μας. Μπορούμε να φανταστούμε ένα firewall, είτε πρόκειται για συσκευή είτε για πρόγραμμα, ως τον ενδιάμεσο ανάμεσα σε δύο δίκτυα υπολογιστών.

Ο χρήστης ενός οικιακού υπολογιστή ή ο administrator ενός δικτύου υπολογιστών θα πρέπει να ορίσει τους κανόνες με βάση τους οποίους θα γίνεται η κυκλοφορία των δεδομένων ανάμεσα στα δύο αυτά δίκτυα.

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

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

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

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

- Θα πρέπει να περνάνε μέσα από το firewall όλες οι συνδέσεις που γίνονται από το δίκτυο της εταιρείας προς το Internet.
- Θα πρέπει να ορισθεί ένας τεχνικός υπεύθυνος για την εγκατάσταση, τη ρύθμιση και τη διαχείριση του firewall, ο οποίος θα πρέπει να ακολουθεί και τακτική εκπαίδευση και ενημέρωση.
- Το εγκατεστημένο firewall θα πρέπει να παρακολουθείται και να ελέγχεται σε τακτά χρονικά διαστήματα.
- Θα πρέπει να απενεργοποιηθούν όλες οι εφαρμογές που δεν είναι απαραίτητες.
- Το firewall θα πρέπει να είναι διαθέσιμο 24 ώρες το 24ωρο.

Συμπερασματικά λοιπόν ένα Firewall μπορεί να κάνει τα εξής :

- Να εμποδίσει ιούς (viruses), σκουλήκια (worms), δούρειους ίππους (trojan horses) και άλλα προγράμματα τύπου spyware από το να εγκατασταθούν στον υπολογιστή μας και να κάνουν ζημιά.
- Να εμποδίσει την πρόσβαση στον υπολογιστή μας σε άγνωστους ή ανεπιθύμητους επισκέπτες.

- Να μας ειδοποιήσει ότι ο υπολογιστής μας δέχεται κάποια επίθεση.
- Να μας παρουσιάσει αναλυτικά στατιστικά στοιχεία σχετικά με την κίνηση από και προς τον υπολογιστή μας.
- Να εμποδίσει κάποιο πρόγραμμα τύπου dialer από το να πραγματοποιήσει υπερπόντιες τηλεφωνικές κλήσεις χωρίς τη θέλησή μας.

10.5.1 Η Αναγκαιότητα Χρήσης των Firewalls

Σε ένα περιβάλλον χωρίς firewalls η δικτυακή ασφάλεια αποτελεί αποκλειστικά μέριμνα του κάθε σταθμού ξεχωριστά και όλοι οι σταθμοί πρέπει να συνεργάζονται ώστε να παρέχουν ένα ομοιόμορφα υψηλό επίπεδο ασφάλειας. Όσο πιο μεγάλο είναι το δίκτυο, τόσο πιο δύσκολα επιτυγχάνεται η διατήρηση όλων των σταθμών σε υψηλά επίπεδα ασφάλειας.

Εξαιτίας της πολυπλοκότητας του δικτύου, τα λάθη και οι παραλήψεις στην ασφάλεια είναι συχνό φαινόμενο, με αποτέλεσμα να δημιουργούνται «οπές» ασφάλειας τις οποίες μπορούν να ανακαλύψουν και να εκμεταλλευτούν οι εισβολείς. Τα firewalls έχουν σχεδιαστεί έτσι ώστε να παρέχουν προηγμένες λειτουργίες παρακολούθησης και καταγραφής και η διαχείριση τους να είναι σχετικά εύκολή.

10.5.2 Δυνατότητες των Firewalls

Η λειτουργικότητα των firewalls εκτείνεται στα ακόλουθα:

- Το firewall αποτελεί το επίκεντρο των αποφάσεων που σχετίζονται με θέματα ασφάλειας: Το firewall απλοποιεί τη διαχείριση ασφάλειας, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο, το οποίο συνδέει τον οργανισμό με τον εξωτερικό κόσμο, και όχι στον κάθε υπολογιστή χωριστά μέσα σε ολόκληρο το δίκτυο.

- Το firewall εφαρμόζει έλεγχο προσπέλασης από και προς το δίκτυο, υλοποιώντας την πολιτική ασφάλειας του οργανισμού: Με βάση την καθορισμένη πολιτική ασφάλειας η οποία περιγράφει σε ποια πακέτα και σε ποιες συνόδους επιτρέπεται η είσοδος ή έξοδος, το firewall αποφασίζει εάν θα επιτρέψει ή θα αρνηθεί τη διέλευση ενός πακέτου ή την έναρξη μιας συνόδου, αφού προηγουμένως πιστοποιήσει την ταυτότητα τόσο των πακέτων, όσο και των συνόδων.

- Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο:

- Εφόσον όλη η κίνηση διέρχεται από το firewall, μπορεί αυτό να καταγράφει όλες τις επιτρεπόμενες και μη δραστηριότητες σε ένα αρχείο συμβάντων, το οποίο είναι διαθέσιμο στο διαχειριστή του δικτύου.

- Το firewall προστατεύει τα διαφορετικά δίκτυα εντός του ίδιου οργανισμού: Μερικές φορές το firewall μπορεί να χρησιμοποιηθεί για να διαχωρίσει ένα τμήμα του δικτύου από κάποιο άλλο. Με τον τρόπο αυτό μπορούμε να αποτρέψουμε την εξάπλωση σε ολόκληρο το δίκτυο ενδεχόμενων προβλημάτων που επηρεάζουν ένα συγκεκριμένο τμήμα.

- Το firewall έχει τη δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης: Τα τελευταία χρόνια το Internet αντιμετωπίζει πρόβλημα διαθέσιμων IP διευθύνσεων. Οι οργανισμοί που επιθυμούν να συνδεθούν με το Internet μπορεί να μην έχουν διαθέσιμες πραγματικές IP διευθύνσεις. Το firewall ενσωματώνει το NAT (Network Address Translator), το οποίο μεταφράζει τις εσωτερικές διευθύνσεις σε πραγματικές, λύνοντας έτσι το πρόβλημα της έλλειψης διευθύνσεων.

10.5.3 Αδυναμίες των Firewalls

Ένα firewall προσφέρει εξαιρετική προστασία απέναντι σε απειλές κατά του δικτύου, αλλά δεν αποτελεί ολοκληρωμένη λύση ασφάλειας. Υπάρχουν συγκεκριμένες απειλές, οι οποίες βρίσκονται πέρα από τις δυνατότητες ελέγχου του firewall.

Οι αδυναμίες των firewalls είναι οι ακόλουθες:

- Το firewall δεν μπορεί να προστατεύσει από προγράμματα ιούς: Τα firewalls δεν ασκούν σε βάθος έλεγχο των δεδομένων που εισέρχονται στο δίκτυο. Απλά εξετάζουν τις διευθύνσεις και τις θύρες προέλευσης και προορισμού, για να καθορίσουν εάν επιτρέπεται η είσοδος στο εσωτερικό δίκτυο.

- Το firewall δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού: Οι εσωτερικοί χρήστες είναι σε θέση να υποκλέψουν δεδομένα, να καταστρέψουν υλικό και λογισμικό, να τροποποιήσουν προγράμματα και γενικότερα να παραβιάσουν την πολιτική ασφάλειας του οργανισμού χωρίς καν να έρθουν σε επαφή με το firewall.

- Το firewall δε μπορεί να προστατέψει τον οργανισμό απέναντι σε επιθέσεις συσχετιζόμενες με δεδομένα: Τέτοιου είδους επιθέσεις συμβαίνουν όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρετητές του οργανισμού, είτε διαμέσου του ηλεκτρονικού ταχυδρομείου, είτε διαμέσου της αντιγραφής από δισκέτα και εκτελούνται με σκοπό να εξαπολύσουν επίθεση εναντίον του συστήματος.

Το firewall δεν μπορεί να προστατέψει το δίκτυο από απειλές άγνωστου τύπου:

- Το firewall μπορεί να προστατέψει το δίκτυο μόνο από γνωστές απειλές που έχουν αντιμετωπιστεί στο παρελθόν, εφόσον διαθέτει την απαιτούμενη τεχνολογία.

- Το firewall δεν μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό: Αν για παράδειγμα επιτρέπεται σε κάποιους έμπιστους χρήστες να έχουν πρόσβαση στο διαδίκτυο παρακάμπτοντας τους μηχανισμούς ασφάλειας του firewall, τότε το firewall δεν μπορεί να προστατέψει τις συνδέσεις αυτές. Ένα firewall μπορεί να ελέγξει αποτελεσματικά την κίνηση που διέρχεται μέσα από αυτό.

- Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του firewall: Είναι δυνατό ένα firewall να ρυθμιστεί με πολύ αυστηρό τρόπο, με κίνδυνο να εμποδίσει τη διαδικτύωση ή να προκαλεί δυσαρέσκεια στους χρήστες, εξαιτίας των πολλών ελέγχων και της ελαττωμένης φιλικότητας και ευχρηστίας που εισάγει.

10.5.4 Συμπεράσματα για τα Firewalls

Οι υποστηρικτές των firewalls τα θεωρούν σημαντικά, ως πρόσθετα μέτρα ασφάλειας, επειδή συγκεντρώνουν λειτουργίες ασφάλειας σε ένα και μόνο σημείο, απλοποιώντας την εγκατάσταση, τη ρύθμιση και τη διαχείριση.

Οι επικριτές των firewalls συνήθως επικαλούνται τη δυσκολία της χρήσης τους καθώς απαιτούν πολλές συνδέσεις και μηχανισμούς. Τους καταλογίζουν επίσης ότι αποτελούν εμπόδια στην ελεύθερη χρήση του Διαδικτύου. Ακόμη υποστηρίζουν ότι τα firewalls δημιουργούν μια ψευδαίσθηση ασφάλειας, οδηγώντας σε χαλάρωση των μέτρων ασφάλειας εντός του προστατευόμενου δικτύου.

Ωστόσο, όλοι συμφωνούν ότι τα firewalls είναι ισχυρά εργαλεία για την ασφάλεια των δικτύων, αλλά δεν αποτελούν πανάκεια για όλα τα προβλήματα ασφάλειας των δικτύων. Συνεπώς, δεν πρέπει να θεωρούνται ως υποκατάστατο μιας προσεκτικής διαχείρισης ασφάλειας μέσα σε ένα εσωτερικό δίκτυο.

Κάθε οργανισμός ηλεκτρονικού εμπορίου οφείλει να διαφυλάσσει τα προσωπικά δεδομένα των πελατών του και να λαμβάνει μέτρα ώστε αυτά να μην εκτίθονται σε μη εξουσιοδοτημένη πρόσβαση. Τα firewalls μπορούν να προσφέρουν αποτελεσματικές υπηρεσίες ελέγχου πρόσβασης για τα εσωτερικά δίκτυα των οργανισμών ηλεκτρονικού εμπορίου καθώς αποτελούν την πρώτη γραμμή άμυνας απέναντι σε εξωτερικές επιθέσεις.

Συνεπώς τα firewalls αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο.

10.6 Φίλτρα Πακέτων

Ένα φίλτρο πακέτων (ή firewall επιπέδου δικτύου) είναι μια δικτυακή συσκευή με πολλές θύρες που εφαρμόζει ένα σύνολο κανόνων σε κάθε εισερχόμενο πακέτο IP ώστε να αποφασίσει για το αν θα του επιτραπεί η διέλευση ή θα απορριφθεί. Τα πακέτα IP φιλτράρονται ανάλογα με τις πληροφορίες που βρίσκονται στην επικεφαλίδα τους (header), όπως:

- Τον αριθμό πρωτοκόλλου που δείχνει το είδος του πρωτοκόλλου που χρησιμοποιείται.
- Τη διεύθυνση IP του αποστολέα.
- Τη διεύθυνση IP του αποδέκτη.
- Το TCP ή UDP port προέλευσης.
- Το TCP ή UDP port προορισμού.
- Άλλες πληροφορίες.

Γενικά τα φίλτρα πακέτων δεν έχουν μνήμη κατάστασης. Κάθε πακέτο IP εξετάζεται ξεχωριστά και ανεξάρτητα του τι συνέβη στο παρελθόν. Υπάρχουν όμως και μερικά πιο εξελιγμένα φίλτρα πακέτων που διατηρούν μια λίστα με τα δεδομένα κατάστασης των πακέτων που φτάνουν στο φίλτρο.

Οι πληροφορίες των πακέτων που προηγήθηκαν, επιτρέπουν στα μελλοντικά πακέτα που αντιστοιχούν στην ίδια σύνοδο να περάσουν ή να απορριφθούν χωρίς πολλούς ελέγχους. Δηλαδή τα συγκεκριμένα φίλτρα πακέτων ελέγχουν συνόδους δικτύου και όχι μεμονωμένα πακέτα. Μια σύνοδος δικτύου αποτελείται από πακέτα τα οποία κινούνται και προς τι δύο κατευθύνσεις.

Τα απλά φίλτρα πακέτων απαιτούν δύο κανόνες για κάθε σύνοδο: Έλεγχος πακέτων τα οποία κατευθύνονται από υπολογιστή προέλευσης προς υπολογιστή προορισμού, και έλεγχος πακέτων τα οποία επιστρέφουν από υπολογιστή προορισμού προς υπολογιστή προέλευσης. Τα εξελιγμένα φίλτρα πακέτων δεν απαιτούν την ύπαρξη του δεύτερου κανόνα.

Επιπλέον με βάση τις πληροφορίες των παλαιότερων πακέτων που μπορούν να αποθηκεύσουν τα εξελιγμένα φίλτρα, μπορούν να εξαχθούν στατιστικά στοιχεία σχετικά με την κίνηση των πακέτων.

Τοποθέτηση ενός φίλτρου πακέτων μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου.

Τα περισσότερα φίλτρα πακέτων συμπεριφέρονται και σαν δρομολογητές και ονομάζονται «δρομολογητές διαλογής». Ένας απλός δρομολογητής όταν δεχθεί ένα πακέτο, κοιτάζει την επικεφαλίδα του και εξετάζει τη διεύθυνση προορισμού. Αν ο δρομολογητής γνωρίζει πώς να στείλει το πακέτο τότε το δρομολογεί.

Αν όμως δε γνωρίζει επιστρέφει το πακέτο στον αποστολέα. Ένας δρομολογητής διαλογής εξετάζει το πακέτο διεξοδικότερα. Έτσι δεν καθορίζει μόνο εάν το πακέτο μπορεί να δρομολογηθεί προς τον προορισμό του, αλλά και το αν πρέπει να δρομολογηθεί, εφαρμόζοντας την πολιτική ασφάλειας που έχει καθορίσει ο οργανισμός. Συνεπώς κάθε δρομολογητής διαλογής φιλτράρει τα πακέτα και επιπλέον τα δρομολογεί.

Ένα firewall επιπέδου δικτύου (φίλτρο πακέτου, δρομολογητής διαλογής) μπορεί να εμποδίσει ή να επιτρέψει συγκεκριμένους τύπους συνδέσεων, εφαρμόζοντας πάντα την πολιτική προσπέλασης του οργανισμού στον οποίο είναι εγκατεστημένο. Οι εξυπηρετητές που παρέχουν συγκεκριμένες Internet υπηρεσίες συνδέονται σε κάποια ειδική θύρα (port). Έτσι προσδιορίζοντας τον κατάλληλο αριθμό θύρας (π.χ. το TCP port 23 Telnet συνδέσεις) μπορεί το firewall να επιτρέψει ή μη συγκεκριμένη σύνδεση. Για παράδειγμα μπορεί κάποιο firewall να επιτρέπει τις υπηρεσίες e-mail (port 25), FTP (File Transfer Protocol, port 21), και Telnet (port 23) και να εμποδίζει όλες τις υπόλοιπες συνδέσεις.

Τα συγκεκριμένα firewalls είναι ίσως τα πιο απλά στην υλοποίηση και χρησιμοποιούνται κυρίως σε δικτυακούς τόπους με μικρή πολυπλοκότητα. Παρουσιάζουν όμως κάποια μειονεκτήματα και για το λόγο αυτό αποφεύγονται σε μεγαλύτερους δικτυακούς τόπους.

10.7 Πύλες Εφαρμογών (Application Gateways)[62]

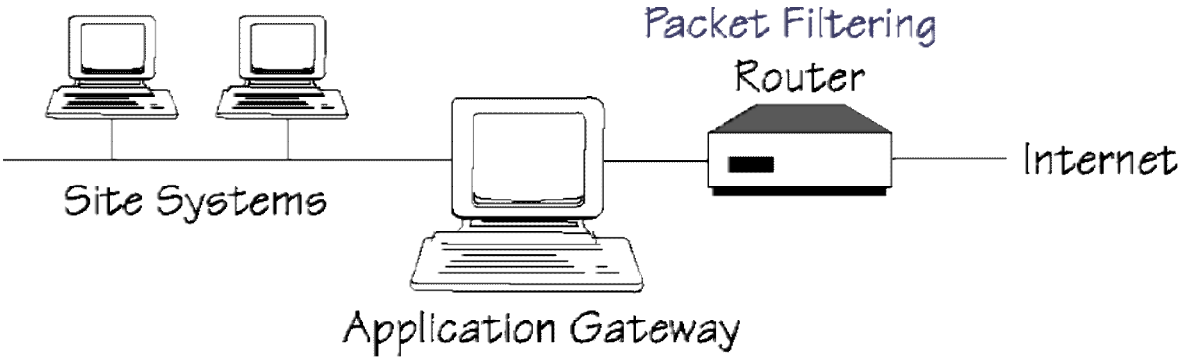
Οι πύλες εφαρμογών επιτρέπουν στον διαχειριστή να υλοποιήσει μια αυστηρότερη πολιτική ασφάλειας. Στο μοντέλο πελάτη/εξυπηρετητή η πύλη εφαρμογών είναι μια ενδιάμεση διεργασία που τρέχει μεταξύ του πελάτη που ζητάει μια συγκεκριμένη υπηρεσία και του εξυπηρετητή που παρέχει αυτή την υπηρεσία. Δηλαδή η πύλη εφαρμογών λειτουργεί ως εξυπηρετητής από τη σκοπιά του πελάτη και ως πελάτης από τη σκοπιά του εξυπηρετητή. Μια πύλη εφαρμογών μπορεί να λειτουργεί είτε στο επίπεδο εφαρμογής είτε στο επίπεδο μεταφοράς του TCP/IP.

Αν η πύλη λειτουργεί στο επίπεδο εφαρμογής ονομάζεται πύλη επιπέδου εφαρμογής (application-level gateway) ή απλά πύλη εφαρμογών. Αντίστοιχα αν η πύλη λειτουργεί στο επίπεδο μεταφοράς ονομάζεται πύλη επιπέδου κυκλώματος (circuit-level gateway). Οι περισσότερες πύλες που χρησιμοποιούνται σε διατάξεις firewalls λειτουργούν στο επίπεδο εφαρμογής, είναι δηλαδή πληρεξούσιοι εξυπηρετητές (proxy servers).

Όταν ένας χρήστης που βρίσκεται στο εσωτερικό δίκτυο θέλει να επικοινωνήσει με μια υπηρεσία του εξωτερικού δικτύου, η πύλη εφαρμογών παρεμβάλλεται. Δηλαδή αντί ο χρήστης να επικοινωνήσει άμεσα με την υπηρεσία, επικοινωνεί με την πύλη εφαρμογών η οποία διαχειρίζεται παρασκηνιακά όλη τη μεταξύ τους επικοινωνία. Συγκεκριμένα όταν ένας πελάτης συνδέεται με την πύλη εφαρμογών χρησιμοποιώντας ένα από τα πρωτόκολλα εφαρμογής του TCP/IP, όπως το Telnet ή το FTP, η πύλη του ζητά πληροφορίες όπως ένα όνομα εισόδου (login) και ένα κωδικό πρόσβασης (password) για την πιστοποίηση της ταυτότητας του.

Αν η πύλη αναγνωρίσει και δεχτεί το χρήστη, ο χρήστης της δίνει το όνομα του απομακρυσμένου συστήματος (υπηρεσία) που επιθυμεί να προσπελάσει, η πύλη εφαρμογών συνδέεται για λογαριασμό του χρήστη με αυτό το απομακρυσμένο σύστημα και εγκαθιστά μια δευτερεύουσα σύνδεση. Στη συνέχεια μετάγει τα δεδομένα της εφαρμογής μεταξύ των δύο συνδέσεων.

Τοποθέτηση μιας πύλης εφαρμογών μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου.



Εικόνα 10.3 **Δικτυακή Διάταξη με χρήση Πύλης Εφαρμογών** (Application Gateway)

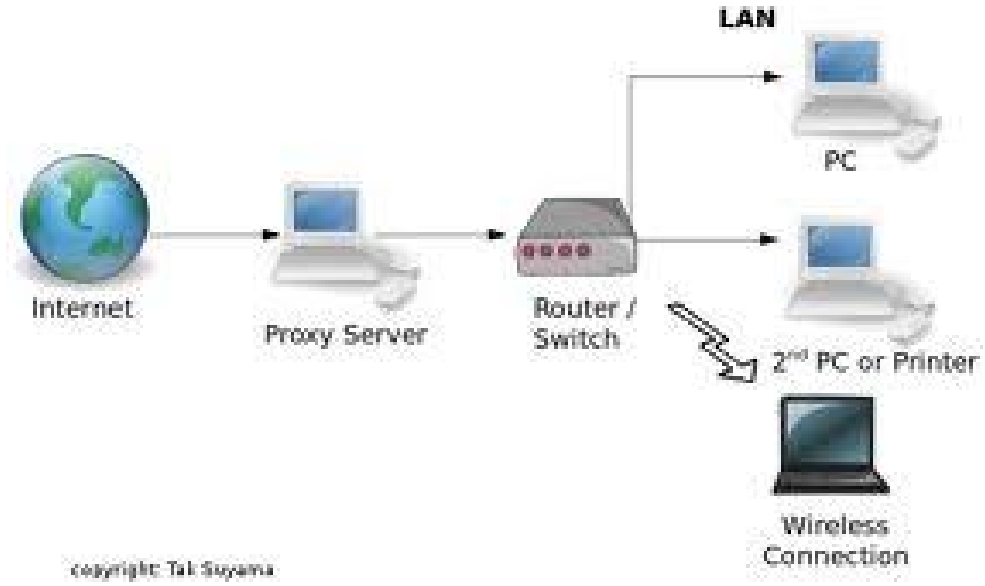
[62] **Πηγή:** ΑΤΕΙ Λαμίας - Ασφάλεια Υπολογιστικών Συστημάτων – Καθηγητής Δρ. Κωνσταντίνος Αντώνης

Η πύλη εφαρμογών φιλοξενείται σε ένα υπολογιστή γενικού σκοπού, ο οποίος ονομάζεται Bastion host (ή υπολογιστής-οχυρό). Ο υπολογιστής-οχυρό απαιτείται να παρέχει μεγάλη ασφάλεια διότι αποτελεί το κύριο σημείο επικοινωνίας για τους χρήστες του εσωτερικού δικτύου. Επιπλέον επειδή ο υπολογιστής-οχυρό εκτίθεται σε άμεσες επιθέσεις από το διαδίκτυο θα πρέπει να είναι ρυθμισμένος με τέτοιο τρόπο ώστε να είναι ιδιαίτερα ασφαλής.

Συνήθως το λειτουργικό σύστημα του bastion host είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητες του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται. Έτσι μειώνεται η πιθανότητα ύπαρξης τυχόν «οπών ασφαλείας» και συνεπώς ενισχύεται η ασφάλεια του bastion host.

10.8 Πληρεξούσιοι Εξυπηρετητές (Proxy Servers)[63]

Μια πύλη επιπέδου εφαρμογής που τρέχει σε ένα υπολογιστή-οχυρό συνήθως στεγάζει διάφορους proxy servers. Οι proxy servers χρησιμοποιούνται προκειμένου να έχουμε πρόσβαση στα δεδομένα με ασφαλή τρόπο. Αν ένας χρήστης του ενδοεπιχειρησιακού δικτύου θέλει να έχει πρόσβαση σε ένα συγκεκριμένο εξυπηρετητή εφαρμογής TCP/IP στο διαδίκτυο, πρέπει η εφαρμογή του εξυπηρετούμενου να εγκαταστήσει μια σύνδεση με τον proxy server που τρέχει για αυτή τη συγκεκριμένη εφαρμογή στον υπολογιστή-οχυρό. Ο proxy server με τη σειρά του πρέπει να πιστοποιήσει την αυθεντικότητα του χρήστη και να τον εξουσιοδοτήσει για πρόσβαση.



Εικόνα 10.4 **Λειτουργία Δικτύου με** Proxy Server

[63] **Πηγή**: Κέντρο ΠΛΗ.ΝΕ.Τ Φλώρινας http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html

Μπορούν να χρησιμοποιηθούν διάφορα σχήματα πιστοποίησης αυθεντικότητας και εξουσιοδότησης. Το απλούστερο σχήμα είναι ο proxy server να κρατά μια λίστα με διευθύνσεις IP που επιτρέπεται να συνδεθούν σε εξωτερικούς εξυπηρετητές εφαρμογών. Αυτό το σχήμα δεν είναι πολύ ασφαλές, αφού οποιοσδήποτε μπορεί να προσποιηθεί ότι έχει εξουσιοδοτημένη διεύθυνση IP. Ένα πιο ασφαλές σχήμα είναι η χρήση ισχυρών μηχανισμών πιστοποίησης αυθεντικότητας μεταξύ του χρήστη και του proxy server.

Μετά την επιτυχή πιστοποίηση αυθεντικότητας και εξουσιοδότηση του χρήστη, ο proxy server εγκαθιστά μια δεύτερη σύνδεση TCP/IP με τον εξυπηρετητή της εφαρμογής που ζητήθηκε. Ο εξυπηρετητής της εφαρμογής μπορεί να θέλει και αυτός με τη σειρά του να πιστοποιήσει την αυθεντικότητα του χρήστη. Αν και εδώ πιστοποιηθεί επιτυχώς η αυθεντικότητα του χρήστη και εξουσιοδοτηθεί, ο εξυπηρετητής της εφαρμογής αρχίζει να εξυπηρετεί την αίτηση. Από τη στιγμή αυτή και μετά ο proxy server απλά μετάγει δεδομένα εφαρμογής μεταξύ των δύο συνδέσεων. Για κάθε πακέτο που ρέει από τον εσωτερικό εξυπηρετούμενο στον εξωτερικό εξυπηρετητή, ο proxy server συνήθως αντικαθιστά τη διεύθυνση IP του αποστολέα με τη δική του διεύθυνση. Έτσι οι εσωτερικές διευθύνσεις IP που χρησιμοποιούνται στο ενδοεπιχειρησιακό δίκτυο είναι ολοκληρωτικά κρυμμένες και δεν εκτίθενται στο διαδίκτυο.

11ο Κεφάλαιο
Ηλεκτρονικά Καταστήματα

11.1 Γενικά

Το ηλεκτρονικό κατάστημα (e-shop) είναι ουσιαστικά μια ιστοσελίδα, η οποία ανήκει σε κάποια επιχείρηση η οποία μπορεί να είναι καθαρά διαδικτυακή ή να έχει και φυσική οντότητα, κτιριακές εγκαταστάσεις, κάπου. Οι επιχειρήσεις στην προσπάθειά τους να επιβιώσουν στον ανταγωνισμό επιλέγουν όλο και περισσότερο την ενσωμάτωση των νέων τεχνολογιών στις πρακτικές τους. Πριν από μερικά χρόνια, η ενσωμάτωση αυτή, περιλάμβανε μόνο την ηλεκτρονική παρουσίαση των καταστημάτων, όχι όμως και όλων των ειδών τους. Ήταν δηλαδή κάτι σαν διαφήμιση-προβολή της επιχείρησης σε έναν άλλο δικτυακό τόπο ή ακόμα και σε ιστοσελίδες των ίδιων των επιχειρήσεων. Ακόμη δεν υπήρχε δυνατότητα άμεσης παραγγελίας κάποιου είδους και πολλές φορές ούτε καν ενημέρωση τιμών για τα προϊόντα.

Θεωρώντας ως πρώτη γενιά ηλεκτρονικών καταστημάτων την προαναφερόμενη κατάσταση μπορούμε να συνεχίσουμε με την δεύτερη γενιά ή οποία έφερε μαζί της τις ηλεκτρονικές παραγγελίες. Ένα ηλεκτρονικό κατάστημα δεύτερης γενιάς έδινε την δυνατότητα στους καταναλωτές να επιλέξουν τα προϊόντα που επιθυμούν από μια περιορισμένη γκάμα, να τα τοποθετήσουν σε καλάθια αγοράς και να ολοκληρώσουν την παραγγελία τους. Στην συνέχεια η επιχείρηση ενημερώνεται για τις παραγγελίες μέσω email και το προσωπικό της επιχείρησης έστελνε τα προϊόντα στους πελάτες οι οποίοι είχαν δυνατότητα πληρωμής μόνο με αντικαταβολή.

Στα μέσα της δεκαετίας του 1990 αρχίζει η τρίτη γενιά ηλεκτρονικών καταστημάτων η οποία είχε σαν κύριο χαρακτηριστικό την σύνδεση των ηλεκτρονικών καταστημάτων με τα ήδη εγκατεστημένα πληροφοριακά συστήματα των επιχειρήσεων. Οι επιχειρήσεις ενημερώνονται on-line για τις παραγγελίες που πραγματοποιούνται και μπορούν να τις εκτελούν άμεσα. Παρέχονται έτσι περισσότερη ευελιξία και ταχύτητα στον τρόπο παραγγελίας καθώς και μεγαλύτερη ποικιλία στα προϊόντα που προσφέρονται στον καταναλωτή. Ο χρήστης μπορεί πλέον να πληρώσει ηλεκτρονικά με πιστωτική ή χρεωστική κάρτα ενώ η τιμολόγηση γίνεται πλέον ηλεκτρονικά.

Τέλος στις αρχές του 2000 έχουμε την εμφάνιση της τέταρτης γενιάς ηλεκτρονικών καταστημάτων τα οποία εστίασαν στην ασφάλεια των συναλλαγών και στην διαχείριση των αποθεμάτων και αποθήκης. Παρουσιάζονται νέες λειτουργίες όπως το

ηλεκτρονικό πορτοφόλι, ο έλεγχος αποθεμάτων με on-line σύνδεση του καταστήματος με την αποθήκη, η καταγραφή του προφίλ του καταναλωτή κ.α. Δίνεται ακόμη μεγαλύτερη βαρύτητα στην ασφάλεια των συναλλαγών και εισάγονται νέοι τρόποι ασφαλών πληρωμών όπως οι προπληρωμένες κάρτες PayPal και Pay Safe.

11.2 Χαρακτηριστικά Ηλεκτρονικών Καταστημάτων

Από την προσωπική μας εμπειρία αλλά και μελετώντας οδηγούς και εγχειρίδια υλοποίησης ηλεκτρονικών καταστημάτων καταλήξαμε σε μια σειρά «κανόνων». Από την στιγμή που μια επιχείρηση θα αποφασίσει να επεκταθεί στον χώρο του ηλεκτρονικού εμπορίου θα πρέπει να λάβει υπ'υπόψιν τα παρακάτω.

Αρχικά να αποφασίσει ποια από τα προϊόντα που εμπορεύεται θα προωθήσει μέσω του διαδικτύου. Αν και θεωρητικά όλα τα προϊόντα μπορούν να πουληθούν από το διαδίκτυο κάποια από αυτά δεν έχουν τόσο μεγάλη πέραση ή μπορεί να μην συμφέρει την επιχείρηση να τα πουλήσει μέσω internet. Για παράδειγμα προϊόντα τα οποία ο καταναλωτής τα κρίνει με την βοήθεια των αισθήσεων (αφή, όσφρηση, γεύση) δεν έχουν τόσο μεγάλη ανταπόκριση όσο κάποια άλλα.

Η επιχείρηση οφείλει να έχει καλή γνώση του ηλεκτρονικού εμπορίου και γενικά του διαδικτύου, ώστε να μπορέσει να υλοποιήσει αλλά και να υποστηρίξει την επιθυμία του να επεκταθεί στο ηλεκτρονικό εμπόριο. Βέβαια μπορεί μια επιχείρηση να αναθέσει σε εξειδικευμένες εταιρίες την υλοποίηση και την διαχείριση του project αλλά σε κάθε περίπτωση η επιχείρηση η ίδια θα πρέπει να έχει τον τελευταίο λόγο.

Η ανάπτυξη μιας ιστοσελίδας ηλεκτρονικού εμπορίου θα πρέπει να είναι εύχρηστη και φιλική προς το χρήστη-πελάτη. Λιτή και κατανοητή έτσι ώστε να δίνει την δυνατότητα στο χρήστη να βρει αυτό που ψάχνει άμεσα. Παράλληλα θα πρέπει να παρέχει και την απαραίτητη εξυπηρέτηση πελατών ώστε ο χρήστης να μπορεί να λάβει βοήθεια από φυσικά πρόσωπα. Έτσι το ηλεκτρονικό κατάστημα δίνει μια πιο φιλική και ανθρώπινη αίσθηση και δεν χάνει και τον πελατοκεντρικό χαρακτήρα του. Ακόμη καλύτερη είναι η περίπτωση της δωρεάν τηλεφωνικής υποστήριξης μέσω

τηλεφωνικών γραμμών τύπου 800## ή με αστική χρέωση απ' όλη την Ελλάδα. Επιπρόσθετα η άμεση, μέσα σε 24 ώρες, απάντηση σε ερωτήσεις που καταφθάνουν με email είναι πολύ θετικό χαρακτηριστικό ενός ηλεκτρονικού καταστήματος.

Οι «κρυφές χρεώσεις» είναι ένα ατόπημα που πρέπει να αποφύγουν οι επιχειρήσεις που αναπτύσσονται στο διαδίκτυο. Για παράδειγμα εμφανίζεται αρχικά μια τιμή για κάποιο προϊόν και αφού ο καταναλωτής επιλέξει να το αγοράσει και το προσθέσει στο καλάθι αγορών να εμφανίζονται εκεί έξτρα χρεώσεις όπως φπα, έξοδα αποστολής και άλλοι φόροι που δεν αναφέρονται στην αρχική τιμή του προϊόντος.

Τέλος το καλό ηλεκτρονικό κατάστημα είναι αυτό που ενημερώνει τον ιστότοπο του τακτικά, δεν έχει νεκρά λινκ και γενικά φαίνεται και είναι ενεργό. Η τακτική ανανέωση των προϊόντων, η προσθήκη νέων, η σαφής και λεπτομερής περιγραφή τους καθώς και οι προσφορές με ημερομηνία λήξης σε συνδυασμό με την υψηλή αίσθηση ασφάλειας που μπορεί να παρέχει μια ιστοσελίδα προσδίδουν περισσότερη αξιοπιστία και γίνονται εύκολα αποδεκτές από το τον μέσο χρήστη του διαδικτύου.

11.3 Πλεονεκτήματα Ηλεκτρονικών Καταστημάτων

Μια επιτυχημένη ανάπτυξη και λειτουργία ενός ηλεκτρονικού καταστήματος έχει πολλά πλεονεκτήματα για την επιχείρηση αλλά και για το αγοραστικό κοινό επίσης.

Αρχικά η επιχείρηση επιτυγχάνει την 24 λειτουργία της, εικονικά τουλάχιστον, αφού το ηλεκτρονικό κατάστημα δεν έχει ωράριο λειτουργία ούτε γνωρίζει από γιορτές και αργίες. Είναι ενεργό 24 ώρες την ημέρα, 365 μέρες το χρόνο και παρουσιάζει τα προϊόντα της επιχείρησης δίνοντας τη δυνατότητα σε κάθε καταναλωτή να το επισπευτεί από όπου και αν βρίσκεται. Αυτό βέβαια μπορεί να θεωρηθεί και ως πλεονέκτημα των χρηστών-πελατών του διαδικτύου αφού και για αυτούς είναι σημαντικό να έχουν την δυνατότητα να κάνουν τις αγορές τους οποιαδήποτε ώρα της ημέρας και από οποιοδήποτε μέρος του κόσμου.

Ένα ακόμη πλεονέκτημα του ηλεκτρονικού εμπορίου για τις επιχειρήσεις είναι το γεγονός ότι η επιχείρηση δεν πληρώνει υπέρογκα ποσά για ενοίκια καταστημάτων σε κεντρικά σημεία πόλεων ή για υπαλλήλους αλλά το μόνο που χρειάζεται είναι μια μεγάλη αποθήκη για το εμπόρευμα και κάποια σχετική υποστήριξη για την ιστοσελίδα.

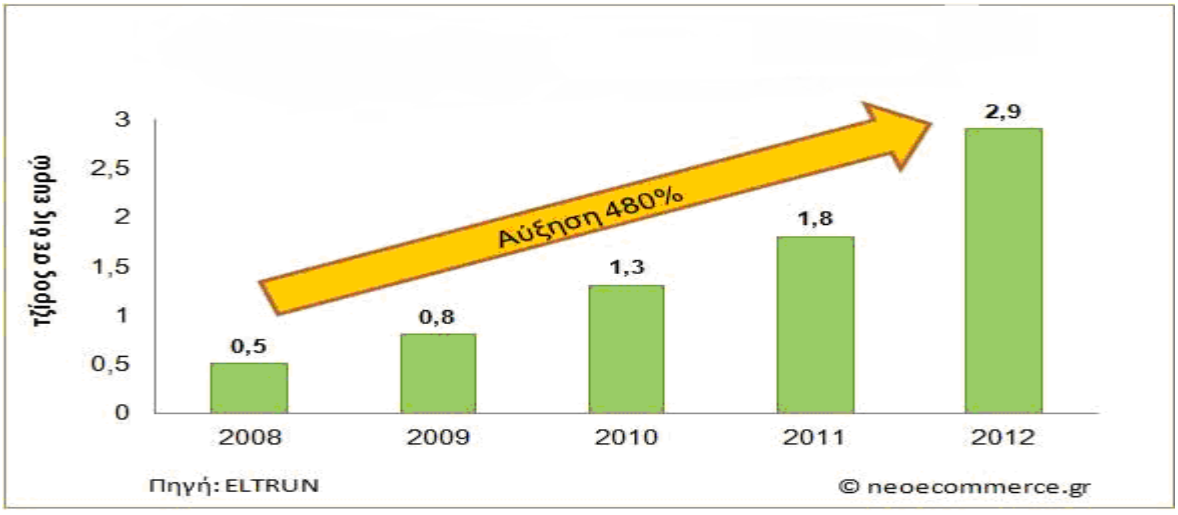
Παράλληλα η επιχείρηση έχει τη δυνατότητα να αποθηκεύει τα στοιχεία αλλά και τις προτιμήσεις των πελατών της και έτσι να δημιουργήσει μια μεγάλη βάση δεδομένων. Έτσι γνωρίζοντας τις προτιμήσεις των πελατών της μπορεί να διαμορφώσει τον κατάλογο των προϊόντων της και να τον εμπλουτίσει με πιο αποδεκτά και χρηστικά προϊόντα. Ακόμη μπορεί να δημιουργήσει πιο συγκεκριμένες προσφορές που θα απευθύνονται και θα καλύπτουν τις ανάγκες των πελατών της και χρησιμοποιώντας τις διευθύνσεις τους θα αποστέλλονται προσωπικά.

Ο πελάτης ενός ηλεκτρονικού καταστήματος έχει την δυνατότητα να επισκέπτεται ταυτόχρονα περισσότερους από έναν διαδικτυακούς τόπους και να συγκρίνει έτσι άμεσα τιμές αλλά και προϊόντα από πολλά καταστήματα. Μπορεί να διαβάζει σχόλια και απόψεις άλλων χρηστών για προϊόντα και έτσι να έχει μια πιο ολοκληρωμένη εικόνα για το προϊόν που θέλει να αγοράσει ή να αποφύγει τυχόν απάτες και παραπλανητικές διαφημίσεις.

Τέλος η άμεση επαφή του πελάτη με την επιχείρηση, που μπορεί να είναι και ο παραγωγός του προϊόντος, εξασφαλίζει καλύτερες τιμές χάρη στην απουσία τυχών μεσαζόντων. Δεδομένου βέβαια ότι τα μεταφορικά για την παραλαβή του προϊόντος δεν θα αυξήσουν πάρα πολύ την τιμή του.

11.4 Ηλεκτρονικά Καταστήματα στην Ελλάδα

Όπως έχουμε προαναφέρει στην Ελλάδα 1,5 εκατομμύρια[64] καταναλωτές ψωνίζουν μέσω Internet, ενώ ο τζίρος που κάνουν στην αγορά του ηλεκτρονικού εμπορίου ανήλθε στα 1,7 δισ. ευρώ το 2011, σημειώνοντας μια αύξηση κατά 30% έναντι του 2010.



Εικόνα 11.1 **Εξέλιξη τζίρου** e-shops **στην Ελλάδα**
2008 – 2012 – (**σε δις Ευρώ**)

[64] **Πηγή** : Έρευνα «Το Ηλεκτρονικό Εμπόριο στην Ελλάδα» - Οικονομικό Πανεπιστήμιο Αθηνών (Εργαστήριο Ηλεκτρονικού Εμπορίου και Επιχειρείν) καθηγητής κ. Γ. Δουκίδης

Τα αποτελέσματα της έρευνα είναι εντυπωσιακά αφού κατεγράφησαν περίπου 3.500 ελληνικά ηλεκτρονικά καταστήματα (e-shops) τα οποία δραστηριοποιούνται στην Ελλάδα, αριθμός αρκετά σημαντικός για μια χώρα σαν την Ελλάδα. Αξιολογήθηκαν 228 ηλεκτρονικά καταστήματα με βάση τους τέσσερις κύριους άξονες που επηρεάζουν την επιτυχία των ηλεκτρονικών καταστημάτων σε σχέση με τους on-line καταναλωτές:

1. Προστασία των καταναλωτών σε σχέση με την άυλη επιχείρηση / συναλλαγή.
2. Υψηλή αισθητική και ευκολία πλοήγησης στο site.
3. Δυνατότητες και ασφάλεια πληρωμών.
4. Προχωρημένες υπηρεσίες για τους on-line καταναλωτές.

Χαρακτηριστικό είναι ότι από τα 3.500 ελληνικά e-shops που λειτουργούν τώρα, τα 2/3 αυτών προσφέρουν όλες τις αναγκαίες υπηρεσίες και δυνατότητες στους καταναλωτές για μια άνετη και αξιόπιστη συναλλαγή, που είναι συγκρίσιμη και εφάμιλλη γνωστών e-shops του εξωτερικού. Το ποσοστό των καταστημάτων που παρέχουν μια σωστή και ολοκληρωμένη υπηρεσία στους πελάτες τους είναι αρκετά μεγάλο και προσδίδει αισιοδοξία για το μέλλον.

Παρόλα αυτά όμως υπάρχει ένα μικρό ποσοστό (10 -15%) το οποίο θα πρέπει να αποφεύγουν οι καταναλωτές λόγω έλλειψης ουσιαστικής εταιρικής πληροφόρησης αφού δεν παρουσιάζουν τα βασικά στοιχεία μιας τυπικής επιχείρησης και δεν έχουν διεύθυνση, τηλέφωνο και email.

Σε σχετικό άρθρο της η εφημερίδα «Έθνος» στις 22/3/12 αναφέρει την σχετική έρευνα και επιπρόσθετος την πεποίθηση του γενικού γραμματέα Εμπορίου κ. Στέφανού Κομνηνού, η οποία διατυπώθηκε σε συνέντευξη Τύπου. Σύμφωνα με τα λεγόμενα του στην προσπάθεια του Υπουργείου για εξυγίανση και έλεγχο των ηλεκτρονικών καταστημάτων, με απώτερο σκοπό την προστασία του καταναλωτή, υλοποιείται με ταχείς διαδικασίες η ηλεκτρονική τιμολόγηση για όσες επιχειρήσεις κάνουν ηλεκτρονική τιμολόγηση. Δημιουργήθηκε ήδη το «πρότυπο» και τις επόμενες δύο εβδομάδες θα πραγματοποιηθεί η σχετική διαβούλευση για το θέμα προκειμένου να περάσουμε στην εφαρμογή του συγκεκριμένου προτύπου άμεσα.

Σημειώνεται[65] ότι το κόστος για τη δημιουργία ενός ηλεκτρονικού καταστήματος έχει πέσει πλέον στο 1/3 (5.000 ευρώ από 30.000 ευρώ) απ' ότι ήταν πριν από δύο χρόνια. Επιπροσθέτως, την τελευταία διετία έχουν αυξηθεί οι πωλήσεις των ελληνικών ηλεκτρονικών καταστημάτων στο καλάθι του Έλληνα καταναλωτή, αποτελώντας πλέον τα 2/3 των ηλεκτρονικών αγορών τους. Αξίζει να αναφέρουμε ότι οι περισσότερες αγορές αφορούν ηλεκτρονικά προϊόντα, αν και τα τελευταία χρόνια έχει αυξηθεί σημαντικά και το μερίδιο της αγοράς τουριστικών πακέτων.

[65] **Πηγή:** Εφημερίδα «Έθνος» 22/3/2012

Τέλος μπορούμε να αναφέρουμε μερικά ηλεκτρονικά καταστήματα τα οποία δραστηριοποιούνται στην Ελλάδα με μεγάλη απήχηση στο αγοραστικό κοινό. Να τονίσουμε ότι η επιλογή έγινε καθαρά από προσωπικές εμπειρίες και γνώσεις και είναι πολύ πιθανό να έχουμε παραλείψει κάποια καταστήματα, γεγονός το οποίο δεν μας απομακρύνει από το στόχο μας.

Έτσι κατηγοριοποιώντας τα ηλεκτρονικά καταστήματα με βάση τα προϊόντα που εμπορεύονται έχουμε:

Καταστήματα **Ηλεκτρικών – Ηλεκτρονικών** ειδών**:**

- http://www.e-shop.gr
- http://www.plaisio.gr
- http://www.emimikos.gr/shop/
- http://markidis.gr/
- http://www.elektronik.gr/eshop/

Καταστήματα ειδών **Ένδυσης - Υπόδησης**:

- http://www.melinamay.com
- http://www.newcult.gr
- http://http://www.fullahsugah.gr
- http://www.inshoes.gr
- http://www.pret-a-beaute.com

Καταστήματα **Παροχής Υπηρεσιών**:

- http://travel.viva.gr/corporate
- http://websynergy.gr/
- http://www.booking.com/
- http://www.tripadvisor.com.gr/
- http://www.hol.gr
- http://www.forthnetgroup.gr

Συμπεράσματα –Επίλογος

Ολοκληρώνοντας την εργασία αυτή και έχοντας μελετήσει αρκετά δεδομένα, από οικονομικά άρθρα μέχρι στατιστικές έρευνες, μπορούμε να συγκλίνουμε στα εξής συμπεράσματα:

Το ηλεκτρονικό εμπόριο στηρίχτηκε και αναπτύχθηκε πάνω στις εφαρμογές και τα μέσα του διαδικτύου. Είχε ραγδαία ανάπτυξη, κυρίως στις πιο εμπορικά εξελιγμένες χώρες της Αμερικής της Ευρώπης και της Ασίας. Πιο ήπια ανάπτυξη παρουσιάζει στην Ελλάδα, με πολύ καλούς οιωνούς για το μέλλον. Ο ρόλος του ηλεκτρονικού εμπορίου είναι να οδηγήσει σε εντεταμένο ανταγωνισμό τιμών, καθότι αυξάνει την ικανότητα των καταναλωτών στη συγκέντρωση πληροφοριών σχετικά με προϊόντα και τιμές. Πράγμα το οποίο το πετυχαίνει σε μεγάλο βαθμό. Από την άλλη δίνει δυνατότητες σε επιχειρήσεις να διευρύνουν το αγοραστικό κοινό τους καθώς και την γεωγραφική κάλυψη.

Η αύξηση των διαδικτυακών αγορών έχει επηρεάσει επίσης, την οργανωτική δομή των βιομηχανιών σε δύο κλάδους, που έχει παρατηρηθεί σπουδαία αύξηση του ηλεκτρονικού εμπορίου και αυτοί οι κλάδοι είναι τα βιβλιοπωλεία και τα ταξιδιωτικά πρακτορεία.

Παράλληλα με την ανάπτυξη του ηλεκτρονικού εμπορίου αναπτύσσεται και ο επιστημονικός κλάδος της ασφάλειας των διαδικτυακών συναλλαγών. Στόχος είναι η δημιουργία ενός ασφαλούς περιβάλλοντος το οποίο θα προσελκύσει περισσότερους χρήστες διασφαλίζοντας τις συναλλαγές των χρηστών. Η προσπάθεια αυτή σίγουρα θα είναι συνεχής αφού οι κίνδυνοι είναι πολλοί και συνεχώς εξελισσόμενοι.
Σε γενικές γραμμές, όμως, μπορούμε να πούμε ότι οι ηλεκτρονικές συναλλαγές σήμερα μπορεί να γίνουν απόλυτα ασφαλείς αν βέβαια ακολουθηθούν και χρησιμοποιηθούν όλα τα σύγχρονα μέσα που υπάρχουν για αυτό το σκοπό.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Πομπόρτσης Α. & Τσουλφάς Α. (2002) Εισαγωγή στο ηλεκτρονικό εμπόριο, Θεσσαλονίκη, Τζιόλα

[Σιδηρόπουλος Θ. (2000) Εισαγωγή στο δίκαιο του ηλεκτρονικού εμπορίου, Αθήνα, Αφοί Κυριακίδη

Αλεξανδρίδου Ε. (2004) Το δίκαιο του ηλεκτρονικού εμπορίου,
Θεσσαλονίκη, Σάκκουλα

Ιγγλεζάκης Δ. (2003) Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Θεσσαλονίκη, Σάκκουλα

Ν. Γεωργόπουλος, Μ. Α. Πανταζή, Χ. Νικολαράκος, Ι. Βαγγελάτος (2001).
Ηλεκτρονικό επιχειρείν, προγραμματισμός και σχεδίαση, εκδόσεις: Ε.Μπένου

Α. Πασχόπουλος, Π. Σκαλτσάς (2001). Ηλεκτρονικό εμπόριο 2η έκδοση, εκδόσεις:
Κλειδάριθμος

Γ. Δουκίδης, Μ. Θεμιστοκλέους, Β. Δράκος, Ν. Παπαζαφειροπούλου (1998).
Ηλεκτρονικό εμπόριο, εκδόσεις: Νέων Τεχνολογιών

Λευκή Βίβλος για την Κοινωνία της Πληροφορίας – 2004, Παρατηρητήριο της ΚτΠ, http://infosoc.gr, Δεκέμβριος 2003

Κοτζαϊβαζόγλου Ιορδάνης – Η Επιχειρησιακή Επικοινωνία και η Εφαρμογές της σε Επιλεγμένες Επιχειρήσεις και Οργανισμούς της Βόρειας Ελλάδας

Γ.Ι Δουκίδης (PhD), Α. Φραγκοπούλου (MSc), Ι. Αναγνωστόπουλος (BSc) “EDI: Η ΠΛΗΡΟΦΟΡΙΚΗ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ”, Εκδόσεις Α. Σταμούλης, Αθήνα – Πειραιάς 1993.

X-RAM, “Ασφάλεια e-επιχειρήσεων”, τεύχος 6, Μάϊος 2001

Πηνελόπη Μαρκέλλου (MSc), Σπύρος Συρμακέσης (PhD) “Μοντέλα Ευχρηστίας για Συστήματα Ηλεκτρονικού Εμπορίου”, Σημειώσεις μαθήματος «Αλληλεπίδραση Ανθρώπου Υπολογιστή», Πάτρα 2001.

Βενάκης Περικλής ,Καζαντζή Αθανασία ,Κούρουπας Γεώργιος (ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ)

Σολδάτος Νίκος ‘‘Εφαρμογές του M- Business στο B2C και στο B2B ,2004’’

Αργυροπούλου Ελισάβετ ‘‘ Παρούσα κατάσταση και διαγραφόμενες τάσεις στην αγορά των CRM συστημάτων, 2002’’

Γενική Γραμματεία Εθνικής Στατιστικής Υπηρεσίας Της Ελλάδος, Δελτίο Τύπου, Έρευνα Χρήσης των Τεχνολογιών Πληροφόρησης και Επικοινωνίας από τα Νοικοκυριά, Έτους 2006, Πειραιάς

Soramäki, K. & Hanssens, B. (2003). E-payments: What are they and what makes them different?

Goldfinger, C. (1999). Secure electronic payments on the Internet.

Peirce, M. (2001). Payment mechanisms designed for the Internet.

Πηγές στο διαδίκτυο - Χρήσιμοι σύνδεσμοι:

- www.securityportal.com
- www.bclab.aueb.gr - Οικονομικό Πανεπιστήμιο Αθηνών (Εργαστήριο Επιχειρηματικής Πληροφορικής (BILab))
- www.eltrun.gr Οικονομικό Πανεπιστήμιου Αθηνών (Εργαστήριο Ηλεκτρονικού Εμπορίου και Ηλεκτρονικού Επιχειρείν (ELTRUN))
- www.cert.org
- http://ganges.cse.tcd.ie/meperice.
- http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html
- www.statistics.gr - Ελληνική Στατιστική Αρχή (ΕΛ.ΣΤΑΤ)
- www.statistics.gr/portal/page/portal/ESYE/PAGE-themes? p_param=A190 ΕΛ.ΣΤΑΤ (Στατιστικά Θέματα: Τεχνολογία - Κοινωνία Πληροφορίας)
- www.web-police.org
- www.web-marketing-resource.com
- www.media.mit.edu/
- www.gefma.com
- ecommerce.wipo.int/domains/process/
- www.sepve.org.gr
- www.kepka.org/Grk/info/ecommerce/eco008.htm http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l24204_el.htm
- www.go-online.gr/ebusiness/specials/article.html?article_id=550 http://www.adwords-solutions.gr/2010/09/ecommerce-study-in-greece-2009/#ixzz13xK9diyJ
- Καθημερινή (2008): Τι είναι internet: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_16/05/2008_232979

- Tee (2000): Η πρόοδος του Ηλεκτρονικού Εμπορίου τα τελευταία χρόνια:: http://www.tee.gr/online/news/2000/2132/,

- Netmode (2005): Η πρόοδος του Ηλεκτρονικού Εμπορίου τα τελευταία χρόνια:www.netmode.ntua.gr/courses/postgraduate/edi/presentations/EC-%20Introduction%202005%20Final.pdf,

- Wikipedia : PayPal:: http://en.wikipedia.org/wiki/PayPal,

- Wikipedia : Security Socket Layer:: http://el.wikipedia.org/wiki/HTTPS,

- Wikipedia : Εισαγωγή ηλεκτρονικών συναλλαγών: el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CFCF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B