ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ ΣΤΗΝ ΝΑΥΤΙΛΙΑ
4ΟΣ ΚΥΚΛΟΣ ΣΠΟΥΔΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ & ΝΑΥΤΙΛΙΑ. ΑΣΦΑΛΕΙΑ & ΣΤΡΑΤΗΓΙΚΕΣ ΕΠΕΝΔΥΣΗΣ & ΑΠΟΔΟΣΗΣ ΣΤΟ E- COMMERCE

ΚΑΘΗΓΗΤΗΣ: κ. ΠΕΛΑΓΙΔΗΣ
ΦΟΙΤΗΤΗΣ: ΔΗΜΗΤΡΗΣ ΤΖΙΤΖΙΝΙΑΣ Α.Μ : ΜΝ/ 04036

ΝΟΕΜΒΡΙΟΣ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

1.1 Αντικείμενο Μελέτης

Πολλές επιχειρήσεις απολαμβάνουν οικονομική ευημερία χρησιμοποιώντας το Διαδίκτυο ως κανάλι διανομής των προϊόντων και υπηρεσιών τους, με απώτερο σκοπό να τα πουλήσουν στους τελικούς καταναλωτές. Αυτή όμως η διαδικασία περιγράφει μόνο το εμπόριο μέσω του Διαδικτύου και δεν αποτελεί τον αντιπροσωπευτικό ορισμό του ηλεκτρονικού εμπορίου. Θα μπορούσαμε να πούμε, πως ηλεκτρονικό εμπόριο είναι η ηλεκτρονική ανταλλαγή πληροφοριών, αγαθών, υπηρεσιών και πληρωμών, απαραίτητη προϋπόθεση της οποίας είναι η δημιουργία και συντήρηση σχέσεων που θα βασίζονται στον παγκόσμιο ιστό.

Αναλυτικότερα, το ηλεκτρονικό εμπόριο περιλαμβάνει, αλλά δεν περιορίζεται μόνο εκεί, το WWW (World Wide Web), τα intranets, τα extranets, την ηλεκτρονική ανταλλαγή δεδομένων (EDI) και άλλα. Παραδείγματα εφαρμογών ηλεκτρονικού εμπορίου είναι οι διαφόρων ειδών πληρωμές με τρόπο ηλεκτρονικό, ο συντονισμός των επιχειρηματικών εταίρων χρησιμοποιώντας intranets, με σκοπό τη γρήγορη και εύκολη διάχυση της πληροφόρησης.

Η πρόοδος των τεχνολογιών πληροφορικής και επικοινωνίας, με το Internet να είναι μια από αυτές, έχουν επιφέρει θεμελιώδεις αλλαγές τόσο στην οργανωτική δομή των επιχειρήσεων όσο και στη δομή κάθε βιομηχανίας. Έτσι, και στη ναυτιλιακή βιομηχανία έχουν επέλθει σημαντικές αλλαγές. Πιο συγκεκριμένα, το ηλεκτρονικό εμπόριο στη ναυτιλία διακρίνεται σε τρεις κατηγορίες:

Πληροφοριακές πύλες (information portals)

Online site ναυλώσεων

Προμήθειες, συμπεριλαμβανομένου καυσίμων (LSE September 2000 σελ. 16-17)

Αυτή η έρευνα αποτελεί μια προσπάθεια καταγραφής των ηλεκτρονικών εφαρμογών που υφίστανται στο χώρο, καθώς και των τάσεων του ηλεκτρονικού εμπορίου. Ειδικότερα, επικεντρώνεται σε εφαρμογές online ναυλώσεων μεταξύ επιχειρήσεων. Αυτές οι εφαρμογές αναλύονται σε όρους διαδικασίας επικοινωνίας - τεχνολογίας, θεμάτων κουλτούρας, καθώς και κοινωνικο-οικονομικών και πολιτικών παραγόντων.

1.2 Σκοπός

Ο κύριος σκοπός τούτης της μελέτης είναι να καταδείξει τον τρόπο με τον οποίο οι ναυτιλιακοί οργανισμοί, και πιο συγκεκριμένα οι πλοιοκτήτριες, οι ναυλομεσιτικές (charteres) και μεσιτικές (shipbrokers) εταιρίες, πραγματοποιούν τη μετάβαση από την παραδοσιακή στην ηλεκτρονική επιχείρηση, καθώς και τους παράγοντες που βοηθούν αλλά και περιορίζουν τη μετάβαση αυτή. Θα επικεντρωθούμε και θα προσπαθήσουμε να δώσουμε απάντηση σε ερωτήματα όπως:

Κατά πόσο χρησιμοποιείται το Διαδίκτυο και διάφορες εφαρμογές ηλεκτρονικού εμπορίου στην Ναυτιλιακή Βιομηχανία;

Ποιοι είναι οι περιορισμοί, δημόσιοι & ιδιωτικοί, στην ανάπτυξη εφαρμογών ηλεκτρονικού εμπορίου;

Κατά πόσο οι παραδοσιακές επιχειρήσεις μπορούν να μεταβούν στο χώρο του ηλεκτρονικού επιχειρήν;

Πως οι ηλεκτρονικές υπηρεσίες μετάλλαξαν το ρόλο των μεσιτών;

Μπορεί το ηλεκτρονικό εμπόριο να μεταβάλλει τον τρόπο με τον οποίο πραγματοποιούνται οι συναλλαγές στη Ναυτιλία, όπως και στις υπόλοιπες βιομηχανίες;

Μπορεί να λειτουργήσουν ικανοποιητικά διαδικασίες ηλεκτρονικής δημοπρασίας στις ναυλώσεις;

1.3 Δομή Έρευνας

Η εργασία είναι δομημένη σε επτά κεφάλαια. Στο Πρώτο Κεφάλαιο αναφέρεται το θέμα που πραγματεύεται η εργασία, οι σκοποί και περιορισμοί που απαντήσαμε. Το Δεύτερο Κεφάλαιο πραγματεύεται με ζητήματα τεχνολογιών πληροφορικής και επικοινωνίας, όπως είναι το Internet, τα Intranets και Extranets, καθώς και με θέματα σχετικά με το Ηλεκτρονικό Εμπόριο. Αναλυτικότερα, δίνεται ο ορισμός του Ηλεκτρονικού Εμπορίου, αναλύεται και περιγράφεται σε

όρους ναυτιλιακών εφαρμογών μεταξύ των επιχειρήσεων. Σε αυτό το κεφάλαιο εξετάζονται εξονυχιστικά οι τάσεις που επικρατούν στους ναυτιλιακούς οργανισμούς, τα εμπόδια που συναντούνται καθώς και άλλα ζητήματα αναφορικά με το ηλεκτρονικό εμπόριο.

Στο Τρίτο Κεφάλαιο εξετάζεται η Αγορά των Ναυλώσεων και των Μεσιτών. Πιο συγκεκριμένα, αναλύονται οι online υπηρεσίες που προσφέρονται, περιγράφονται τα συστήματα πλειστηριασμών, όπως επίσης και οι online διαπραγματεύσεις. Επιπρόσθετα, στο ίδιο κεφάλαιο αναφέρονται μερικά αντιπροσωπευτικά παραδείγματα και εξετάζονται τα χαρακτηριστικά τους.

Στο τέταρτο κεφάλαιο αναφερόμαστε στην ασφάλεια του διαδικτύου, ενώ στο πέμπτο οι πολιτικές ασφάλειας. Στο έκτο κεφάλαιο αναφέρονται οι διάφορες στρατηγικές απόδοσης και στο έβδομο οι στρατηγικές επιβίωσης από την ηλεκτρονική καταστροφή. Τα συμπεράσματα της μελέτης μας αποτυπώνονται στο όγδοο κεφάλαιο και, τέλος, η βιβλιογραφία στο ένατο. Ακολουθεί το παράρτημα, όπου παρατίθενται πίνακες που αναφέρονται μέσα στο κυρίως κείμενο.

2. ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

2.1 Εισαγωγή

Η ανακάλυψη του τηλέγραφου, του τηλεφώνου, του ασυρμάτου και των υπολογιστών θέτουν τη βάση πάνω στην οποία είναι δυνατόν να αναπτυχθούν πρωτόγνωρες δυνατότητες. Το Internet, το μεγαλύτερο δίκτυο στον πλανήτη, αποτελεί μηχανισμό διάχυσης πληροφοριών, καθώς και μέσο για τη συνεργασία και αλληλεπίδραση, τόσο μεμονωμένων ατόμων, όσο και επιχειρήσεων, ανεξάρτητα από γεωγραφικούς και χρονικούς περιορισμούς.

2.2 Η Ιστορία του Διαδικτύου

Το Διαδίκτυο υφίσταται από το 1978 και αποτελεί το αποτέλεσμα της προσπάθειας του Αμερικανικού Υπουργείου Αμύνης να αναπτύξει ένα δίκτυο για αμυντικούς σκοπούς, μέσα στο οποίο θα ήταν καταχωρημένες αρκετές έρευνες. Ο αρχικός σκοπός των σχεδιαστών του ήταν να αναπτύξουν ένα δίκτυο τόσο δυνατό που θα άντεχε ακόμη και σε περίπτωση πυρηνικού πολέμου (Leer A, 2000).

Από τότε όμως, έχει σημειωθεί αξιοθαύμαστη πρόοδος στον τομέα της πληροφορικής και επικοινωνίας. Τα πρωτόκολλα μεταφοράς που έχουν εισαχθεί σε αυτόν τον τομέα, επιτρέπουν τη γρήγορη και εύκολη χρήση διαφορετικών μέσων επικοινωνίας. Το 1983 το Arpanet μετονομάστηκε στο γνωστό σε όλους μας Internet. Τις επόμενες δεκαετίες η πρόοδος της τεχνολογίας παρείχε τη δυνατότητα στις επιχειρήσεις να εκμεταλλευτούν τα πλεονεκτήματα που πήγαζαν από το Διαδίκτυο.

Η Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange) αποτέλεσε τη βάση πάνω στην οποία οι επιχειρήσεις που χρησιμοποιούσαν το Internet, δημιούργησαν αποτελεσματικότερες γραμμές επικοινωνίας, τόσο μεταξύ των διαφόρων τμημάτων του οργανισμού, όσο και με τους εξωτερικούς συνεργάτες, προμηθευτές και πελάτες (Shim, 2000 σελ. 52).

Το Διαδίκτυο είναι ταυτόχρονα ένα τεχνολογικό και κοινωνιολογικό φαινόμενο. Η εξέλιξή του είναι τόσο ραγδαία, που επιφέρει ριζικές αλλαγές στον τρόπο με τον οποίο τα

συστήματα των ηλεκτρονικών υπολογιστών (Η\Υ) και δικτύων χρησιμοποιούνται. Ο αριθμός των συνδεδεμένων Η\Υ και των χρηστών τους συνεχώς αυξάνεται. Όμως, το σημαντικότερο μέτρο ανάπτυξης των δικτύων είναι ο αριθμός και το επίπεδο των παρεχόμενων υπηρεσιών.

Αρχικά προσφέρονταν μόνο βασικές υπηρεσίες, όπως η μεταφορά αρχείων και το ηλεκτρονικό ταχυδρομείο. Η πραγματική επανάσταση όμως, επήλθε με την ανακάλυψη του World Wide Web, το γνωστό σε όλους μας www, που αποτελεί το δημοφιλέστερο τρόπο σύνδεσης με το Διαδίκτυο.

Το www αρχικά σχεδιάστηκε για τη διάχυση επιστημονικών πληροφοριών, που είχαν τη μορφή κειμένου. Αργότερα, όμως με την πρόοδο της τεχνολογίας υποστήριζε γραφικές απεικονίσεις, ήχο, κίνηση καθώς και ταινίες. Ένας σημαντικός νεωτερισμός ήταν η εισαγωγή των ενεργών στοιχείων (HTML forms) στις ιστοσελίδες. Τα στοιχεία αυτά επιτρέπουν την αμφίδρομη ροή πληροφορίας ανάμεσα στον web server και τον πελάτη και επομένως αυξάνουν το επίπεδο αλληλεπίδρασης ανάμεσα στον παροχέα των υπηρεσιών και τον καταναλωτή.

Στη σύγχρονη πραγματικότητα όμως, η ουσιαστικότερη καινοτομία είναι η εισαγωγή τεχνολογιών που επιτρέπουν τη χρήση εκτελέσιμων προγραμμάτων, τόσο από την πλευρά του πελάτη, όσο και από τον server. Αυτό μετάλλαξε ριζικά τις υπηρεσίες που παρέχει το www. Έτσι, οι web servers δεν αποτελούν πλέον αποθηκευτικούς χώρους όπου φυλάσσονται στατικά αρχεία, αλλά μετατράπηκαν σε παγκόσμιες ψηφιακές πλατφόρμες, όπου κάθε είδους εφαρμογή μπορεί να δημιουργηθεί. Η σταθερή τεχνολογική πρόοδος οδηγεί σε ένα σημείο όπου το www μπορεί να χρησιμοποιηθεί σε ποικίλα πεδία ηλεκτρονικών εφαρμογών, όπως το ηλεκτρονικό εμπόριο.

2.3 Ενδοδίκτυα & Υπερενδοδίκτυα (Intranets & Extranets)

Μερικά από τα μεγαλύτερα οφέλη που αποκομίζουν οι οργανισμοί από την τεχνολογία του Internet προέρχονται από εφαρμογές που μειώνουν το κόστος μεσολάβησης και συντονισμού. Αν και αρκετές επιχειρήσεις χρησιμοποιούν επί πολλά χρόνια ενδοδίκτυα ή αλλιώς εσωτερικά δίκτυα για τη διαχείριση και το συντονισμό των εσωτερικών επιχειρησιακών διεργασιών τους, τα ενδοδίκτυα μετατρέπονται με γοργό ρυθμό η τεχνολογία που επιλέγουν για την επιχειρηματική τους δραστηριότητα[1].

[1] Ηλεκτρονικό Εμπόριο Αρσένης Πασχόπουλος και Παναγιώτης Σκαλτσάς Εκδόσεις Κλειδάριθμος

Αναλυτικότερα, τα ενδοδίκτυα έχουν χαμηλό κόστος, δυνατότητα επέκτασης ή συρρίκνωσης όταν οι ανάγκες της εταιρίας αλλάζουν και η πρόσβαση σε αυτά είναι δυνατό να πραγματοποιείται από τα περισσότερα υπολογιστικά περιβάλλοντα. Οι περισσότερες εταιρίες, και ιδιαίτερα οι μεγάλες, είναι υποχρεωμένες να υποστηρίζουν μια πλειάδα από υπολογιστικά περιβάλλοντα τα οποία δεν μπορούν να επικοινωνούν μεταξύ τους, τα ενδοδίκτυα εξασφαλίζουν άμεση συνδεσιμότητα και ενοποιούν όλους τους υπολογιστές σε ένα, πρακτικά ενιαίο, σύστημα δικτύου.

Το λογισμικό του Ιστού παρουσιάζει μια ομοιόμορφη διασύνδεση, η οποία μπορεί να χρησιμοποιηθεί για την ενοποίηση πολλών διαφορετικών διεργασιών και συστημάτων σε ολόκληρη την εταιρία. Οι επιχειρήσεις είναι σε θέση να συνδέουν το εσωτερικό δίκτυό τους με τις βάσεις δεδομένων τους, δίνοντας τη δυνατότητα στο προσωπικό τους να συμμετέχει στις κεντρικές λειτουργίες τους.

Τα intranets βοηθούν τους οργανισμούς να δημιουργήσουν ένα πλουσιότερο περιβάλλον πληροφοριών, που να ανταποκρίνεται αποτελεσματικότερα και αποδοτικότερα στις ανάγκες τους. Οι εσωτερικές εταιρικές εφαρμογές που βασίζονται σε μοντέλα ιστοσελίδας μπορούν να γίνουν αλληλεπιδραστικές με τη χρήση ποικιλίας μέσων, κειμένου, ήχου και εικόνας.

Η κυριότερη χρήση των intranets είναι η δημιουργία ηλεκτρονικών – δικτυακών αποθηκών πληροφοριών, που μπορούν να ενημερώνονται όσο και όποτε απαιτείται. Κατάλογοι προϊόντων, εγχειρίδια για το προσωπικό, τηλεφωνικοί κατάλογοι ή πληροφορίες παροχών είναι δυνατό να ενημερώνονται αμέσως μετά τη διενέργεια οποιασδήποτε μεταβολής. Αυτή η οδηγούμενη από συμβάντα δημοσίευση επιτρέπει στους οργανισμούς να ανταποκρίνονται πιο γρήγορα σε μεταβαλλόμενες συνθήκες από ότι η παραδοσιακή πρακτική (σε χαρτί), η οποία προϋποθέτει ένα πιο δύσκαμπτο πρόγραμμα παραγωγής. Τα έγγραφα που διατίθενται μέσω των ενδοδικτύων μπορούν να είναι πάντοτε ενημερωμένα, χωρίς κόστος χαρτιού, εκτύπωσης και διανομής.

Σε εταιρίες που έχουν ήδη εγκατεστημένη υποδομή δικτύων, η εγκατάσταση και λειτουργία ενδοδικτύων έχει ελάχιστο κόστος. Με τα εργαλεία ανάπτυξης ιστοσελίδων, ο προγραμματισμός τους είναι απλός και εύκολος. Τα εσωτερικά δίκτυα διαθέτουν καθολικό σύστημα ηλεκτρονικού ταχυδρομείου, η πρόσβαση σε αυτά μπορεί να γίνεται από απόσταση, περιλαμβάνουν εργαλεία ομαδικής εργασίας, ηλεκτρονική βιβλιοθήκη, συστήματα κοινής χρήσης

εφαρμογών και δίκτυο εταιρικής επικοινωνίας. Ο ακόλουθος πίνακας συνοψίζει τα οφέλη που απολαμβάνουν οι οργανισμοί από τη χρήση intranets[2].

Οφέλη Χρήσης Ενδοδικτύων από Οργανισμούς	
1.	Συνδεσιμότητα: δυνατότητα πρόσβασης από τα περισσότερα υπολογιστικά περιβάλλοντα
2.	Μπορούν να συνδεθούν με συστήματα και βάσεις δεδομένων συναλλαγών
3.	Έχουν τη δυνατότητα δημιουργίας αλληλεπιδραστικών εφαρμογών με κείμενο, εικόνα και ήχο
4.	Μπορούν να επεκτείνονται ή συρρικνώνονται όταν αλλάζουν οι ανάγκες
5.	Έχουν εύχρηστη και ομοιόμορφη διασύνδεση περιήγησης στον ιστό
6.	Το αρχικό κόστος τους είναι χαμηλό
7.	Το περιβάλλον πληροφοριών είναι πλουσιότερο
8.	Μειώνουν το κόστος διανομής – διάχυσης πληροφοριών

Πηγή: Laudon & Laudon, "Management Information Systems", σελ. 297

Επιπρόσθετα, τα εσωτερικά δίκτυα και οι άλλες συναφείς τεχνολογίες περιέχουν ένα αρκετά μεγάλο σύνολο εργαλείων για τη δημιουργία περιβάλλοντος συνεργασίας, στα πλαίσια του οποίου τα μέλη ενός οργανισμού μπορούν να ανταλλάσσουν ιδέες, να χρησιμοποιούν από κοινού πληροφορίες και να συνεργάζονται σε κοινά έργα και αναθέσεις εργασίας, ανεξάρτητα από τον τόπο της φυσικής – γεωγραφικής θέσης τους. Σε αυτά τα εργαλεία περιλαμβάνεται το ηλεκτρονικό και φωνητικό ταχυδρομείο, το φαξ, η τηλεδιάσκεψη και εικονοδιάσκεψη, το λογισμικό συλλογικής χρήσης, τα συστήματα ομιλίας, οι ομάδες ειδήσεων.

Εφαρμογές Ενδοδικτύων για Ηλεκτρονική Επιχειρηματική Δραστηριότητα

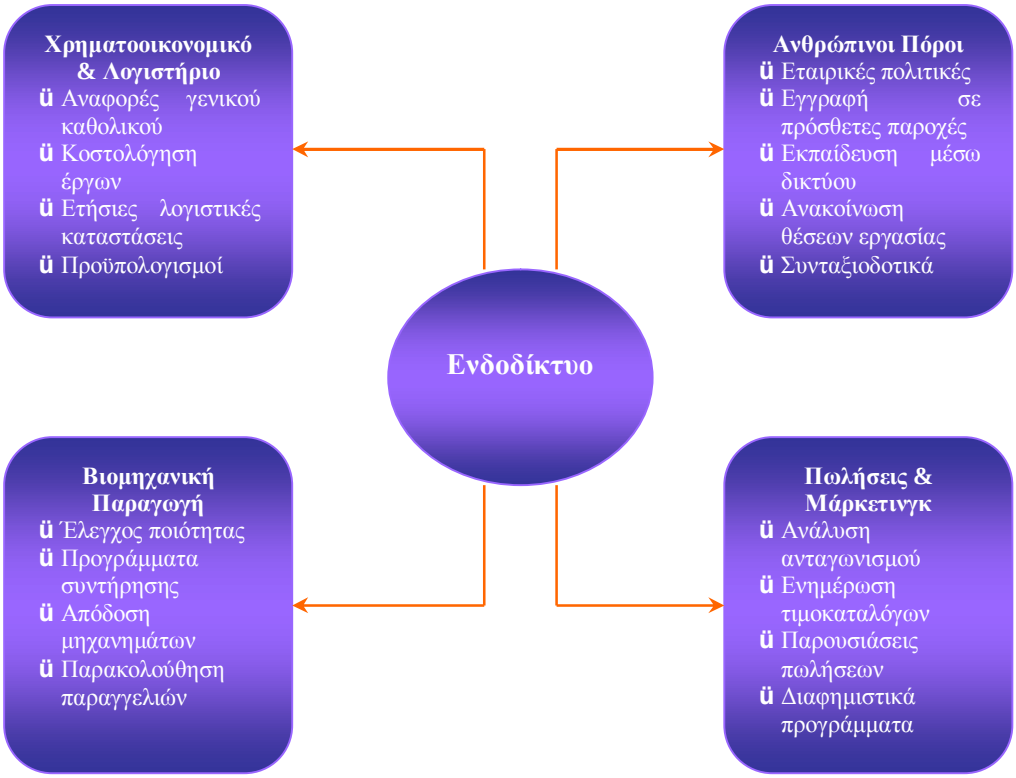
Τα ενδοδίκτυα εξαπλώνονται συνεχώς σε όλους τους κύριους τομείς των επιχειρήσεων και επιτρέπουν την ηλεκτρονική διαχείριση όλο και περισσότερων επιχειρηματικών διεργασιών. Η ακόλουθη εικόνα απεικονίζει μερικές εφαρμογές εσωτερικών δικτύων που έχουν

2 K.C. Laudon, J.P. Laudon, "Management Information Systems", εκδόσεις Κλειδάριθμος, 2002

αναπτυχθεί για τη χρηματοοικονομική διαχείριση και το λογιστήριο, τους ανθρώπινους πόρους, τις πωλήσεις και το μάρκετινγκ και τη βιομηχανική παραγωγή[3].

Σχήμα 1

Λειτουργικές Εφαρμογές Ενδοδικτύων



Πηγή: Laudon & Laudon, "Management Information Systems", σελ. 298

Χρηματοοικονομική Διοίκηση & Λογιστήριο: Πολλοί οργανισμοί διαθέτουν εκτεταμένα συστήματα επεξεργασίας συναλλαγών, που συλλέγουν λειτουργικά δεδομένα για τις οικονομικές δραστηριότητες τους, διότι τα παραδοσιακά συστήματα διοικητικών αναφορών τους (π.χ. συστήματα γενικού καθολικού, λογιστικά φύλλα), δεν περιέχουν το βαθμό λεπτομέρειας που απαιτείται για τη λήψη αποφάσεων και τη μέτρηση της απόδοσης. Τα ενδοδίκτυα μπορεί να αποδειχθούν πολύτιμα για τη χρηματοοικονομική διοίκηση και το λογιστήριο γιατί είναι σε θέση να παρέχουν ολοκληρωμένη εικόνα των οικονομικών και λογιστικών πληροφοριών, μέσω του δικτύου και σε μορφή εύχρηστη (βλ. Πίνακα 1 παραρτήματος).

3 K.C. Laudon, J.P. Laudon, "Management Information Systems", εκδόσεις Κλειδάριθμος, 2002

Ανθρώπινοι Πόροι: Μια από τις κύριες αρμοδιότητες του τμήματος ανθρωπίνων πόρων είναι να παρέχουν πληροφορίες στο προσωπικό για ζητήματα της εταιρίας, καθώς και να διατηρούν αρχεία με στοιχεία του προσωπικού και των πρόσθετων παροχών των υπαλλήλων. Μπορούν λοιπόν να χρησιμοποιηθούν εσωτερικά δίκτυα για τη δημοσίευση σε αυτά των εγχειριδίων με τις εταιρικές πολιτικές, τις ανακοινώσεις κενών θέσεων εργασίας και των εσωτερικών μετακινήσεων, τους εταιρικούς τηλεφωνικούς καταλόγους και τα προγράμματα εκπαίδευσης. Το προσωπικό από την άλλη, μπορεί να χρησιμοποιεί το ενδοδίκτυο για να δηλώνει συμμετοχή στην υγειονομική περίθαλψη, σε συνταξιοδοτικά και άλλα προγράμματα πρόσθετων παροχών ή να παίρνει μέρος σε εξετάσεις επάρκειας. Η διεύθυνση ανθρώπινων πόρων μπορεί να ανακοινώνει έγκαιρα στο προσωπικό τα προγραμματισμένα γεγονότα ή θέματα της εταιρίας μέσω ομάδων ειδήσεων ή με το ηλεκτρονικό ταχυδρομείο (βλ. Πίνακα 2 παραρτήματος).

Πωλήσεις & Μάρκετινγκ: Οι νέες τεχνολογίες πληροφορικής και επικοινωνίας μπορούν επίσης να χρησιμοποιηθούν για την εσωτερική διοίκηση – παρακολούθηση των διαδικασιών πωλήσεων και μάρκετινγκ. Μια από τις πιο δημοφιλείς εφαρμογές των εταιρικών ενδοδικτύων είναι η επίβλεψη και ο συντονισμός του προσωπικού πωλήσεων. Οι πωλητές έχουν τη δυνατότητα να συνδέονται στο σύστημα δικτύου και να ενημερώνονται για τις τιμές, τα προγράμματα προώθησης πωλήσεων, τις εκπτώσεις ή τους πελάτες και να αντλούν πληροφορίες σχετικά με τον ανταγωνισμό. Μπορούν ακόμα, να έχουν πρόσβαση σε παρουσιάσεις και έγγραφα πωλήσεων και να τα προσαρμόζουν στις ανάγκες των εκάστοτε πελατών (βλ. Πίνακα 3 παραρτήματος).

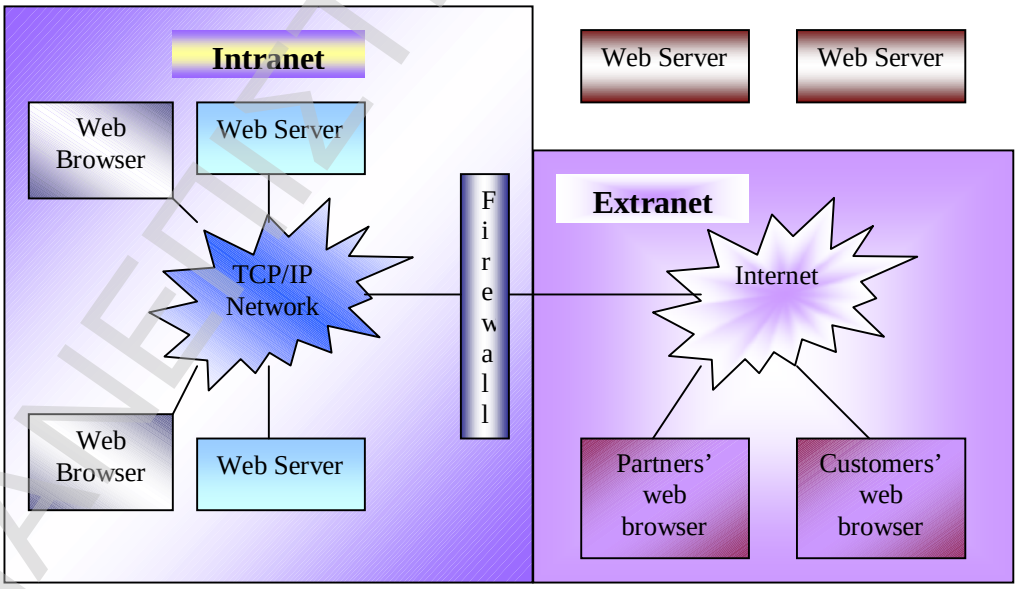
Βιομηχανική Παραγωγή: Στη βιομηχανία τα ζητήματα διαχείρισης πληροφοριών είναι περίπλοκα και περιλαμβάνουν ογκώδεις καταλόγους μηχανημάτων, συγκέντρωση και ενσωμάτωση ροών δεδομένων παραγωγής σε πραγματικό χρόνο, αλλαγή σχέσεων με προμηθευτές και παρακολούθηση των μεταβλητών εξόδων. Η βιομηχανική λειτουργία κατά κανόνα χρησιμοποιεί πολλούς τύπους δεδομένων, συμπεριλαμβανομένου γραφικών και εικόνων, τα οποία είναι διασκορπισμένα σε αρκετά ανόμοια συστήματα. Οι πληροφορίες της βιομηχανικής παραγωγής είναι συνήθως πολύ ευαίσθητες στο χρόνο και δύσκολο να ανακτηθούν επειδή τα αρχεία συνεχώς πρέπει να ενημερώνονται. Η ανάπτυξη εσωτερικών δικτύων που ενοποιούν τα βιομηχανικά δεδομένα σε μια ομοιόμορφη διασύνδεση χρήστη είναι πιο σύνθετη από ότι στους άλλους λειτουργικούς τομείς.

Παρά την ύπαρξη αυτών των δυσκολιών, οι εταιρίες εγκαθιστούν εφαρμογές ενδοδικτύων στο βιομηχανικό τους κλάδο. Τα intranets συντονίζουν τη ροή πληροφοριών μεταξύ των μερών ενός συστήματος παραγωγής, με αποτέλεσμα οι πληροφορίες να γίνονται πιο προσιτές στα διάφορα τμήματα του οργανισμού, να αυξάνεται η ακρίβεια και να μειώνεται το κόστος (βλ. Πίνακα 4 παραρτήματος).

Τα υπερενδοδίκτυα ή extranets από την άλλη, είναι ιδιωτικά δίκτυα που χρησιμοποιούν πρωτόκολλα Διαδικτύου και δημόσια συστήματα τηλεπικοινωνιών, έτσι ώστε ασφαλώς να μοιράζεται μερική πληροφόρηση ανάμεσα σε έναν οργανισμό και τους προμηθευτές της, τους πωλητές, τους εταίρους, τους πελάτες ή άλλους οργανισμούς. Ένα υπερενδοδίκτυο αποτελεί το μέρος του ενδοδικτύου της επιχείρησης, που επεκτείνεται στους χρήστες εκτός από τα όρια αυτής. Τα extranets απαιτούν ασφάλεια, που επιτυγχάνεται από την εγκατάσταση και χρήση firewalls, ψηφιακά πιστοποιητικά ή άλλα παρόμοια μέσα πιστοποίησης χρήστη, κρυπτογράφησης μηνυμάτων και εικονικών ιδιωτικών δικτύων (Virtual Private Networks) (Shim 2000). Το ακόλουθο σχήμα απεικονίζει τις σχέσεις ανάμεσα στο Internet, intranets και extranets[4].

Σχήμα 2

Σχέσεις μεταξύ Internet, intranet & extranet



Πηγή: King D., "Intranets: An Internet Inside the Organization", σελ. 530

4 King D., "Intranets: An Internet inside the Organization", 2000

2.4 Ηλεκτρονικό Εμπόριο

2.4.1 Ορισμός Ηλεκτρονικού Εμπορίου

Θα μπορούσαμε να πούμε πως δεν υφίσταται ένας ορισμός που να αποδίδει πλήρως το περιεχόμενο του ηλεκτρονικού εμπορίου. Κατά καιρούς αρκετοί είναι αυτοί που έχουν επιχειρήσει να περιγράψουν το περιεχόμενό του. Μερικοί από τους πιο ευρέως διαδεδομένους ορισμούς παραθέτονται ακόλουθα:

Μια νέα προσέγγιση στην διαδικασία προμήθειας εφοδίων και υπηρεσιών, χρησιμοποιώντας τεχνολογία πληροφοριακών συστημάτων (Fischer 1999, σελ. 12-13).

Κάθε επιχείρηση που διεκπεραιώνει τις λειτουργίες της ηλεκτρονικά, συμπεριλαμβανομένου της διεξαγωγής έρευνας αγοράς, την αναγνώριση ευκαιριών και εταίρων, την καλλιέργεια σχέσεων με τους προμηθευτές και τους πελάτες, την ανταλλαγή εγγράφων και τον από κοινού σχεδιασμό προϊόντων (Cameron 1997, σελ. 6).

Η αγοραπωλησία πληροφοριών, προϊόντων και υπηρεσιών μέσω δικτύων υπολογιστών.Το ηλεκτρονικό εμπόριο και το Διαδίκτυο δημιουργούν μια νέα αγορά με νέα επιχειρηματικά μοντέλα. Το πεδίο του ηλεκτρονικού εμπορίου, ανάλογα με τη φύση της συναλλαγής διακρίνεται σε ηλεκτρονικό εμπόριο:

1. Επιχείρησης προς Επιχείρηση (Business to Business): συναλλαγές μεταξύ δύο επιχειρήσεων, που αφορούν την ηλεκτρονική παραγγελία και οικονομική συναλλαγή διαμέσου τηλεπικοινωνιακών δικτύων.

2. Επιχείρησης προς Καταναλωτή (Business to Customer): η εφαρμογή αυτή αναφέρεται στην ηλεκτρονική παραγγελία, αγορά και πληρωμή, μέσω του Διαδικτύου και απευθύνεται πλέον στην παγκόσμια καταναλωτική κοινότητα.

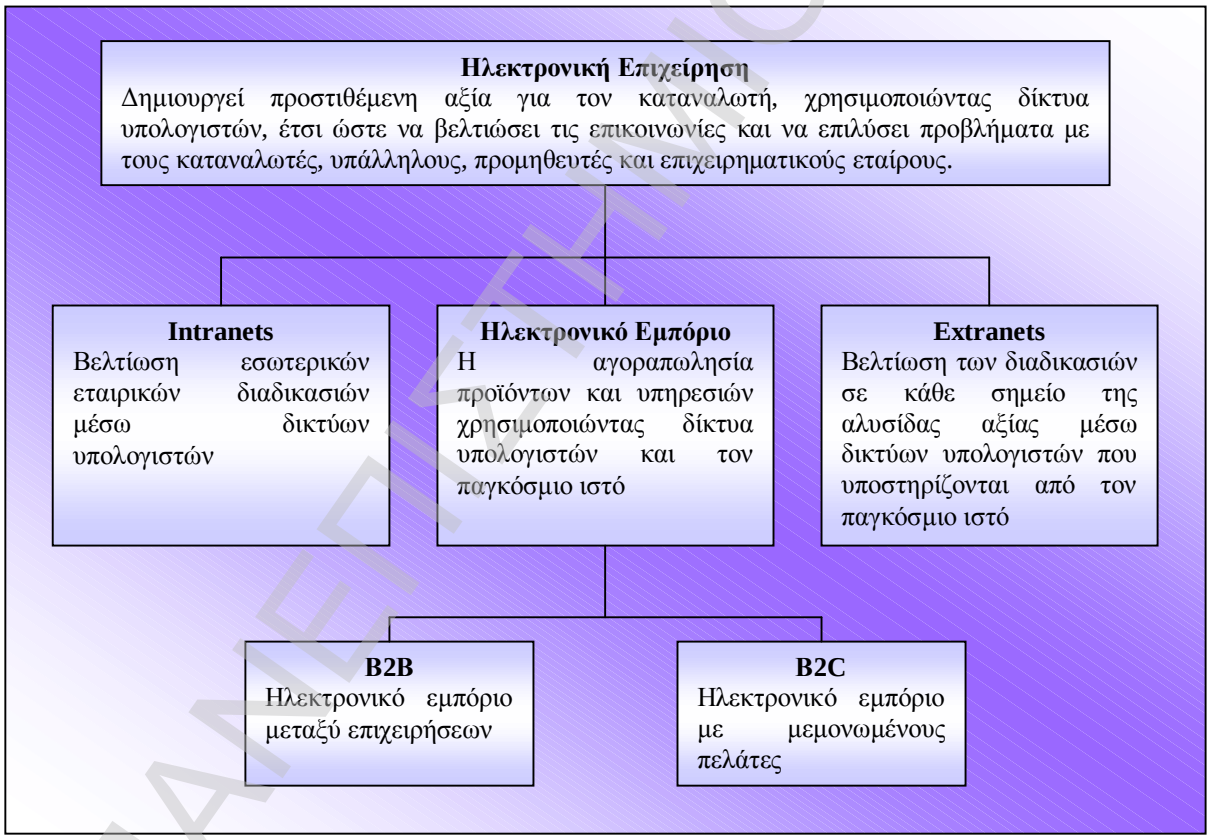
3. Επιχειρήσεων προς Δημόσιους Φορείς (Business to Public Administration): περιλαμβάνει ηλεκτρονικές συναλλαγές, όπως επεξεργασία φόρου εισοδήματος ή άλλων υποχρεώσεων μεταξύ ιδιωτικών εταιρειών και δημόσιων φορέων.

4. Δημόσιων Φορέων προς Πολίτες (Public Administration to Citizen): βρίσκεται σε νηπιακή ηλικία ακόμα, αλλά με την ανάπτυξη και τις εφαρμογές της αναμένεται να μεταβάλλει ουσιαστικά το τοπίο του ηλεκτρονικού εμπορίου στο μέλλον.

Οι παραπάνω διακρίσεις είναι σημαντικές αφού κάθε κατηγορία ηλεκτρονικού εμπορίου έχει διαφορετικές πληροφοριακές και τεχνολογικές απαιτήσεις για την εφαρμογή του.

Σχήμα 3

Ηλεκτρονικοί Ορισμοί



Πηγή: The Economist Intelligence Units (EIU)

2.4.2 Επιχείρηση προς Επιχείρηση (B2B) Ηλεκτρονικό Εμπόριο

Το ηλεκτρονικό εμπόριο αυτής της κατηγορίας αποτελεί την ηλεκτρονική διοίκηση – διαχείριση ολόκληρης της επιχειρηματικής δραστηριότητας, του κύκλου ζωής των προϊόντων και των καταναλωτών, από το μάρκετινγκ, τις παραγγελίες και τις πωλήσεις μέχρι την κατασκευή, τη διανομή, την εξυπηρέτηση πελατών και των ανεφοδιασμό των αποθηκών.

Η πρώτη ολοκληρωμένη προσέγγιση ηλεκτρονικού εμπορίου B2B ήταν η ηλεκτρονική ανταλλαγή δεδομένων (EDI). Μόνο 300.000 οργανισμοί παγκοσμίως έχουν υιοθετήσει EDI, λόγω τόσο της πολυπλοκότητας τους όσο και της πολυδάπανης εγκατάστασής τους[5].

Ο κύριος στόχος των εφαρμογών ηλεκτρονικού εμπορίου B2B είναι να εξαλείψει, όσο το δυνατόν, τις παραδοσιακές (χειρόγραφες) διαδικασίες, με το να επιτρέπει σε εσωτερικές εφαρμογές διαφορετικών οργανισμών να συνδέονται απευθείας και να πραγματοποιείται η ηλεκτρονική ανταλλαγή των πληροφοριών.

Οι παρεχόμενες εφαρμογές ηλεκτρονικού εμπορίου B2B είναι οι:

- Έλεγχος Διάχυσης Εγγράφων: Το ηλεκτρονικό εμπόριο βελτιώνει τον τρόπο με τον οποίο τα ναυτιλιακά έγγραφα, οι παραγγελίες προμηθειών, οι φορτωτικές και οι απαιτήσεις μεταβιβάζονται. Επιπρόσθετα, μέσω των εφαρμογών αυτών οι πληροφορίες των εγγράφων είναι περισσότερο ακριβείς και επίκαιρες.
- Διαχείριση Αποθηκών: Με τις εφαρμογές του ηλεκτρονικού εμπορίου, ο χρόνος που μεσολαβεί ανάμεσα στις παραγγελίες και την αποστολή των εμπορευμάτων μειώνεται. Οι πληροφορίες που σχετίζονται με την κατάσταση των αποθηκών μεταδίδονται – μεταβιβάζονται αυτόματα. Υπάρχει καλύτερη παρακολούθηση και επομένως έλεγχος των εγγράφων που σχετίζονται με τα φορτία και τις αποθήκες. Ως αποτέλεσμα αυτών, ο αριθμός των αποθηκών που μια επιχείρηση διατηρεί μπορεί να μειωθεί, όπως επίσης και ο όγκος των αποθεμάτων.

[5] J. Ricker, D. Munro & D. Hopeman, “XML and EDI: Peaceful Co-Existence”, 2000.

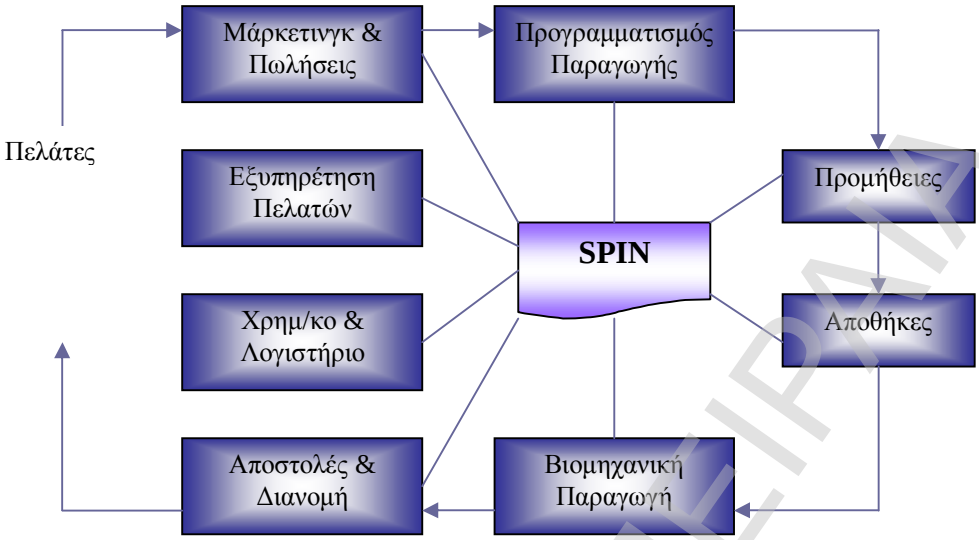
- Με τις νέες αυτές τεχνολογίες πληροφορικής και επικοινωνίας μπορούν ευκολότερα και αποτελεσματικότερα να αναπτυχθούν ηλεκτρονικές εφαρμογές εφοδιαστικής διαχείρισης (just-in-time logistics). Έτσι, τα εμπορεύματα παραγγέλνονται τη στιγμή που χρειάζονται στην παραγωγική διαδικασία, δεν υπάρχει ακινητοποιημένο κεφάλαιο και οι οργανισμοί μπορούν να εξοικονομήσουν πόρους για η χρηματοδότηση άλλων επιχειρηματικών δραστηριοτήτων.
- Σχέσεις με Προμηθευτές: Το ηλεκτρονικό εμπόριο και οι εφαρμογές του μπορούν να μειώσουν τον αριθμό των προμηθευτών, με τους οποίους η επιχείρηση συνεργάζεται, όσο και το κόστος παραγγελίας. Λιγότερο υπαλληλικό προσωπικό απαιτείται στη διαδικασία παραγγελίας προμηθειών και ο κύκλος ζωής του προϊόντος μειώνεται.
- Διαχείριση Πληρωμών: Συνδέοντας ηλεκτρονικά τις επιχειρήσεις με τους προμηθευτές και τους διανομείς, επιτυγχάνεται η ηλεκτρονική – αυτόματη μεταβίβαση πληρωμών, η οποία συνεπάγεται ορθότερο υπολογισμό τιμολογίων, γρηγορότερη έκδοσή τους και χαμηλότερο κόστος συναλλαγών.
- Διαχείριση Καναλιών Διανομής: στην κοινωνία της πληροφορίας που ζούμε, οι αλλαγές στις συνθήκες τις αγοράς ανακοινώνονται γρηγορότερα ανάμεσα στα εμπλεκόμενα μέρη, από ότι στο παρελθόν. Σε ένα ηλεκτρονικό πίνακα ανακοινώσεων είναι δυνατό να αναρτηθούν πληροφορίες σχετικές με τις τιμές, τις διαθέσιμες ποσότητες, τις παρεχόμενες υπηρεσίες και τις τεχνικές προδιαγραφές.

Για να καταστούν σαφέστερα τα παραπάνω, παραθέτουμε ακόλουθα ένα σχήμα όπου απεικονίζεται η ηλεκτρονική εφαρμογή διαχείρισης της αλυσίδας εφοδιασμού της Chrysler[6].

Σχήμα 4

Η Εφαρμογή SPIN της Chrysler

6 K.C. Laudon, J.P. Laudon, "Management Information Systems", εκδόσεις Κλειδάριθμος, 2002



Πηγή: Laudon & Laudon, "Management Information Systems", σελ. 301

Η εφαρμογή SPIN (Supplier Partner Information Network) είναι ένα σύστημα διαχείρισης αλυσίδας εφοδιασμού που ανέπτυξε η Chrysler. Το SPIN δίνει τη δυνατότητα σε 3.500 από τους 12.000 προμηθευτές της να έχουν επιλεκτική πρόσβαση σε πληροφορίες, όπου μπορούν να αναζητούν τα πιο πρόσφατα δεδομένα αλλαγών σχεδίων, ελλείψεις εξαρτημάτων, πληροφορίες συσκευασίας και παρακολούθηση τιμολογίων.

Η Chrysler θεωρεί ότι με τον εκσυγχρονισμό της παράδοσης προϊόντων και τη μείωση του χρόνου επικοινωνίας των αλλαγών σε διεργασίες ή σχέδια, το SPIN μείωσε το χρόνο ολοκλήρωσης διαφόρων επιχειρηματικών διεργασιών κατά 25 με 50%. Η Chrysler μπορεί να χρησιμοποιήσει τις πληροφορίες που εμπεριέχονται στο σύστημα για την αποδοτικότερη διεύθυνση του υπαλληλικού προσωπικού της. Μια εφαρμογή παρακολούθησης κρίσιμων εξαρτημάτων επιτρέπει την εναλλαγή καθηκόντων του εργατοτεχνικού προσωπικού, έτσι ώστε να μην παρατηρούνται ελλείψεις και να σταματούν οι γραμμές συναρμολόγησης.

Η εταιρία πρόσθεσε και την παρακολούθηση τιμολογίων στο σύστημα, ώστε οι υπάλληλοι να μην χάνουν χρόνο σε τηλεφωνήματα προμηθευτών με ερωτήσεις σχετικά με την πληρωμή τους. Το SPIN αναθεωρήθηκε για να περιλάβει το ιδιωτικό σύστημα ηλεκτρονικής ανταλλαγής δεδομένων και την τεχνολογία προώθησης της Chrysler. Το SPIN μπορεί να ειδοποιεί αυτόματα τους προμηθευτές σε περίπτωση έλλειψης ζωτικών εξαρτημάτων. Εκτός από τη μείωση

του κόστους, το SPIN συμβάλλει στην καλύτερη εξυπηρέτηση των πελατών της επιτρέποντας στις λειτουργίες της επιχείρησης να καθοδηγούνται από τη ζήτηση των πελατών.

Τα παλαιότερα συστήματα διαχείρισης της εφοδιαστικής αλυσίδας καθοδηγούνταν από γενικά προγράμματα παραγωγής που βασίζονταν σε προβλέψεις και εκτιμήσεις της ζήτησης των προϊόντων. Με τις νέες ροές πληροφοριών η διαχείριση της αλυσίδας εφοδιασμού μπορεί να ακολουθεί το μοντέλο καθοδήγησης από τη ζήτηση.

2.5 Το Ηλεκτρονικό Εμπόριο στη Ναυτιλία

Οι παραδοσιακές ναυτιλιακές επιχειρήσεις μετασχηματίζονται ριζικά από την αλματώδη πρόοδο των τεχνολογιών επικοινωνίας, που επιφέρουν από τη μια τη δημιουργία νέας ζήτησης και από την άλλη παρέχουν τα απαραίτητα εργαλεία έτσι ώστε οι επιχειρήσεις να αναδομηθούν και να ανταποκριθούν στη ζήτηση αυτή. Οι τεχνολογίες επικοινωνίας όπως το Διαδίκτυο και οι τεχνολογίες πληροφορικής όπως η γλώσσα προγραμματισμού XML επιτρέπουν τη συλλογή και διάχυση των πληροφοριών εύκολα, γρήγορα και με μικρότερο κόστος.

Διάφοροι συγγραφείς υποστηρίζουν ότι τα πλεονεκτήματα που απορρέουν από τη χρήση του Internet για τους ναυλομεσίτες αναφέρονται στον επακριβή προσδιορισμό των αναγκών των φορτωτών. Επιπρόσθετα, οι υπηρεσίες που οι ναυλομεσίτες παρέχουν μπορούν να βελτιωθούν μέσω των διανεμημένων πληροφοριών για ιδιαίτερα πλοία και φορτία, πλοιοκτήτες και μεταφορείς.

Παρόλα αυτά, οι ψηφιακές αγορές αναφαίνονται ως κόμβοι συναλλαγών και ανταλλαγής πληροφοριών στη ναυτιλιακή βιομηχανία. Η εμφάνιση αυτών των αγορών έχει εκτεταμένη επίδραση στη ναυτιλία, επιτρέποντας την εύκολη διεκπεραίωση των συναλλαγών ανάμεσα στους επιχειρηματικούς εταίρους. Οι ναυτιλιακές επιχειρήσεις μπορούν να επωφεληθούν από την ανάπτυξη αυτών των τεχνολογιών συμμετέχοντας σε αυτές τις αγορές, έτσι ώστε να μειώσουν τα λειτουργικά τους έξοδα, να αναγνωρίσουν νέους συνεργάτες και να βελτιώσουν την αποτελεσματικότητα τους από τη εύκολη πρόσβαση στην αγορά.

2.5.1 Κατηγοριοποίηση των Portals στη Ναυτιλιακή Βιομηχανία

Τα Portals προσφέρουν μια ενοποιημένη εικόνα μιας μεγάλης ποικιλίας περιεχομένων στους χρήστες τους. Τέτοιου είδους περιεχόμενα παρέχουν στους χρήστες πρόσβαση σε διαφόρων ειδών πληροφορίες, εφαρμογές και άλλες υπηρεσίες. Παρέχοντας πρόσβαση σε πληροφορίες που είναι σχετικές με τις προτιμήσεις των χρηστών, τα Portals μετατρέπονται σε one stop υπηρεσία για την πρόσβαση σε πληροφορίες του Διαδικτύου και των Ενδοδικτύων. Η βασική αρχή σχεδίασης των portals είναι να παρέχουν στους χρήστες του Internet και των Intranets πρόσβαση σε υγιείς πληροφορίες και υπηρεσίες ηλεκτρονικού εμπορίου προσφέροντας συνδέσμους σε άλλους συναφείς δικτυακούς τόπους και εφαρμογές.

Ο βασικός στόχος δημιουργίας και ανάπτυξης των portals είναι η μείωση του χρόνου που οι χρήστες απαιτείται να δαπανήσουν για την άντληση εκείνων των πληροφοριών που είναι απαραίτητες για την διεκπεραίωση των καθηκόντων τους (Rajput E. 2000).

Στην ναυτιλιακή βιομηχανία απατούνται τριών ειδών portals: α) πληροφοριακά portals, β) online ναυλώσεων portals και γ) portals προμηθειών εφοδίων συμπεριλαμβανομένου και καυσίμων.

2.5.1.1 Πληροφοριακά Portals

Αυτή η κατηγορία προσφέρει μια ποικιλία υπηρεσιών όπως online ναυτιλιακά νέα, δεδομένα για τη ναυλαγορά και λίστες στόλων. Ο Πίνακας 2 παρουσιάζει μερικά από τα πιο αξιόλογα portals αυτής της κατηγορίας.

Πίνακας 2

Πληροφοριακά Portals
clarksons.net
fairplay.co.uk
infomarine.gr
Lloydslist.com
marinelink.com
marine-net.com
marinetalk.com
mgn.com
shipping-markets.com
tankerworld.com
tradewinds.no
tshipping.com

2.5.1.2 Portals Online Ναυλώσεων

Η βασική αρχή των online ναυλώσεων είναι να φέρουν σε επαφή τους προμηθευτές (στην προκειμένη περίπτωση πλοιοκτήτες) και τους πελάτες (στην προκειμένη περίπτωση ναυλωτές) κατά τρόπο αποτελεσματικό, προκειμένου να βρεθεί μια η όσο το δυνατόν αποδοτικότερη από πλευράς κόστους συμφωνία και για τα δύο μέρη. Ο Πίνακας 3 παρουσιάζει μερικά Online Portals Ναυλώσεων.

Αυτά τα portals παρέχουν στους πλοιοκτήτες, στους ναυλωτές και τους ναυλομεσίτες τη δυνατότητα να “ταιριάζουν” τις απαιτήσεις των φορτίων για κατάλληλα πλοία, να συλλέγουν

και να μοιράζουν πληροφορίες για την κατάσταση της αγοράς, καθώς και να διευκολύνουν την ανταλλαγή των απαραίτητων εγγράφων στη διαδικασία της ναύλωσης. Πέρα από αυτά, η πιο σημαντική υπηρεσία που προσφέρουν αρκετά από τα ναυτιλιακά portals είναι οι web – based πλειστηριασμοί.

Πίνακας 3

Λίστα Online Portals Ναυλώσεων	
AXSMarine.com	NetChartering.com
balticexchange.com	networkchartering.com
Cargobiz.com	portship.com
charteringsolutions.com	ratequery.com
Chinsay.com	seanet.co.uk
conconnect.com	shipbrokerexchange.com
CyVoyage.com	shipbrokering.com
e-bro.co.uk	ShipIQ.com
e-janworld.co.jp	ShippingDesk.com
enrononline.com	Shipping-direct.com
eshipbroker.com	shippingonthenet.com
globalfreightmarket.com	ship-search.com
Gotomar.com	ssyfutures.com
i-shipping.com	strategicimx.com
laycan.com	webshipbroker.com
Levelseas.com	worldfixture.com
marine-net.com	

2.5.1.3 Portals Προμηθειών Εφοδίων

Οι online προμήθειες αποτελούν την ηλεκτρονική προσφορά και παροχή αγαθών και υπηρεσιών. Στη ναυτιλία, τα portals προμηθειών επικεντρώνονται στην παροχή προμηθειών παρέχοντας ηλεκτρονικά εργαλεία που επιτρέπουν να πραγματοποιούνται οι αγορές εφοδίων επί του πλοίου. Ακόλουθα παρουσιάζονται μερικά από τα πιο αξιόλογα portals προμηθειών.

Πίνακας 4

Λίστα Online Portals Προμηθειών	
e4marine.com	quotegate.com
Eqsys.com	seainfo.com
ishipexchange.com	seavantage.com
line.net	setfair.com
marine-online.com	shipserv.com
marineprovider.com	shipvertical.com
primesupplier.net	

Τα portals αυτής της κατηγορίας παρέχουν στους πλοιοκτήτες σημαντικά πλεονεκτήματα όπως:

1. Αυξημένη παραγωγικότητα υπαλλήλων, αφού δεν σπαταλούν εργατοώρες προς εξεύρεση εφοδίων
2. Φθηνότερα εφόδια λόγω της εύκολης και γρήγορης σύγκρισης των τιμών

Από την πλευρά των πωλητών τα πλεονεκτήματα προέρχονται από τον αυξημένο όγκο πωλήσεων, το χαμηλότερο κόστος διανομής και διατήρησης αποθεμάτων. Σύμφωνα με το Lloyd's List μερικές επιχειρήσεις online προμηθειών όπως η ShipServ έχουν πραγματοποιήσει σημαντικά κέρδη, εκτελώντας το σύνολο των προμηθειών επιχειρήσεων όπως η Laurizen. Η συγκεκριμένη εταιρία έχει μειωμένα κόστη που σχετίζονται με τις προμήθειες της τάξεως του 8% ετησίως. Επιπλέον, η iShipExchange και η Shipserv είναι οι μόνες επιχειρήσεις που χαρακτηρίζονται ως "τέλειοι εταίροι" από τον International Ship Supplier Association[7].

Θα μπορούσαμε να πούμε πως για τους πλοιοκτήτες η δυνατότητα επιλογής από μια μεγάλη γκάμα προμηθευτών οδηγεί σε χαμηλότερο κόστος, καλύτερη ποιότητα, βελτιωμένη διανομή και εν κατακλείδι μειωμένο κόστος προμηθειών. "Οι ηλεκτρονικές προμήθειες στη

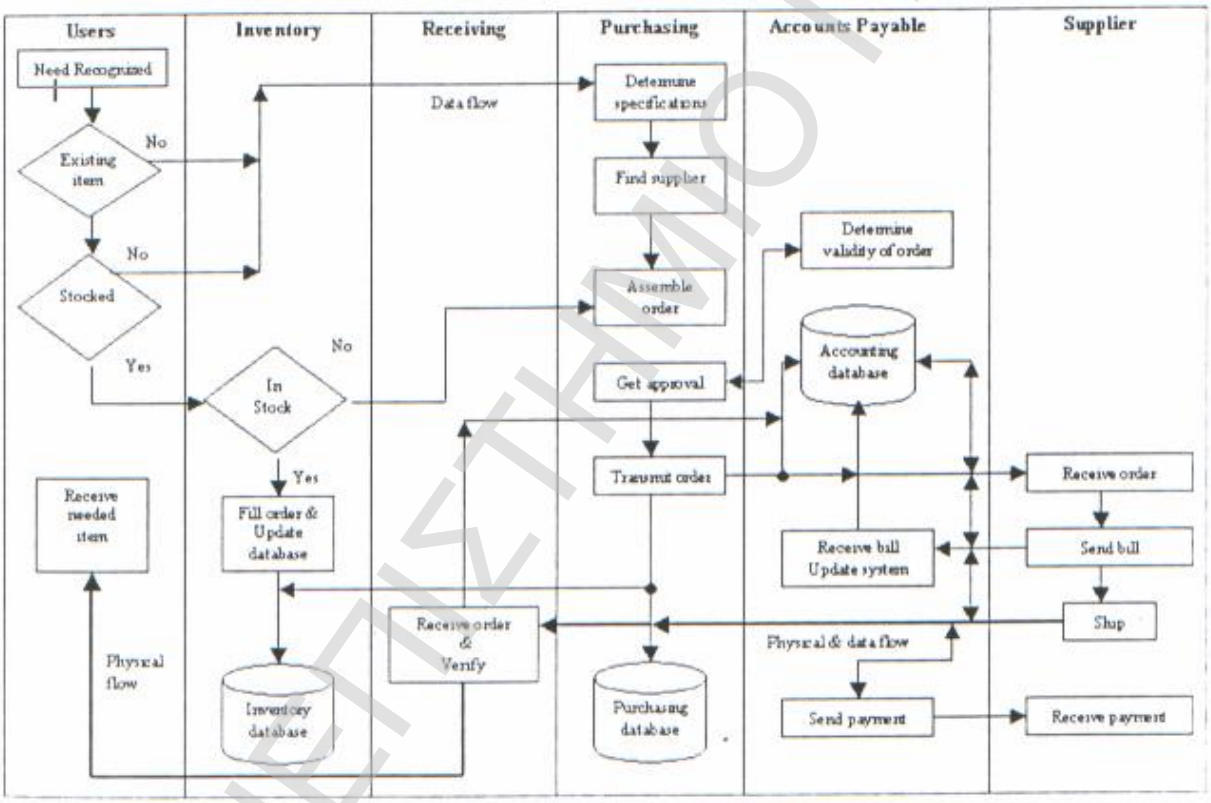
7Lloyd's List, 14/07/2001, "E-commerce Ventures Aim for a Sexier Identity".

ναυτιλία είναι η προφανής και απλή λύση της μείωσης του χρόνου που απαιτείται για να φθάσουν οι προμήθειες στο πλοίο"[8].

Επίσης, οι επιχειρήσεις ηλεκτρονικών προμηθειών παρέχουν τη δυνατότητα παραγγελιών επί του πλοίου. Το ακόλουθο σχήμα απεικονίζει τη ροή πληροφοριών και εφοδίων στη διαδικασία παραγγελίας προμηθειών.

Σχήμα 5

Γενικευμένη Εικόνα της Διαδικασίας Παραγγελίας Προμηθειών



Πηγή: Baron, 2000

Στην παραδοσιακή διαδικασία παραγγελίας προμηθειών, οι πληροφορίες μεταβιβάζονται και αλλάζουν μορφή αρκετές φορές. Κάθε μεταβίβαση και αλλαγή συνεισφέρει

8 Lloyd's List, 18/03/2000, "On the Crest of an E-Com Wave: Internet Mania is Sweeping through the Shipping Industry though some may be in Anger of Missing the Boat".

στην πιθανότητα αναποτελεσματικότητας και λάθους. Αυτοματοποιώντας τη διαδικασία παραγγελίας προμηθειών μέσω του ηλεκτρονικού εμπορίου, απλοποιείται η συνολική διαδικασία που επιφέρει αυξημένη αποτελεσματικότητα και μείωση της πιθανότητας λάθους.

Online Παραγγελία Καυσίμων

Εκτός από τα portals ηλεκτρονικών παραγγελιών εφοδίων, υπάρχουν και άλλα που εξειδικεύονται στις παραγγελίες καυσίμων. Ο πίνακας που ακολουθεί παρουσιάζει ορισμένα από αυτά. Ένα από τα πιο επιτυχημένα portals αυτής της κατηγορίας είναι το bunkerworld.com, το πιο πρόσφατα εισερχόμενο σε αυτή την αγορά, το οποίο έχει προσελκύσει ένα μεγάλο αριθμό χρηστών και παρέχει σε σταθερή βάση πληροφορίες για την κατάσταση της αγοράς και τις τιμές των καυσίμων.

Το Oceanconnect.com είναι ένας άλλος δικτυακός τόπος, οι δραστηριότητες του οποίου απατώνται σε ορισμένα στρατηγικά λιμάνια ανά την υφήλιο και που έχει δημιουργήσει σημαντικά κέρδη για τους επενδυτές του. Από τη θεωρία της Ναυτιλιακής Οικονομικής γνωρίζουμε πως ένα από τα μεγαλύτερα κόστη που επωμίζεται ο πλοιοκτήτης ή ο ναυλωτής, ανάλογα με το είδος της ναύλωσης, είναι τα καύσιμα. Από αυτό και μόνο το γεγονός, μπορούμε να αντιληφθούμε τον ζωτικής σημασίας ρόλο που διαδραματίζουν τα portals αυτά για τα εμπλεκόμενα μέρη.

Πίνακας 5

Λίστα Online Portals Παραγγελίας Καυσίμων
bunkerworld.com
eBunkers.com
oceanconnect.com
smartbunkers.net
transportedge.com

2.6 Ζητήματα & Εμπόδια στην Υιοθέτηση του Ηλεκτρονικού Εμπορίου

Αυτή η ενότητα του παρόντος κεφαλαίου αναφέρεται στα εμπόδια και τα ζητήματα που σχετίζονται με την υιοθέτηση ηλεκτρονικών εφαρμογών στην ναυτιλία, καθώς επίσης και με την εξεύρεση δυνητικών λύσεων για την άρση των εμποδίων αυτών.

Συνοπτικά τα ζητήματα που σχετίζονται με την ναυτιλιακή βιομηχανία είναι:

1. Νομικά
    - Ηλεκτρονικές Υπογραφές
    - Ψηφιακές Υπογραφές
    - Δικαιοδοσία
2. Ασφάλεια και Κοινά Πρότυπα
3. Υιοθέτηση από το Σύνολο της Αγοράς
4. Ζητήματα Υλοποίησης
5. Ζητήματα Κουλτούρας

2.6.1 Ηλεκτρονικές Υπογραφές

Η συνεχώς αυξανόμενη χρήση εφαρμογών ηλεκτρονικού εμπορίου σε όλες τις βιομηχανίες απαιτεί αλλαγές στις παραδοσιακές χειρόγραφες υπογραφές. Η Νομοθετική Πράξη: Ηλεκτρονικές Υπογραφές στο Παγκόσμιο και Εθνικό Εμπόριο με την ονομασία E-SIGN (Electronic Signature in Global and National Commerce Act), που υπογράφτηκε στις Ηνωμένες Πολιτείες της Αμερικής τον Οκτώβριο του 2000, κατοχυρώνει νομικά τις ηλεκτρονικές και ψηφιακές υπογραφές, πράγμα που σημαίνει ότι έχουν την ίδια νομική ισχύ με τις χειρόγραφες υπογραφές.

Σύμφωνα με το CIO Magazine, η παραπάνω πράξη ορίζει μια ηλεκτρονική υπογραφή ως “ένα ηλεκτρονικό ήχο, σύμβολο ή διαδικασία”, που εκτελείται ή υιοθετείται με σκοπό την υπογραφή ενός συμβολαίου ή εγγραφής και ο νόμος δεν δίνει παραδείγματα ή συγκεκριμένες τεχνολογίες. Η πράξη περιλαμβάνει ως ηλεκτρονικές υπογραφές τα πεδία κειμένου στο τέλος των e-mails, τα κουμπιά στα ηλεκτρονικά συμβόλαια, τις ψηφιοποιημένες εικόνες χειρόγραφων

υπογραφών, τα ονόματα των χρηστών και τα passwords τους (http://www.cio.com/archive/011501/fine.html).

Πιο συγκεκριμένα για τη ναυτιλία, η ενότητα 201 της παραπάνω νομοθετικής πράξης επιτρέπει την μεταβίβαση συμβολαίων και άλλων νόμιμων εγγράφων (π.χ. φορτωτικές) με τρόπο ηλεκτρονικό. Όμως, σύμφωνα πάντα με το νομοθέτημα αυτό, τα συμβόλαια και τα έγγραφα πρέπει να είναι σε μορφή τέτοια που να μπορούν να διατηρηθούν και επακριβώς να αναπαραχθούν για μελλοντική χρήση όλων των μερών που έχουν έννομο συμφέρον από τα έγγραφα αυτά. Αν αυτά τα πρότυπα δεν επιτευχθούν, η νομοθετική πράξη, η εγκυρότητα ή και ακόμα η επιβολή της, είναι δυνατόν να συναντήσει εμπόδια στην εφαρμογή της.

Από την πλευρά της Ευρωπαϊκής Ένωσης δημιουργήθηκε η Electronics Communication Act 2000, που εξασφαλίζει νομική παραδεκτότητα στις ψηφιακές υπογραφές, προκειμένου να υλοποιηθεί η Οδηγία Ηλεκτρονικών Υπογραφών της Ευρωπαϊκής Ένωσης (European Union's Electonic Signature Directive). Τα ηλεκτρονικά έγγραφα, γενικά, λαμβάνονται ως αποδεικτικά στοιχεία από τα Αγγλικά δικαστήρια, αρκεί να μην ανήκουν στην κατηγορία εγγράφων που υποχρεωτικά πρέπει να διατηρούνται σε χειρόγραφη μορφή (εκχωρητήρια).

2.6.2 Ψηφιακές Υπογραφές

Αξίζει να προχωρήσουμε σε μια πιο εκτενή ανάλυση των ψηφιακών υπογραφών καθώς όλα δείχνουν ότι μάλλον θα χρησιμοποιηθούν περισσότερο στις ναυτιλιακές επιχειρήσεις. Αναλυτικότερα, οι ψηφιακές υπογραφές αποτελούν ένα πολύπλοκο μηχανισμό κρυπτογράφησης, έτσι ώστε να διασφαλιστούν ασφαλείς επικοινωνίες και πιστοποίηση εγγράφων και υπογραφών. Βασικά, ένα έγγραφο υπογράφεται επισυνάπτοντας ένα κρυπτογραφημένο κείμενο με ένα ιδιωτικό κλειδί . Ο παραλήπτης μπορεί τότε να πιστοποιήσει την ταυτότητα του αποστολέα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Με αυτόν τον τρόπο τα εμπλεκόμενα μέρη ελαχιστοποιούν τον κίνδυνο της απάτης.

Οι ψηφιακές υπογραφές αναμένεται να παίξουν σημαντικό ρόλο στο ηλεκτρονικό εμπόριο και σε άλλους τομείς όπου τα προσωπικά δεδομένα, η εμπιστευτικότητα και η αυθεντικότητα είναι εξέχοντα ζητήματα. Η ναυτιλιακή βιομηχανία πιθανότερο είναι να

χρησιμοποιήσει τις ψηφιακές υπογραφές δεδομένης της ευαισθησίας και του όγκου των πληροφοριών που ανταλλάσσονται.

2.6.3 Δικαιοδοσία

Ένα πρόβλημα που είναι άμεσα συνυφασμένο με τις συναλλαγές μέσω του Διαδικτύου είναι αυτό της Δικαιοδοσίας, δηλαδή το δίκαιο που θα εφαρμοστεί στην περίπτωση που προκύψει κάποια απαίτηση από τα ενδιαφερόμενα μέρη. Τα ερωτήματα που γεννούνται εδώ είναι δύο:

1.που μια επιχείρηση είναι εγκατεστημένη στο web, και

2.που είναι εγκατεστημένος ο διακομιστής της επιχείρησης ή το διοικητικό κέντρο της κατά τη συμβατική έννοια

Έτσι, είναι σημαντικό να αναλογιστούμε την τοποθεσία των πελατών της επιχείρησης και να δηλώσουμε την επιλογή των νομικών διατάξεων που θα διέπουν τη σύμβαση.

Πάνω στο ζήτημα αυτό υπάρχουν κάποιες κατευθυντήριες οδηγίες, όπως για παράδειγμα το American Bar Association's Business Law Section, μέσω της Επιτροπής του για τον Νόμο που διέπει τον Κυβερνοχώρο (Committee on Cyberspace Law), έχει δημιουργήσει μια έκθεση με τον τίτλο "Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issued Created by the Internet". Έναν άλλο οδηγό αποτελεί η U.S. Uniform Computer Information Transaction Act (UCITA), που παρέχει κατευθυντήριες οδηγίες για τον προσδιορισμό των νόμων που θα διέπουν μια ηλεκτρονική συναλλαγή, στην περίπτωση που κάτι τέτοιο δεν έχει συμφωνηθεί από τα δύο μέρη.

2.6.4 Ασφάλεια & Κοινά Πρότυπα

Η ασφάλεια των συναλλαγών και η προστασία των προσωπικών δεδομένων των χρηστών είναι ένα φλέγων ζήτημα για την εξέλιξη του ηλεκτρονικού εμπορίου.

Σύμφωνα με τον Bloch, η ασφάλεια των συναλλαγών μπορεί να επιφέρει τις αντιδράσεις των προμηθευτών που χρησιμοποιούν τέτοια συστήματα ή των καταναλωτών που θα

αποφεύγουν τη χρήση αυτών των συστημάτων. Επιπλέον, θεωρεί ότι οι ανερχόμενες τεχνολογικές λύσεις και τα συστήματα ασφαλείας θα υπερπηδήσουν το πρόβλημα αυτό.

Κατά τους Gray και Igbaria ένα σύστημα ασφάλειας είναι επαρκές όταν:

1.διατηρείται η εμπιστευτικότητα στα εμπλεκόμενα μέρη μιας συναλλαγής

2.πιστοποιείται η αυθεντικότητα των μερών

3.παρέχεται η ακεραιότητα των δεδομένων

4.τα δεδομένα της συναλλαγής φυλάσσονται για μελλοντική νόμιμη χρήση

5.τρίτα μέρη δεν έχουν τη δυνατότητα να παρακολουθήσουν μια συναλλαγή

Επίσης, οι ίδιοι αναγνωρίζουν την ανάγκη για δημιουργία γενικών προτύπων, έτσι ώστε να επιλυθούν τα προβλήματα ασφάλειας συναλλαγών μέσω του Διαδικτύου.

Τα κοινά λειτουργικά πρότυπα και τα πρωτόκολλα είναι αυτά που επιτρέπουν στο Internet να λειτουργεί. Επί του παρόντος δεν υφίσταται ένα τυποποιημένο πλαίσιο για το ηλεκτρονικό εμπόριο ή έστω ένα πλαίσιο που να αναγνωρίζεται από την πλειοψηφία των ενδιαφερόμενων, έτσι ώστε εκ των πραγμάτων να θεωρείτε πρότυπο. Νεωτερισμοί, όπως το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HTTP) και η Γλώσσα Σημείωσης Υπερκειμένου (HTML) αποτελούν τη ραχοκοκαλιά του Διαδικτύου. Όμως καθώς οι οργανισμοί ολοένα και περισσότερο μεταβαίνουν από την παραδοσιακή στην ηλεκτρονική επιχείρηση, νέα πρότυπα και υποστηριχτηκές τεχνολογίες ζητούνται. Το Πρωτόκολλο Ασύρματης Εφαρμογής (WAP) και η Επεκτάσιμη Γλώσσα Σήμανσης (XML) είναι ορισμένα από αυτά τα νέα πρότυπα που μεταβάλλουν το Web. Παρά τις όποιες αλλαγές, παλαιότερες, αξιόπιστες όμως, τεχνολογίες, όπως η Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI) συνεχίζουν να υπηρετούν τις ηλεκτρονικές επιχειρήσεις.

2.6.4.1 Ηλεκτρονική Ανταλλαγή Δεδομένων

Αποτελεί την ανταλλαγή μηνυμάτων, που περιέχουν δεδομένα εμπορίου, έτσι ώστε τα εμπλεκόμενα μέρη να είναι σε θέση να ολοκληρώσουν μια συναλλαγή. Αυτή η τεχνολογία περιορίζει τις χειρόγραφες διαδικασίες, επιτρέποντας σε εσωτερικές εφαρμογές διαφορετικών

επιχειρήσεων να ανταλλάσσουν πληροφορίες άμεσα. Η EDI είχε σχεδιαστεί για να υπηρετήσει τη μεταφορική βιομηχανία, ως μέσω περιορισμού της γραφειοκρατίας και σταδιακά αποτέλεσε πρότυπο αυτής. Αφού εδραιώθηκε στις μεταφορές, άρχισαν να την υιοθετούν και άλλες βιομηχανίες, με τις κατάλληλες μετατροπές βέβαια, έτσι ώστε να ανταποκριθεί στις ιδιαίτερες ανάγκες που απαντώνται στην κάθε μια.

Όμως, οι σχεδιαστές της EDI κυρίως ενδιαφέρονταν για το μέγεθος των μηνυμάτων. Το εύρος ζώνης για τα δίκτυα ηλεκτρονικής ανταλλαγής δεδομένων είναι πολύ δαπανηρά ακόμα και σήμερα. Επιπρόσθετα, τα μηνύματα αυτά είναι συμπιεσμένα και χρησιμοποιούν κώδικα για να παρουσιάζουν πολύπλοκες τιμές. Η πολυπλοκότητα της Ηλεκτρονικής Ανταλλαγής Δεδομένων κάνει δύσκολη και δαπανηρή την εκπαίδευση των προγραμματιστών, με αποτέλεσμα οι εφαρμογές αυτές να είναι ακριβές (αγορά – συντήρηση). Έτσι, ο εξοπλισμός και η πείρα που απαιτείται για να υποστηριχτούν τα συστήματα αυτά, είναι πέρα από τις δυνατότητες των μικρομεσαίων επιχειρήσεων, που τις περισσότερες φορές αρκούνται στις παραδοσιακές διαδικασίες.

2.6.4.2 Επεκτάσιμη Γλώσσα Σήμανσης

Η XML, αντίθετα από την HTML που επικεντρώνεται μόνο στην παρουσίαση των δεδομένων, οργανώνει τα δεδομένα κατά τρόπο ώστε να είναι εύκολη τόσο επεξεργασία τους, όσο και η προβολή τους.

Όπως και στην Ηλεκτρονικής Ανταλλαγή δεδομένων, η XML επιτρέπει σε εσωτερικές εφαρμογές διαφορετικών οργανισμών να μοιράζονται πληροφορίες κατευθείαν. Το βασικό πλεονέκτημα της XML σε σχέση με την EDI, είναι ότι η πρώτη διαβάζεται τόσο από υπολογιστή όσο και από άνθρωπό, ενώ η δεύτερη μόνο από υπολογιστή.

Συγκρίνοντας με την EDI, τα μηνύματα XML είναι πλούσια σε μετα-δεδομένα, κάνοντάς τα ευανάγνωστα και εύκολα στην εξεύρεση του λάθους. Λόγω της απλότητας της XML δεν απαιτείται χρονοβόρα και δαπανηρή εκπαίδευση των χρηστών πάνω σε αυτή και έτσι οι εφαρμογές αυτές είναι λιγότερο δαπανηρές να αγοραστούν και να συντηρηθούν από ότι οι εφαρμογές EDI.

Πίνακας 6

Σύγκριση XML & EDI	
XML	**EDI**
Εύκολη στον προγραμματισμό	Τα μηνύματα είναι συμπιεσμένα
Χρησιμοποιεί την υπάρχουσα σύνδεση Internet	Συχνά χρησιμοποιεί δίκτυα προστιθέμενης αξίας (VAN) χρεώνοντας από $1 μέχρι $20 ανά μήνυμα
Εύκολη στην εκμάθηση	Η εκμάθηση μπορεί να είναι χρονοβόρα
Απαιτεί απλά σκρίπτα	Απαιτεί πολύ καλά εκπαιδευμένους προγραμματιστές

Πηγή: Ricker

Επιπλέον, η XML έχει μειώσει τα εμπόδια εισόδου στο ηλεκτρονικό εμπόριο, σε όρους κόστους και πολυπλοκότητας. Αυτό με τη σειρά του άρχισε να ενθαρρύνει τους πλοιοκτήτες, τα ναυπηγεία, τους προμηθευτές μηχανημάτων και εξοπλισμού να χρησιμοποιούν τέτοιες εφαρμογές. Αποτέλεσμα αυτών, ήταν να δημιουργηθεί μια διαφορετική εκδοχή της XML, η Maritime Trading Markup Language (MTML), που σχεδιάστηκε αποκλειστικά και μόνο για τις ηλεκτρονικές παραγγελίες ναυτιλιακών προμηθειών (Lloyd's List 13/12/2000).

Η αυξανόμενη χρήση των εφαρμογών XML δεν θα πρέπει να ερμηνευτεί όμως ως το τέλος της EDI. Η XML δεν αντικαταστά την EDI, μάλλον την επεκτείνει ώστε να εισέλθουν και οι μικρομεσαίες επιχειρήσεις στο χώρο του ηλεκτρονικού επιχειρήν. Η XML πιθανώς να μετατραπεί σε παγκόσμιο πρότυπο.

2.6.5 Υιοθέτηση από την Αγορά

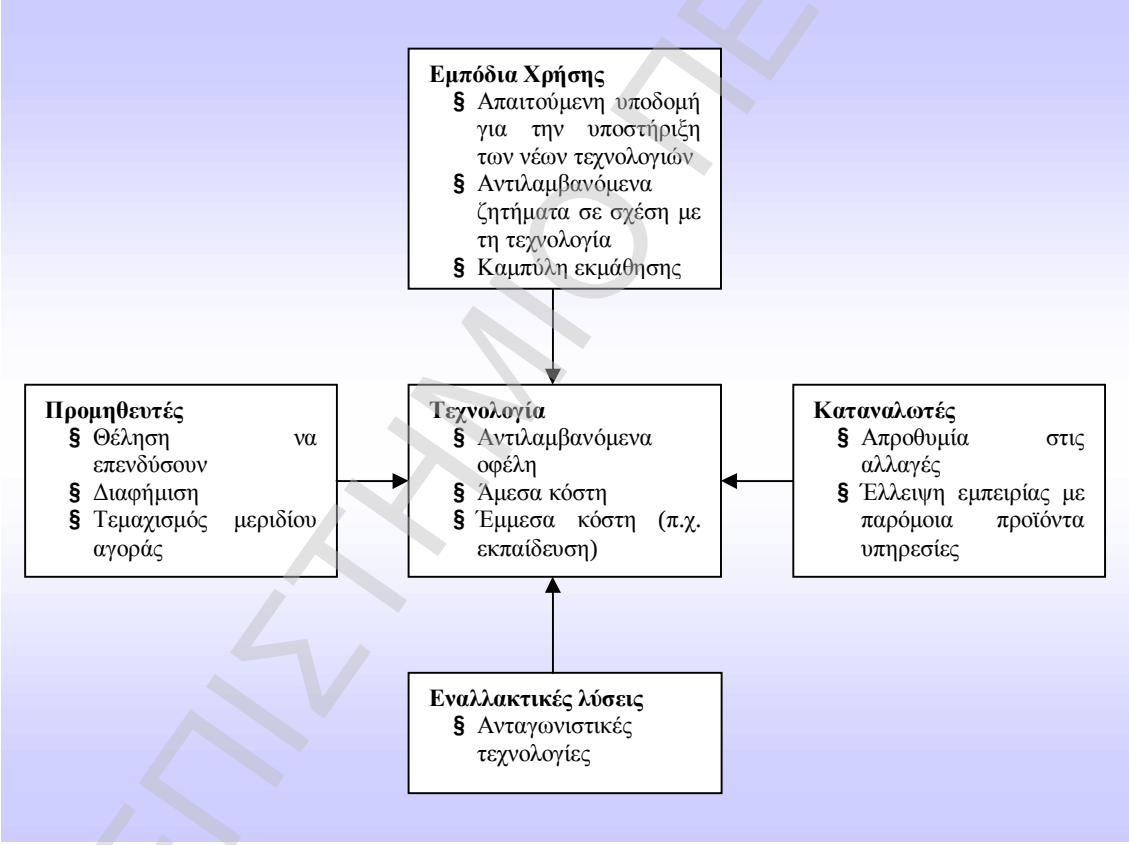
Η υιοθέτηση των νέων τεχνολογιών είναι ένα άλλο εμπόδιο στη ναυτιλία. Αυτός ο παράγοντας είναι ιδιαίτερα σημαντικός σε μια βιομηχανία που πάντα ήταν αντίθετη στο να προσαρμόζεται στα νέα δεδομένα. Τα τηλέφωνα και τα telexes είναι ακόμα τα βασικά μέσα επικοινωνίας στη ναυτιλία και ιδιαίτερα μεταξύ των ναυλωτών και των ναυλομεσιτών. Κλειδί για την επιτυχία ενός συστήματος ηλεκτρονικού εμπορίου στη ναυτιλία είναι η ευρεία υιοθέτηση αυτών νέων τεχνολογιών. Δεν είναι σαφές πότε θα πραγματοποιηθεί αυτό και παρόλο που έχει ήδη

αποκομιστεί σοβαρή γνώση και οφέλη, η υιοθέτηση των εφαρμογών ηλεκτρονικού εμπορίου στη ναυτιλία θα πάρει αρκετό καιρό για να έρθει.

Το ακόλουθο σχήμα απεικονίζει μερικούς παράγοντες που σχετίζονται με την υιοθέτηση των νέων τεχνολογιών[9].

Σχήμα 6

Παράγοντες που Επηρεάζουν την Υιοθέτηση νέων Τεχνολογιών



Πηγή: Bloch

2.6.6 Ζητήματα Υλοποίησης

Αρκετοί συγγραφείς υποστηρίζουν ότι τα ζητήματα που σχετίζονται με την υλοποίηση και οι διοικητικές συνέπειες από τη δημιουργία, τη διοίκηση και την προσκόμιση των

[9] M. Bloch, Y. Pigneur, A. Sefev, "On the Road of Electronic Commerce – A Business Value Framework, Gaining Competitive Advantage and Some Research Issues", 1996.

ωφελειών του ηλεκτρονικού εμπορίου περιστρέφονται γύρω από την αντίληψη ότι η τεχνολογία από μόνη της δεν θα δημιουργήσει πλεονεκτήματα. Η τεχνολογία πρέπει να ενοποιηθεί με τα υπόλοιπα συστήματα και να γίνει μέρος των αξιών ενός οργανισμού για να υπάρξει ωφέλεια. Με άλλα λόγια θεωρούν ότι η επιτυχία από την εισαγωγή των νέων τεχνολογιών είναι ζήτημα εξεύρεσης της χρυσής τομής ανάμεσα στη στρατηγική και την τεχνολογία, ανάμεσα στην τεχνολογία και των επιχειρηματικών διαδικασιών και ανάμεσα στην τεχνολογία και τους ανθρώπους του οργανισμού.

2.6.7 Ζητήματα Κουλτούρας

Ένα από τα σημαντικότερα εμπόδια εισαγωγής νέων τεχνολογιών στη ναυτιλία αποτελεί η κουλτούρα. Τα ζητήματα που σχετίζονται με την κουλτούρα μπορούν να θεωρηθούν ως έλλειψη κατανόησης των νέων τεχνολογιών αλλά και έλλειψη εμπιστοσύνης προς τις νέες τεχνολογίες. Η έλλειψη εμπιστοσύνης και κατανόησης δημιουργεί κάποιο βαθμό αδιαφορίας προς τις νέες τεχνολογίες.

2.7 Επιδράσεις του Ηλεκτρονικού Εμπορίου στη Δομή της Ναυτιλιακής Αγοράς

Η πρόοδος των Τεχνολογιών Πληροφορικής ευρύτατα αναγνωρίζεται πως προκαλεί θεμελιώδεις αλλαγές τόσο στην επιχειρησιακή δομή των οργανισμών, όσο και στη δομή των αγορών γενικότερα. Οι νέες συναλλαγές που βασίζονται στο Web, γνωστές και ως B2B συναλλαγές, έχουν ήδη αρχίσει να αναπτύσσονται στη ναυτιλιακή βιομηχανία. Το ηλεκτρονικό εμπόριο αυτής της κατηγορίας δημιουργεί νέες μορφές ηλεκτρονικών αγορών στη ναυτιλία, όπως οι ηλεκτρονικοί πλειστηριασμοί. Η επίδραση των ηλεκτρονικών αγορών στη ναυτιλιακή βιομηχανία απαντάται κυρίως στους μεσάζοντες, δηλαδή τους ναυλομεσίτες. Τα πρώτα δικτυακά ναυλομεσιτικά γραφεία έχουν ήδη εμφανιστεί, με κύριο έργο τους τις ηλεκτρονικές ναυλώσεις και τις ηλεκτρονικές παραγγελίες προμηθειών. Όλα αυτά απαιτούν τον επαναπροσδιορισμό του ρόλου των ναυλομεσιτών στη ναυτιλία.

2.7.1 Ηλεκτρονικά Ναυλομεσιτικά Γραφεία

Οι ηλεκτρονικές αγορές δημιουργούν ευκαιρίες άνευ προηγουμένου για την ανάπτυξη νέων τύπων ναυλομεσιτών. Αυτά τα νέα επιχειρησιακά μοντέλα, που ονομάζονται ψηφιακές, ηλεκτρονικές ή εικονικές επιχειρήσεις. Οι οργανισμοί αυτοί βασίζονται πλήρως στις τεχνολογίες πληροφορικής και επικοινωνίας, τόσο για την αλληλεπίδραση με τους καταναλωτές, όσο και για την εσωτερικοί διοίκησή τους.

2.7.2 Disintermediation

Κατά τον Wigand ο όρος αυτός μεταφράζεται ως το εκτόπισμα ή η εξάλειψη των μεσιτών από την αγορά, επιτρέποντας έτσι το άμεσο εμπόριο μεταξύ πωλητή και αγοραστή. Επίσης, ο Don Frost το ορίζει ως "cut out the middlemen or women"[10]. Το ζήτημα αυτό συζητείται διεξοδικά στην ενότητα 3.8.1 του παρόντος.

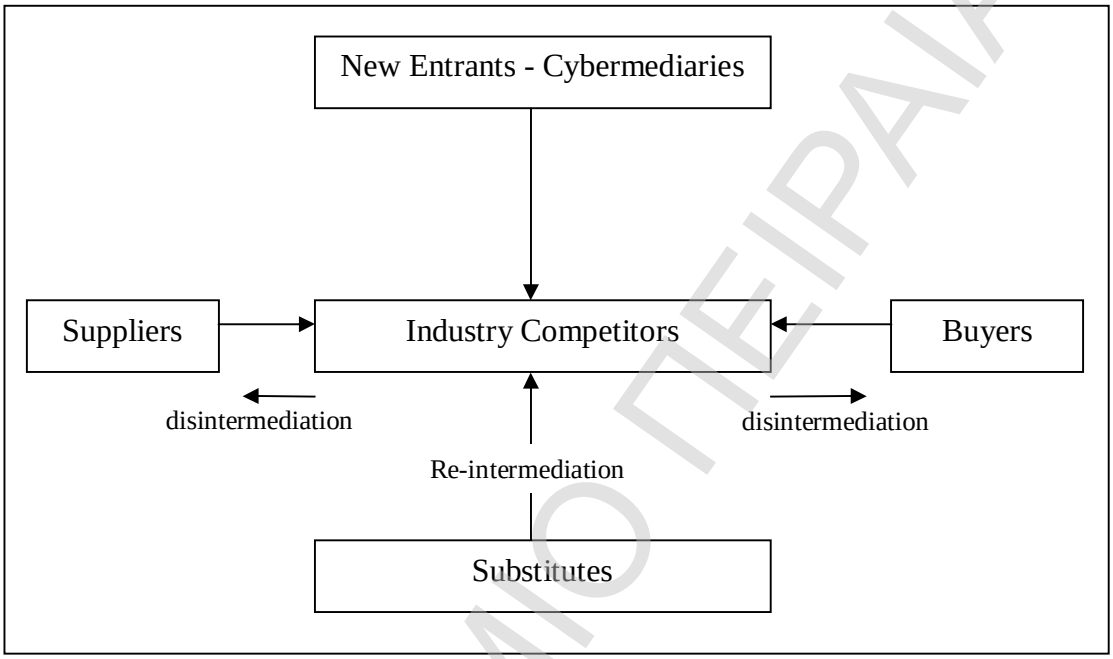
2.7.3 Επαναμεσολάβηση

Αυτή είναι η περίπτωση όπου οι υπάρχοντες ναυλομεσίτες προσθέτουν αξία στην επιχείρησή τους με μέσα και υπηρεσίες που παρέχονται από το Διαδίκτυο και τις ηλεκτρονικές αγορές. Οι παραδοσιακοί ναυλομεσίτες για παράδειγμα, μπορούν να βρουν ευκαιρίες να αυξήσουν τα κέρδη τους και να συνεχίσουν να διαδραματίζουν καθοριστικό ρόλο στη διεξαγωγή εμπορικών συναλλαγών. Επιπρόσθετα, μπορούν να βρουν ευκαιρίες ώστε να διαφοροποιηθούν (μέσω των τιμών – υπηρεσιών που προσφέρουν) και/ή να επικεντρωθούν σε συγκεκριμένα τμήματα της αγοράς.

[10] Frost D., 1999, http://www.emaconnect.com/archive/MarketC/0599market.html.

Σχήμα 7

Επίδραση του Ηλεκτρονικού Εμπορίου σε μια Βιομηχανία



Πηγή: Porter

3. ΗΛΕΚΤΡΟΝΙΚΕΣ ΝΑΥΛΩΣΕΙΣ

3.1 Εισαγωγή

Σκοπός τούτης της μελέτης είναι να εξετάσει και να συγκρίνει τις ηλεκτρονικές ναυλώσεις και τις επιπτώσεις τους στα εμπλεκόμενα μέρη, έτσι ώστε να γίνει αντιληπτός ο δυνητικός ρόλος τους και να προσδιοριστεί το πιθανότερο μοντέλο ναυλώσεων στη μελλοντική ναυτιλιακή αγορά.

Η ναυτιλιακή επιχείρηση είναι μια διεθνής επιχείρηση. Η δραστηριότητά της συνήθως ξεκινά με ένα συμβόλαιο ναυπήγησης ή αγοράς ενός μεταχειρισμένου. Ο κύριος σκοπός της εταιρίας είναι η δημιουργία κέρδους μακροχρόνια από τη διαχείριση, ναύλωση ή αγοραπωλησία των πλοίων της, προσπαθώντας ταυτόχρονα να ελαχιστοποιήσει τα σταθερά και μεταβλητά της κόστη.

Ένας μεσίτης που συνεργάζεται στενά με έναν πλοιοκτήτη διενεργεί εμπορικές πράξεις. Η εργασία του ουσιαστικά συνίσταται στην ανταλλαγή πληροφοριών ανάμεσα στα διάφορα μέρη (πλοιοκτήτες – ναυλωτές). "Κατάλληλη πληροφόρηση την κατάλληλη στιγμή είναι απαραίτητη σε αυτή την αγορά, προκειμένου να επιτύχεις" (Gordon). Κύριο μέρος της εργασίας του, επίσης είναι, η διαμεσολάβηση προκειμένου να έρθουν σε επαφή ένας ναυλωτής και ένας πλοιοκτήτης και να συνάψουν ένα συμβόλαιο θαλάσσιας μεταφοράς.

Είναι σημαντικό να αντιληφθούμε το ρόλο των ναυλομεσιτών καθώς και των καναλιών επικοινωνίας και συναλλαγών μέσω αυτών, έτσι ώστε να προσδιορίσουμε την επίδραση του ηλεκτρονικού εμπορίου σε αυτή την αγορά.

3.2 Δίκτυο Πληροφοριών & Επικοινωνίας

Η ανταλλαγή πληροφοριών είναι βασική προϋπόθεση για τα τμήματα ναυλώσεων προκειμένου να είναι σε θέση να γνωρίζουν την υφιστάμενη προσφορά και ζήτηση θαλάσσιων μεταφορικών υπηρεσιών. Σύμφωνα με τους Roche και Blaine η συλλογή και επεξεργασία πληροφοριών γίνεται με σκοπό την ελαχιστοποίηση της αβεβαιότητας που προκαλείται από το μεταβαλλόμενο περιβάλλον και τις ανταγωνιστικές συνθήκες που επικρατούν στην αγορά. Δεδομένου των ανταγωνιστικών συνθηκών και της ευαισθησίας στους περιβαλλοντικούς –

εξωτερικούς παράγοντες που απαντώνται στη ναυτιλία, η συλλογή και επεξεργασία των πληροφοριών είναι ζωτικής σημασίας.

Στη ναυτιλιακή βιομηχανία, η ναυλομεσιτεία μπορεί να αναφερθεί ως ένα δίκτυο πληροφοριών. Σύμφωνα με αρκετούς συγγραφείς, είναι σημαντικό για τους πλοιοκτήτες, τους ναυλομεσίτες και τους πράκτορες να εγκαθιστούν ένα δίκτυο επαφών, που να συλλαμβάνει όλες τις δυνητικές ευκαιρίες και μέσω του οποίου ακριβείς πληροφορίες γρήγορα να μεταδίδονται. Κατά τους Pisania και Willcocks ένα δίκτυο πληροφοριών αποτελείται από τον εξοπλισμό (τεχνολογικό) εκείνο και τους ανθρώπους έτσι ώστε να διευκολύνεται και να εξυπηρετείται η επικοινωνία και η ανταλλαγή πληροφοριών[11]. Αυτά τα δίκτυα μπορούν να θεωρηθούν ως δίκτυα πληροφοριακών και επικοινωνιακών ροών.

3.3 Πηγές Πληροφοριών

Θα μπορούσαμε να πούμε πως υπάρχουν διάφορα μέσα ανταλλαγών πληροφοριών καθώς και ποικίλες πηγές πληροφοριών, μερικές από τις οποίες είναι οι εκθέσεις για την κατάσταση της αγοράς, οι διαπραγματεύσεις ναύλων και γενικές πληροφορίες.

Οι εκθέσεις για την κατάσταση της αγοράς καταρτίζονται από τα μεγάλα ναυλομεσιτικά γραφεία και δημοσιεύονται στους πλοιοκτήτες, τους ναυλωτές και σε άλλους μεσίτες και πράκτορες που συνεργάζονται, δίνοντας μια συνολική εικόνα της κατάστασης που υφίσταται μια συγκεκριμένη ημέρα ή εβδομάδα. Μια περιεκτική έκθεση αυτού του είδους, περιέχει σχόλια για τις κύριες αγορές (π.χ. χύδην ξηρών και υγρών φορτίων), καθώς επίσης και τιμές αγοραπωλησίας πλοίων.

Τα σημαντικότερα μέρη των πληροφοριών ανταλλάσσονται κατά τη διάρκεια των διαπραγματεύσεων ανάμεσα στα εμπλεκόμενα μέρη. Σε αυτές τα μέρη προσδίδουν την κατάσταση της αγοράς και οι πληροφορίες που συλλέγονται είναι εξίσου σημαντικές με το ναυλοσύμφωνο αυτό καθαυτό. Για την κατανόηση της κατάστασης της αγοράς αυτού του είδους οι πληροφορίες είναι σημαντικότατες, ανεξάρτητα από το αν τα μέρη καταλήξουν σε συμφωνία.

[11] N. Pisanias & L. Willccocks, “Understanding Slow Internet Adoption: Infomediation in Ship-Broking Markets”, 1999.

Άλλες απαραίτητες πληροφορίες αφορούν τα κόστη για τη λειτουργία και επίσπευση του πλοίου, π.χ. κόστος χειρισμού συγκεκριμένου φορτίου σε διάφορα λιμάνια, λιμενικά τέλη και χρεώσεις, κόστος διέλευσης από κανάλια και διώρυγες, τιμές καυσίμων κ.τ.λ.

Το Baltic Exchange, που ιδρύθηκε το 1744, είναι ένα ινστιτούτο με έδρα το Λονδίνο, το οποίο ενεργεί ως ρυθμιστικό σώμα για την ανταλλαγή ναυτιλιακών πληροφοριών, όπου ναυλομεσίτες και ναυλωτές συναντώνται για τη διανομή των εγκυκλίων φορτίου και την ανταλλαγή πληροφοριών. Το ινστιτούτο αυτό, ρυθμίζει το 50% του παγκόσμιου εμπορίου πετρελαίου και το 1/3 των ξηρών φορτίων, όπως τα σιτηρά και το σιδηρομετάλλευμα.

3.4 Ο Ρόλος των Ναυλομεσιτών

Βασικές αρχές που πρέπει να διέπουν έναν καλό ναυλομεσίτη είναι η τιμιότητα, η εμπιστοσύνη, η ακεραιότητα του χαρακτήρα του, καθώς και η εμπειρία και η βαθιά γνώση της αγοράς.

Οι ναυλομεσίτες δρουν ως πληροφοριακοί σύμβουλοι, διαμεσολαβητές και συντονιστές στη διαδικασία της ναύλωσης. Σύμφωνα με τον Kotler, οι ναυλομεσιτικές εταιρίες μπορούν να θεωρηθούν ως αλληλεξαρτώμενοι οργανισμοί, που συμμετέχουν στη διαδικασία δημιουργίας μιας αξιόλογης, συμφέρουσας και υλοποιήσιμης προσφοράς.

Ο ναυλομεσίτης είναι το πρόσωπο που φέρνει σε επαφή τους πωλητές και αγοραστές. Κατά αυτή την έννοια, ο πωλητής και αγοραστής απευθύνεται με τους ίδιους όρους σε αυτόν, είτε πρόκειται για φορτίο είτε πρόκειται για πλοίο. Ενώ ο ναυλομεσίτης φέρνει σε επαφή δύο μέρη, τον πλοιοκτήτη και τον ναυλωτή ένας μεσίτης αγοραπωλησίας πλοίων φέρνει σε επαφή των πωλητή και αγοραστή του πλοίου και ενεργεί για λογαριασμό μόνο του ενός. Συνήθως και τα δύο μέρη έχουν τους δικούς τους μεσίτες. Έτσι, και τα δύο μέρη διαπραγματεύονται μέσω των αντιπροσώπων τους[12].

Υπάρχουν διάφορες κατηγορίες μεσιτών, οι κυριότερες από τις οποίες αναφέρονται ακόλουθα:

[12] Κ. Γκιζιάκης, Α. Παπαδόπουλος, Ε. Πλωμαρίτου, "Εισαγωγή στις Ναυλώσεις", εκδόσεις Σταμούλης, Αθήνα 2002

1. Μεσίτης Πλοιοκτήτη (Owner's Broker): αυτοί οι μεσίτες προσλαμβάνονται από τους πλοιοκτήτες με σκοπό τη διασφάλιση των συμφερόντων τους κατά τη διαδικασία των διαπραγματεύσεων.
2. Μεσίτης Ναυλωτή (Charterer's Broker): υπό τις οδηγίες του ναυλωτή, ο ναυλομεσίτης αυτός δημοσιοποιεί τις εντολές του πρώτου για ζήτηση χωρητικότητας (ολόκληρου του πλοίου ή μέρους αυτού), με τρόπο που θα διασφαλίζονται, με τους πλέον αποδοτικούς και αποτελεσματικούς όρους, τα συμφέροντά του.
3. Ανεξάρτητος Μεσίτης: είτε αντιπροσωπεύει χωρητικότητα ενός πλοιοκτήτη, είτε φορτία ενός ναυλωτή, αυτός ο μεσίτης προσπαθεί να εισέλθει σε μια θαλάσσια συναλλαγή ως διαμεσολαβητής.
4. Μεσίτης Αγοραπωλησίας Πλοίων (Sales & Purchase Broker): όλες οι προηγούμενες κατηγορίες μεσιτών πρέπει να είναι πεπειραμένοι και να έχουν γνώση του τρόπου με τον οποίο λειτουργεί η ναυτιλιακή αγορά για να είναι αποτελεσματικοί. Οι μεσίτες αγοραπωλησίας πλοίων απαιτείται να γνωρίζουν γενικά από πλοία (τεχνικά χαρακτηριστικά), έτσι ώστε να είναι σε θέση να αξιολογούν τις τιμές των νεότευκτων, των μεταχειρισμένων και τις τιμές διάλυσης πλοίων. Οι μεσίτες αυτοί αντιπροσωπεύουν συνήθως μόνο το ένα μέρος (είτε τον πωλητή είτε τον αγοραστή) για τη σύναψη συμφωνίας.

Σε μια συναλλαγή τα μέρη ενδιαφέρονται για τις πηγές πληροφόρησης των μεσιτών, τις ειδικές τους γνώσεις, καθώς και για τις ικανότητες διαπραγμάτευσής τους. Σύμφωνα με τους Pisania και Willcocks [13] οι μεσίτες διακρίνονται σε αποκλειστικούς, ημι-αποκλειστικούς και ανταγωνιστικούς. Ένας εντολέας μπορεί να παραχωρήσει σε ένα μεσίτη το αποκλειστικό δικαίωμα αντιπροσώπευσης των συμφερόντων του, πράγμα που σημαίνει ότι οποιαδήποτε συμφωνία που αφορά φορτίο ή πλοίο του εντολέα θα πραγματοποιηθεί μέσω αυτού.

Εναλλακτικά, οι εντολείς μπορεί να προτιμούν να συνεργάζονται με ένα μικρό αριθμό, συνήθως δύο ή τρεις, ημι-αποκλειστικούς μεσίτες, οι οποίοι να μετέχουν σε ένα δίκτυο μεσιτών με σκοπό την εξεύρεση κατάλληλων πλοίων ή φορτίων και τελικά τη σύναψη ναυλοσύμφωνου. Αυτοί είναι επίσης γνωστοί και ως ανταγωνιστικοί μεσίτες.

13

3.5 Μέσα Επικοινωνίας & Ανταλλαγής Πληροφοριών

Στις ναυτιλιακές επιχειρήσεις, οι άνθρωποι που είναι επιφορτισμένοι με την εργασία των ναυλώσεων, χρησιμοποιούν μια ποικιλία τεχνολογικών μέσων επικοινωνίας και ανταλλαγής πληροφοριών. Από την ανακάλυψη του τηλέγραφου, γύρω στο 1850, υπάρχουν και άλλα μέσα επικοινωνίας, τα οποία έχουν θεμελιώδεις επιδράσεις στη ναυτιλιακή βιομηχανία. Από τεχνολογικής πλευράς, τα κύρια μέσα επικοινωνίας που χρησιμοποιούνται είναι το τηλέφωνο, το telex, τα faxes και το ηλεκτρονικό ταχυδρομείο (e-mail).

Το τηλέφωνο, που εισήχθη το 1876 ενώ το κινητό το 1981, χρησιμοποιείται ευρέως σε όλες τις φάσεις της διαδικασίας ναύλωσης, καθώς είναι κατάλληλο για άμεση και σε πραγματικό χρόνο αλληλεπιδραστική επικοινωνία, που απαιτείται για την υποστήριξη των διαπραγματεύσεων. Αυτό το μέσο επιτρέπει την ανεπίσημη και εμπιστευτική επικοινωνία και συνεπώς μεγάλος όγκος πληροφοριών για την κατάσταση της αγοράς μεταδίδεται μέσω αυτού.

Το telex είναι ένα άλλο συχνότατα χρησιμοποιούμενο μέσο, που εισήχθη για πρώτη φορά το 1928 . Πρόκειται για ένα ασφαλές μέσο ανταλλαγής πληροφοριών και διαπραγματεύσεων και μέχρι πρόσφατα αποτελούσε το μόνο αποδεικτικό στοιχείο επικοινωνίας στις δικαστικές διαμάχες. Ένα άλλο στοιχείο που το κατέστησε τόσο δημοφιλές ήταν η διαθεσιμότητα του δικτύου αυτού ακόμα και στις υπό ανάπτυξη χώρες.

Το fax εισήχθη το 1966 και υιοθετήθηκε ευρέως καθώς αποτελεί φθηνό μέσο επικοινωνίας και είναι ευκολότερο στη χρήση από το telex. Η εισαγωγή του fax επέφερε θεμελιώδεις μεταβολές στο τρόπο με τον οποίο διεξάγονταν οι ναυλώσεις[14].

Η έκρηξη του World Wide Web τα τελευταία πέντε έτη έχει αυξήσει τη χρήση του ηλεκτρονικού ταχυδρομείου και των ηλεκτρονικών διασκέψεων και πολλές ναυτιλιακές τα έχουν υιοθετήσει. Η London Shipbroker Galbraith's διεξήγαγε τις επικοινωνίες της μέσω email σε ποσοστό 85% το 1999, ποσοστό αυξημένο κατά 10% από το προηγούμενο έτος[15]. Η σημαντική ανάπτυξη και γρήγορη υιοθέτηση του Internet οδηγεί σε άλλες μορφές πληροφοριακών και επικοινωνιακών ροών, που είναι η σε πραγματικό χρόνο ανταλλαγή πληροφοριών μέσω εφαρμογών ηλεκτρονικού εμπορίου B2B.

[14] Lloyd's List, 12/05/1999, "Quarterpoints: Are shipbrokers complete Luddites?"
[15] Lloyd's List, 23/10/1999, "Technology: Changing the Structure of Dry Cargo Shipping: IT maters".

Κάθε μια από τις παραπάνω τεχνολογίες χρησιμοποιείται σε διαφορετικές φάσεις της διαδικασίας ναύλωσης πλοίου. Για παράδειγμα η γνωστοποιήσει πλοίου προς ναύλωση ή φορτίου προς μεταφορά, πραγματοποιείται συχνότερα μέσω faxes ή telexes, ενώ το τηλέφωνο χρησιμοποιείται για εμπιστευτικές πληροφορίες. Κατά τη διάρκεια των διαπραγματεύσεων οι προσφορές και αντιπροσφορές ανταλλάσσονται βασικά μέσω fax και telex, με την ταυτόχρονη χρήση του τηλεφώνου.

Σύμφωνα με τους Pisania και Willcocks, το κόστος επικοινωνίας για τις ναυτιλιακές εταιρίες είναι το τρίτο μεγαλύτερο έξοδο μετά τις προμήθειες μεσιτών και τους μισθούς. Εκτός από τα τεχνολογικά μέσα επικοινωνίας, η διαπροσωπική επαφή είναι ένας άλλος τρόπος ανταλλαγής πληροφοριών όταν αυτές είναι πολύτιμές ή εμπιστευτικές[16].

3.6 Επεξεργασία Πληροφοριών

Ιδιαίτερη έμφαση δίνεται στο ρόλο της επεξεργασίας των πληροφοριών για την μείωση της αβεβαιότητας. Εκτός όμως από αυτό τονίζεται και η αναγκαιότητα μείωσης της αμφισημίας των πληροφοριών. Η αμφισημία είναι ο βαθμός στον οποίο οι πληροφορίες είναι διφορούμενες ή προκαλούν σύγχυση ή δύσκολες στην κατανόηση και ερμηνεία. Παρόλο που η επιπρόσθετη πληροφόρηση συχνά θα μείωνε την αβεβαιότητα, θα μπορούσε να μην μειώνει την αμφισημία διότι προβλήματα ερμηνείας ήταν δυνατό να παρέμειναν. Έτσι, θα λέγαμε πως δεν είναι η ποσότητα των πληροφοριών που μειώνει την αμφισημία, αλλά η ποιότητα των πληροφοριών. Ανάλογα με την ποιότητα των πληροφοριών και τον όγκο δεδομένων τους, οι Daft και Lengel ταξινομούν τους διάφορους τρόπους επικοινωνίας ως εξής:

1. Οι διαπροσωπικές συζητήσεις και οι τηλεφωνικές συνδιαλέξεις είναι ποιοτικές άλλα ο όγκος των δεδομένων τους είναι μικρός
2. Οι επίσημες γραπτές αναφορές καθώς και οι αριθμητικές εκθέσεις έχουν μεγάλο όγκο δεδομένων άλλα πολλές φορές δεν είναι ποιοτικές (πολλά ανούσια στοιχεία)
3. Τα προσωπικά γράμματα, τα σημειώματα και τα emails είναι μέτρια τόσο στην ποιότητα των ανταλλασσόμενων πληροφοριών, όσο και στον όγκο των δεδομένων τους.

[16] N. Pisanias & L. Willccocks, “Understanding Slow Internet Adoption: Infomediation in Ship-Broking Markets”, 1999.

Οι Blaine & Bowen επισημαίνουν ότι σύμφωνα με τον Ngurenyanu, τα emails μπορεί να περιέχουν ποιοτικές πληροφορίες, παρόλο της έλλειψης άμεσης ανατροφοδότησης, της έλλειψης διαπροσωπικής επαφής και της μειωμένης γλωσσολογικής ποικιλίας. Εξήγησε τα ευρήματά του σημειώνοντας ότι τα διοικητικά στελέχη δεν στέλνουν και λαμβάνουν απλώς ηλεκτρονικά μηνύματα, αλλά ενεργά δημιουργούν σχέσεις καθώς αλληλεπιδρούν μεταξύ τους. Με αυτό τον τρόπο αναπτύσσουν ένα διερμηνευτικό πλαίσιο που προσθέτει αξία στις πληροφορίες και ευνοεί την επικοινωνία.

3.7 Ηλεκτρονικές Ναυλώσεις

3.7.1 Ηλεκτρονικές Αγορές

Η ιδέα των "Ηλεκτρονικών Αγορών" δημοσιεύτηκε στην επιστημονική κοινότητα από τους Malone, Yates και Benjamin[17]. Μια ηλεκτρονική αγορά αναπαριστά ένα εικονικό τόπο όπου προμηθευτές και καταναλωτές συναντώνται για την ανταλλαγή αγαθών και υπηρεσιών. Αυτές οι ιδιαίτερες αγορές χρησιμοποιούν τεχνολογίες δικτύων και πρότυπα για τη διανομή των δεδομένων των προϊόντων, έτσι ώστε να διεκπεραιωθούν οι ηλεκτρονικές συναλλαγές.

Οι εταιρίες που εξειδικεύονται στις ηλεκτρονικές ναυλώσεις είναι εικονικοί οργανισμοί. Παρέχουν μια αγορά η οποία φέρνει σε επαφή τους προμηθευτές (πλοιοκτήτες) και τους καταναλωτές (ναυλωτές), καθώς επίσης και μια ποικιλία μηχανισμών διαπραγματεύσεων. Εξ ορισμού, δεν υφίσταται καμιά διαφορά στο ρόλο που διαδραματίζουν, εκτός του ότι η δραστηριότητά τους λαμβάνει χώρα σε μια ηλεκτρονική αγορά.

Σύμφωνα με τους Gray & Igbaria, ένας τέτοιος οργανισμός χρειάζεται μια ταυτότητα στο Internet (μια ιστοσελίδα για παράδειγμα), ικανότητα να ενεργεί ως μεσίτης, καλές τηλεπικοινωνίες και γενικότερα τεχνολογική υποδομή[18]. Η υποδομή αυτή και οι τεχνολογίες που χρησιμοποιεί μπορεί να έχουν αναπτυχθεί από την ίδια την επιχείρηση ή να έχει προσλάβει μια άλλη εξειδικευμένη εταιρία με σκοπό την ανάπτυξη αυτών των τεχνολογικών εφαρμογών.

[17] C. Bauer, "Requirements and Infrastructure for Modelling of Electronic Market Transactions", 1999.
[18] Gray P., Igbaria M., "Virtual Organizations and E-Commerce", 2000.

Οι εταιρίες ηλεκτρονικών ναυλώσεων βοηθούν τους πελάτες τους με δύο τρόπους. Πρώτα, επιτρέπουν την εύκολη αναζήτηση στις βάσεις δεδομένων τους για εξεύρεση πλοίου ή φορτίου και δεύτερον, προσφέρουν μηχανισμούς πλειστηριασμών για την υποστήριξη της διαπραγμάτευσης τιμών ανάμεσα στους ναυλωτές και τους πλοιοκτήτες. Επίσης, αρκετές από αυτές τις επιχειρήσεις παρέχουν και εργαλεία για την υλοποίηση ενός ναυλοσύμφωνου.

3.7.2 Πλειστηριασμοί

Μια περιοχή των τεχνολογιών πληροφορικής που θα σταθεί πολύτιμο εργαλείο για τις ναυτιλιακές επιχειρήσεις είναι οι ηλεκτρονικοί πλειστηριασμοί (Lloyd's List 20/01/2001).

Οι πλειστηριασμοί σε μια ηλεκτρονικοί αγορά προσδιορίζουν ένα πρωτόκολλο για την αλληλεπίδραση των προμηθευτών και καταναλωτών, με σκοπό τον καθορισμό της τιμής της συναλλαγής[19]. Πρόκειται για μια τεχνολογία κατάλληλη για εφαρμογές ηλεκτρονικού εμπορίου. Οι ηλεκτρονικοί πλειστηριασμοί προσφέρουν την ηλεκτρονική υλοποίηση δοσίματος μιας προσφοράς τιμής, που είναι επίσης γνωστή από τους παραδοσιακούς πλειστηριασμούς. Αυτό μπορεί να συνοδεύεται από την παρουσίαση με πολυμέσα των προϊόντων.

Συνήθως δεν περιορίζονται μόνο σε αυτή τη λειτουργία, αλλά μπορούν επίσης να παρέχουν την ολοκλήρωση της διαδικασίας προσφοράς τιμής με τη σύναψη συμβολαίου, την πληρωμή και διανομή. Οι πηγές εισοδήματος του παροχέα ηλεκτρονικών πλειστηριασμών προέρχονται από την πώληση της ηλεκτρονικής πλατφόρμας, από τις προμήθειες συναλλαγών και από τη διαφήμιση[20].

[19] M. Strobel, "On Auctions as the Negotiation Paradigm of Electronic Markets", Electronic Markets volume 10 number 2000

20 Timers Paul Electronic Commerce "Strategies and Models for Business-to-Business Trading", Jony Wiley & Sons Ltd., Chichester, 1999

3.7.3 Θεμελιώδεις Αρχές Επιχειρησιακών Συναλλαγών & Διαπραγματεύσεων

Οι συναλλαγές μέσω ηλεκτρονικού εμπορίου περιλαμβάνουν τρία κύρια μέρη: α) τον πωλητή, β) τον αγοραστή και γ) του φορέα παροχής υπηρεσιών Internet (Internet Service Provider - ISP). Ο φορέας αυτός δρα ως διαμεσολαβητής παρέχοντας μια ευρεία γκάμα υπηρεσιών όπως EDI ή άλλες εφαρμογές, ηλεκτρονικό ταχυδρομείο, μεταφορά αρχείων, ηλεκτρονική μεταφορά κεφαλαίων κ.τ.λ.[21].

Οι επιχειρησιακές συναλλαγές, που μπορεί να είναι προϊόντα, υπηρεσίες ή και συνδυασμός των δύο, αποτελούνται από ένα πεπερασμένο αριθμό αλληλεπιδραστικών διαδικασιών ανάμεσα στα μέρη και ταξινομούνται στις ακόλουθες τέσσερις φάσεις (Schmid 1998):

1.Φάση Συλλογής Πληροφοριών (για προϊόντα, υπηρεσίες, εταίρους): τα ενδιαφερόμενα μέρη συλλέγουν πληροφορίες από διάφορες πηγές όπως είναι οι δείκτες, διάφορα ναυλοσύμφωνα, οι γενικότερες κοινωνικοοικονομικές εξελίξεις κ.τ.λ.

2.Φάση Καθορισμού Προσφοράς & Ζήτησης: σε αυτή τη φάση οι πλοιοκτήτες και ναυλωτές ή οι αντιπρόσωποί τους αποστέλλουν τις ανάγκες τους.

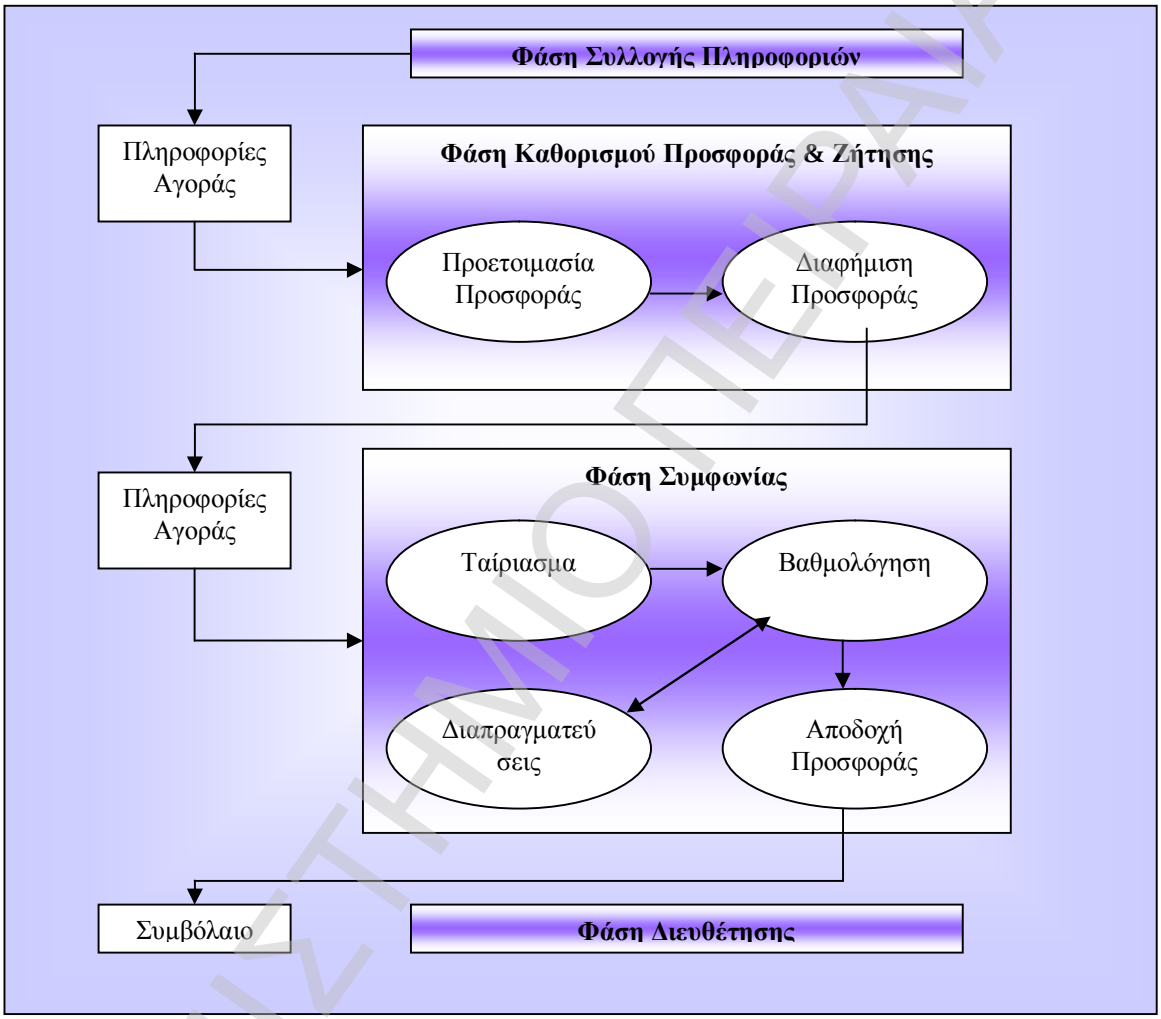
3.Φάση Συμφωνίας (συζητούνται οι όροι της συναλλαγής): αυτή η φάση ξεκινά αφού έχει βρεθεί κατάλληλο πλοίο για τη μεταφορά ενός φορτίου και αντίστροφα. Ο πλοιοκτήτης και ναυλωτής ταιριάζουν τις απαιτήσεις τους σύμφωνα με τον όγκο του φορτίου και τη θέση του πλοίου. Το δεύτερο στάδιο αυτής της φάσης είναι η δημιουργία οικονομικής προσφοράς από τον πλοιοκτήτη για τη μεταφορά του φορτίου. Έπειτα ακολουθούν διαπραγματεύσεις έως ότου τα δύο μέρη συμφωνήσουν τους όρους, τις ρήτρες και καταλήξουν στην υπογραφή ναυλοσύμφωνου.

4.Φάση Διευθέτησης: σε αυτή την τελευταία φάση εκτελούνται οι όροι του συμβολαίου.

[21] Y. Shee, Daniel & Tang, Tzung-I, “Modeling the Supply-Demand Interaction in Electronic Commerce”, 2000.

Σχήμα 8

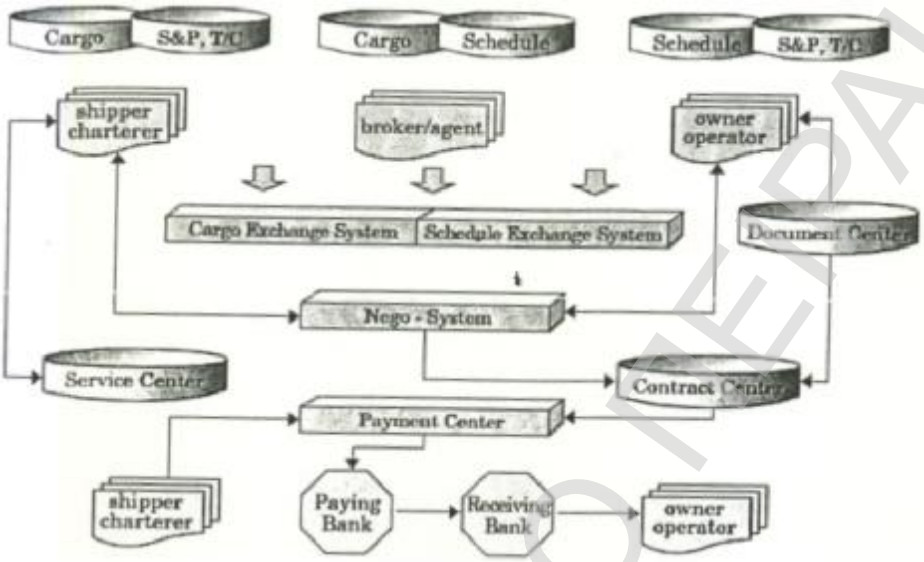
Φάσεις Συναλλαγών



Πηγή: Schmid 1998

Το ακόλουθο σχήμα απεικονίζει το σύστημα συναλλαγών της CyVoyage[22]

Σχήμα 9



Σύστημα Συναλλαγών CyVoyage

Πηγή: http://www.cyvoyage.com/CVGDefault.asp

3.7.4 Τύποι Πλειστηριασμών

Στις ηλεκτρονικές ναυτιλιακές αγορές υφίστανται και χρησιμοποιούνται δύο τύποι πλειστηριασμών:

α) οι πλειστηριασμοί κράτησης και

β) οι πλειστηριασμοί ανοικτής προσφοράς.

Οι πλειστηριασμοί κράτησης είναι η πιο κοινή κατηγορία όπου οι πλοιοκτήτες ή οι ναυλομεσίτες τους κάνουν μια προσφορά για ένα συγκεκριμένο φορτίο, που έχει τοποθετηθεί από ναυλωτή ή τον μεσίτη του, μέχρι το τέλος της προθεσμίας (ημερολογιακή) που έχει τεθεί. Σε αυτούς τους πλειστηριασμούς η μικρότερη προσφορά κερδίζει.

[22] http://www.cyvoyage.com/CVGDefault.asp.

Αντίθετα στους πλειστηριασμούς ανοικτής προσφοράς ο αγοραστής είναι αυτός που επιλέγει τον πωλητή που θα συνεργαστεί. Εταιρίες ηλεκτρονικών παραγγελιών, όπως η eBunkers.com, παρέχουν και τις δύο κατηγορίες πλειστηριασμών.

3.7.5 Αντιπροσωπευτικά Παραδείγματα

AXSMarine.com

Υποστηριζόμενη από μεγάλους ναυλομεσίτες όπως η Barry Rogliano Salles (BRS-Paris) και η Fearnbulk, η AXSMarine αναπτύσσει ολοκληρωμένες ηλεκτρονικές λύσεις ναυλώσεων, ξεκινώντας από την αγορά χύδην ξηρών φορτίων και επεκτείνοντας τις δραστηριότητες της και σε άλλες αγορές. Αυτή η ηλεκτρονική εταιρία σκοπεύει στην παροχή ενός σετ ηλεκτρονικών εφαρμογών που απευθύνεται στους πλοιοκτήτες, στους ναυλωτές και ναυλομεσίτες. Πιο συγκεκριμένα οι υπηρεσίες είναι:

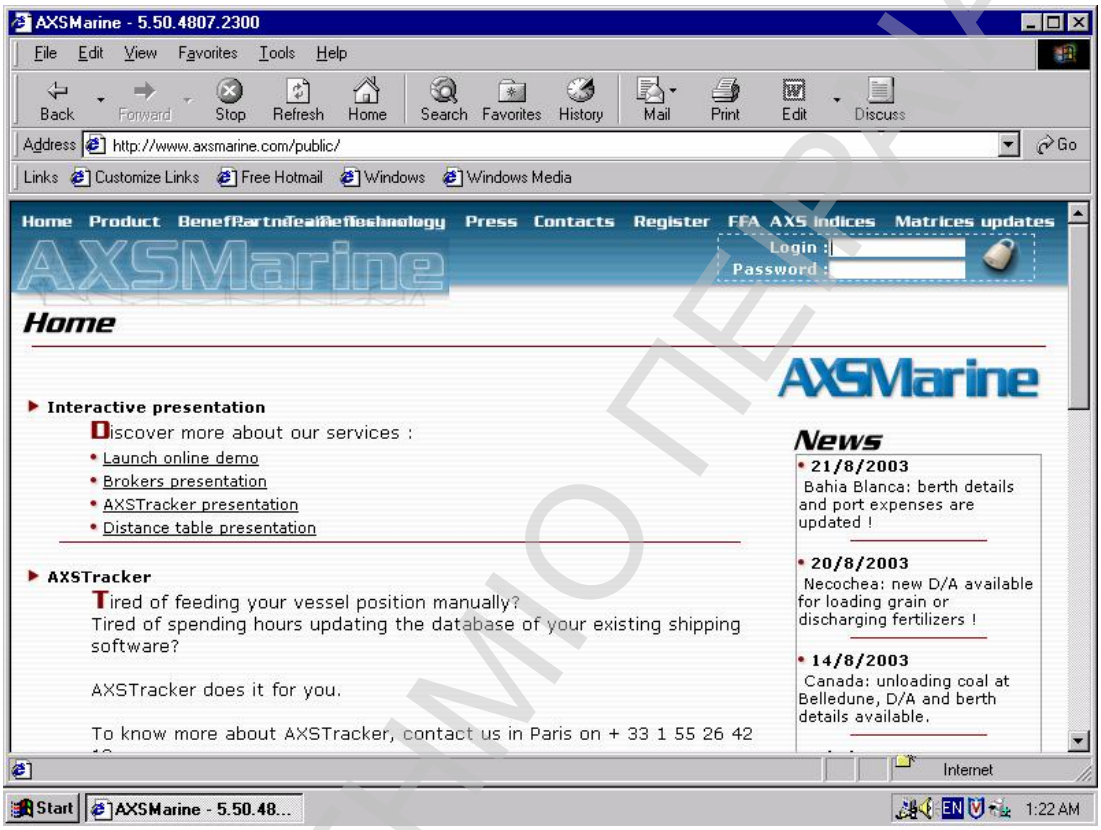
1.πληροφορίες αγοράς

2.διαπραγματεύσεις και

3.κλείσιμο ναυλοσύμφωνων

Εικόνα 1

Κεντρική Σελίδα AXSMarine.com[23]



Πηγή: http://www.AXSMarine.com

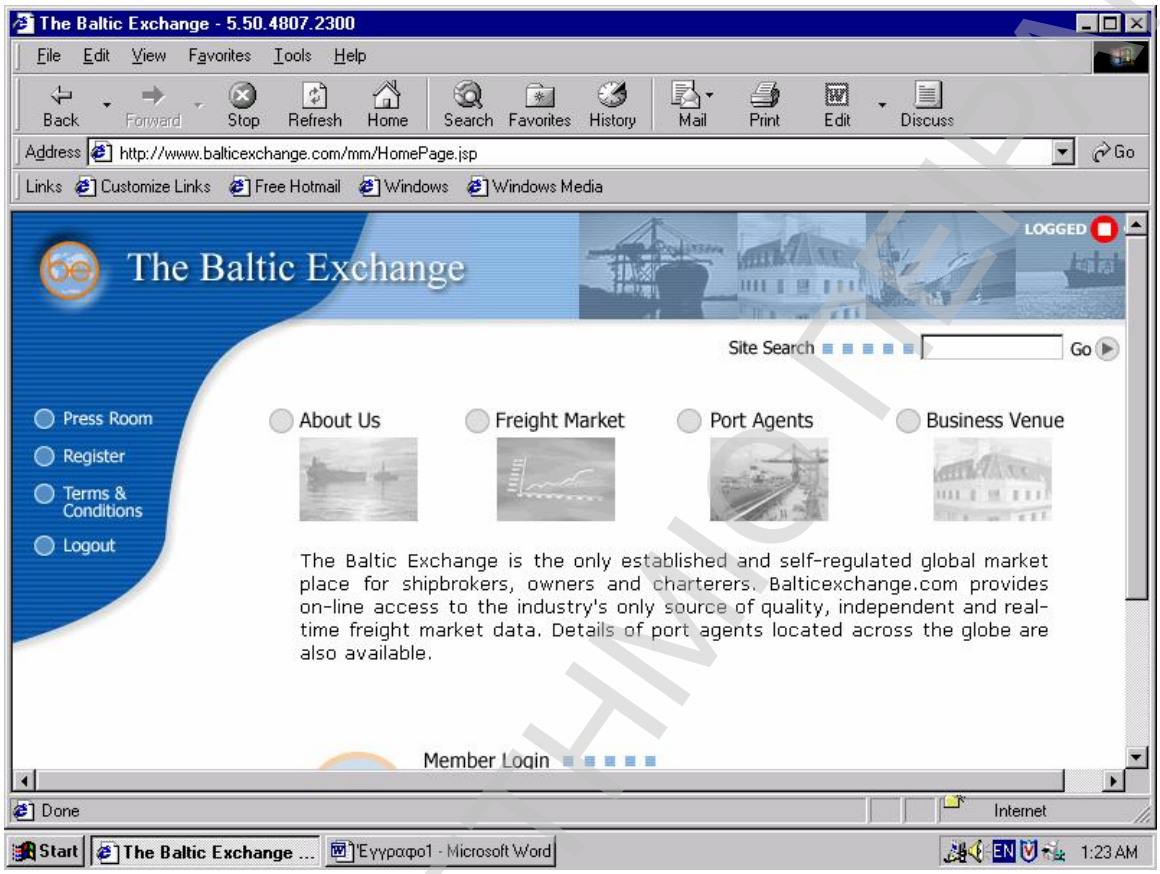
Balticexchange.com

Ο σκοπός του Balticexchange.com, που συστάθηκε τον Αύγουστο του 2001, είναι να φέρει σε επαφή την προσφορά και ζήτηση (πλοιοκτήτες – ναυλωτές) για θαλάσσιες μεταφορικές υπηρεσίες, μέσω των εφαρμογών εικονικού εμπορίου της. Το κύριο χαρακτηριστικό αυτής της ιστοσελίδας είναι η μηχανή αναζήτησης για φορτία και πλοία και ένα σύστημα που πληροφορεί τους ναυλομεσίτες όταν βρεθούν νέα πλοία και φορτία.

[23] http://www.AXSMarine.com

Εικόνα 2

Κεντρική Σελίδα Balticexchange.com[24]



Πηγή: http://www.balticexchange.com

Cargobiz.com

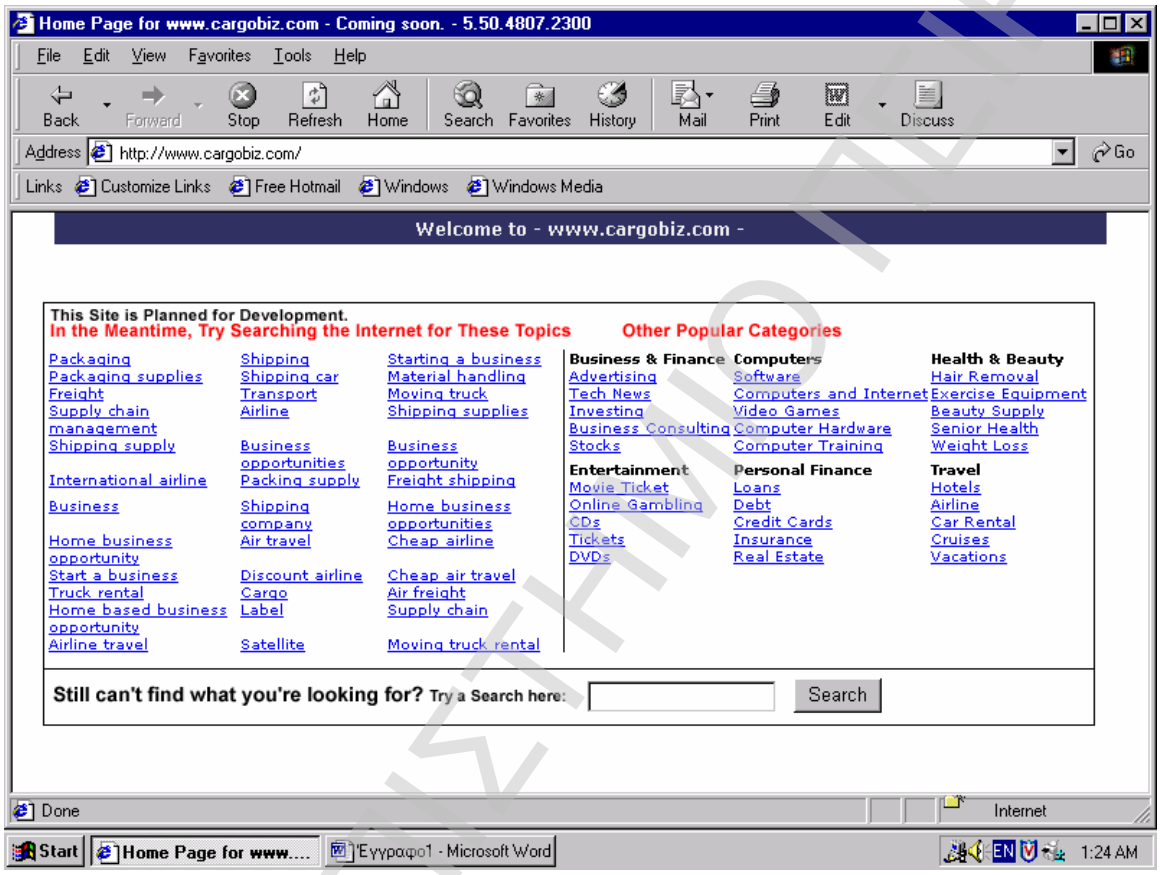
Πρόκειται για ένα ανεξάρτητο portal, που υποστηρίζει εφαρμογές ηλεκτρονικού εμπορίου B2B. Αναλυτικότερα, υποστηρίζει ολοκληρωμένες διαδικασίες ανταλλαγής συμπεριλαμβανομένου πλειστηριασμών, αυτόματων υπηρεσιών ειδοποίησης για την εύρεση πλοίων και φορτίων, καθώς και γενικές πληροφορίες όπως πληροφορίες για την κατάσταση της αγοράς. Επιπρόσθετα, προσφέρει υπηρεσίες για τη διαπραγμάτευση και τελικά υπογραφή ναυλοσύμφωνου, όπως και επιχειρησιακή βοήθεια κατά τη διάρκεια του ταξιδιού. Το cargobiz.com

[24] http://www.balticexchange.com

εξειδικεύεται στις αγορές των χύδην ξηρών φορτίων και των containers. Τέλος, ο δικτυακός αυτός τόπος υποστηρίζεται από το Internet Capital Group, που επένδυσε 12 εκατομμύρια DM το 2000.

Εικόνα 3

Κεντρική Σελίδα Cargobiz.com[25]



Πηγή: http://www.cargobiz.com

Levelseas.com[26]

Η Levelseas ιδρύθηκε τον Απρίλιο του 2000 και υποστηρίζεται από μια σειρά μεγάλων εταιριών όπως η Shell, η BP, η Cargill, η Clarkson και η eVolution Partners. Σχεδιάστηκε

[25] http://www.cargobiz.com
[26] http://www.levelseas.com

με σκοπό να γίνει μια παγκόσμια ηλεκτρονική αγορά για την αγοραπωλησία και διαχείριση – διοίκηση των θαλάσσιων μεταφορικών μέσων.

Η Levelseas επικεντρώνεται στις ναυλώσεις και στις Προθεσμιακές Συμφωνίες Ναύλωσης (Forward Freight Agreement ή FFAs) . Πρόκειται για μια ιστοσελίδα ηλεκτρονικών συναλλαγών όπου πλοιοκτήτες, ναυλομεσίτες και ιδιοκτήτες φορτίων διεξάγουν επιχειρηματικές συμφωνίες. Η Levelseas.com προσφέρει υπηρεσίες που επιτρέπουν τη διαχείριση των απαιτήσεων ενός ταξιδιού, τη διαχείριση του φορτίου, υπηρεσίες που περιέχουν πληροφορίες για την αγορά, ηλεκτρονικές ναυλώσεις, υπογραφή ναυλοσύμφωνων και εργαλεία διαχείρισης ρίσκου.

Αρχικά οι υπηρεσίες που παρείχε προσφέρονταν μέσω της εφαρμογής LSX 1.0, η οποία επέτρεπε στους πλοιοκτήτες, στους ναυλομεσίτες και στους ναυλωτές να διεξάγουν εμπορικές συναλλαγές, να επικοινωνούν και να διαχειρίζονται πληροφορίες της αγοράς. Πιο συγκεκριμένα, περικλείει ένα σύστημα αποστολής – λήψης μηνυμάτων, τις γεωγραφικές θέσεις των φορτίων, δεδομένα για φορτία, εργαλεία αναζήτησης πληροφοριών και φιλτραρίσματος, καθώς και δεδομένα για συγκεκριμένα πλοία.

Η εξέλιξη της εφαρμογής αυτής, η LSX 2.0, περιέχει κύριους όρους διαπραγμάτευσης, ερωτηματολόγια και δυνατότητα επεξεργασίας ναυλοσύμφωνου, που επιτρέπουν την ολοκλήρωση της συναλλαγής. Τέλος σε αυτόν τον δικτυακό τόπο δεν υφίσταται σύστημα πλειστηριασμού.

Εικόνα 4

Κεντρική Σελίδα της Levelseas.com

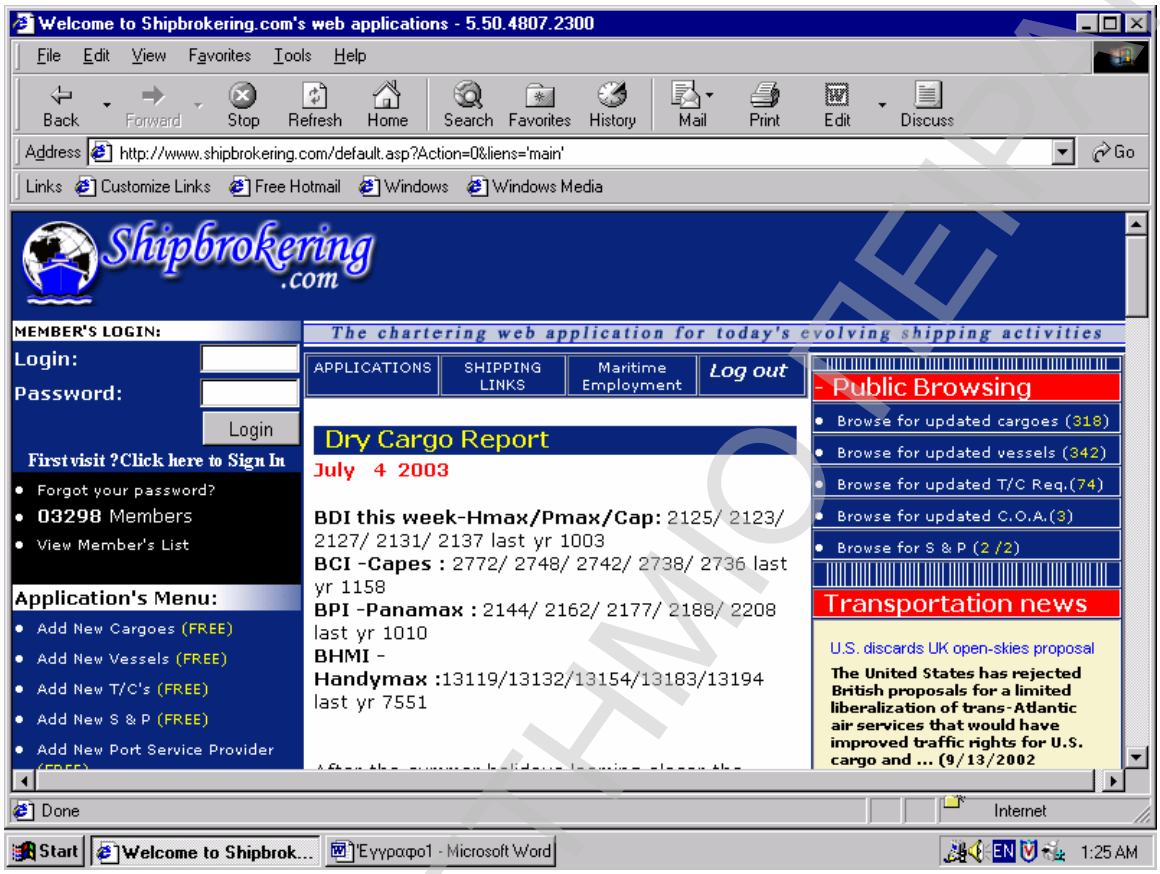
Πηγή: http://www.levelseas.com

Shipbrokering.com

Η ιστοσελίδα αυτή επιτρέπει στους πλοιοκτήτες και ναυλωτές την αναζήτηση σε πραγματικό χρόνο φορτίων και πλοίων. Επιπλέον, η Shipbrokering.com επιτρέπει στους φορτωτές και ναυλωτές να καθορίζουν την παραγγελία άμεσα, χωρίς επιπρόσθετη προμήθεια. Όμως, το site αυτό δεν παρέχει τα εργαλεία εκείνα που απαιτούνται για την ολοκλήρωση μιας εμπορικής συναλλαγής (υπογραφή ναυλοσύμφωνου), και τα δύο μέρη πρέπει να την υπογράψουν με τον παραδοσιακό τρόπο.

Εικόνα 5

Κεντρική Σελίδα της Shipbrokering.com[27]



Πηγή: http://www.shipbrokering.com

Shipbrokerexchange.com[28]

Υποστηριζόμενο από τις Η.Π.Α., το ShiBroker Exchange ιδρύθηκε από την εταιρία ανάπτυξης ναυτιλιακού λογισμικού Dataworks και την εξειδικευμένη εταιρία στις εφαρμογές Διαδικτύου Network Chartering. Η Shipbrokerexchange.com επικεντρώνεται κύρια στις αγορές των

[27] http://www.shipbrokering.com
[28] http://www.shipbrokerexchange.com

χύδην υγρών και ξηρών φορτίων. Τα μέλη αυτού του δικτυακού τόπου μπορούν να επιλέγουν και να αποστέλλουν συγκεκριμένες πληροφορίες σε άλλα μέλη απευθείας.

Το ShipBroker Exchange δεν είναι ένα site διευθέτησης εμπορικών συναλλαγών, αλλά ένα ολοκληρωμένο σύστημα ανταλλαγής πληροφοριών που βασίζεται στο Διαδίκτυο. Παρέχει όλα τα στοιχεία που απαιτούνται από τους χρήστες για να φθάσουν στην υπογραφή ναυλοσύμφωνου, όπως αναζήτηση θέσης πλοίου, δυνατότητα επικοινωνίας με άλλους εντολείς και δυνατότητα διαπραγμάτευσης, καθώς και μια βάση δεδομένων με τρέχοντα και ιστορικά στοιχεία πλοίων και πληροφορίες αγοράς. Οι υπηρεσίες που προσφέρει είναι συνδρομητικές.

Εικόνα 6

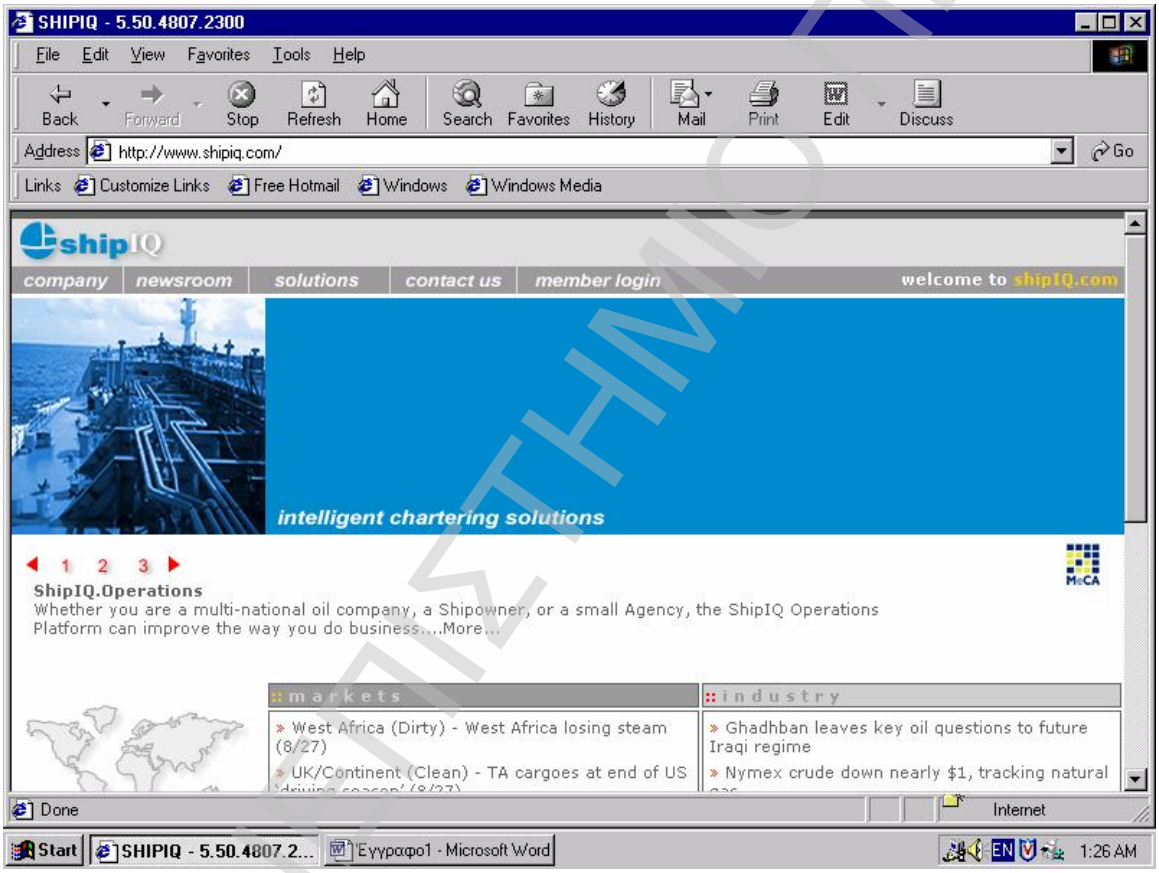
Κεντρική Σελίδα της Shipbrokerexchange.com

Πηγή: http://www.shipbrokerexchange.com

Η ShipIQ προσφέρει επίσης ένα ηλεκτρονικό σύστημα ναυλώσεων που επιτρέπει στους ναυλωτές, στους πλοιοκτήτες και στους ναυλομεσίτες τους να διαπραγματεύονται και να ολοκληρώνουν μια συναλλαγή ηλεκτρονικά. Παρέχει όλα τα εργαλεία και τους πόρους για τη διευθέτηση εμπορικών συναλλαγών και διαπραγματεύσεων. Τέλος, αυτό το site ειδικεύεται στην αγορά των χύδην υγρών φορτίων.

Εικόνα 7

Κεντρική Σελίδα της ShipIQ.com



Πηγή: http://www.shipiq.com

3.7.6 Χαρακτηριστικά & Διακριτικά

Παρόλο που οι προσεγγίσεις των εταιριών παροχής ηλεκτρονικών ναυλώσεων ποικίλουν σημαντικά ως προς τις λεπτομέρειές τους, εντούτοις κάποια στοιχεία είναι κοινά, όπως οι πλειστηριασμοί, οι διαδικασίες υπογραφής ναυλοσύμφωνου και η μέθοδος προσκόμισης των εσόδων τους.

Οι λύσεις διαφέρουν σε σχέση με την διάσταση, όπως την εστίαση, τα κίνητρα και τα μοντέλα προσκόμισης εσόδων. Οι λύσεις μπορούν επίσης να διακριθούν ανάλογα με το στάδιο της διαδικασίας αγοραπωλησίας που υποστηρίζουν, συμπεριλαμβανομένου της προσφοράς τιμής, των διαπραγματεύσεων και της πληρωμής. Σε μερικές περιπτώσεις, επιπρόσθετες υπηρεσίες εμπεριέχονται για τους πωλητές και αγοραστές, όπως είναι τα συστήματα υποστήριξης αποφάσεων.

Τα κύριο χαρακτηριστικό των εταιριών παροχής ηλεκτρονικών ναυλώσεων είναι ότι σκοπεύουν να επεκτείνουν τις επιχειρήσεις τους σε άλλους τομείς της αγοράς. Σκόπιμο κρίνεται να σημειώσουμε ότι ανάμεσα στις εταιρίες που εξειδικεύονται σε μια μόνο αγορά, είτε αυτή η είναι των χύδην υγρών, είτε των χύδην ξηρών, τείνουν να επεκτείνουν τις επιχειρηματικές δραστηριότητές τους και σε άλλες αγορές και να καλύπτουν όλο το φάσμα, ακόμα και την αγορά S & P και τα containers. Αντιπροσωπευτικά παραδείγματα αποτελούν η Glomap, η ShippingDesk, και η Charteringsolutions.

Συνήθως, οι εταιρίες αυτές θέτουν σε εφαρμογή διαφορετικές πολιτικές με την είσοδο νέων συμμετεχόντων. Ενώ δεν εφαρμόζουν “σκληρούς” κανόνες, συνήθως είναι επιλεκτικοί και όχι εντελώς ανοικτοί στην είσοδο νέων μελών. Στις περισσότερες των περιπτώσεων, πριν παραχωρηθεί άδεια συμμετοχής, πραγματοποιείται ένα είδος έρευνας των δυνητικών συμμετεχόντων με την έκδοση ID και password. “We make sure that we do not activate any accounts that are not known to us or that we did not at least talk to”. P.A. Joerss .

Το μοντέλο προσκόμισης εσόδων είναι ένας άλλος τρόπος διάκρισης των διαφορετικών προσεγγίσεων. Υπάρχουν κυρίως δύο κατηγορίες: α) οι συνδρομές από τα μέλη και β) οι προμήθειες συναλλαγής. Αυτό είναι ένα σημαντικό θέμα διότι προβλήματα που συμβαίνουν

στην ανάπτυξη εφαρμογών ηλεκτρονικού εμπορίου είναι η έλλειψη προσοχής στη μέθοδο αποκόμισης εσόδων (Lloyd's List 22/01/2001).

Μερικές από τις εταιρίες που ασχολούνται με τις ηλεκτρονικές ναυλώσεις χρεώνουν και με τις δύο μεθόδους. Τέτοιες εταιρίες είναι η AXSMarine, η Seanet, η Maritimeexchange, η SSYfeatures, η ShippingDesk και η E-janworld. Εταιρίες που χρεώνουν τις υπηρεσίες τους με βάση τη συνδρομή των μελών τους είναι η Shipbrokering, η Shippingonthenet, η Networkchartering και η Asiashippingmarket, ενώ εταιρίες που βασίζουν τα έσοδά τους στις προμήθειες από τις συναλλαγές που διεκπεραιώνουν είναι η Cargobiz, η Glomap, η ShipIQ, η Ship-Search, η Shipping-direct, η Ratequery και η Charteringsolutions. Σε πολλές περιπτώσεις, οι επιπρόσθετες υπηρεσίες που προσφέρονται στους πελάτες, όπως η διαφήμιση χρεώνονται επιπλέον.

Οι συνδρομές των μελών κυμαίνονται από $100 έως $50,000 ετησίως. Οι προμήθειες συναλλαγής βασίζονται στον όγκο του φορτίου που χρεώνεται όταν ολοκληρώνεται μια συναλλαγή. Κυμαίνεται από 0.1% έως 1%. Από τα παραπάνω μπορούμε να πούμε ότι το αποδοτικότερο μοντέλο είναι το δεύτερο, δηλαδή αυτό που βασίζεται στον όγκο του μεταφερόμενου φορτίου.

Κλείνοντας, διαφορετικές προσεγγίσεις υποστηρίζουν διαφορετικά μέρη της διαδικασίας συναλλαγής. Ενώ μερικές εταιρίες (ShipIQ, Chinsay), εστιάζουν στην υποστήριξη όλων των δραστηριοτήτων ηλεκτρονικά, παρέχοντας εργαλεία εφαρμογών όπως αναζήτηση και εξεύρεση πλοίων και φορτίων, πλειστηριασμούς και διαπραγμάτευση όρων, ηλεκτρονικά ναυλοσύμφωνα, άλλες παρέχουν μόνο μερικές από τις παραπάνω υπηρεσίες ηλεκτρονικά και έπειτα τα μέρη διεκπεραιώνουν τις συναλλαγές τους με τον παραδοσιακό τρόπο.

Για παράδειγμα, η Shipbroking επιτρέπει στους φορτωτές και ναυλωτές να δώσουν την εντολή απευθείας. Όμως, το site της εταιρίας δεν προσφέρει εργαλεία για να ολοκληρωθεί η συναλλαγή ηλεκτρονικά. Έτσι τα μέρη προβαίνουν στην υπογραφή του ναυλοσύμφωνου με τον παραδοσιακό τρόπο.

Ανόμοια με άλλα site ηλεκτρονικού εμπορίου, το ShipbrokerExchange δεν έχει μια κεντρική βάση δεδομένων. Οι χρήστες του χρησιμοποιώντας την υπηρεσία διατηρούν τις δικές τους βάσεις δεδομένων στα δικά τους υπολογιστικά συστήματα και η συγκεκριμένη εταιρία εξυπηρετεί μόνο τη μεταφορά δεδομένων ανάμεσα στις διάφορες βάσεις δεδομένων.

Επιπρόσθετα το E-bro και το Ship-search δεν προσφέρουν online υπηρεσίες συναλλαγών. Σύμφωνα με την έκθεση του Drewry η CharteringSolutions δεν επιτρέπει στους ναυλωτές και πλοιοκτήτες να χρησιμοποιήσουν το σύστημα εκτός αν δεν διορίσουν τον αντιπρόσωπό τους (ναυλομεσίτη)[29].

Έτσι, θα μπορούσαμε να πούμε ότι ενώ μερικές εταιρίες παροχής ηλεκτρονικών ναυλώσεων βασίζονται στην καλλιέργεια παρά στην αντικατάσταση ναυλομεσιτών, άλλες παρέχουν όλα τα εργαλεία στους εντολείς για τη διαπραγμάτευση και υπογραφή ναυλοσύμφωνων χωρίς τη μεσολάβηση μεσιτών, γεγονός που τις προσδίδουν το ρόλο των μεσιτών.

Τέλος, οι προαναφερθείσες εταιρίες δεν έχουν τελειοποιήσει τα επιχειρησιακά τους μοντέλα. Οι προσπάθειες τους να εδραιωθούν και να πετύχουν υψηλά μερίδια αγοράς σε όρους αριθμού χρηστών, οδηγεί σε συχνές αλλαγές των στρατηγικών του οργανισμού.

[29] Drewry, “Recent Development in Web-Based Maritime Services”, Digital Ship & Drewry Shipping Consultants Ltd. 2000.

4. Η ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Το ηλεκτρονικό εμπόριο είναι ένας νέος τρόπος ανταλλαγής προϊόντων που πραγματοποιείται μέσω του διαδικτύου. Η φύση αυτή του Διαδικτύου έχει καταστήσει διαρκώς αυξανόμενη την ανάγκη προστασίας των δεδομένων αφού η μη εξουσιοδοτημένη πρόσβαση στις διακινούμενες πληροφορίες είναι σχετικά εύκολη, έχει ενδεχομένως καταστρεπτικές συνέπειες για την εύρυθμη λειτουργία οργανισμών (οικονομικών, στρατιωτικών, πολιτικών) και κρατών και επιπλέον ανιχνεύεται δύσκολα[30].

Η ασφάλεια στο ηλεκτρονικό εμπόριο έχει δημιουργήσει πλήθος συζητήσεων και έρευνας, πράγμα που καθιστά επιφυλακτικό ένα μεγάλο μέρος του αγοραστικού και επιχειρηματικού κόσμου. Οι βασικοί κίνδυνοι που απειλούν τις ηλεκτρονικές συναλλαγές έχουν να κάνουν με την ακεραιότητα, την εμπιστευτικότητα των δεδομένων ,την άρνηση υπηρεσίας και την εξακρίβωση της γνησιότητας. Οι απαιτήσεις ασφάλειας στο ηλεκτρονικό εμπόριο επικεντρώνονται στα :

• Authentication (Έλεγχος αυθεντικότητας) Η διαδικασία αυτή έχει στόχο την εξακρίβωση της ταυτότητας του χρήστη.

• Authorization (Εξουσιοδότηση) Περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί.

• Confidentiality (Εμπιστευτικότητα) Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. Παρέχεται μέσω κρυπτογράφησης και είναι απαραίτητο στοιχείο της ιδωτικότητας του χρήστη. Κυρίως για το ηλεκτρονικό εμπόριο, αποτελεί υψίστης σημασίας συστατικό τόσο στην προστασία των οικονομικών δεδομένων, όσο και στην προστασία πληροφοριών ανάπτυξης, οργανωτικών δομών και άλλων προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση.

• Integrity (Ακεραιότητα) Η ακεραιότητα έχει να κάνει με την ασφαλή μεταφορά των δεδομένων στο δίκτυο. Αυτό σημαίνει ότι με κανένα τρόπο δεν πρέπει να υπάρξει, μη εξουσιοδοτημένη τροποποίηση των δεδομένων και αυτό διασφαλίζεται με διάφορες μεθόδους (π.χ. ψηφιακές υπογραφές).

[30] "E-Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή " Κωνσταντίνος Μουλίνος , Κωνσταντίνα Καμπουράκη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

• Non-repudiation (Μη αποποίηση της ευθύνης) Αποτελεί ένα πολύ σημαντικό τομέα στην ασφάλεια στο ηλεκτρονικό εμπόριο. Για να ολοκληρωθεί μια συναλλαγή θα πρέπει να μην μπορεί κάποιος να ισχυρισθεί ότι δεν συμμετείχε σε αυτή.

Το Διαδίκτυο είναι γνωστό για την αφοσίωσή του σε ανοιχτά πρότυπα. Αυτή η υποστήριξη στα ανοιχτά πρότυπα, σε συνδυασμό με την ανοιχτή ανταλλαγή πληροφορίας πάνω από το Διαδίκτυο, ίσως οδηγήσει στη σκέψη ότι Διαδίκτυο και ασφάλεια είναι όροι αμοιβαία αποκλειόμενοι. Κάτι τέτοιο απέχει από την πραγματικότητα. Το Διαδίκτυο έχει εξοπλιστεί με ποικιλία στάνταρτ που καλύπτουν πολλά επίπεδα δικτύωσης, από ασφάλεια σε επίπεδο πακέτου μέχρι ασφάλεια σε επίπεδο εφαρμογών.

Το secure HTTP αναπτύχθηκε με σκοπό να παρέχει ασφαλείς μηχανισμούς επικοινωνίας μεταξύ HTTP πελατών και εξυπηρετητών και να τους δώσει τη δυνατότητα για ασφαλείς εμπορικές συναλλαγές. Οι εταιρείες πιστωτικών καρτών σε συνεργασία με οικονομικούς οργανισμούς, εμπόρους και κατόχους καρτών αναπτύσσουν ασφαλείς και πρωτοποριακές λύσεις για το ηλεκτρονικό εμπόριο (e-commerce). Από παιχνίδια ως υπολογιστές, από λουλούδια ως ρούχα, οι άνθρωποι θα μπορούν να τα αγοράζουν online με εμπιστοσύνη. Αυτή τη στιγμή υπάρχουν δύο τύποι αξιόπιστων τεχνολογιών ασφαλείας, το SSL και το SETTM, που είναι διαθέσιμες για online αγορές.

Όταν κάνουμε συναλλαγές με εμπόρους που γνωρίζουμε, τότε μπορούμε να χρησιμοποιήσουμε SSL για να προστατέψουμε την μυστικότητα της συναλλαγής μας.

Το Secure Sockets Layer (SSL) παρέχει βάσιμη προστασία μυστικότητας με την κρυπτογράφηση του καναλιού μεταξύ του καταναλωτή και του εμπόρου[31]. Για να βρούμε εάν η συναλλαγή μας διασφαλίζεται από το SSL, μπορούμε να ελέγξουμε το άθικτο κλειδί ή το κλειστό σύμβολο κλειδαριάς στο πλαίσιο του παραθύρου του browser μας. Μπορούμε ακόμα να ελέγξούμε το URL του εμπόρου- θα πρέπει να αλλάξει από “http” σε “https” όταν επεξεργαζόμαστε ασφαλείς συναλλαγές. Τόσο το Netscape Navigator όσο και ο Microsoft Internet Explorer χρησιμοποιούν SSL.

Η τεχνολογία SET (Secure Electronic Transaction) αναπτύχθηκε για τη μέγιστη online ασφάλεια που κάνει ικανούς τους καταναλωτές και τους εμπόρους να εξακριβώνουν τη γνησιότητα

[31] An Overview of SSL : http://www.homeport.org./~adam/ssl.html

του άλλου πριν από μια συναλλαγή. Σχεδόν σε όλα τα περιβάλλοντα κατανεμημένων συστημάτων, το ηλεκτρονικό ταχυδρομείο (e-mail) είναι η πιο πολυχρησιμοποιούμενη δικτυακή εφαρμογή. Με την ανερχόμενη εξάρτηση της χρήσης του ηλεκτρονικού ταχυδρομείου για οποιοδήποτε σκοπό μπορεί κανείς να αντιληφθεί, υπάρχει μία αυξανόμενη ανάγκη για υπηρεσίες εξακρίβωση γνησιότητας (authentication) και εμπιστευτικότητας (confidentiality).

Δύο σχήματα κυριαρχούν σήμερα στον τομέα της ασφάλειας στο ηλεκτρονικό ταχυδρομείο: το Pretty Good Privacy (PGP) και το Private-Enhanced Mail (PEM)[32].

Το ηλεκτρονικό σύστημα πληρωμών θα πρέπει να υποστηρίζεται από τις κατάλληλες κρυπτογραφικές τεχνικές δημόσιου κλειδιού. Βασικό στοιχείο των μηχανισμών ασφάλειας αποτελούν και οι ψηφιακές υπογραφές καθώς και η έκδοση και χρησιμοποίηση ψηφιακών πιστοποιητικών. Δίχως αυτά τα στοιχεία πολλοί είναι οι κίνδυνοι και οι απειλές που μπορούν να προκύψουν. Όμως και πάλι προκύπτει ένα πρόσθετο βασικό ζήτημα προς επίλυση. Δεν πρέπει να υπάρξουν κάποιοι περιορισμοί και κάποιες κατευθυντήριες γραμμές στην υλοποίηση όλων αυτών των διαδικασιών; Φυσικά και πρέπει. Ένας από τους πιο διαδεδομένους τρόπους ασφαλείας ενός δικτύου είναι η χρήση firewall. Firewall είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Ένα firewall λειτουργεί σαν μία πύλη από την οποία περνάει όλη η κίνηση από και προς το δίκτυο. Με την χρήση ενός Firewall περιορίζεται η επικοινωνία ανάμεσα στο προστατευόμενο δίκτυο και ένα οποιοδήποτε άλλο δίκτυο.

Υπάρχουν κάποιες βασικές αρχές ασφάλειας και μυστικότητας των προσωπικών δεδομένων που δεν πρέπει να παραβλέπονται και που είναι διεθνώς αποδεκτοί. Με γνώμονα αυτές τις αρχές και γνωρίζοντας την ανάγκη για κοινές με τους Ευρωπαίους εταίρους πολιτικές, πρέπει να πορευτούμε για την εκπόνηση μιας πολιτικής ασφάλειας. Η επιλογή κάποιων σημαντικών οντοτήτων μπορεί να βοηθήσει ή να δυσκολέψει την προσπάθεια εκπόνησης αυτής της πολιτικής.

4.1 Σημασία της ασφάλειας στο ηλεκτρονικό εμπόριο

Η ραγδαία διάδοση του Διαδικτύου (Internet), έχει συμβάλλει κατά πολύ στη διαμόρφωση της σύγχρονης κοινωνίας[33]. Τα αποτελέσματα αυτής της διάδοσης τα ζούμε

[32] PGP FAQ: http://www.cam.ac.uk.pgp.net/pgpnet/pgp-faq/

καθημερινά, σε όλους τους τομείς και όχι μόνο σε μια κλειστή ομάδα ανθρώπων που χρησιμοποιούν τους υπολογιστές. Με βάση αυτό ως δεδομένο αναμενόμενο και λογικό ήταν, η εξέλιξη αυτή να επηρεάσει σημαντικά και έναν καθοριστικό τομέα της ζωής μας, που είναι το εμπόριο. Έτσι, δημιουργήθηκε ένας καινούριος τρόπος ανταλλαγής προϊόντων, το ηλεκτρονικό εμπόριο.

Τι είναι το ηλεκτρονικό εμπόριο ;

Ηλεκτρονικό εμπόριο είναι η ικανότητα να πραγματοποιούνται συναλλαγές, που σχετίζονται με την ανταλλαγή αγαθών ή υπηρεσιών, μεταξύ δύο ή περισσότερων χρησιμοποιώντας ηλεκτρονικά εργαλεία και τεχνικές.

Το χαμηλό κόστος, η εύκολη πρόσβαση, η γρήγορη και συνεχής ενημέρωση, είναι μερικοί μόνο από τους παράγοντες που βοήθησαν στην ανάπτυξη του ηλεκτρονικού εμπορίου. Είναι ένας τρόπος εμπορίου, ο οποίος μπορεί να υιοθετηθεί από όλες τις επιχειρήσεις, ανεξαρτήτως κατηγορίας. Δεν υπάρχει πλέον το πλεονέκτημα των μεγάλων επιχειρήσεων σε σχέση με τις μικρές και μικρομεσαίες. Το κόστος, όπως προαναφέραμε είναι χαμηλό, έτσι παρέχεται η δυνατότητα σε όλους να το εκμεταλλευθούν και να αυξήσουν τις πωλήσεις τους.

Μέχρι εδώ παρουσιάσαμε μόνο θετικά στοιχεία για το ηλεκτρονικό εμπόριο και δεν αναφέραμε τα μειονεκτήματά του. Αυτά είναι και τα οποία φράζουν την εξάπλωσή του και εμποδίζουν την περαιτέρω εξέλιξή του. Το πιο σημαντικό από όλα τα προβλήματα, και το πιο καίριο είναι η ασφάλεια των συναλλαγών[34].

Ο δισταγμός των περισσότερων επιχειρήσεων αλλά και των καταναλωτών οφείλεται κυρίως στην ανησυχία για την ασφάλεια του δικτύου αλλά και των συναλλαγών που πραγματοποιούνται σ' αυτό. Αυτό είναι και το μείζον πρόβλημα που πρέπει να αντιμετωπισθεί και να καθησυχάσει έτσι τόσο τους επιχειρηματίες, όσο και τους υποψήφιους πελάτες. Είναι γνωστές πολλές περιπτώσεις καταστροφής δεδομένων, εξαπάτησης ή κλοπής χρημάτων, υποκλοπής προσωπικών ή οικονομικών πληροφοριών (π.χ. αριθμοί πιστωτικών καρτών) κλπ.

---

[33] Β΄Γνωμοδοτήσεις – Μελέτες «Η πρόταση της οδηγίας της ΕΕ για το ηλεκτρονικό εμπόριο και προστασία του καταναλωτή» Αλεξανδρίδου Ελίζα (περιοδικό «Δίκαιο Επιχειρήσεων & Εταιριών» έτος 6ο, αρ. τεύχους 58, σ. 113)
[34] e-Επιχειρείν Πλήρης Οδηγός Ανάλυσης Τεχνικών Και Εμπορικών Θεμάτων Εκδότης Μ. Γκιούρδας 2001 McGraw Hill Companies

Με βάση αυτά ως δεδομένα διαπιστώνουμε ότι ασφάλεια στο ηλεκτρονικό εμπόριο σημαίνει εξασφάλιση στον καταναλωτή ότι οι συναλλαγές που πραγματοποιεί μέσω του δικτύου είναι απόρρητες και δεν μπορούν να επεξεργασθούν από κανένα τρίτο πρόσωπο. Επίσης, να γνωρίζει ότι η συγκεκριμένη σελίδα του Web που επισκέπτεται ανήκει στη συγκεκριμένη εταιρεία και ότι δε θα δει τα προσωπικά του στοιχεία δημοσιευμένα κάπου στο Internet.

Ένα σύστημα ηλεκτρονικού εμπορίου για να είναι επιτυχημένο θα πρέπει να είναι ασφαλές. Αυτός είναι ο κύριος παράγοντας που το κρίνει. Για να μπορέσει όμως το σύστημα να είναι ασφαλές, θ πρέπει να είναι καταγραμμένα με πλήρη σαφήνεια τα σημεία στα οποία είναι ευάλωτο και με συγκεκριμένες τεχνικές να τα αντιμετωπίσει με επιτυχία. Οι κυριότερες απειλές και επιθέσεις στις οποίες οι εμπορικές δραστηριότητες σε δικτυωμένα περιβάλλοντα είναι ευάλωτα και χρειάζονται επισήμανση είναι τα εξής[35] :

• Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους.

• Καταστροφή πληροφοριών και πόρων.

• Μεταβολή πληροφοριών ή εισαγωγή νέων.

• Αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα.

• Πρόκληση διάρρηξης και διακοπής δικτυακών υπηρεσιών.

• Κλοπή πληροφοριών και δικτυακών πόρων.

• Άρνηση λήψης υπηρεσιών και άρνηση λήψης ή αποστολής πληροφοριών.

• Κατοχή υπηρεσιών χωρίς άδεια.

• Αποκάλυψη σε τρίτους κατά τη διάρκεια της συναλλαγής εμπιστευτικών στοιχείων.

Θεωρείται ίσως το πλέον σημαντικό στοιχείο η κατανόηση αυτών των προβλημάτων. Μόνο με αυτό τον τρόπο μπορούν οι εφαρμογές και οι τεχνολογίες του ηλεκτρονικού εμπορίου να αντιμετωπίσουν τα θέματα αυτά. Με βάση αυτό μπορεί ο διαχειριστής του συστήματος ή ο

[35] Commerce Technology Handbook Daniel Minoli –Emma Minoli McGraw Hill Series

υπεύθυνος ασφαλείας μιας επιχείρησης να επιλέξει κατάλληλα και με καλή απόδοση συστήματα που ελέγχουν και προστατεύουν τις πληροφορίες που είναι κρίσιμες για το τομέα αυτό.

Οι πλέον διαδεδομένοι μέθοδοι προστασίας είναι οι εξής :

• Σύστημα password.

• Απόκρυψη των στοιχείων.

• Ασφάλεια βασισμένη στην εμπιστοσύνη.

Για να μπορέσει το ηλεκτρονικό εμπόριο να διαδοθεί ευρέως και να αναπτυχθεί θα πρέπει να δοθεί ιδιαίτερη σημασία στην εγγυημένη ασφάλεια. Μόνο έτσι θα μπορέσει να ανταγωνισθεί το συμβατικό εμπόριο.

Σε αυτό ακριβώς το σημείο βρίσκεται και η μεγάλη πρόκληση για τους υποστηρικτές του ηλεκτρονικού εμπορίου. Πως θα μπορέσει η ασφάλεια του απλού εμπορίου, που βασίζεται στο χαρτί και στην αμοιβαία εμπιστοσύνη εμπόρου - καταναλωτή, να μεταβεί και στο ηλεκτρονικό εμπόριο. Και για να είμαστε και πιο ακριβείς, πρέπει να πεισθεί και ο υποψήφιος καταναλωτής του αγαθού ή της παρεχόμενης υπηρεσίας για την ασφάλεια και αξιοπιστία του συστήματος ηλεκτρονικού εμπορίου, για να δεχθεί να ολοκληρώσει τη συνδιαλλαγή και να δώσει τα προσωπικά του στοιχεία και δεδομένα.

4.2 Απειλές ασφάλειας στο web

Ένας τρόπος για ομαδοποίηση αυτών των απειλών είναι σε παθητικές και ενεργές επιθέσεις. Οι παθητικές επιθέσεις περιλαμβάνουν την υποκλοπή (eavesdropping) στη δικτυακή κίνηση μεταξύ του browser και του server, και την πρόσβαση σε ένα Web site που υποτίθεται ότι είναι περιορισμένη. Οι ενεργές επιθέσεις περιλαμβάνουν το να υποδύεσαι κάποιον άλλο χρήστη, την αλλαγή του περιεχομένου μηνυμάτων μεταξύ client και server, και την αλλαγή των πληροφοριών σε ένα Web site[36].

Ένας άλλος τρόπος για ταξινόμηση των απειλών έχει να κάνει με την τοποθεσία της απειλής: στο Web server, το Web browser, και τη δικτυακή κίνηση μεταξύ browser και server. Το

[36] e-Επιχειρείν Πλήρης Οδηγός Ανάλυσης Τεχνικών Και Εμπορικών Θεμάτων Εκδότης Μ. Γκιούρδας 2001 McGraw Hill Companies

θέμα της ασφάλειας της κυκλοφορίας είναι στην κατηγορία της δικτυακής ασφάλειας που μας ενδιαφέρει περισσότερο.

Μέχρι εδώ έχει γίνει σαφές ότι η ασφάλεια στο ηλεκτρονικό εμπόριο είναι το πιο σημαντικό δεδομένο που πρέπει να αντιμετωπισθεί σοβαρά για την υλοποίηση ενός ασφαλούς συστήματος. Υπάρχουν διάφορες απαιτήσεις για τη δημιουργία του, οι οποίες σε γενικές γραμμές μπορούν να χωρισθούν στα παρακάτω θέματα :

• Authentication (Έλεγχος αυθεντικότητας) Η διαδικασία αυτή έχει στόχο την εξακρίβωση της ταυτότητας του χρήστη. Όλα τα μέρη που εμπλέκονται στη συναλλαγή πρέπει να αισθάνονται σίγουρα ότι επικοινωνούν με άλλα μέλη που συνεργάζονται και όχι με κάποιον που ισχυρίζεται ότι είναι κάποιος άλλος. Ο έλεγχος αυτός πραγματοποιείται πριν την έναρξη οποιασδήποτε ηλεκτρονικής συναλλαγής και υλοποιείται με τη χρήση διαφόρων τεχνολογιών. Συγκεκριμένα, ο χρήστης παρέχει πληροφορίες για τη ταυτότητά του και συγκρίνονται με αυτές που το σύστημα ήδη γνωρίζει για το χρήστη. Αν το σύστημα λάβει από το χρήστη τις σωστές πληροφορίες (δηλαδή, ταυτίζονται με αυτές που έχει καταχωρημένες), τότε αναγνωρίζει το χρήστη και τον πιστοποιεί σαν το μέλος του συστήματος με τα συγκεκριμένα στοιχεία. Οι μέθοδοι που ακολουθούνται για την πιστοποίηση βασίζονται στα εξής χαρακτηριστικά :

• Επιβεβαίωση κάποιου τύπου ιδιοκτησιακών πληροφοριών, όπως login name και password.

• Κατοχή κάποιας πληροφορίας όπως ένα κλειδί ή μια κάρτα.

• Απόδειξη ότι ένα τρίτο έμπιστο μέλος (π.χ. administrator) έχει ήδη εγκαταστήσει πιστοποίηση γι'αυτόν που τη διεκδικεί. Για να εξακριβωθεί η ταυτότητα ενός χρήστη, τα χαρακτηριστικά αυτά θα πρέπει να συνδυάζονται παρά να τα λαμβάνουμε υπόψη ξεχωριστά. Μερικοί κοινοί τρόποι σε συστήματα ασφαλείας δικτύων, που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών περιλαμβάνουν passwords, προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers - PINs) και διάφορα άλλα.

• Authorization (Εξουσιοδότηση) Το θέμα αυτό περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Στην πράξη εξουσιοδότηση σημαίνει παραχώρηση δικαιωμάτων στο χρήστη από τον ιδιοκτήτη. Για

παράδειγμα κλασσική περίπτωση αποτελεί η εξουσιοδότηση από τον πελάτη στον έμπορο ο έλεγχος των στοιχείων της πιστωτικής του κάρτας και αν τα χρήματα στο λογαριασμό καλύπτουν το ποσό των συναλλαγών. Έτσι, περιορίζονται οι χειρισμοί, οι ενέργειες κάποιου χρήστη στο περιβάλλον αυτό. Η εξουσιοδότηση αποτελείται από μηχανισμούς ελέγχου πρόσβασης, δικτυακούς πόρους και δικαιώματα πρόσβασης. Αυτά περιγράφουν προνόμια πρόσβασης ή άδειες σχετικά με τις συνθήκες κάτω από τις οποίες διάφορες οντότητες μπορούν να έχουν πρόσβαση σε δικτυακούς πόρους και πως επιτρέπεται να μπουν σ' αυτούς τους δικτυακούς πόρους. Τέτοια παραδείγματα αδειών, είναι :

1. • Δημιουργία ή καταστροφή
2. • Διάβασμα ή γράψιμο
3. • Προσθήκη, διαγραφή ή μετατροπή κειμένου.
4. • Εισαγωγή - εξαγωγή
5. • Εκτέλεση

Τα δικαιώματα αυτά ελέγχονται από μια λίστα πρόσβασης. Αυτή καταγράφει τις άδειες των χρηστών. Οι υπηρεσίες πρόσβασης επιβάλλοντα αρχικά από τις υπηρεσίες ελέγχου πρόσβασης.

• Confidentiality (Εμπιστευτικότητα) Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. Παρέχεται μέσω κρυπτογράφησης και είναι απαραίτητο στοιχείο της ιδωτικότητας του χρήστη. Κυρίως για το ηλεκτρονικό εμπόριο, αποτελεί υψίστης σημασίας συστατικό τόσο στην προστασία των οικονομικών δεδομένων, όσο και στην προστασία πληροφοριών ανάπτυξης, οργανωτικών δομών και άλλων προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Είναι χρήσιμη ακόμη και σε πληροφορίες που η δημοσιοποίησή τους εξαρτάται από το χρόνο. Αυτό αφορά για λίστες τιμών ή για κάποια αναφορά που ίσως για κάποιο συγκεκριμένο χρονικό διάστημα να είναι απόλυτα εμπιστευτικές και μετά από αυτό απόλυτα διαθέσιμες στον οποιονδήποτε. Για να καλυφθούν και να συμβιβαστούν αυτές οι ανάγκες και πολιτικές ελέγχου ροής της πληροφορίας, απαραίτητο είναι να περιλαμβάνονται στην εμπιστευτικότητα καθώς και στον έλεγχο της αυθεντικότητας.

Η εμπιστευτικότητα πρέπει να εξασφαλίζει τα εξής :

1. η πληροφορία δεν μπορεί να διαβαστεί, αντιγραφεί, μετατραπεί ή αποκαλυφθεί χωρίς την απαραίτητη εξουσιοδότηση και

2. οι επικοινωνίες μέσω των δικτύων δεν μπορούν να διακοπούν. Τεχνικές κρυπτογράφησης και κωδικοποίησης έχουν σχεδιαστεί για να ικανοποιούν αυτές τις απαιτήσεις.

• Integrity (Ακεραιότητα) Η ακεραιότητα έχει να κάνει με την ασφαλή μεταφορά των δεδομένων στο δίκτυο. Αυτό σημαίνει ότι με κανένα τρόπο δεν πρέπει να υπάρξει, μη εξουσιοδοτημένη τροποποίηση των δεδομένων και αυτό διασφαλίζεται με διάφορες μεθόδους (π.χ. ψηφιακές υπογραφές). Υπάρχουν συγκεκριμένοι μέθοδοι που ελέγχουν αν ένα μήνυμα έχει μεταβληθεί τη στιγμή της μεταφοράς. Στα συστήματα ηλεκτρονικού εμπορίου απαραίτητο είναι η εφαρμογή τέτοιων μεθόδων ώστε να μπορεί να διασφαλισθεί ο χρήστης ότι τα δεδομένα που έστειλε φθάνουν στον προορισμό τους αναλλοίωτα, δηλαδή χωρίς την προσθήκη, αφαίρεσης ή αναδιάταξης μερών των δεδομένων.

• Non-repudiation (Μη αποποίηση της ευθύνης) Αποτελεί ένα πολύ σημαντικό τομέα στην ασφάλεια στο ηλεκτρονικό εμπόριο. Για να ολοκληρωθεί μια συναλλαγή θα πρέπει να μην μπορεί κάποιος να ισχυρισθεί ότι δεν συμμετείχε σε αυτή. Απαραίτητη είναι η διασφάλιση όλων των πλευρών ότι η συνδιαλλαγή τους θα ολοκληρωθεί και από τη στιγμή αυτή, δεν μπορεί κανείς να παρέμβει και να ισχυρισθεί το αντίθετο. Καθίσταται σαφές ότι οι υπηρεσίες μη αποποίησης της ευθύνης θα πρέπει ανά πάσα στιγμή να μπορούν να αποδείξουν την προέλευση, μεταφορά, παράδοση και μετάδοση των δεδομένων, αν φυσικά τους ζητηθεί από κάποιο εξουσιοδοτημένο μέλος. Απαραίτητο είναι να αναφέρουμε ότι η ανάγκη για τέτοιες υπηρεσίες, αντικατοπτρίζει τις ατέλειες που έχει κάθε περιβάλλον επικοινωνίας, και φανερώνει το γεγονός ότι πρέπει να υπάρξουν κατάλληλοι μηχανισμοί ασφαλείας για την ολοκλήρωση των συναλλαγών και των επικοινωνιών.

4.3 Συστήματα ασφάλειας στο διαδίκτυο

Υπάρχουν πολλά διαφορετικά είδη απειλών τα οποία διακυβεύουν την ασφάλεια στο ηλεκτρονικό εμπόριο. Προκειμένου να εξουδετερωθούν αυτές οι απειλές, έχει αναπτυχθεί ένας ικανός αριθμός πρωτοκόλλων και εφαρμογών βασισμένων σε τεχνικές κρυπτογράφησης που ήδη αναλύθηκαν.

Το Διαδίκτυο είναι γνωστό για την αφοσίωσή του σε ανοιχτά πρότυπα. Αυτή η υποστήριξη στα ανοιχτά πρότυπα, σε συνδυασμό με την ανοιχτή ανταλλαγή πληροφορίας πάνω από το Διαδίκτυο, ίσως οδηγήσει στη σκέψη ότι Διαδίκτυο και ασφάλεια είναι όροι αμοιβαία αποκλειόμενοι. Κάτι τέτοιο απέχει από την πραγματικότητα. Το Διαδίκτυο έχει εξοπλιστεί με ποικιλία στάνταρτ που καλύπτουν πολλά επίπεδα δικτύωσης, από ασφάλεια σε επίπεδο πακέτου μέχρι ασφάλεια σε επίπεδο εφαρμογών. Αν επιμένει κανείς να θεωρεί το Διαδίκτυο ανασφαλές μέσο λόγω της αποκεντρωμένης φύσης του, αξίζει να σημειωθεί ότι τα δεδομένα που εμπλέκονται σε συναλλαγές μπορούν να διασφαλιστούν κάνοντας χρήση ενός ικανού αριθμού στάνταρτ.

Πρότυπα ασφάλειας για το Διαδίκτυο:

1. Πρότυπο Λειτουργία Εφαρμογή Secure HTTP (S-http). Καθιστά ασφαλείς τις web συναλλαγές Browsers, web servers και
2. Internet εφαρμογές Secure Sockets Layer (SSL) Παρέχει ασφάλεια σε πακέτα δεδομένων στο επίπεδο δικτύου Browsers, web servers.
3. Internet εφαρμογές Secure MIME (S/MIME) Καθιστά τα προσαρτημένα σε μηνύματα ηλεκτρονικού ταχυδρομείου αρχεία ασφαλή (secure mail attachments)
4. Πακέτα ηλεκτρονικού ταχυδρομείου με RSA κρυπτογράφηση και ψηφιακές υπογραφές Secure Electronic Transactions (SET). Εγγυάται ασφάλεια σε συναλλαγές με πιστωτικές κάρτες, Έξυπνες κάρτες, Transaction Servers

Τα στάνταρτ που καλύπτονται εδώ κατηγοριοποιούνται σύμφωνα με το αν παρέχουν ασφάλεια σύνδεσης ή ασφάλεια εφαρμογών. Στάνταρτ όπως το Secure Sockets Layer (SSL) έχουν σχεδιαστεί με σκοπό να επιτύχουν ασφαλή επικοινωνία στο Διαδίκτυο, αν και το SSL χρησιμοποιείται κυρίως για web εφαρμογές. Το Secure HTTP (S-HTTP) και το Secure MIME (S/MIME), από την άλλη πλευρά, στοχεύουν στην παροχή αυθεντικοποίησης και εμπιστευτικότητας στις εφαρμογές (το S-HTTP για web εφαρμογές και το S/MIME για ηλεκτρονικό ταχυδρομείο και συναφείς εφαρμογές)[37]. Το SET προχωρά ένα βήμα περισσότερο προσφέροντας ασφάλεια στις συναλλαγές ηλεκτρονικού εμπορίου.

[37] SHTTP: The Protocol: http://cis.nyu.edu/xiaodong/security/protocol.html

4.3.1. Secure HTTP

Το secure HTTP αναπτύχθηκε με σκοπό να παρέχει ασφαλείς μηχανισμούς επικοινωνίας μεταξύ HTTP πελατών και εξυπηρετητών και να τους δώσει τη δυνατότητα για ασφαλείς εμπορικές συναλλαγές. Είναι ένα ασφαλές, προσανατολισμένο σε μηνύματα πρωτόκολλο, που σχεδιάστηκε για χρήση σε συνδυασμό με το απλό HTTP. Παρέχει ένα πλήθος από μηχανισμούς ασφάλειας και στους πελάτες και στους εξυπηρετητές, με συμμετρικές υπηρεσίες και δυνατότητες και για τους δύο, ενώ παράλληλα διατηρεί το μοντέλο επικοινωνίας και τα χαρακτηριστικά του HTTP[38].

Το S-HTTP παρέχει ασφαλείς από άκρο-εις-άκρο συναλλαγές, αντίθετα με τους μηχανισμούς εξουσιοδότησης στο HTTP, καθώς οι πελάτες ωθούνται στο να αρχίζουν ασφαλείς συναλλαγές χρησιμοποιώντας πληροφορίες στις επικεφαλίδες των μηνυμάτων. Με το S-HTTP καμιά «ευαίσθητη» πληροφορία δεν είναι ανάγκη να μεταδοθεί στο δίκτυο ανέλεγκτα. Επίσης το S-HTTP παρέχει πλήρη ευελιξία σε αλγορίθμους κρυπτογράφησης και παραμέτρους. Η δημιουργία ενός S-HTTP μηνύματος γίνεται από τον αποστολέα ενσωματώνοντας τις δικές του κρυπτογραφικές επιλογές με αυτές του παραλήπτη. Το αποτέλεσμα είναι μία λίστα από κρυπτογραφικές εμπλουτίσεις και κλειδιά, έτοιμα να εφαρμοστούν. Για να γίνει αυτό, μπορεί να χρειαστεί η μεσολάβηση του χρήστη. Για παράδειγμα, μπορεί να παρέχονται πολλά κλειδιά για να υπογραφεί το μήνυμα. Με βάση αυτά τα δεδομένα, ο αποστολές εφαρμόζει τις εμπλουτίσεις στο κείμενο του μηνύματος και δημιουργεί ένα S-HTTP μήνυμα.

Ο αποστολέας μπορεί ήδη να έχει δηλώσει ότι θα εκτελέσει κάποιες κρυπτογραφικές λειτουργίες πάνω στο μήνυμα. Για να ανακτήσει το S-HTTP μήνυμα, ο παραλήπτης πρέπει να διαβάσει τις επικεφαλίδες για να ανακαλύψει ποιες κρυπτογραφικοί μετασχηματισμοί έγιναν στο μήνυμα, μετά να αφαιρέσει τους μετασχηματισμούς, χρησιμοποιώντας κάποιο συνδυασμό των κλειδιών του αποστολέα και του παραλήπτη, ενώ παράλληλα θα σημειώνει ποιες εμπλουτίσεις έγιναν. Ο παραλήπτης μπορεί επίσης να επιλέξει να επικυρώσει ότι οι εφαρμοσμένες εμπλουτίσεις ταιριάζουν τόσο με τις εμπλουτίσεις που ο αποστολέας είπε ότι θα εφάρμοζε όσο και με αυτά που ο παραλήπτης ζήτησε, καθώς και με τις τρέχουσες κρυπτογραφικές προτιμήσεις, για να δει αν το S-HTTP μήνυμα μετασχηματίστηκε κατάλληλα. Αυτή η διαδικασία μπορεί να απαιτεί αλληλεπίδραση με το χρήστη για να επικυρώσει ότι οι εμπλουτίσεις είναι αποδεκτές στο χρήστη.

[38] SHTTP: The Protocol: http://cis.nyu.edu/xiaodong/security/protocol.html

Για να προσφέρουν ευελιξία στα κρυπτογραφικές εμπλουτίσεις που χρησιμοποιούνται, ο πελάτης και ο εξυπηρετητής διαπραγματεύονται τις εμπλουτίσεις που ο καθένας προτίθεται να χρησιμοποιήσει, δεν προτίθεται να χρησιμοποιήσει, ή θα απαιτήσει να χρησιμοποιηθούν. Τα μπλοκ διαπραγμάτευσης αποτελούνται από τέσσερα μέρη: ιδιότητα, τιμή, κατεύθυνση και ένταση. Εάν οι πράκτορες δεν είναι ικανοί να ανακαλύψουν ένα κοινό σύνολο αλγορίθμων θα πρέπει να γίνουν οι κατάλληλες ενέργειες. Η συνεχής αίτηση μιας αρνούμενης επιλογής θεωρείται αναποτελεσματική και ακατάλληλη.

Προστασία του μηνύματος

Η προστασία του μηνύματος μπορεί να παρέχεται σε τρεις άξονες:

1. Υπογραφή
2. Εξακρίβωση γνησιότητας
3. Κρυπτογράφηση

Πολλαπλοί μηχανισμοί διαχείρισης κλειδιού υποστηρίζονται, συμπεριλαμβανομένου διαμοιραζόμενων μυστικών, με στυλ κωδικών, ανταλλαγή δημοσίου κλειδιού και διανομή εισιτηρίου (ticket) στον Κέρβερο.

Συγκεκριμένα έχει γίνει πρόβλεψη για προκαθορισμένα συμμετρικά session κλειδιά με σκοπό να σταλούν εμπιστευτικά μηνύματα σε αυτούς που δεν έχουν ζευγάρι δημόσιου/ιδιωτικού κλειδιού. Επιπρόσθετα ένας μηχανισμός απόκρισης-πρόκλησης («nonce») παρέχεται για να επιτρέπει σε όσους θέλουν να επιβεβαιωθούν για το ότι η συναλλαγή έχει γίνει πρόσφατα.

Αν εφαρμόζεται ο εμπλουτισμός της ηλεκτρονικής υπογραφής, είτε ένα κατάλληλο πιστοποιητικό μπορεί να προσαρτηθεί στο μήνυμα, είτε ο αποστολέας μπορεί να αναμένει από τον παραλήπτη να αποκτήσει το απαιτούμενο πιστοποιητικό ανεξάρτητα.

Για την υποστήριξη της bulk κρυπτογράφησης, το S-HTTP ορίζει δύο μηχανισμούς μεταφοράς κλειδιού, έναν που χρησιμοποιεί ανταλλαγή κρυπτογραφημένου κλειδιού και έναν άλλο με κλειδιά που είναι κανονισμένα εξωτερικά. Στην πρώτη περίπτωση, η παράμετρος του συστήματος συμμετρικής κρυπτογράφησης περνιέται κρυπτογραφημένη με το δημόσιο κλειδί του παραλήπτη. Στην άλλη περίπτωση κρυπτογραφούμε το περιεχόμενο χρησιμοποιώντας ένα

καθορισμένο session κλειδί με τις πληροφορίες αναγνώρισης κλειδιού να ορίζονται σε μία από τις γραμμές της επικεφαλίδας. Τα κλειδιά μπορούν ακόμα να εξαχθούν από τα εισιτήρια του Κέρβερου.

Το S-HTTP παρέχει ένα τρόπο για να επικυρώνει την ακεραιότητα του μηνύματος και την εξακρίβωση γνησιότητας του αποστολέα για ένα μήνυμα μέσω του υπολογισμού ενός κωδικού εξακρίβωσης γνησιότητας μηνύματος (Message Authentication Code – MAC), που υπολογίζεται σαν ένα hash κλειδιού πάνω από το κείμενο, χρησιμοποιώντας ένα διαμοιραζόμενο μυστικό-το οποίο θα μπορούσε να έχει κανονιστεί με διάφορους τρόπους. Αυτή η τεχνική δεν απαιτεί ούτε τη χρήση κρυπτογραφίας δημοσίου κλειδιού, ούτε κρυπτογράφησης.

Το πρωτόκολλο παρέχει ένα απλό μηχανισμό απόκρισης/πρόκλησης, επιτρέποντας και στα δύο μέρη να επιβεβαιώσουν ότι οι μεταδόσεις έγιναν πρόσφατα. Επιπρόσθετα, η προστασία της ακεραιότητας που παρέχεται στις επικεφαλίδες του HTTP, αποδέχεται οι υλοποιήσεις να θεωρούν την επικεφαλίδα «Date:» ως ένα δείκτη ανανέωσης, όπου είναι δυνατό.

Τα Nonces είναι αδιαφανείς, προσωρινοί, προσανατολισμένοι-στη-σύνοδο (session-oriented) identifiers, που μπορούν να χρησιμοποιηθούν για να παρέχουν μία ένδειξη ανανέωσης. Οι τιμές των nonces είναι ένα θέμα τοπικό, αν και μπορεί απλά να είναι τυχαίοι αριθμοί που παράγονται από τον αποστολέα. Η τιμή παρέχεται απλά για να επιστραφεί από τον παραλήπτη.

Η σύνταξη του S-HTTP επίτηδες μιμείται τη σύνταξη του HTTP σε μία προσπάθεια να διευκολύνει την ενσωμάτωση στα συστήματα που ήδη χρησιμοποιούν το HTTP. Επιπλέον, ορισμένες HTTP επικεφαλίδες γίνονται S-HTTP επικεφαλίδες, γιατί παρέχουν χρήσιμες λειτουργίες που έχουν προεκτάσεις στην ασφάλεια. Ένα S-HTTP μήνυμα αποτελείται από μία γραμμή αίτησης ή κατάστασης (όπως και στο HTTP) ακολουθούμενη από τις επικεφαλίδες που καθορίζονται στο RFC-822, ακολουθούμενα από ένα κρυμμένο κείμενο. Όταν ανακτάται το περιεχόμενο του κειμένου, μπορεί να είναι είτε ένα άλλο S-HTTP μήνυμα, είτε απλά δεδομένα.

Το S-HTTP παρέχει διάφορες δυνατότητες για το στάνταρ που θα ακολουθηθεί στη μορφή του μηνύματος από τους πελάτες και τους εξυπηρετητές, αλλά κυρίως χρησιμοποιούνται το [PKCS-7] και το [MOSS].

Ορισμένες HTTP ευκολίες, και ιδιαίτερα εκείνες που αναφέρονται με το caching και τους αντιπροσώπους (proxies), απαιτούν ειδική θεώρηση, όταν εφαρμόζεται S-HTTP επεξεργασία.

Το S-HTTP παρέχει ειδική μεταχείριση για αυτά τα χαρακτηριστικά, αντιγράφοντας τις σχετικές HTTP επικεφαλίδες με S-HTTP σύνταξη. Οι επικεφαλίδες που έχουν εισαχθεί από το HTTP φαίνονται στον παρακάτω πίνακα.

Η χρήση του S-HTTP παρουσιάζει και κάποια θέματα υλοποίησης στη χρήση των HTTP αντιπροσώπων. Ενώ είναι απλό να επιτρέπεις στον αντιπρόσωπο να προωθεί τις αιτήσεις, θα ήταν προτιμότερο να μπορούσαν οι S-HTTP αντιπρόσωποι να κρατάνε σε προσωρινή μνήμη (Cache) τις απαντήσεις, τουλάχιστο σε ορισμένες περιπτώσεις. Επιπλέον, το S-HTTP παρέχει εξακρίβωση γνησιότητας σε πελάτη και σε αντιπρόσωπο.

Όταν ένας S-HTTP αντιπρόσωπος παραλαμβάνει μία αίτηση (S-HTTP ή HTTP) που απαιτεί να εξακριβωθεί η προέλευσή της, επιστρέφει τον κωδικό κατάστασης 422. Ο πελάτης, που λαμβάνει την απάντηση αυτή διαβάζει τις κρυπτογραφικές επιλογές που έστειλε ο αντιπρόσωπος και αν είναι πρόθυμος να παρέχει αυτές τις εμπλουτίσεις στο μήνυμα, ενθυλακώνει το προηγούμενο μήνυμα, χρησιμοποιώντας τις ζητούμενες επιλογές.

Αν και είναι καλό να αποφεύγεται η προσωρινή αποθήκευση (caching) για λόγους ασφάλειας και εμπιστευτικότητας, αυτό συμβαίνει μόνο σε ορισμένες περιπτώσεις, π.χ. όταν η εμπιστευτικότητα χρησιμοποιείται για να περιορίσει την πρόσβαση ορισμένων χρηστών σε μία κλάση εγγράφων. Για να ζητήσει δεδομένα που έχουν αποθηκευτεί προσωρινά στον αντιπρόσωπο, ο πελάτης στέλνει στον αντιπρόσωπο ολόκληρη τη γραμμή του URL για να του δώσει να καταλάβει ότι ζητούνται αποθηκευμένα δεδομένα. Ο αντιπρόσωπος πρέπει να αναγνωρίζει ποια URLs βρίσκονται στην προσωρινή του μνήμη και να ελέγχει την επικεφαλίδα Content-MD5 για να είναι σίγουρος ότι συνέβη μία έγκυρη αίτηση στην προσωρινή μνήμη.

4.3.2 Socket Secure Layer (SSL)

Το SSL προήλθε από την Netscape. Όταν ήρθε η ανάγκη για τυποποίηση στο Internet, η ομάδα TLS σχηματίστηκε στην IETF για να αναπτύξει ένα κοινό πρότυπο. Το SSL έχει σχεδιαστεί ώστε να κάνει χρήση του TCP και να παρέχει αξιόπιστη end-to-end ασφαλή υπηρεσία. Μάλιστα, το SSL δεν είναι ένα πρωτόκολλο αλλά δύο επίπεδα πρωτοκόλλων[39].

[39] PC Magazine , “Secure Sockets Layer –SSL 3.0 ”, May 26, 1998

Το SSL Record Protocol παρέχει βασικές υπηρεσίες ασφάλειας σε διάφορα πρωτόκολλα υψηλότερων επιπέδων, όπως το HTTP. Τρία πρωτόκολλα υψηλότερων επιπέδων ορίζονται ως μέρη του SSL: το Handshake Protocol, το Change Cipher Spec Protocol και το Alert Protocol. Αυτά τα SSL-specific πρωτόκολλα χρησιμεύουν στη διαχείριση των SSL ανταλλαγών.

Το SSL Record Protocol παρέχει δύο υπηρεσίες για SSL συνδέσεις:

1. εμπιστευτικότητα: Το Handshake Protocol ορίζει ένα διαμοιραζόμενο μυστικό κλειδί που χρησιμεύει στη συμβατική κρυπτογράφηση των SSL payloads.
2. ακεραιότητα μηνύματος: Το Handshake Protocol επίσης ορίζει ένα διαμοιραζόμενο μυστικό κλειδί που χρησιμοποιείται για το σχηματισμό του message authentication code (MAC).

Το Record Protocol παίρνει το μήνυμα της εφαρμογής που θα μεταδοθεί, τμηματοποιεί τα δεδομένα σε εύχρηστα blocks, προαιρετικά συμπιέζει τα δεδομένα, εφαρμόζει ένα MAC, κρυπτογραφεί, προσθέτει μια επικεφαλίδα, και μεταδίδει το αποτέλεσμα αυτό σε ένα TCP segment. Τα δεδομένα που λαμβάνονται αποκρυπτογραφούνται, επιβεβαιώνονται, αποσυμπιέζονται, επανασυγκεντρώνονται και διανέμονται στους χρήστες των ανώτερων επιπέδων.

Το πρώτο βήμα είναι η τμηματοποίηση. Κάθε μήνυμα υψηλότερού επιπέδου τμηματοποιείται σε blocks των 214 bytes (16384 bytes) ή λιγότερο. Η συμπίεση εφαρμόζεται προαιρετικά. Το επόμενο βήμα είναι να υπολογιστεί το message authentication code πάνω από τα συμπιεσμένα δεδομένα. Για αυτό το σκοπό χρησιμοποιείται ένα διαμοιραζόμενο μυστικό κλειδί. Στη συνέχεια, το αποτέλεσμα κρυπτογραφείται χρησιμοποιώντας συμμετρική κρυπτογράφηση. Οι παρακάτω αλγόριθμοι είναι επιτρεπτοί:

1. Clock Cipher Stream Cipher
2. Αλγόριθμος Μέγεθος κλειδιού Αλγόριθμος Μέγεθος κλειδιού
3. IDEA 128 RC4-40 40
4. RC2-40 40 RC4-128 128
5. DES-40 40
6. DES 56
7. 3DES 168
8. Fortezza 80

Για την κρυπτογράφηση ρεύματος, το συμπιεσμένο μήνυμα μαζί με το MAC κρυπτογραφούνται. Για block κρυπτογράφηση, μπορεί να προστεθεί padding μετά το MAC πριν τη κρυπτογράφηση. Το τελικό βήμα της επεξεργασίας του SSL Record Protocol είναι η προσθήκη μιας επικεφαλίδας.

Change Cipher Spec Protocol

Είναι το απλούστερο από τα τρία SSL-specific πρωτόκολλα που χρησιμοποιούν το SSL Record Protocol. Αποτελείται από ένα απλό μήνυμα μήκους ενός byte με τιμή ίση με 1. Ο μόνος σκοπός αυτού του μηνύματος είναι να προκαλέσει την εκκρεμή κατάσταση να αντιγραφεί στην τρέχουσα κατάσταση που ενημερώνει το cipher suite να χρησιμοποιηθεί σε αυτή τη σύνδεση.

Alert Protocol

Χρησιμοποιείται για να μεταφέρει συναγερμούς στην ομότιμη οντότητα. Κάθε μήνυμα στο πρωτόκολλο αποτελείται από δύο bytes. Το πρώτο byte παίρνει την τιμή προειδοποίηση (1) ή μοιραίο (2) για να μεταφέρει τη σημασία του μηνύματος. Το δεύτερο byte περιέχει ένα κώδικα που ορίζει το συγκεκριμένο συναγερμό.

Handshake Protocol

Το πιο περίπλοκο τμήμα του SSL είναι το Handshake Protocol. Αυτό το πρωτόκολλο επιτρέπει στον server και τον client να εξακριβώσουν την γνησιότητα του άλλου, να διαπραγματευτούν τον αλγόριθμο κρυπτογράφησης και MAC, και τα κλειδιά κρυπτογράφησης που θα προστατέψουν τα δεδομένα στο SSL record. Το handshake protocol χρησιμοποιείται πριν μεταδοθούν τα δεδομένα. Αποτελείται από μια σειρά μηνυμάτων που ανταλλάσσονται μεταξύ του client και του server. Κάθε μήνυμα έχει τρία πεδία:

1. Τύπος (1 byte),
2. Μήκος (3 bytes) και
3. Περιεχόμενο (>1 byte).

Η ανταλλαγή μηνυμάτων μπορεί να θεωρηθεί ότι έχει τέσσερις φάσεις.

Φάση 1. Εγκατάσταση Ικανοτήτων Ασφάλειας

Η φάση αυτή χρησιμοποιείται για να αρχικοποιήσει μια λογική σύνδεση και να εγκαταστήσει τις ικανότητες ασφάλειας που θα συνδεθούν με αυτή. Αυτή η ανταλλαγή αρχικοποιείται από τον client, που στέλνει μήνυμα client_hello με τις ακόλουθες παραμέτρους: έκδοση, random, session ID, Cipher Suite, μέθοδο συμπίεσης. Αφού σταλεί το μήνυμα αυτό, ο client περιμένει το μήνυμα server_hello, που έχει τις ίδιες παραμέτρους με αυτές του client_hello.

Φάση 2. Εξακρίβωση γνησιότητας Server και Ανταλλαγή κλειδιών. Ο server ξεκινά αυτή τη φάση στέλνοντας το πιστοποιητικό του, εάν χρειάζεται να εξακριβωθεί η γνησιότητά του. Το μήνυμα certificate απαιτείται για οποιαδήποτε συμφωνημένη μέθοδο ανταλλαγής, εκτός από τη μέθοδο anonymous Diffie-Hellman. Στη συνέχεια, ένα μήνυμα server_key_exchange μπορεί να σταλεί αν αυτό απαιτείται. Μετά ένας non-anonymous server μπορεί να απαιτήσει ένα πιστοποιητικό από τον πελάτη. Το μήνυμα certificate_request περιλαμβάνει δύο παραμέτρους: τύπο πιστοποιητικού και εξουσιοδοτήσεις πιστοποιητικού. Το τελικό μήνυμα της φάσης 2 είναι το server_done, που σηματοδοτεί το τέλος του μηνύματος hello.

Φάση 3. Εξακρίβωση γνησιότητας Client και Ανταλλαγή κλειδιών

Εάν ο server έχει απαιτήσει πιστοποιητικό, ο client αρχίζει τη φάση αυτή στέλνοντας μήνυμα certificate. Στη συνέχεια είναι το μήνυμα client_key_exchange που πρέπει να σταλεί σε αυτή την φάση. Τέλος, ο client μπορεί να στείλει ένα μήνυμα certificate_verify για να παρέχει επικύρωση του πιστοποιητικού.

Φάση 4. Τέλος

Αυτή η φάση ολοκληρώνει την εγκατάσταση μιας ασφαλούς σύνδεσης. Ο client στέλνει μήνυμα change_cipher_spec και αντιγράφει το εκκρεμές CipheSpec στο τρέχον CipherSpec. Μετά, ο client στέλνει το μήνυμα finished που επικυρώνει ότι οι διεργασίες ανταλλαγής κλειδιών και εξακρίβωσης γνησιότητας ήταν επιτυχημένες. Σε απάντηση αυτών των δύο μηνυμάτων, ο server στέλνει το δικό του μήνυμα change_cipher_spec, μεταφέρει το εκκρεμές CipherSpec στο τρέχον CipherSpec, και στέλνει το μήνυμα finished. Σε αυτό το σημείο το handshake έχει ολοκληρωθεί και ο client με τον server μπορούν να ξεκινήσουν να την ανταλλαγή δεδομένων του επιπέδου εφαρμογής.

Υπάρχει ένας αριθμός από κλειδιά που χρησιμοποιούνται: το δημόσιο κλειδί του server, το serverwrite- key, και το client-write-key. Το server-write-key, και το client-write-key παράγονται μέσω μιας hash από το master key, ένα ordinal χαρακτήρα, την πρόκληση και το id της σύνδεσης.

4.3.3 Ασφάλεια στο ηλεκτρονικό εμπόριο -SET

Το SET είναι μια ανοικτή προδιαγραφή κρυπτογράφησης και ασφάλειας που σχεδιάστηκε για να προστατέψει τις συναλλαγές με πιστωτικές κάρτες σε ένα ανοικτό δίκτυο, όπως το Internet. Από τον Απρίλιο του 1997, προγράμματα SET λαμβάνουν χώρα σε 39 χώρες παγκοσμίως όπως τις Η.Π.Α, Νότια Αφρική, Αυστραλία, Μαλαισία, Χονγκ-Κονγκ, Κορέα, Μεγάλη Βρετανία και Καναδά. Μάλιστα, νέες αγορές έρχονται στο προσκήνιο[40].

Το SET δεν είναι από μόνο του ένα σύστημα πληρωμής, αλλά ένα σύνολο από πρωτόκολλα και τυποποιήσεις που βοηθάνε τους χρήστες να χρησιμοποιήσουν την υπάρχουσα υποδομής πληρωμής με πιστωτικές κάρτες στο Internet, με ασφαλή τρόπο. Βασικά το SET προσφέρει τρεις υπηρεσίες:

1. Παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ όλων των συμμέτοχων στη συναλλαγή.
2. Παρέχει εμπιστοσύνη με τη χρήση των ηλεκτρονικών πιστοποιητικών (digital certificates) X.509v3 για να επιβεβαιώσει ότι οι καταναλωτές και οι έμποροι εξουσιοδοτούνται να χρησιμοποιούν και να δέχονται αντίστοιχα πιστωτικές κάρτες. Αυτό είναι το ηλεκτρονικό ισοδύναμο ενός καταναλωτή που ψάχνει την επιγραφή της πιστωτικής του εταιρείας στη βιτρίνα ενός καταστήματος, και του εμπόρου που ελέγχει την υπογραφή του καταναλωτή στο πίσω μέρος της πιστωτικής του κάρτας.
3. Εγγυάται την μυστικότητα επειδή η πληροφορία είναι διαθέσιμη στους ενδιαφερομένους μόνο όταν και όπου αυτό είναι αναγκαίο. Έτσι η πληροφορία της κάρτας πληρωμής του καταναλωτή προστατεύεται έως ότου φτάσει στον οικονομικό οργανισμό. Ο έμπορος δεν μπορεί να διαβάσει αυτή την πληροφορία στη συναλλαγή πληρωμής.

40 The World Wide Web Security FAQ: http://www.w3.org/Security/faq/wwwsf1.html

Το SET ορίζει τις παρακάτω απαιτήσεις για ασφαλή επεξεργασία πληρωμής με πιστωτικές κάρτες πάνω από το Internet:

1. Παρέχει εμπιστευτικότητα στις πληροφορίες πληρωμής και παραγγελίας.
2. Εγγυάται την ακεραιότητα των μεταδιδόμενων δεδομένων.
3. Παρέχει πιστοποίηση ότι ο κάτοχος της κάρτας είναι νόμιμος χρήστης του λογαριασμού της πιστωτικής κάρτας.
4. Παρέχει πιστοποίηση ότι ο έμπορος μπορεί να δεχτεί συναλλαγές με πιστωτική κάρτα μέσω της συνεργασίας του με κάποιο οικονομικό οργανισμό.
5. Εγγυάται τη χρήση των καλύτερων πρακτικών ασφαλείας και τεχνικών σχεδίασης συστημάτων για να προστατέψει όλους τους νόμιμους συμμέτοχους στη συναλλαγή ηλεκτρονικού εμπορίου.
6. Δημιουργεί ένα πρωτόκολλο που δεν εξαρτάται από τους μηχανισμούς μεταφοράς ασφαλείας ούτε εμποδίζει την χρήση τους.
7. Διευκολύνει και ενθαρρύνει την αλληλεπίδραση μεταξύ software και network providers.
8. Το SET ενσωματώνει τα ακόλουθα χαρακτηριστικά:
9. Εμπιστευτικότητα της πληροφορίας
10. Ακεραιότητα των δεδομένων
11. Εξακρίβωση γνησιότητας του λογαριασμού του κατόχου της κάρτας
12. Εξακρίβωση γνησιότητας του εμπόρου

Οι συμμέτοχοι του SET

1. Κάτοχος της κάρτας.
2. Έμπορος.
3. Πάροχος (Issuer): Είναι οικονομικός οργανισμός, όπως μια τράπεζα, που παρέχει την πιστωτική κάρτα στον κάτοχο αυτής.
4. Acquirer: Είναι οικονομικός οργανισμός που ανοίγει ένα λογαριασμό με ένα έμπορο και επεξεργάζεται τις πληρωμές και τις εξουσιοδοτήσεις πληρωμής των καρτών.
5. Payment Gateway: Είναι μια λειτουργία που επιτελείται από τον acquirer ή κάποιο τρίτο, και επεξεργάζεται τα μηνύματα πληρωμής του εμπόρου.

6. Υπηρεσία πιστοποίησης (Certificate Authority): Είναι μια οντότητα που εκδίδει X.509v3 πιστοποιητικά δημοσίου-κλειδιού σε κατόχους κάρτας, εμπόρους, και payment gateways.

Η συναλλαγή στο SET

Περιγράφουμε την ακολουθία των γεγονότων που απαιτούνται για μια συναλλαγή.

1. Ο πελάτης αποκτά το ηλεκτρονικό πορτοφόλι (digital wallet), το software που επικοινωνεί με το SET software του εμπόρου αυτόματα για να επιβεβαιώσει το πιστοποιητικό του εμπόρου και τη σχέση του με ένα έμπιστο οικονομικό οργανισμό.
2. Ο πελάτης ανοίγει ένα λογαριασμό, από μια τράπεζα που υποστηρίζει ηλεκτρονική πληρωμή και SET.
3. Ο πελάτης λαμβάνει ένα X.509v3 ηλεκτρονικό πιστοποιητικό, το οποίο επιβεβαιώνει το δημόσιο-κλειδί RSA του πελάτη και την ημερομηνία λήξης του πιστοποιητικού.
4. Οι έμποροι έχουν τα δικά τους πιστοποιητικά: ένα πιστοποιητικό δημοσίου-κλειδιού για την υπογραφή μηνυμάτων και ένα άλλο για την ανταλλαγή κλειδιού.
5. Ο πελάτης κάνει μια παραγγελία.
6. Ο έμπορος επιβεβαιώνεται, δηλαδή στέλνει ένα αντίγραφο του πιστοποιητικού του στον πελάτη.
7. Η παραγγελία και η πληρωμή στέλνονται στον έμπορο, μαζί με το πιστοποιητικό του πελάτη.
8. Ο έμπορος ζητά εξουσιοδότηση πληρωμής από το payment gateway, δηλαδή ότι η πίστωση του πελάτη είναι επαρκής για την αγορά.
9. Ο έμπορος επιβεβαιώνει την παραγγελία στον πελάτη.
10. Ο έμπορος παρέχει τα αγαθά ή την υπηρεσία.
11. Ο έμπορος απαιτεί την πληρωμή από το payment gateway, που χειρίζεται την επεξεργασία πληρωμών.

Διπλή υπογραφή

Μια σημαντική καινοτομία που εισάγεται στο SET είναι η διπλή υπογραφή (dual signature). Ο σκοπός της είναι να συνδέσει δύο μηνύματα που απευθύνονται σε δύο διαφορετικούς

παραλήπτες. Ο πελάτης θέλει να στείλει την πληροφορία παραγγελίας (Order Information - OI) στον έμπορο και την πληροφορία πληρωμής (Payment Information - PI) στην τράπεζα, και του παρέχεται επιπλέον προστασία σε μυστικότητα για να κρατήσει ξεχωριστά αυτά τα δύο αντικείμενα. Ο σύνδεσμος χρειάζεται έτσι ώστε ο πελάτης να μπορεί να αποδείξει ότι αυτή η πληρωμή προορίζεται για τη συγκεκριμένη παραγγελία και όχι για άλλα αγαθά ή υπηρεσία.

Ας υποθέσουμε ότι ο πελάτης στέλνει δύο μηνύματα στον έμπορο- ένα υπογεγραμμένο OI και ένα υπογεγραμμένο PI - και ότι ο έμπορος δίνει το PI στην τράπεζα. Αν ο έμπορος μπορεί να αποκτήσει άλλο OI από τον πελάτη θα μπορούσε να ισχυριστεί ότι το δεύτερο OI πηγαίνει με το PI αντί για το γνήσιο OI. Ετσι, ο έμπορος όταν λάβει το OI και τη διπλή υπογραφή (DS) μπορεί να την επιβεβαιώσει. Η τράπεζα όταν λάβει το PI και το DS μπορεί να επιβεβαιώσει την υπογραφή. Ο πελάτης έχει συνδέσει το OI και το PI και μπορεί να αποδείξει το σύνδεσμο. Από τους τύπους συναλλαγών του SET οι πιο σημαντικοί είναι οι παρακάτω:

ΑΙΤΗΣΗ ΑΓΟΡΑΣ (PURCHASE REQUEST)

Η ανταλλαγή αίτησης αγοράς αποτελείται από τέσσερα μηνύματα: Initiate Request, Initiate Response, Purchase Request, και Purchase Response. Ο κάτοχος της κάρτας πρέπει να έχει αντίγραφα των πιστοποιητικών του εμπόρου και του payment gateway, οπότε και ζητά τα πιστοποιητικά αυτά στο μήνυμα Initiate Request προς τον έμπορο. Ο έμπορος αποκρίνεται και υπογράφει με το ιδιωτικό του κλειδί. Το Initiate Response μήνυμα περιλαμβάνει τα πιστοποιητικά του εμπόρου και του payment gateway. Ο κάτοχος της κάρτας επιβεβαιώνει τα πιστοποιητικά μέσω των αντίστοιχων CA υπογραφών τους, και στη συνέχεια δημιουργεί το OI και το PI. Μετά, ετοιμάζει το Purchase Request μήνυμα, και για αυτό το σκοπό παράγει ένα one-time συμμετρικό κλειδί κρυπτογράφησης, το Ks. Το μήνυμα περιλαμβάνει τα ακόλουθα:

• Πληροφορία σχετική με την αγορά. Αυτή η πληροφορία θα προωθηθεί στο payment gateway από τον έμπορο.

• Πληροφορία σχετικά με την παραγγελία. Αυτή η πληροφορία χρειάζεται από τον έμπορο.

• Πιστοποιητικό του κατόχου της κάρτας. Αυτό περιέχει το δημόσιο κλειδί του κατόχου, και χρειάζεται από τον έμπορο και το payment gateway.

Όταν ο έμπορος λάβει το μήνυμα Purchase Request, εκτελεί τις παρακάτω ενέργειες:

• Επιβεβαιώνει τα πιστοποιητικά του κατόχου της κάρτας.

• Επιβεβαιώνει τη διπλή υπογραφή, χρησιμοποιώντας το δημόσιο κλειδί του πελάτη.

• Επεξεργάζεται την παραγγελία και προωθεί την πληροφορία πληρωμής στο payment gateway.

• Στέλνει μήνυμα purchase response στον κάτοχο της κάρτας.

ΜΗΝΥΜΑ ΑΠΟΚΡΙΣΗΣ ΑΓΟΡΑΣ (PURCHASE RESPONSE)

Αποτελείται από ένα block απόκρισης που αναγνωρίζει την παραγγελία και αναφέρει τον κατάλληλο αριθμό συναλλαγής. Όταν το software του κατόχου της κάρτας λάβει το μήνυμα, επιβεβαιώνει το πιστοποιητικό του εμπόρου και την υπογραφή στο block απόκρισης.

ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΛΗΡΩΜΗΣ (PURCHASE AUTHORIZATION)

Η εξουσιοδότηση πληρωμής εγγυάται ότι η συναλλαγή έγινε δεκτή από τον issuer, δηλαδή ότι ο έμπορος θα πληρωθεί. Στη συνέχεια ο έμπορος μπορεί να παρέχει τις υπηρεσίες ή τα αγαθά στον πελάτη. Ο έμπορος στέλνει ένα μήνυμα Authorization Request στο payment gateway που αποτελείται από

• Πληροφορίες σχετικές με την αγορά

• Πληροφορίες σχετικές με την εξουσιοδότηση

• Πιστοποιητικά

Το payment gateway έχοντας αποκτήσει την εξουσιοδότηση από τον issuer, επιστρέφει μήνυμα Authorization Response στον έμπορο, που περιλαμβάνει τα ακόλουθα:

• Πληροφορίες σχετικές με την εξουσιοδότηση

• Capture token πληροφορία. Αυτή η πληροφορία θα χρησιμοποιηθεί για να πραγματοποιηθεί η πληρωμή αργότερα.

• Πιστοποιητικό του gateway

ΑΠΟΚΤΗΣΗ ΠΛΗΡΩΜΗΣ (PAYMENT CAPTURE)

Για να πληρωθεί ο έμπορος, ανταλλάσσει με το payment gateway ένα μήνυμα capture request και ένα μήνυμα capture response. Το Capture Request μήνυμα περιλαμβάνει το ποσό πληρωμής, το id της συναλλαγής και το capture token από το Authorization Response. Όταν το payment gateway λάβει το μήνυμα αφού ελέγξει για τη συνέπεια μεταξύ του capture request και του capture token, δημιουργεί ένα αίτημα συμψηφισμού που στέλνεται στον issuer, και έτσι μεταφέρονται τα χρήματα στο λογαριασμό του εμπόρου. Εν συνεχεία, το gateway ειδοποιεί τον έμπορο για την πληρωμή με ένα μήνυμα Capture Response. Πρέπει να τονιστεί ότι το SET δεν επηρεάζει την απόδοση του συστήματος ή της συναλλαγής. Μελέτη του Gartner Group το 1998, δείχνει ότι η απόδοση των εγκαταστάσεων SETTM είναι περισσότερο από επαρκής για απαιτήσεις μεγάλου όγκου συναλλαγών Ασφάλεια στο ηλεκτρονικό ταχυδρομείο: PEM, S/MIME και PGP.

Όσον αφορά, τώρα, την προστασία των ηλεκτρονικών ταχυδρομείων ενδεικτικά αναφέρουμε τα εξής standards:

• Privacy Enhanced Mail (PEM) το οποίο όμως έχει ιστορική αξία πλέον,

• MOSS, το οποίο δεν έτυχε ιδιαίτερης εμπορικής υποστήριξης,

• Pretty Good Privacy (PGP), το οποίο αποτελείται από πέντε υπηρεσίες: κρυπτογράφηση μηνύματος, ψηφιακή υπογραφή, συμπίεση, e-mail συμβατότητα, κατάτμηση.

PRIVACY ENHANCED MAIL (PEM)

Το Privacy Enhanced Mail (PEM) είναι ένα στάνταρτ για την ασφάλεια ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας συμμετρική ή ασύμμετρη κρυπτογραφία. Το PEM έχει φθίνουσα πορεία διότι αδυνατεί να διαχειριστεί το νεώτερο πολυμελές ηλεκτρονικό ταχυδρομείο (multipart e-mail) το οποίο υποστηρίζεται από το MIME (Multipurpose Internet Mail Extensions), ενώ απαιτεί

αυστηρή ιεραρχία αρχών πιστοποίησης για να εκδώσει κλειδιά. S/MIME (Multipurpose Internet Mail)

Το S/MIME είναι ένα standard για αποστολή αρχείων με binary attachments μέσω του internet.Το Secure/MIME είναι μια επέκταση του MIME standard για την αναγνώριση των κρυπτογραφημένων email. Αντίθετα από το PGP ,το S/MIME δεν εφαρμόσθηκε σαν ένα αυτόνομο πρόγραμμα , αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου. Επειδή το εργαλείο προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγόριθμους και όλες τις πατέντες , και επειδή οι μεγαλύτερες εταιρείες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security , είναι πιθανό το S/MIME να υιοθετηθεί περισσότερο από το PGP, από τους πωλητές e-mail προγραμμάτων.

Το S/MIME προσφέρει εμπιστευτικότητα , εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα , εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώρισης γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων. Το σύστημα μπορεί να χρησιμοποιηθεί με δυνατή ή αδύνατη κρυπτογράφηση . Για να στείλουμε κρυπτογραφημένα μηνύματα σε κάποιον με το S/MIME ,πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του. Τα περισσότερα προγράμματα που χρησιμοποιούν το S/MIME κάνουν χρήση των X.509 v3 Public Key Infrastructures σαν και αυτές που δημιουργούνται από την VeriSign και άλλες αρχές πιστοποίησης .

Pretty Good Privacy (PGP)

Το PGP είναι ένα φαινόμενο, αφού πρόκειται για τη δουλειά ουσιαστικά ενός μόνο ανθρώπου, του Phil Zimmerman και παρέχει τις υπηρεσίες της εμπιστευτικότητας (confidentiality) και της εξακρίβωσης γνησιότητας (authentication) που μπορούν να χρησιμοποιηθούν στις εφαρμογές ηλεκτρονικού ταχυδρομείου και αποθήκευσης αρχείων. Από τη στιγμή της γέννησης του και πέρα το PGP χρησιμοποιείται ευρύτατα και αυτό εξαιτίας των παρακάτω λόγων:

1. Είναι διαθέσιμο παντού και μπορεί να τρέξει σε οποιαδήποτε πλατφόρμα.

2. Βασίζεται σε αλγορίθμους που είναι ευρέως αποδεκτοί σαν απόλυτα ασφαλείς.

3. Είναι κατάλληλο για ένα ευρύ φάσμα εφαρμογών.

4. Δεν αναπτύχθηκε, ούτε ελέγχεται από κυβερνητικό ή άλλο οργανισμό για τυποποιήσεις.

Η λειτουργία του PGP αποτελείται από πέντε υπηρεσίες, οι οποίες συνοψίζονται παρακάτω: εξακρίβωση γνησιότητας, εμπιστευτικότητα, συμπίεση, συμβατότητα ηλ. ταχυδρομείου (e-mail) και τμηματοποίηση.

Για την εξακρίβωση γνησιότητας (authentication) πρώτα ο αποστολέας στέλνει το μήνυμα. Στη συνέχεια ο MD5 χρησιμοποιείται για να παράγει ένα 128-bit hash code του μηνύματος. Ο κωδικός αυτός κρυπτογραφείται χρησιμοποιώντας RSA και το private key του αποστολέα και το αποτέλεσμα προσκολλάται στο μήνυμα. Ο παραλήπτης του μηνύματος χρησιμοποιεί με τη σειρά τον RSA με το public key του αποστολέα για να αποκρυπτογραφήσει και να βρει τον hash code. Τέλος, ο παραλήπτης παράγει ένα νέο hash code για το μήνυμα και το συγκρίνει με το αποκρυπτογραφημένο hash code που έχει βρει. Αν ταιριάζουν, τότε δέχεται το μήνυμα ως αυθεντικό. Όπως βλέπουμε, ο συνδυασμός του MD5 και του RSA παρέχουν έναν αποτελεσματικό σχήμα ηλεκτρονικής υπογραφής (digital signature). Ακόμα, μπορούν να υποστηριχθούν υπογραφές που παράγονται και μεταδίδονται ξεχωριστά από το μήνυμα.

Η εμπιστευτικότητα (Confidentiality) παρέχεται με την κρυπτογράφηση των μηνυμάτων προτού αποσταλούν ή αποθηκευτούν σαν αρχεία. Και στις δύο περιπτώσεις χρησιμοποιείται ο αλγόριθμος IDEA, και συγκεκριμένα η 64-bit cipher feedback (CFB) mode του IDEA με πίνακα αρχικοποίησης (initialization vector) όλο μηδενικά. Στο PGP κάθε συμβατικό (conventional) κλειδί χρησιμοποιείται μόνο μία φορά, οπότε για κάθε μήνυμα παράγεται με τυχαίο τρόπο ένα κλειδί 128-bits. Για την προστασία του, το κλειδί αυτό, προτού μεταδοθεί, κρυπτογραφείται με βάση το public key του παραλήπτη. Η σειρά των γεγονότων έχει ως εξής: Ο αποστολέας παράγει ένα μήνυμα και ένα τυχαίο 128-bit αριθμό για να χρησιμοποιηθεί σαν session key για το μήνυμα αυτό μόνο. Στη συνέχεια το μήνυμα κρυπτογραφείται χρησιμοποιώντας το IDEA μαζί με το session key. Το session key κωδικοποιείται με RSA, χρησιμοποιώντας το public key του παραλήπτη και προσδένεται στο μήνυμα. Τέλος, ο παραλήπτης χρησιμοποιεί RSA με το δικό του private key, για να βρει το session key, το οποίο χρησιμοποιεί για να αποκρυπτογραφήσει

το μήνυμα. Για το μέγεθος του κλειδιού που θα χρησιμοποιήσει ο RSA, υπάρχουν οι δυνατότητες του Συνήθους (Casual - 384 bits), του Εμπορικού (commercial - 512 bits) και του στρατιωτικού (Military – 1024 bits) κλειδιού.

Εμπιστευτικότητα και Εξακρίβωση γνησιότητας. Όταν και οι δύο υπηρεσίες χρησιμοποιούνται, αρχικά, ο αποστολέας παράγει μία ηλεκτρονική υπογραφή το μήνυμα, με βάση το private key του, και την τοποθετεί στο τέλος του μηνύματος. Στη συνέχεια, το μήνυμα μαζί με την υπογραφή κρυπτογραφείται χρησιμοποιώντας τον IDEA και ένα session key και το session key κρυπτογραφείται χρησιμοποιώντας τον RSA και το public key του παραλήπτη.

Το PGP συμπιέζει από μόνο του το μήνυμα αφού τοποθετηθεί η υπογραφή και πριν κρυπτογραφηθεί. Έτσι κερδίζουμε χώρο και κατά την μετάδοση και κατά την αποθήκευση του μηνύματος. Ο αλγόριθμος που χρησιμοποιείται είναι ο ZIP.

Συμβατότητα ηλεκτρονικού ταχυδρομείου

Όταν χρησιμοποιείται PGP, ολόκληρο ή τουλάχιστον ένα μέρος του block που αποστέλλεται είναι κρυπτογραφημένο και αποτελείται από μία σειρά από τυχαία 8-bit octets. Λόγω του περιορισμού που υπάρχει σε ορισμένα συστήματα ηλεκτρονικού ταχυδρομείου για μόνο ASCII text μηνύματα, το PGP παρέχει μία υπηρεσία που μετατρέπει τη σειρά αυτή σε εκτυπώσιμους ASCII χαρακτήρες. Για το σκοπό αυτό χρησιμοποιείται η radix-64 μετατροπή, που παίρνει κάθε ομάδα τριών octets και τα μετατρέπει σε 4 χαρακτήρες ASCII, καθώς επίσης προσθέτει στο τέλος ένα CRC, για την ανίχνευση τυχόν λαθών. Το PGP ακόμα, μπορεί να μετατρέπει σε radix-64 μορφή μόνο το μέρος όπου υπάρχει η υπογραφή, ώστε ο αποστολέας να μπορεί να διαβάζει τα μηνύματα, χωρίς να χρησιμοποιεί PGP, και μόνο αν θέλει να πιστοποιήσει την υπογραφή να χρειάζεται το PGP. Κατά τη μετάδοση, αν αυτό απαιτείται, σχηματίζεται μία υπογραφή χρησιμοποιώντας ένα hash κωδικό του συμπιεσμένου κειμένου. Μετά το κείμενο μαζί με την υπογραφή συμπιέζονται και αν χρειάζεται η εμπιστευτικότητα, το όλο μπλοκ κρυπτογραφείται με το RSA-κρυπτογραφημένο κλειδί κρυπτογράφησης. Τέλος, ολόκληρο το μπλοκ αυτό μετασχηματίζεται στην radix-64 μορφή. Κατά τη λήψη του μηνύματος, το εισερχόμενο μπλοκ πρώτα μετατρέπεται από την radix-64, στην αρχική δυαδική μορφή του και, αν είναι κρυπτογραφημένο, ο παραλήπτης ανακτά το session κλειδί και αποκρυπτογραφεί το μήνυμα. Το τελικό μπλοκ αποσυμπιέζεται και αν είναι υπογεγραμμένο, ο παραλήπτης ανακτά τον hash code που έχει μεταδοθεί και το συγκρίνει με αυτόν που έχει υπολογίσει αυτός.

Μια δημοφιλής εφαρμογή που αναπτύχθηκε με σκοπό την ασφάλεια μηνυμάτων και αρχείων είναι το Pretty Good Privacy (PGP). Είναι ίσως η ευρύτερα διαδεδομένη εφαρμογή ασφαλείας για ηλεκτρονικό ταχυδρομείο στο Διαδίκτυο. Το PGP (Pretty Good Privacy) είναι πακέτο λογισμικού που παρέχει ρουτίνες κρυπτογράφησης για e-mail και εφαρμογές αποθήκευσης αρχείων. Το PGP απαρτίζεται από υπάρχοντα κρυπτοσυστήματα και πρωτόκολλα κρυπτογράφησης. Τρέχει σε διάφορες πλατφόρμες. Προσφέρει κρυπτογράφηση μηνύματος, ψηφιακές υπογραφές, συμπίεση δεδομένων και e-mail συμβατότητα. Η τελευταία έκδοσή του για χρήστες εκτός των ΗΠΑ παρέχει έναν εύκολο τρόπο κρυπτογράφησης, διαχείρισης κλειδιών μέσα από γραφικό περιβάλλον. Το PGP συνδυάζει και τους δύο τρόπους κρυπτογράφησης, μεταφέροντας με ασφαλή τρόπο το ιδιωτικό κλειδί μέσα από τεχνικές δημόσιου κλειδιού. Μετά την εγκατάσταση του προγράμματος και κατά τη διαδικασία δημιουργίας του δημόσιου κλειδιού ο χρήστης καλείται να δώσει το επιθυμητό μέγεθος του κλειδιού. Εδώ πρέπει να τονιστεί ότι χρησιμοποιείται συμμετρικός αλγόριθμος για να μεταδώσει με ασφαλή τρόπο το ιδιωτικό κλειδί, το οποίο χρησιμοποιείται τελικά για την κρυπτογράφηση του κυρίως μηνύματος. Το PGP προσφέρει 3 συμμετρικούς αλγορίθμους, οι οποίοι είναι οι: CAST και IDEA με 128 bits μέγεθος κλειδιού, καθώς και ο Triple-DES με 168 bits μέγεθος κλειδιού.

Εκτός από την κρυπτογράφηση, το PGP επιτρέπει στο χρήστη να υπογράψει ψηφιακά οποιοδήποτε κείμενο αποστέλλει, καθώς επίσης και να ελέγξει την πατρότητα του ψηφιακά υπογεγραμμένου κειμένου που έχει λάβει. Το PGP σχεδιάστηκε γύρω από την ιδέα ενός αξιόπιστου web το οποίο θα επιτρέπει στους χρήστες να μοιράζονται τα κλειδιά τους χωρίς να απαιτείται η ιεραρχία των αρχών πιστοποίησης.

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Η ψηφιακή υπογραφή (digital signature) θεωρείται ως το ηλεκτρονικό ισοδύναμο της συμβατικής υπογραφής και είναι μια συμβολοσειρά που προκύπτει από το συνδυασμό των δυαδικών ψηφίων ενός μηνύματος και αυτών ενός μυστικού κλειδιού[41]. Η χρησιμοποίηση της ψηφιακής υπογραφής σε ένα σύστημα ασφαλείας ενός δικτύου είναι απαραίτητη καθώς παρέχει αυθεντικοποίηση του αποστολέα, εμπιστευτικότητα και ακεραιότητα του μηνύματος. Οι ασύμμετροι αλγόριθμοι είναι υπολογιστικά αργοί για την κρυπτογράφηση ενός ολόκληρου μηνύματος.

[41] Ηλεκτρονικό Εμπόριο Αρσένης Πασχόπουλος και Παναγιώτης Σκαλτσάς Εκδόσεις Κλειδάριθμος

Έστω λοιπόν ότι ο Α επιθυμεί να στείλει υπογεγραμμένο έγγραφο ή μήνυμα στον Β. Το πρώτο βήμα είναι γενικά να εφαρμόσει μια hash συνάρτηση στο μήνυμα και να δημιουργήσει ένα message digest. Το message digest είναι συνήθως αισθητά μικρότερο από το πρωτότυπο μήνυμα. Ουσιαστικά η δουλειά της hash συνάρτησης είναι να πάρει ένα μήνυμα οποιουδήποτε μεγέθους και να το συρρικνώσει σε προκαθορισμένο μέγεθος. Για να δημιουργήσει κανείς μια ψηφιακή υπογραφή κρυπτογραφεί συνήθως το message digest και όχι το ίδιο το μήνυμα (μ' άλλα λόγια το κρυπτογραφημένο message digest είναι η ψηφιακή υπογραφή του αποστολέα). Ο Α στέλνει στον Β το κρυπτογραφημένο message digest και το μήνυμα κρυπτογραφημένο ή όχι. Προκειμένου ο Β να αυθεντικοποιήσει την υπογραφή κάνει τα εξής:

1. Εφαρμόζει, πρώτα απ' όλα, την ίδια hash συνάρτηση με τον Α στο μήνυμα που παρέλαβε (το οποίο επαναλαμβάνουμε είναι κρυπτογραφημένο ή απλό κείμενο). Δημιουργεί έτσι τη δική του εκδοχή για το ορθό message digest.
2. Στη συνέχεια αποκρυπτογραφεί τη ψηφιακή υπογραφή την οποία παρέλαβε συνημμένη με το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α. Η διαδικασία αυτή οδηγεί στην αναπαραγωγή του message digest το οποίο δημιούργησε ο Α.
3. Ο Β έχει τώρα στη διάθεση του δύο message digests. Τα συγκρίνει και αν ταιριάζουν, αυθεντικοποίησε επιτυχώς τη ψηφιακή υπογραφή του Α. Αν όχι, υπάρχουν λίγες πιθανές εξηγήσεις. Είτε κάποιος προσποιείται τον Α, ή το μήνυμα μεταβλήθηκε από τη στιγμή που το υπέγραψε ο Α, ή υπήρξε λάθος στη μετάδοση.

ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Είναι γεγονός αναμφισβήτητο ότι η απόκτηση εμπιστοσύνης που επιτυγχάνεται κατά τις συμβατικές συναλλαγές μέσω της οπτικής επαφής των δύο συναλλασσομένων μερών δεν είναι δυνατή όταν πρόκειται για συναλλαγές μέσω Web. Έτσι, είναι αναγκαία η ύπαρξη ενιαίας υποδομής, η οποία θα προστατεύει τις ιδιωτικές πληροφορίες από τρίτους (Privacy). Η πληροφορία που ανταλλάσσεται ανάμεσα στα δύο μέρη (αποστολέας και παραλήπτης, πελάτης και έμπορος) δεν πρέπει να καταλήγει σε τρίτους. Εξίσου σημαντικό στοιχείο είναι η επικύρωση της ταυτότητας (authentication) των επικοινωνούντων μερών. Ο αποστολέας πρέπει να γνωρίζει ότι οι πληροφορίες που στέλνει έχουν ως παραλήπτη το συγκεκριμένο πρόσωπο. Ο Α πρέπει να είναι σίγουρος ότι ο Β, με τον οποίο επικοινωνεί, είναι όντως αυτός που ισχυρίζεται ότι είναι. Άλλο σημαντικό θέμα είναι η διασφάλιση της ακεραιότητας των δεδομένων που αποστέλλονται. Τα στοιχεία μιας συναλλαγής

πρέπει να φτάσουν στον προορισμό τους αυτούσια. Ακόμα κι αν πέσουν σε χέρια τρίτων, να είναι έτσι κρυπτογραφημένα ώστε να τους είναι άχρηστα - να μην μπορούν να τα εκμεταλλευτούν. Τα συναλλασσόμενα μέρη πρέπει να μην έχουν τη δυνατότητα άρνησης της συμμετοχής τους σε μια συναλλαγή.

Το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές τραπεζικές συναλλαγές πρέπει να αναγνωρίζονται από το νομικό καθεστώς της χώρας στην οποία πραγματοποιείται. Μια ψηφιακή υπογραφή σε ένα κείμενο πρέπει να έχει την ίδια βαρύτητα με τη φυσική υπογραφή σε μια νομική αρχή, σε ένα δικαστήριο. Η ασφάλεια των αριθμών των πιστωτικών καρτών είναι βασική προϋπόθεση για την ευρεία διάδοση του ηλεκτρονικού εμπορίου. Οι πελάτες θέλουν να είναι σίγουροι ότι οι πληροφορίες των πιστωτικών καρτών τους είναι ασφαλείς καθώς μεταβιβάζονται μέσω Internet και ότι έχουν ως αποδέκτη έναν νόμιμο πωλητή ή αρχή. Αντίστοιχα, οι έμποροι πρέπει να γνωρίζουν ότι οι πληροφορίες που λαμβάνουν αντιστοιχούν σε νόμιμους κατόχους πιστωτικών καρτών. Η υποδομή αυτή στηρίζεται στην κρυπτογράφηση.

Με τη συμμετρική κρυπτογράφηση επιτυγχάνεται η διασφάλιση του απορρήτου και της ακεραιότητας των πληροφοριών που στέλνονται μεταξύ των συναλλασσόμενων μερών. Έτσι, αν βρεθούν στα χέρια τρίτων, θα τους είναι άχρηστες, αφού οι τελευταίοι δε θα μπορούν να αντιληφθούν το περιεχόμενό τους. Για την επίτευξη της ταυτοποίησης χρησιμοποιείται κρυπτογράφηση δημόσιου κλειδιού. Με αυτό τον τρόπο κάθε συναλλασσόμενο μέρος αναγνωρίζεται ως τέτοιο με βάση το ψηφιακό πιστοποιητικό (Digital ID) που έχει αποκτήσει. Το ψηφιακό πιστοποιητικό είναι αντίστοιχο με την ταυτότητα, το δίπλωμα οδήγησης, το διαβατήριο και την πιστωτική κάρτα και εκδίδεται από αρχές πιστοποίησης (Certification Authorities, CA). Η ακεραιότητα διασφαλίζεται και με τη χρήση των ψηφιακών υπογραφών. Ο αποστολέας υπογράφει ψηφιακά την πληροφορία με το ιδιωτικό κλειδί του και την αποστέλλει. Όταν ο παραλήπτης λάβει το μήνυμα, ελέγχει την ψηφιακή υπογραφή του αποστολέα. Αν όντως υπάρχει, το μήνυμα έχει φτάσει ακέραιο, διαφορετικά έχει αλλάξει κατά τη μεταφορά του.

Τι χρειαζόμαστε όμως, στην πράξη τα προσωπικά πιστοποιητικά; Οι browsers χρησιμοποιούν το πιστοποιητικό για να αποκρυπτογραφήσουν πληροφορία που στέλνεται προς εμάς. Με τη δημιουργία του πιστοποιητικού δημιουργούμε ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό). Όποιος θέλει να μας στείλει εμπιστευτικές πληροφορίες τις κρυπτογραφεί με το δημόσιο κλειδί μας, οπότε μόνο εμείς με το ιδιωτικό κλειδί μας μπορούμε να τις αποκρυπτογραφήσουμε.

Μπορούμε επίσης να στείλουμε πληροφορία κρυπτογραφημένη μέσω e-mail, χρησιμοποιώντας το πρωτόκολλο S/MIME. Επίσης μπορούν να χρησιμοποιηθούν για την είσοδό μας σε sites με ελεγχόμενη πρόσβαση, σε sites ηλεκτρονικών καταστημάτων, τραπεζών κλπ. Πολλά sites, μάλιστα, για διευκόλυνσή μας, συλλέγουν πληροφορίες με βάση την ταυτότητά μας για να δημιουργήσουν προφίλ με τις προτιμήσεις μας - οπότε, αν ξαναμπούμε στο συγκεκριμένο site, ανακτάται το προφίλ μας και εμφανίζονται πληροφορίες που ουσιαστικά εμείς θέλουμε να δούμε, σύμφωνα με τα στοιχεία που είχαμε δώσει την πρώτη φορά.

Η συνεχής εξέλιξη των πρωτοκόλλων ασφαλείας στο Internet αποτελεί την καλύτερη εγγύηση αλλά και την πιο ικανοποιητική απάντηση στο ερώτημα αν οι πραγματοποίηση τραπεζικών συναλλαγών μέσω του Διαδικτύου είναι σίγουρη και ασφαλής.

ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία είναι η τέχνη ή η επιστήμη που παρέχει ασφάλεια στην πληροφορία. Έχει καταστεί εξαιρετικά σημαντική και αποτελεί πλέον δομικό στοιχείο της λειτουργίας οργανισμών και επιχειρήσεων, καθώς και εργαλείο προστασίας προσωπικών δεδομένων ιδιωτών[42]. Αγοροπωλησίες, συναλλαγές, μεταφορά πληροφορίας και άλλες λειτουργίες έχουν εδραιωθεί ως αξιόπιστες βάσει της τεχνολογικής ανάπτυξης της κρυπτογραφίας. Παραδοσιακά, η κρυπτογραφία περιλαμβάνει διάφορες τεχνικές για την απόκρυψη της πληροφορίας κατά τη διακίνηση και αποθήκευσή της, όπως είναι η συγχώνευση λέξεων με εικόνες, οι εικόνες σε σμίκρυνση μεγέθους τελείας στιγμής (microdots) κ.ά. Ωστόσο, σήμερα, η κρυπτογραφία σχετίζεται περισσότερο με το scrabbling (μετατροπή της πληροφορίας σε μη αναγνώσιμη), μια διαδικασία η οποία είναι ευρέως γνωστή ως κρυπτογράφηση, και την αντίστροφη διαδικασία της μετατροπής ενός κρυπτογραφήματος σε αναγνώσιμο κείμενο (αποκρυπτογράφηση). Η κρυπτογράφηση και η αποκρυπτογράφηση κάνουν συνήθως χρήση ενός κλειδιού, και η μέθοδος κωδικοποίησης πρέπει να είναι τέτοια έτσι ώστε η αποκρυπτογράφηση να είναι εκτελέσιμη μόνο αν υπάρχει γνώση του κατάλληλου αυτού κλειδιού. Η κρυπτογραφία έχει τέσσερις αντικειμενικούς σκοπούς:

Εμπιστευτικότητα: η πληροφορία δεν πρέπει να γίνεται κατανοητή από κανέναν, πλην του πραγματικά επιδιωκόμενου παραλήπτη της.

[42] Cryptography –An Overview : http://www.hack.gr/users/dij/crypto/

Ακεραιότητα: η πληροφορία δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της πραγματοποιηθείσας αλλοίωσης. Αυτό ισχύει και στην περίπτωση που είναι αποθηκευμένη σε μια αποθήκη υλικού και στην περίπτωση που διακινείται από τον αποστολέα στον παραλήπτη.

Μη αποκήρυξη: Ο δημιουργός/ αποστολέας της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της δημιουργίας ή μετάδοσης της πληροφορίας.

Πιστοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητες τους καθώς και την αρχή και τον προορισμό της πληροφορίας.

Η κρυπτογραφία είναι στενά συνδεδεμένη με τις αρχές της κρυπτανάλυσης και της κρυπτολογίας. Κρυπτανάλυση είναι η τέχνη της αποκωδικοποίησης των κρυπτογραφημάτων (παράγει το καθαρό κείμενο - plaintext) χωρίς τη γνώση του κατάλληλου κλειδιού. Η κρυπτολογία είναι ο κλάδος των μαθηματικών που μελετά όλες τις μαθηματικές θεμελιώσεις των κρυπτογραφικών μεθόδων και περιλαμβάνει και την κρυπτογραφία και την κρυπτανάλυση.

ΑΝΑΓΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ –ΑΠΟΚΡΥΨΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η κρυπτογραφία από τα αρχαία χρόνια, οπότε και πρωτοχρησιμοποιήθηκε, είχε ένα κύριο στόχο, την απόκρυψη της πληροφορίας κάποιου κειμένου από μη επιθυμητά πρόσωπα. Αυτή η ανάγκη προέκυψε για δύο λόγους. Ο πρώτος λόγος ήταν η ανάγκη επικοινωνίας και μεταφοράς μυστικών, ιδιαίτερα σε περιόδους πολέμου. Ο δεύτερος λόγος ήταν η πρόθεση κάποιων να αποκρύψουν πληροφορίες – γνώσεις από τους υπολοίπους. Συνήθως επρόκειτο για ιερείς ή αξιωματούχους που ήθελαν να αποκρύψουν πληροφορίες ή γνώσεις από το λαό. Σήμερα η ανάγκη αυτή έχει επεκταθεί από την προστασία των απλών προσωπικών δεδομένων μέχρι την προστασία βιομηχανικών και κρατικών μυστικών.

Καθώς η κρυπτολογία αναπτύσσεται ο αριθμός των στόχων της έχει επεκταθεί, όπως και ο αριθμός των εργαλείων που είναι διαθέσιμα για την επίτευξη αυτών των στόχων. Η κρυπτολογία παρέχει τρόπους με τους οποίους μπορεί να βοηθήσει κάποιον να αναπτύξει εμπιστοσύνη κατά τις επικοινωνίες του και να τους δώσει τις επιθυμητές ιδιότητες, παρά τις προσπάθειες των κακόβουλων χρηστών για το αντίθετο.

Έτσι εκτός από την απόκρυψη της πληροφορίας ή αλλιώς την ιδιωτικότητα (privacy) η κρυπτογραφία ικανοποιεί και μια σειρά από άλλες ανάγκες, οι οποίες περιγράφονται με συντομία παρακάτω:

Ταυτοποίηση (authentication). Πρέπει να είναι δυνατό για τον παραλήπτη ενός μηνύματος να επιβεβαιώσει τον αποστολέα του και να μην μπορεί ένας εισβολέας να πάρει τη θέση κάποιου άλλου χρήστη.

Απόδειξη γνησιότητας-υπογραφές (signatures). Ο παραλήπτης του μηνύματος μπορεί να πείσει κάποιον τρίτο ότι το μήνυμα που έλαβε προέρχεται από αυτόν που το υπογράφει και ο υπογράφων να πείσει για την ταυτότητά του.

Ακεραιότητα –(Integrity). Πρέπει να μπορεί ο παραλήπτης ενός μηνύματος να επιβεβαιώσει ότι το μήνυμα δεν έχει τροποποιηθεί κατά τη διαδρομή του και ένας εισβολέας να μην μπορεί να αντικαταστήσει ένα κανονικό μήνυμα με ένα πλαστό.

Μη δυνατότητα άρνησης (nonrepudiation). Ένας αποστολέας πρέπει να μην μπορεί να αρνηθεί ψευδώς ότι έστειλε κάποιο μήνυμα.

Μινιμαλισμός (minimality). Τίποτα δεν μεταδίδεται σε τρίτους εκτός από αυτό που σαφώς έχει οριστεί πως πρέπει να μεταδοθεί.

Ταυτόχρονη ανταλλαγή (simultaneous exchange). Τίποτα με αξία (π.χ. μια υπογραφή σε ένα συμβόλαιο) δεν μεταδίδεται πριν κάτι άλλο με αξία (π.χ. η υπογραφή του άλλου μέρους) δεν παραληφθεί.

Συντονισμός (coordination). Σε μια επικοινωνία με πολλά μέρη, οι συμμετέχοντες μπορούν να συντονίσουν τις δραστηριότητές τους προς ένα κοινό σκοπό ακόμα και με την παρουσία ανεπιθύμητων – εχθρικών μερών.

Οριο συνεργασίας (Collaboration Threshold). Σε μια επικοινωνία πολλών μερών οι επιθυμητές ιδιότητες διατηρούνται μέχρι ο αριθμός των ανεπιθύμητων – εχθρικών μερών δεν υπερβαίνει ένα συγκεκριμένο όριο.

Όλες αυτές είναι βασικές απαιτήσεις για κοινωνικές αλληλεπιδράσεις μέσω των υπολογιστών, που είναι ανάλογες αυτών που ισχύουν για τις διαπροσωπικές σχέσεις.

Η χρήση της κρυπτογράφησης

Από τη στιγμή που άρχισαν να μεταφέρονται πληροφορίες ξεκίνησε και η ιδέα της κρυπτογράφησης ή του κώδικα για να ασφαλιστούν τα μηνύματα . Το παρόν σύστημα αποστολής μηνυμάτων μέσω του internet βασίζεται στην ίδια γενική ιδέα κρυπτογράφησης που έχει χρησιμοποιηθεί εδώ και αιώνες. Η διαφορά μεταξύ των προηγούμενων και των τωρινών μορφών κρυπτογράφησης βρίσκεται στο κλειδί που αποκρυπτογραφεί τον κώδικα. Στο παρελθόν ο παραλήπτης για να μπορεί να επαναφέρει το μήνυμα ξανά σε αναγνώσιμη μορφή , χρειαζόταν το κλειδί του μυστικού κώδικα. Το σύστημα δούλευε θαυμάσια τις περισσότερες φορές , επειδή σε κάποιο σε κάποιο σημείο τα δυο μέρη συναντιόντουσαν προσωπικά και μπορούσαν να ανταλλάξουν κώδικα , ώστε να ήταν σίγουρο ότι θα είναι μυστικός . Αν μια προσωπική συνάντηση δεν ήταν δυνατή , τα δυο μέρη έχουν τον κίνδυνο να υποκλαπεί ο μυστικός κώδικας και να αντιγραφεί .

ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

Υπάρχουν δύο τύποι αλγορίθμων που βασίζονται σε κλειδιά: οι συμμετρικοί ή μυστικού κλειδιού και οι μη συμμετρικοί ή δημόσιου κλειδιού. Οι συμμετρικοί αλγόριθμοι διαιρούνται σε δύο κατηγορίες. Μερικοί λειτουργούν στο αρχικό κείμενο σε ένα bit τη φορά και καλούνται stream αλγόριθμοι. Άλλοι λειτουργούν πάνω σε μια ομάδα από bits οπότε καλούνται block αλγόριθμοι. Παρακάτω παρουσιάζονται ορισμένοι αντιπροσωπευτικοί αλγόριθμοι των παραπάνω κατηγοριών:

Αλγόριθμοι μυστικού κλειδιού

Οι αλγόριθμοι μυστικού κλειδιού (ή συμμετρικοί αλγόριθμοι) χρησιμοποιούν το ίδιο κλειδί, το οποίο καλείται και μυστικό (secret key), για την κρυπτογράφηση και αποκρυπτογράφηση. Σ' αυτούς τους αλγορίθμους απαιτείται και από τον αποστολέα και από τον παραλήπτη να συμφωνήσουν πάνω σε πιο κλειδί θα επικοινωνούν με ασφάλεια. Η ασφάλεια των αλγορίθμων μυστικού κλειδιού έγκειται στην προστασία του κλειδιού: όποιος κατέχει το κλειδί μπορεί να κρυπτογραφήσει και να αποκρυπτογραφήσει μηνύματα.

Παρακάτω παρουσιάζονται ορισμένοι από τους πιο δημοφιλείς αλγορίθμους μυστικού κλειδιού.

Αλγόριθμος Feistel

Οι αλγόριθμοι Feistel είναι μια ειδική τάξη επαναληπτικών block αλγορίθμων κρυπτογράφησης, όπου το κρυπτογραφημένο κείμενο υπολογίζεται από το κανονικό με επαναλαμβανόμενες εφαρμογές του ίδιου μετασχηματισμού ή συνάρτησης.

Σε έναν Feistel αλγόριθμο, το κείμενο που κρυπτογραφείται χωρίζεται σε δύο ίσα μέρη. Μια συνάρτηση f εφαρμόζεται στο ένα μέρος χρησιμοποιώντας ένα υποκλειδί και η έξοδος της f γίνεται XOR με το άλλο μέρος. Τα δύο μέρη μετά εναλλάσσονται. Κάθε γύρος ακολουθεί την ίδια διαδικασία εκτός από τον τελευταίο όπου τα μέρη δεν εναλλάσσονται. Ένα ενδιαφέρον χαρακτηριστικό ενός Feistel αλγορίθμου είναι ότι η κρυπτογράφηση και η αποκρυπτογράφηση είναι ίδιες, λαμβάνοντας υπόψη τα υποκλειδιά που χρησιμοποιούνται για κάθε γύρο παίρνονται με την αντίστροφη σειρά στην αποκρυπτογράφηση. Είναι δυνατόν να σχεδιαστούν επαναληπτικοί αλγόριθμοι οι οποίοι δεν είναι Feistel και η κρυπτογράφηση και η αποκρυπτογράφησή τους είναι δομικά η ίδια. Ένα τέτοιο παράδειγμα είναι και ο IDEA.

Data Encryption Standard (DES)

Ο DES (Data Encryption Standard) είναι ένας block αλγόριθμος κρυπτογράφησης ο οποίος ορίστηκε από την κυβέρνηση των Η.Π.Α. το 1977 σαν επίσημο πρότυπο. Αρχικά ο DES αναπτύχθηκε από την IBM, έχει μελετηθεί εκτενώς από την μέρα της δημοσίευσής του και είναι το πιο γνωστό και ευρέως χρησιμοποιούμενο κρυπτοσύστημα στον κόσμο. Ο DES έχει μέγεθος block 64-bit και χρησιμοποιεί ένα 56-bit κλειδί για την κρυπτογράφηση. Είναι ένας 16 γύρων Feistel αλγόριθμος κρυπτογράφησης και αρχικά σχεδιάστηκε για υλοποίηση στο hardware. Ο DES μπορεί να χρησιμοποιηθεί και για κρυπτογράφηση σε συστήματα ενός χρήστη όπως στην αποθήκευση κρυπτογραφημένων αρχείων σε έναν σκληρό δίσκο.

RC2 και RC4

Ο RC2 είναι ένας μεταβλητού-μεγέθους-κλειδιού block αλγόριθμος κρυπτογράφησης ο οποίος σχεδιάστηκε από τον Rivest για την RSA Data Security. Τα αρχικά RC σημαίνουν "Rod's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και σχεδιάστηκε σαν αντικαταστάτης

του DES. Μπορεί να φτιαχτεί ως λιγότερο ή περισσότερο ασφαλής από τον DES ενάντια στο "εξαντλητικό ψάξιμο κλειδιού" χρησιμοποιώντας κατάλληλο μέγεθος κλειδιού κάθε φορά. Το μέγεθος του block είναι 64-bits και είναι δύο με τρεις φορές γρηγορότερος από τον DES υλοποιημένος σε λογισμικό. Ο αλγόριθμος είναι μυστικός και είναι ιδιοκτησία της RSA Data Security. Μια συμφωνία μεταξύ της Software Publishers Association (SPA) και της αμερικάνικης κυβέρνησης δίνει στους RC2 και RC4 ειδική μεταχείριση με το να επιτρέπει απλούστερη και γρηγορότερη έγκριση εξαγωγής τους από τους συνηθισμένους κρυπτογραφικούς αλγορίθμους. Ωστόσο, για να μπορεί να εγκριθεί η σύντομη εξαγωγή ενός προϊόντος πρέπει το μέγεθος του RC2 και RC4 κλειδιού να μην υπερβεί τα 40 bits. Κλειδιά με 56 bit επιτρέπονται μόνο σε γραφεία αμερικανικών επιχειρήσεων που βρίσκονται σε ξένες χώρες. Μία πρόσθετη συμβολοσειρά (40 με 88 bits μέγεθος) η οποία καλείται και αλάτι μπορεί να χρησιμοποιηθεί στο να αποθαρρύνει τρίτους που προσπαθούν να προ-υπολογίσουν ένα μεγάλο look-up πίνακα με πιθανές κρυπτογραφήσεις. Το αλάτι προστίθεται στο τέλος του κλειδιού και το επιμηκυμένο κλειδί χρησιμοποιείται στην κρυπτογράφηση του μηνύματος. Το αλάτι στέλνεται μη κρυπτογραφημένο μαζί με το μήνυμα. Οι RC2 και RC4 χρησιμοποιούνται ευρέως από ανθρώπους που θέλουν να εξάγουν τα προϊόντα τους, ενώ ο DES σχεδόν ποτέ δεν εγκρίνεται για εξαγωγή.

International Data Encryption Algorithm (IDEA)

Ο IDEA (International Data Encryption Algorithm) είναι η δεύτερη έκδοση ενός block αλγόριθμου κρυπτογράφησης ο οποίος σχεδιάστηκε και παρουσιάστηκε από τους Lai και Massey. Είναι ένας 64-bit επαναληπτικός αλγόριθμος με ένα 128-bit κλειδί και 8 γύρους. Η δομή του αλγορίθμου έχει σχεδιαστεί για την εύκολη υλοποίηση τόσο στο λογισμικό όσο και στο υλικό, και η ασφάλεια του έγκειται στην χρησιμοποίηση τριών ασύμβατων τύπων αριθμητικών πράξεων πάνω σε λέξεις των 16 bit. Η ταχύτητα του IDEA είναι ίδια στο λογισμικό με αυτή του DES.

Το πιο σημαντικό κρυπταναλυτικό αποτέλεσμα οφείλεται στον Daemen. Αυτός βρήκε μια μεγάλη τάξη από 251 αδύνατα κλειδιά για τα οποία η χρήση ενός από αυτά κατά την διάρκεια της κρυπτογράφησης μπορούσε να ανιχνευθεί και το κλειδί να βρεθεί. Ωστόσο, επειδή υπάρχουν 2128 πιθανά κλειδιά το προηγούμενο αποτέλεσμα δεν έχει επιπτώσεις στην ασφάλεια του αλγορίθμου. Ο IDEA γενικά θεωρείται ασφαλής και τόσο η ανάπτυξη του αλγορίθμου όσο και η θεωρητική του βάση έχουν ανοιχτά και ευρέως συζητηθεί.

Αλγόριθμοι δημόσιου κλειδιού

Οι αλγόριθμοι δημοσίου κλειδιού (public key) (ή αλλιώς μη-συμμετρικοί αλγόριθμοι) σχεδιάζονται έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από αυτό της αποκρυπτογράφησης. Ακόμα, το κλειδί της αποκρυπτογράφησης δεν μπορεί να υπολογισθεί γρήγορα από το κλειδί της κρυπτογράφησης. Αυτοί οι αλγόριθμοι ονομάζονται δημοσίου κλειδιού διότι το κλειδί της κρυπτογράφησης μπορεί να είναι δημόσιο. Ένας ξένος μπορεί να χρησιμοποιήσει το κλειδί της κρυπτογράφησης για να κρυπτογραφήσει ένα μήνυμα, αλλά μόνο ένα συγκεκριμένο άτομο με το αντίστοιχο κλειδί αποκρυπτογράφησης μπορεί να αποκρυπτογραφήσει το μήνυμα. Σε τέτοια συστήματα το κλειδί της αποκρυπτογράφησης ονομάζεται ιδιωτικό (private key) και το κλειδί της κρυπτογράφησης δημόσιο (public key).

Επιπροσθέτως οι αλγόριθμοι δημοσίου κλειδιού δεν χρησιμοποιούνται μόνο για κρυπτογράφηση αλλά και για εξακρίβωση γνησιότητας (ηλεκτρονικές υπογραφές). Παρακάτω δίνονται δύο παραδείγματα κρυπτογράφησης και εξακρίβωσης γνησιότητας (authentication), χρησιμοποιώντας αλγόριθμο δημοσίου κλειδιού.

Κρυπτογράφηση

Όταν η Ελένη θέλει να στείλει ένα μυστικό μήνυμα στον Νίκο κοιτάζει το δημόσιο κλειδί του Νίκου και το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα και στην συνέχεια το στέλνει. Με την σειρά του ο Νίκος χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το μήνυμα και το διαβάζει.

Ηλεκτρονική υπογραφή

Για την υπογραφή ενός μηνύματος, η Ελένη κάνει έναν υπολογισμό εμπεριέχοντας το ιδιωτικό της κλειδί και το μήνυμα το ίδιο. Το αποτέλεσμα λέγεται ηλεκτρονική υπογραφή και επικολλάται στο μήνυμα, το οποίο και στέλνεται. Ο Νίκος για να επιβεβαιώσει την υπογραφή, κάνει έναν υπολογισμό χρησιμοποιώντας το μήνυμα, την υπογραφή της Ελένης και το δημόσιο κλειδί της Ελένης. Αν το αποτέλεσμα δείξει ότι το μήνυμα υπολογισμένο με το δημόσιο κλειδί της Ελένης είναι ίδιο με την υπογραφή της τότε το μήνυμα είναι αυθεντικό, διαφορετικά υπάρχει περίπτωση αλλοίωσης του μηνύματος. Συνεπώς η κρυπτογράφηση και η εξακρίβωση γνησιότητας λαμβάνουν χώρα χωρίς το διαμοιρασμό ιδιωτικών κλειδιών, κάθε άτομο χρησιμοποιεί μόνο τα δημόσια κλειδιά του άλλου και το δικό του ιδιωτικό κλειδί. Καθένας μπορεί να στείλει κρυπτογραφημένα μηνύματα ή να επιβεβαιώσει ένα υπογεγραμμένο μήνυμα, χρησιμοποιώντας

μόνο δημόσια κλειδιά, αλλά μόνο κάποιος ο οποίος έχει στην κατοχή του το σωστό ιδιωτικό κλειδί μπορεί να κρυπτογραφήσει και να υπογράψει ένα μήνυμα. Στη συνέχεια παρουσιάζονται οι πιο δημοφιλείς αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού.

RSA

Ο RSA είναι ένα κρυπτοσύστημα δημοσίου κλειδιού για κρυπτογράφηση και εξακρίβωση γνησιότητας. Εφευρέθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Δουλεύει ως εξής: Παίρνουμε δύο μεγάλους πρώτους αριθμούς, p και q και βρίσκουμε το γινόμενό τους n=pq, το n λέγεται διαιρέτης. Διαλέγουμε έναν αριθμό e ο οποίος είναι μικρότερος από τον n και σχετικά πρώτος με το (p-1)(q-1), δηλαδή ο e και το (p-1)(q-1) δεν έχουν κοινούς διαιρέτες εκτός από το 1. Βρίσκουμε άλλον έναν αριθμό d τέτοιος ώστε το (ed-1) να είναι διαιρέσιμο από το (p-1)(q-1). Οι τιμές e και d ονομάζονται δημόσιοι και ιδιωτικοί δείκτες αντίστοιχα. Το δημόσιο κλειδί είναι το ζευγάρι (n,e) και το ιδιωτικό το (n,d). Οι παράγοντες p και q μπορεί να κρατηθούν μαζί με το ιδιωτικό κλειδί ή να καταστραφούν.

Είναι δύσκολο πιθανώς να βρεθεί το ιδιωτικό κλειδί d από το δημόσιο (n,e). Εάν κάποιος μπορέσει να αναλύσει το n σε p και q, θα μπορέσει να πάρει την τιμή d. Η ασφάλεια του RSA βασίζεται στην θεώρηση ότι η ανάλυση σε παράγοντες γινομένου είναι δύσκολη. Μια μέθοδος εύκολης ανάλυση σε παράγοντες γινομένου ή κάποια άλλη εφικτή επίθεση θα μπορούσε να "σπάσει" τον RSA. Παρακάτω παρουσιάζεται ένα απλουστευμένο παράδειγμα για το πώς δουλεύει ο αλγόριθμος για κρυπτογράφηση και εξακρίβωση γνησιότητας:

RSA κρυπτογράφηση: Ας υποθέσουμε ότι η Αλίκη θέλει να στείλει ένα μήνυμα m στον Μπομπ. Η Αλίκη δημιουργεί το κρυπτογραφημένο μήνυμα c ως εξής : c=me mod n, όπου e και n είναι του Μπομπ το δημόσιο κλειδί και το στέλνει στον Μπομπ. Για την αποκρυπτογράφηση ο Μπομπ κάνει το εξής: m=cd mod n, η σχέση μεταξύ e και d εξασφαλίζει ότι ο Μπομπ θα αποκρυπτογραφήσει σωστά το m. Εφόσον μόνο ο Μπομπ κατέχει το d, μόνο αυτός μπορεί να το αποκρυπτογραφήσει.

RSA εξακρίβωση γνησιότητας: Τώρα ας υποθέσουμε ότι η Αλίκη θέλει να στείλει ένα μήνυμα m στον Μπομπ έτσι ώστε αυτός να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και προέρχεται από την Αλίκη. Η Αλίκη δημιουργεί μια ηλεκτρονική υπογραφή s ως εξής: s=md mod n, όπου d, n είναι το ιδιωτικό κλειδί της Αλίκης, και στέλνει τα m, s στον Μπομπ. Για να γίνει η

επιβεβαίωση της υπογραφής ο Μπομπ ελέγχει το μήνυμα m που πήρε με αυτό που βγαίνει από την πράξη se mod n, όπου e,n είναι το δημόσιο κλειδί της Αλίκης.

Diffie-Hellman

Ο αλγόριθμος Diffie-Hellman είναι ένα πρωτόκολλο συμφωνίας που επιτρέπει την ανταλλαγή ενός μυστικού κλειδιού χρησιμοποιώντας τεχνικές των αλγορίθμων δημοσίου κλειδιού. Αναπτύχθηκε από τους Diffie και Hellman το 1976. Το πρωτόκολλο έχει δύο παραμέτρους συστήματος p και g. Είναι και οι δύο δημόσιες και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες σε ένα σύστημα. Η παράμετρος p είναι ένας πρώτος αριθμός και η παράμετρος g είναι ένας ακέραιος μικρότερος του p, ο οποίος είναι ικανός να παράγει κάθε αριθμό από το 1 έως το p-1 όταν πολλαπλασιαστεί με τον εαυτό του ορισμένες φορές modulo τον πρώτο p.

Ας υποτεθεί ότι η Ελένη και ο Νίκος θέλουν να συμφωνήσουν σε ένα μυστικό κλειδί χρησιμοποιώντας το παραπάνω πρωτόκολλο. Προχωρούν ως ακολούθως: Πρώτα η Ελένη παράγει μια τυχαία ιδιωτική τιμή α και ο Νίκος παράγει μια τυχαία ιδιωτική τιμή b. Έπειτα και οι δύο παράγουν τις δημόσιες τιμές χρησιμοποιώντας τις παραμέτρους p και g και τις ιδιωτικές τους τιμές. Η δημόσια τιμή της Ελένης είναι η gα mod p και του Νίκου gb mod p. Στη συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τελικά, η Ελένη υπολογίζει kαb=(gb)α mod p και ο Νίκος kbα=(gα)b mod p. Εφόσον kαb=kbα=k, η Ελένη και ο Νίκος τώρα έχουν μοιραστεί ένα μυστικό κλειδί k.

Η ασφάλεια του πρωτοκόλλου εξαρτάται πάνω στο πρόβλημα του διακριτού λογάριθμου. Υποτίθεται ότι είναι υπολογιστικά μη πρακτικό να υπολογιστεί το κοινό μυστικό κλειδί k όταν δοθούν δύο δημόσιες τιμές gα mod p και gb mod p όταν ο πρώτος p είναι αρκετά μεγάλος. Το πρωτόκολλο Diffie-Hellman είναι ευάλωτο σε μια επίθεση παρεμβαλλόμενου προσώπου. Σε αυτή την επίθεση ένας αντίπαλος η Κάρολ, εμποδίζει την δημόσια τιμή της Αλίκης να σταλεί στον Μπομπ και στέλνει την δική της σ' αυτόν. Όταν ο Μπομπ στέλνει την δική του τιμή, η Κάρολ την αντικαθιστά με την δική της και την στέλνει στην Αλίκη. Η Κάρολ και η Αλίκη συμφωνούν σε ένα μυστικό κλειδί και η Κάρολ και ο Μπομπ συμφωνούν σε άλλο. Μετά την ανταλλαγή αυτή η Κάρολ μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα στέλνεται από τους άλλους δύο και πιθανόν να το αλλάξει και να το επαναμεταδώσει στους αντίστοιχους παραλήπτες. Η αδυναμία του αλγορίθμου οφείλεται στο γεγονός ότι το πρωτόκολλο δεν πιστοποιεί τους συμμετέχοντες σ' αυτήν την διαδικασία. Ορισμένες πιθανές λύσεις συμπεριλαμβάνουν την χρήση ηλεκτρονικών υπογραφών και άλλων ειδών πρωτοκόλλων.

Digital Signature Algorithm και Digital Signature Standard

Ο DSA είναι ένας αλγόριθμος ηλεκτρονικών υπογραφών και τα αρχικά του σημαίνουν Digital Signature Algorithm. Ο DSA δημοσιεύθηκε από το NIST στα πλαίσια του Digital Signature Standard (DSS), ενός σχεδίου για την κυβέρνηση των Η.Π.Α. Ο DSA είναι βασισμένος επάνω στο πρόβλημα του διακριτού λογάριθμου και προέρχεται από τα κρυπτοσυστήματα που προτάθηκαν από τους Schnorr και ElGamal. Είναι μόνο για εξακρίβωση γνησιότητας. Ο αλγόριθμος γενικά θεωρείται ασφαλής όταν το κλειδί του είναι αρκετά μεγάλο. Το πρότυπο DSS αρχικά προτάθηκε για μέγεθος κλειδιού 512-bit αλλά μετά από αρκετή κριτική λόγω του ότι δεν ήταν ασφαλής αναθεωρήθηκε το πρότυπο DSS με χρήση κλειδιού μεγέθους μέχρι 1024-bits.

Στον DSA η δημιουργία της υπογραφής είναι πιο γρήγορη από την επιβεβαίωσή της, αντίθετα με τον RSA όπου εκεί η επιβεβαίωση της υπογραφής είναι πιο γρήγορη από την δημιουργία της. Μια σύντομη περιγραφή του αλγορίθμου είναι η εξής:

1. Επιλέγεται ένας μεγάλος πρώτος αριθμός p μεταξύ 512 και 1024 bits.
2. Βρίσκεται ένας πρώτος παράγοντας q του p-1 160 bits. Υπολογίζεται g=h(p-1)/q mod p, όπου h ένας αριθμός μικρότερος από p-1.
3. Διαλέγουμε έναν άλλο αριθμό x<q ως το private key του αποστολέα.
4. Υπολογίζεται y=gx mod p και χρησιμοποιείται ως το public key του αποστολέα.
5. Ο αποστολέας υπογράφει το μήνυμα με το ζευγάρι (r,s) όπου r=(gk mod p) mod q και s=(k-1 (SHA1(m)+xr)) mod q, όπου m το μήνυμα, k ένας τυχαίος αριθμός και SHA1 η συνάρτηση για message digest.

Το παρόν κρυπτοσύστημα είναι αρκετά καινούργιο και δεν έχει γίνει αρκετή μελέτη πάνω σ' αυτό έτσι ώστε οι χρήστες να είναι πεπεισμένοι για την ασφάλειά του. Η πιστοποίηση της υπογραφής του DSA είναι αρκετά αργή. Η ύπαρξη ενός δεύτερου προτύπου πιστοποίησης θα ταλαιπωρήσει τις βιομηχανίες υπολογιστών διότι έχουν ήδη δεχθεί ως πρότυπο τον RSA.

Συναρτήσεις κατακερματισμού (Hash Functions)

Μια συνάρτηση κατακερματισμού H είναι ένας μετασχηματισμός ο οποίος παίρνει μία μεταβλητού μεγέθους είσοδο m και επιστρέφει ένα σταθερού μεγέθους string, το οποίο

ονομάζεται τιμή κατακερματισμού h, δηλαδή (h=H(m)). Αυτές οι συναρτήσεις με μόνο αυτή την ιδιότητα έχουν μια ποικιλία από πολλές γενικού περιεχομένου εφαρμογές αλλά όταν χρησιμοποιούνται στην κρυπτογραφία τότε επιλέγονται με κάποιες επιπρόσθετες ιδιότητες. Οι βασικές απαιτήσεις για μια κρυπτογραφική συνάρτηση κατακερματισμού είναι:

1. Η είσοδος μπορεί να έχει οποιοδήποτε μέγεθος
2. Η έξοδος έχει σταθερό μέγεθος
3. Η H(x) είναι εύκολο να υπολογισθεί για οποιοδήποτε x
4. Η H(x) είναι μιας κατεύθυνσης: Μια συνάρτηση κατακερματισμού λέγεται μιας κατεύθυνσης αν είναι δύσκολο να αντιστραφεί, δηλαδή αν δοθεί μια τιμή κατακερματισμού h τότε είναι δύσκολο να βρούμε αυτό το x για το οποίο θα ισχύει H(x)=h.
5. Η H(x) δεν έχει συγκρούσεις: Μια συνάρτηση H(x) δεν έχει συγκρούσεις αν είναι υπολογιστικά μη πρακτικό να βρούμε δύο εισόδους x και y τέτοιες ώστε H(x)=H(y).

Μια τιμή κατακερματισμού αντιπροσωπεύει με λιτό τρόπο ένα μεγαλύτερο μήνυμα ή κείμενο από το οποίο υπολογίστηκε. Παραδείγματα από γνώστες συναρτήσεις κατακερματισμού είναι οι MD2, MD5 και SHA. Επειδή οι συναρτήσεις κατακερματισμού είναι γρηγορότερες από τους αλγορίθμους ηλεκτρονικών υπογραφών, συνηθίζεται αντί να υπολογίζεται η ηλεκτρονική υπογραφή ενός κειμένου, να υπολογίζεται η ηλεκτρονική υπογραφή της τιμής κατακερματισμού του που είναι και πιο μικρή από το ίδιο το κείμενο.

MD2, MD4 και MD5

Οι MD2, MD4 και MD5 είναι αλγόριθμοι σύνοψης μηνυμάτων (message digest) και αναπτύχθηκαν από τον Rivest. Ο προορισμός τους είναι για εφαρμογές ηλεκτρονικών υπογραφών όπου ένα μεγάλο μήνυμα πρέπει να συμπιεστεί με ασφάλεια προτού υπογραφθεί με το ιδιωτικό κλειδί. Και οι τρεις αλγόριθμοι παίρνουν ένα μήνυμα με αυθαίρετο μέγεθος και παράγουν μια 128-bit σύνοψή του. Παρόλο που οι δομές και των τριών αλγορίθμων μοιάζουν κάπως, ο σχεδιασμός του MD2 διαφέρει λίγο από τους υπόλοιπους δύο και έχει βελτιστοποιηθεί για μηχανές των 8-bit, ενώ οι MD4 και MD5 προορίζονται για 32-bit μηχανές. Στον MD2 το μήνυμα πρώτα "γεμίζεται" στο τέλος με bytes έτσι ώστε το μέγεθος του σε bytes να είναι διαιρέσιμο με το 16. Έπειτα ένα 16-byte άθροισμα ελέγχου προστίθεται στο τέλος και στη συνέχεια υπολογίζεται πάνω σ' αυτό η τιμή κατακερματισμού του.

Στον MD4 το μήνυμα "γεμίζεται" στο τέλος με bits έτσι ώστε να εξασφαλισθεί ότι το μέγεθός του σε bits είναι διαιρέσιμο με το 512 αν προσθέσουμε και το 448. Μια 64-bit αναπαράσταση του αρχικού μήκους του μηνύματος προστίθεται με το μήνυμα. Ύστερα το μήνυμα επεξεργάζεται σε 512-bit μέρη στην επαναληπτική δομή των Damgard-Merkle και κάθε μέρος επεξεργάζεται σε τρεις διακεκριμένους γύρους. Γρήγορα ανακαλύφθηκαν διάφορες επιθέσεις γι' αυτόν τον αλγόριθμο και ο Dobbertin έδειξε πως μπορούν να βρεθούν συγκρούσεις σε χρόνο μικρότερο από ένα λεπτό σε ένα τυπικό PC. Έτσι ο MD4 σήμερα θεωρείται ότι έχει σπαστεί.

Ο MD5 είναι ένας MD4 με ζώνες ασφαλείας. Είναι πιο αργός από τον MD4 αλλά και πιο ασφαλής. Ο αλγόριθμος αποτελείται από τέσσερις διακεκριμένους γύρους οι οποίοι έχουν λίγο διαφορετική σχεδίαση απ'αυτούς του MD4. Το μέγεθος του συνοπτικού μηνύματος καθώς και οι απαιτήσεις "γεμίσματος" παραμένουν οι ίδιες.

Secure Hash Algorithm (SHA)

Ο SHA, που σημαίνει Secure Hash Algorithm, καθορίστηκε στο Secure Hash Standard (SHS) και αναπτύχθηκε από το NIST. Ο σχεδιασμός του μοιάζει αρκετά με αυτούς της οικογένειας των συναρτήσεων κατακερματισμού του MD4. Ο αλγόριθμος παίρνει έναν μήνυμα μικρότερο από 264 bits σε μέγεθος και παράγει ένα συνοπτικό μήνυμα των 160 bit. Ο αλγόριθμος είναι λίγο αργότερος από τον MD5 αλλά το μεγαλύτερο συνοπτικό μήνυμα τον κάνει πιο ασφαλή απέναντι σε brute-force συγκρούσεις και επιθέσεις αντιστροφής.

Στεγανογραφία

Η στεγανογραφία είναι η τεχνική του να κρύβονται μυστικά μηνύματα μέσα σε άλλα μηνύματα, έτσι ώστε η παρουσία των μυστικών μηνυμάτων να μη γίνεται αντιληπτή. Ιστορικά κόλπα περιλαμβάνουν αόρατα μελάνια, πολύ μικρές διατρήσεις πάνω σε επιλεγμένους χαρακτήρες, μικρές διαφορές μεταξύ χειρόγραφων χαρακτήρων, σημάδια από μολύβι πάνω σε χαρακτήρες τυπωμένους, κομμάτια που καλύπτουν το μεγαλύτερο μέρος του μηνύματος εκτός από ορισμένους χαρακτήρες κ.ο.κ. Τελευταία συνηθίζεται να κρύβονται μυστικά μηνύματα πάνω σε γραφικές εικόνες.

Firewalls

Ένας από τους αποτελεσματικότερους τρόπους για την προστασία του δικτύου από πιθανούς παραβάτες είναι η χρήση ενός συστήματος Firewall μεταξύ του τοπικού δικτύου και του Internet. Το Firewall εξασφαλίζει ότι όλη η επικοινωνία μεταξύ του δικτύου μιας επιχείρησης και το Διαδίκτυο είναι σύμφωνη με την πολιτική ασφάλειας της επιχείρησης. Για να το πετύχει αυτό, ένα Firewall πρέπει να εντοπίζει και να ελέγχει τη ροή επικοινωνίας που περνάει μέσα από αυτό. Για να πετύχει τον έλεγχο των υπηρεσιών που βασίζονται στο TCP/IP, αν δηλαδή θα επιτρέψει, απορρίψει, κρυπτογραφήσει ή καταγράψει την επικοινωνία, το Firewall πρέπει να λαμβάνει, αποθηκεύει και να διαχειρίζεται πληροφορία που προέρχεται από όλα τα επίπεδα επικοινωνίας και από άλλες εφαρμογές. Οι συσκευές Firewall ενώ συχνά είναι απαραίτητες για την προστασία του site, αποτελούν επίσης και πηγή κινδύνου, γιατί, πρώτον οι χρήστες πιστεύουν ότι από την στιγμή που αγοράσθηκε το προϊόν, η ασφάλεια έχει εξασφαλισθεί, πράγμα που απέχει πολύ από την αλήθεια, και δεύτερον, γιατί ο ίδιος ο κώδικας είναι πιθανόν να μην συμπεριφέρεται όπως θα έπρεπε, με αποτέλεσμα να αφήνει τις πίσω πόρτες ανοικτές. Ένα firewall αποτελείται από τρεις ομάδες συνιστωσών:

1. φίλτρα για μπλοκάρισμα και/ή παρακολούθηση μετάδοσης συγκεκριμένου είδους μηνυμάτων (καθορισμένα από τον τύπο, τον προορισμό τους ή συνδυασμό και των δύο),
2. gateways για προώθηση των αποδεκτών μηνυμάτων από τη μια μεριά του firewall στην άλλη,
3. application proxies που εκτελούν έλεγχο ειδικής πρόσβασης σε εφαρμογές, παρακολούθηση και αναφορά.

Από κει και πέρα, για την επίτευξη της ασφάλειας σε μεμονωμένες περιπτώσεις χρήσης διαφόρων υπηρεσιών το πιο συνηθισμένο μέτρο ασφάλειας είναι τα γνωστά μας Ids και Passwords, τα οποία όμως δεν αποτελούν εγγύηση καθώς πολλοί χρήστες προτιμούν ένα ευκολομνημόνευτο password που όμως είναι πολύ εύκολο να βρεθεί από έναν αποφασισμένο hacker. Επίσης, θα πρέπει να γνωρίζουμε ότι οι περισσότερες απειλές (το 80% σύμφωνα με έρευνες) προέρχονται από νόμιμους χρήστες με έγκυρο password. Μεγαλύτερη ασφάλεια προσφέρουν τα συστήματα που κάνουν χρήση των έξυπνων καρτών. Σε αυτά τα συστήματα, ο χρήστης για να μπει στο λογαριασμό του δεν χρειάζεται να είναι κάτοχος του password μόνο, άλλα και της προσωπικής

του κάρτας. Τα επόμενα χρόνια επίσης θα είμαστε μάρτυρες μιας ραγδαίας ανάπτυξης βιομετρικών τεχνικών, όπως αυθεντικοποίηση με την ίριδα των ματιών, της φωνής, των αποτυπωμάτων κτλ.

Ένα άλλο μέτρο είναι η χρήση κρυπτογραφικών μεθόδων. Ένα ευρύτατα χρησιμοποιούμενο εργαλείο για την προστασία της μυστικότητας είναι αυτό που οι κρυπτογράφοι αποκαλούν «μυστικό κλειδί». Τα passwords σύνδεσης και οι αριθμοί PIN των πιστωτικών καρτών είναι παραδείγματα μυστικών κλειδιών. Οι καταναλωτές μοιράζονται αυτά τα κλειδιά μόνο με τους τρίτους που θέλουν να επικοινωνήσουν, όπως online υπηρεσίες συνδρομής και τράπεζες. Έτσι οι προσωπικές πληροφορίες αποκρύβονται και μόνο μία από τις δυο πλευρές που έχει το μυστικό κλειδί στην κατοχή της μπορεί να τις αποκρυπτογραφήσει.

Όμως, το παραπάνω σύστημα, παρά την ευρεία χρήση του, παρουσιάζει κάποιους περιορισμούς. Από τη μία, λόγω της τεράστιας εξάπλωσης του διαδικτύου, είναι άβολο για τους χρήστες να δημιουργούν και να θυμούνται διαφορετικά passwords για κάθε περίσταση. Από την άλλη, κατά την αποστολή του, το password μπορεί να πέσει σε λάθος χέρια ή κάποια από τις δυο πλευρές να το χρησιμοποιήσει σε «υποχθόνιες» πράξεις και μετά να αρνηθεί το όλο συμβάν. Έτσι πάμε στην τεχνολογία ψηφιακών ταυτοτήτων η οποία λύνει αυτά τα προβλήματα γιατί δεν βασίζεται στη διαμοίραση μυστικών κλειδιών.

Ο σχεδιασμός ασφαλείας πρέπει να αποτελεί μέρος κάθε εφαρμογής ηλεκτρονικού εμπορίου. Είναι σημαντικό όμως να λαμβάνεται υπόψη από την αρχή του σχεδιασμού της εφαρμογής, γιατί είναι πολύ πιο δαπανηρό να προστεθεί ασφάλεια κατά τη διάρκεια της. Υπάρχουν πέντε βασικά βήματα για το σχεδιασμό της ασφάλειας των συστημάτων ηλεκτρονικού εμπορίου:

1. Καθορισμός της πολιτικής ασφαλείας.
2. Προσθήκη των απαραίτητων μηχανισμών ασφαλείας στην εφαρμογή.
3. Σχεδιασμός της ασφάλειας του φυσικού, δικτυακού και υπολογιστικού περιβάλλοντος του συστήματος.
4. Ανάπτυξη μηχανισμών ανάδρασης, επίβλεψης και περιοδικού ελέγχου για παρατήρηση της ορθής λειτουργίας του συστήματος.
5. Χρήση των αποτελεσμάτων της ανάδρασης, επίβλεψης και περιοδικού ελέγχου για βελτίωση του σχεδιασμού, υλοποίησης και λειτουργίας του συστήματος.

5 ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Καθορισμός της πολιτικής ασφαλείας

Το πρώτο βήμα στο σχεδιασμό ασφαλείας είναι ο καθορισμός της πολιτικής ασφαλείας[43]. Η πολιτική θα πρέπει να καλύπτει όλο το σύστημα, περιλαμβάνοντας συστήματα πληροφοριών (δίκτυα και υπολογιστές), δεδομένα (πληροφορίες ανάπτυξης, παραγωγής και αποθήκευσης) και ανθρώπινο δυναμικό (χειριστές, προσωπικό συντήρησης, πελάτες). Η πολιτική θα πρέπει να περιέχει αναφορές για το τι προστατεύεται, τι είδος προστασίας χρειάζεται, ποιος είναι υπεύθυνος για τα διάφορα μέρη του συστήματος, για την απαραίτητη εκπαίδευση, και τι είδος επίβλεψης και περιοδικού ελέγχου απαιτείται.

Σχεδιασμός του περιβάλλοντος

Το δεύτερο βήμα είναι ο σχεδιασμός του περιβάλλοντος της εφαρμογής. Ο σχεδιασμός του περιβάλλοντος περιλαμβάνει όλες τις συνιστώσες έξω από την ίδια την εφαρμογή, όπως είναι οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα και οι φυσικές εγκαταστάσεις. Συχνά το περιβάλλον μπορεί να παρέχει κάποιες δυνατότητες προστασίας της εφαρμογής, έτσι ώστε η εφαρμογή να μη χρειάζεται να τις αντιγράψει. Αξίζει να σημειωθεί όμως ότι τέτοιες δυνατότητες πρέπει να καταγράφονται έτσι ώστε η εφαρμογή να μπορεί να επαναδημιουργηθεί οπουδήποτε εμφανισθεί ανάγκη. Σε άλλες περιπτώσεις το ίδιο το περιβάλλον πρέπει να δεσμεύει την εφαρμογή με διάφορους τρόπους ή να απαιτεί ειδικές μεθόδους ασφαλείας να λαμβάνονται από την εφαρμογή αν δεν περιλαμβάνονται από το περιβάλλον. Για παράδειγμα, ας υποτεθεί ότι μια εφαρμογή λειτουργεί σε συστήματα προστατευμένα με δυνατή φυσική ασφάλεια. Επιπλέον, οι χειριστές εκτελούν όλες τις εργασίες τους τοπικά. Σ' αυτήν την περίπτωση, η εφαρμογή θα δώσει λιγότερη προσοχή στον έλεγχο πιστοποίησης και στον έλεγχο πρόσβασης σε λειτουργίες διαχείρισης, γιατί μπορεί να υποθέσει ότι οι χειριστές έχουν την απαραίτητη πιστοποίηση από την αρχή όταν απέκτησαν πρόσβαση. Όμως σε μια εφαρμογή όπου η διαχείριση της είναι σχεδιασμένη να πραγματοποιείται εξ αποστάσεως έχει διαφορετικές απαιτήσεις. Γενικά είναι καλή πρακτική για την εφαρμογή να έχει τα δικά της μέσα για έλεγχο πιστοποίησης και πρόσβασης γιατί είναι πιθανόν οι μηχανισμοί φυσικής ασφαλείας να «κρεμάσουν».

[43] Simon, H,. Hidden Champions: Lessons from 500 of the Worlds Best unknown Companies, Harvard Business School Press, Boston, 1996

Στην πράξη ο σχεδιασμός του περιβάλλοντος και ο σχεδιασμός των μηχανισμών ασφαλείας της εφαρμογής θα πρέπει να αλληλεπιδρούν με χρήσιμο τρόπο. Μερικά προβλήματα ασφαλείας είναι ευκολότερο να λυθούν από την εφαρμογή παρά από το περιβάλλον και το αντίστροφο. Σε μερικές περιπτώσεις, ειδικά στο σχεδιασμό των προϊόντων, η εφαρμογή μπορεί να επιβάλλει κάποιες απαιτήσεις στο περιβάλλον στο οποίο θα χρησιμοποιηθεί. Τελικά το πιο σημαντικό θέμα κατά την ανάπτυξη του σχεδίου ασφαλείας είναι ο σχεδιασμός ολόκληρου του συστήματος (εφαρμογής και περιβάλλοντος).

Σχεδιασμός των μηχανισμών ασφαλείας της εφαρμογής

Το τρίτο βήμα στο σχεδιασμό ασφαλείας είναι η παροχή μηχανισμών ασφαλείας για την ίδια την εφαρμογή. Ο γενικός σχεδιασμός της εφαρμογής μαζί με την πολιτική ασφαλείας θα πρέπει να παρέχει τις απαιτήσεις για το τι προστατεύεται και να δίνει μια καθοδήγηση για το είδος της προστασίας που χρειάζεται. Το σχέδιο ασφαλείας τότε μπορεί να χρησιμοποιήσει διάφορες συνιστώσες τεχνολογιών όπως συστήματα κρυπτογράφησης, πιστοποίησης και εξουσιοδότησης. Επιπρόσθετα σ' αυτούς τους γενικούς μηχανισμούς για έλεγχο της πρόσβασης στις πληροφορίες, μπορεί να υπάρχουν και κάποιες ειδικές απαιτήσεις της ίδιας της εφαρμογής. Για παράδειγμα, αν πρόκειται για εφαρμογή πωλήσεων λογισμικού πάνω από το δίκτυο, το σύστημα ασφαλείας μπορεί να περιέχει ειδικά κλειδιά που επιτρέπουν το λογισμικό να τρέχει μόνο στο συγκεκριμένο υπολογιστή του πελάτη.

Επίβλεψη και περιοδικός έλεγχος

Πέρα από τις ειδικές απαιτήσεις της εφαρμογής, η ασφάλεια απαιτεί μηχανισμούς ανάδρασης ώστε να εξασφαλίζεται ότι οι μηχανισμοί ασφαλείας λειτουργούν σωστά, μηχανισμούς αποθήκευσης ώστε να περιορίζεται η έκταση της ζημιάς, και μηχανισμούς ανάκτησης όταν παρουσιάζεται το πρόβλημα. Στο φυσικό κόσμο, είναι απαραίτητος ο νυχτοφύλακας που διασφαλίζει ότι οι πόρτες των χώρων είναι κλειδωμένες. Στον ηλεκτρονικό χώρο, αυτοί οι έλεγχοι αναλαμβάνονται από μηχανισμούς παρακολούθησης, ελέγχου ταχύτητας και υπηρεσίες πελατών. Η πληροφορία που παρέχεται από αυτούς τους μηχανισμούς μπορεί να χρησιμοποιηθεί με διάφορους τρόπους: για επαναλειτουργία σε περίπτωση προβλήματος, για έλεγχο ώστε να εξασφαλίζεται ότι οι επιθέσεις ήταν ανεπιτυχείς, για επιβεβαίωση ότι η λειτουργία συμφωνεί με την πολιτική ασφαλείας, και για αξιολόγηση αν η πολιτική ασφαλείας, ο σχεδιασμός και οι μηχανισμοί είναι αποτελεσματικοί για την εφαρμογή.

Ειδικοί στην ασφάλεια υπολογιστών συχνά επισημαίνουν ότι η ασφάλεια πρέπει να περικλείει ολόκληρο το σύστημα. Οι σχεδιαστές και οι χειριστές μιας υπηρεσίας πρέπει να λαμβάνουν σοβαρά υπόψη τους θέματα σχετικά με την εφαρμογή και τους κινδύνους πριν αποφασίσουν για το επίπεδο της ασφάλειας που θα παρέχεται, και εσωτερικά σε κάθε επίπεδο πρέπει να σκεφθούν τη σχετιζόμενη δύναμη των μηχανισμών ασφαλείας που θα αναπτυχθούν.

Ανάθεση ρόλων και υπευθυνοτήτων

Πολύ σημαντικό μέρος του σχεδιασμού της πολιτικής ασφαλείας είναι οι ρόλοι και οι αντίστοιχες υπευθυνότητες (του κάθε ρόλου) που πρέπει να ανατεθούν σε πρόσωπα-κλειδιά για την ορθή λειτουργία ενός συστήματος ηλεκτρονικού εμπορίου.

• Υπεύθυνος Ασφαλείας

Ο ρόλος του Υπεύθυνου Ασφαλείας περιλαμβάνει:

1. την έγκαιρη και αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας και ατυχημάτων ή έκτακτων γεγονότων.
2. τη διαχείριση των δικαιωμάτων προσπέλασης.
3. τη δημιουργία σχεδίου για την εκπαίδευση και ενημέρωση του υπόλοιπου προσωπικού.
4. τη σύνταξη αναφορών για την ασφάλεια του συστήματος ανά τακτά χρονικά διαστήματα.
5. την έγκαιρη ενημέρωση του σχετικά με οποιεσδήποτε αλλαγές που μπορούν να επηρεάσουν την ασφάλεια του συστήματος όπως διακοπές για συντήρηση ή επισκευή, πρόσληψη προσωπικού, αλλαγές στον εξοπλισμό κ.λπ.

• Διαχειριστής Συστήματος

Ο Διαχειριστής Συστήματος έχει τις ακόλουθες υπευθυνότητες:

1. τη διαχείριση του υλικού και του εξοπλισμού του συστήματος και την καταγραφή του.
2. τη διαχείριση (σε συνεργασία με τον Υπεύθυνο Ασφαλείας) των δικαιωμάτων προσπέλασης.
3. την επίβλεψη του συστήματος για την ορθή του λειτουργία και το χειρισμό σε περίπτωση δυσλειτουργιών.

4. την έγκαιρη ενημέρωση του σχετικά με οποιεσδήποτε αλλαγές που μπορούν να επηρεάσουν την ασφάλεια του συστήματος όπως διακοπές για συντήρηση ή επισκευή, πρόσληψη προσωπικού, αλλαγές στον εξοπλισμό κ.λπ.

• Διοικητικός Υπεύθυνος

Πρόκειται για το πρόσωπο που επικοινωνεί με τη διοίκηση και το προσωπικό του συστήματος. Έτσι παράλληλα με τις διάφορες διοικητικές του αρμοδιότητες είναι υπεύθυνος για:

1. την επίβλεψη του Υπεύθυνου Ασφαλείας και του Διαχειριστή Συστήματος.
2. τη μεταφορά των οδηγιών της διοίκησης στο υπόλοιπο προσωπικό.
3. την παρακολούθηση της σωστής ολοκλήρωσης των προβλεπόμενων διαδικασιών.
4. τη διατήρηση του ηθικού του προσωπικού σε ικανοποιητικό επίπεδο, ενός πολύ σημαντικού παράγοντα για την ασφάλεια του συστήματος.

• Χειριστές Συστήματος

Είναι υπεύθυνοι για την εκπλήρωση των καθηκόντων που τους ανατίθενται από τον Υπεύθυνο Ασφαλείας και το Διαχειριστή Συστήματος. Άλλες υπευθυνότητες τους είναι: αναφορά περιστατικών σχετικών με την ασφάλεια του συστήματος και συνεισφορά τους στην επίλυση τους, ενημέρωση για θέματα ασφαλείας, η ακριβής τήρηση των κανονισμών του συστήματος, η αποφυγή δραστηριοτήτων που μπορούν να επιφέρουν δυσλειτουργίες στο σύστημα.

Πλάνο Ασφαλείας. Το πλάνο ασφαλείας πρέπει να είναι πλήρες ώστε να ικανοποιεί όλες τις απαιτήσεις ασφαλείας που αναφέρθηκαν παραπάνω σε όποιο σημείο της υλοποίησης του συστήματος και αν εμφανίζονται αυτές.

Αναγνώριση και έλεγχος αυθεντικότητας

Αναγνωριστικά χρηστών. Με τη βοήθεια των αναγνωριστικών εξασφαλίζεται η ταυτοποίηση κάθε χρήστη ότι πραγματοποίησε μια ενέργεια.

Επιλογή συνθηματικών. Τα συνθηματικά (passwords) που υιοθετούν οι χρήστες πρέπει να έχουν αρκετό μήκος και να επιλέγονται με τέτοιο τρόπο, ώστε να είναι δύσκολο για κάποιον εισβολέα να τα μαντέψει ή να τα αποκρυπτογραφήσει από το αρχείο συνθηματικών.

Αποθήκευση συνθηματικών. Τα συνθηματικά των χρηστών θα πρέπει να αποθηκεύονται σε κατάλληλη μορφή, ώστε κανείς, ακόμα και ο Διαχειριστής του συστήματος να μην μπορεί να τα διαβάσει.

Συχνότητα αλλαγής των συνθηματικών. Τα συνθηματικά θα πρέπει να αλλάζουν αρκετά συχνά, ώστε να διασφαλίζεται η εμπιστευτικότητα τους.

Έλεγχος πρόσβασης.

Δικαιώματα πρόσβασης

Για κάθε νέο λογαριασμό χρήστη θα πρέπει να καθορίζονται τα δικαιώματα πρόσβασης στους πόρους του συστήματος.

Αδρανής σταθμός εργασίας. Οι σταθμοί εργασίας θα πρέπει να κλειδώνονται όταν μένουν αδρανείς για κάποιο χρονικό διάστημα (προτεινόμενος χρόνος 10 λεπτά) ώστε να περιοριστεί η πιθανότητα ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση.

Διαχείριση δικαιωμάτων. Κατάλληλος μηχανισμός επιτρέπει την πρόσβαση σε ιδιαίτερες λειτουργίες του συστήματος μόνο σε χρήστες που πρέπει να έχουν πρόσβαση σ' αυτές.

Πολιτική ελέγχου πρόσβασης. Πρόκειται για την απαραίτητη ύπαρξη καταγεγραμμένης πολιτικής για τον έλεγχο πρόσβασης.

Ασφάλεια του λογισμικού εφαρμογών. Η πρόσβαση στα αρχεία του λογισμικού εφαρμογών θα πρέπει να ελέγχεται με τη βοήθεια κατάλληλων προγραμμάτων.

Απόδοση ευθυνών

Καταγραφή των γεγονότων. Πρόκειται για την καταγραφή όλων των περιστατικών (γεγονότων ή λειτουργιών) που λαμβάνουν χώρα στο σύστημα κάθε χρονική στιγμή, ώστε κάθε επεισόδιο να μπορεί να διερευνηθεί και να αποδοθούν ευθύνες. Διατήρηση των αρχείων καταγραφής γεγονότων Θα πρέπει να διατηρείται κατάλληλο αρχείο καταγραφής γεγονότων για αρκετό χρονικό διάστημα. Επίσης θα πρέπει να υπάρχει ο κατάλληλος χώρος για την αποθήκευση του αρχείου καταγραφής γεγονότων.

Επιθεώρηση των αρχείων καταγραφής γεγονότων. Τα αρχεία καταγραφής γεγονότων θα πρέπει να επιθεωρούνται ανά τακτά χρονικά διαστήματα, ώστε να εξασφαλίζεται ότι όλοι οι χρήστες εκτελούν τις εργασίες για τις οποίες είναι εξουσιοδοτημένοι.

Διερεύνηση επεισοδίων. Όταν κάποια επεισόδια ανιχνεύονται ή υπάρχουν υποψίες γι' αυτά, πρέπει να διερευνούνται σε βάθος.

Προστασία από ιούς

Πρόληψη και αποτροπή. Θα πρέπει να ελαχιστοποιηθεί η πιθανότητα να προσβληθεί το σύστημα από ιούς οποιασδήποτε μορφής.

Ανίχνευση. Το σύστημα θα πρέπει να περιλαμβάνει μηχανισμούς περιοδικού ελέγχου για ιούς.

Αντιμετώπιση. Τέλος, θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί απομόνωσης και καταστροφής των ιών.

Διαχείριση ασφάλειας δικτύου

Διαχείριση δικτύου. Η διαχείριση των δικτύων πρέπει να γίνεται με ασφαλή τρόπο. Για οποιαδήποτε προβλήματα θα πρέπει να ενημερώνεται ο Υπεύθυνος Ασφαλείας.

Παρακολούθηση του δικτύου. Η κατάσταση του δικτύου θα πρέπει να παρακολουθείται, ώστε να διευκολύνεται η έγκαιρη ανίχνευση των προβλημάτων.

Εμπιστευτικότητα δεδομένων στο δίκτυο. Η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω δικτύου θα πρέπει να προστατεύεται.

Έλεγχος πρόσβασης μέσω δικτύου

Έλεγχος αυθεντικότητας εφαρμογών. Η επικοινωνία μεταξύ εφαρμογών θα πρέπει να γίνεται με ασφαλή τρόπο.

Απομακρυσμένη πρόσβαση σε μη ενεργές πόρτες. Μόνο οι είσοδοι (ports) που χρησιμοποιούνται θα πρέπει να είναι ενεργές και οι υπόλοιπες πρέπει να είναι κλειδωμένες.

Firewalls. Θα πρέπει να υπάρχει διαχωρισμός μεταξύ των δικτύων και προστασία τους με τη χρήση firewalls.

Ηλεκτρονικό Εμπόριο και Προσωπικά Δεδομένα. Οι έμποροι προκειμένου να μετρήσουν τις καταναλωτικές προτιμήσεις του κοινού με σκοπό να προσαρμόσουν στη βάση ζήτησης τις γραμμές παραγωγής τους και να προωθήσουν τις πωλήσεις τους μέσω του διαδικτύου, δημιουργούν νέους τρόπους συλλογής, επεξεργασίας και διασύνδεσης των προσωπικών δεδομένων. Τα προσωπικά δεδομένα συνήθως συλλέγονται κατά την αρχική φάση σύνδεσης του πελάτη με το δικτυακό χώρο του πωλητή και στην συνέχεια χρησιμοποιούνται σύγχρονες τεχνικές εξόρυξης δεδομένων (data mining) για την περαιτέρω ανάλυσή τους. Αποτέλεσμα της παραπάνω διαδικασίας είναι η δημιουργία βάσεων καταναλωτικών προφίλ των πελατών. Προφίλ ενός ατόμου νοείται ως μια συλλογή δεδομένων που μπορεί μοναδικά να προσδιορίσει την ταυτότητα του ατόμου αυτού.

Οι οντότητες οι οποίες τυπικά εμπλέκονται στην εγκατάσταση μιας ηλεκτρονικής σύνδεσης, με έμφαση στων πραγματοποίηση ηλεκτρονικών συναλλαγών και οι οποίες είναι ταυτόχρονα η πηγή και ο αποδέκτης των προσωπικών δεδομένων των χρηστών είναι οι εξής:

1. Χρήστης: Ο ενδιαφερόμενος για την απόκτηση μιας υπηρεσίας του διαδικτύου, την απόκτηση ενός προϊόντος με χρήση τεχνολογιών που βοηθούν στην ανάπτυξη του ηλεκτρονικού εμπορίου κ.λ.π.

2. Παροχέας Υπηρεσιών Διαδικτύου, ΠΥΔ, (Internet Service Provider, ISP): Η οντότητα που παρέχει, τυπικά σε χρήστες, το υλικό (hardware) και πιθανώς λογισμικό (software), για την απόκτηση πρόσβασης στις βασικές υπηρεσίες του διαδικτύου.

3. Παροχέας Φυσικού Μέσου επικοινωνίας, ΠΦΜ, (Carrier Provider): Η οντότητα που παρέχει το φυσικό τεχνολογικό μέσο μετάδοσης και επικοινωνίας δεδομένων π.χ. αναλογικές ή/και ψηφιακές γραμμές, εξοπλισμός αναμετάδοσης σημάτων με χρήση ψηφιακών κέντρων, δορυφόρων κ.λ.π. Οι οντότητες αυτές τυπικά αντιπροσωπεύονται από μεγάλους τηλεπικοινωνιακούς οργανισμούς π.χ. ΟΤΕ.

4. Παροχέας Τελικής Υπηρεσίας ΠΤΥ. Η οντότητα που παρέχει με χρήση κάποιου πρωτοκόλλου επικοινωνίας, την ζητούμενη από τον χρήστη υπηρεσία π.χ. αναζήτηση πληροφοριών

με χρήση μηχανών αναζήτησης (search machines), αγορά προιόντων με χρήση τεχνολογιών ανάπτυξης ηλεκτρονικού εμπορίου κ.λ.π.

Δύο επιπλέον οντότητες που παίζουν σημαντικό ρόλο στην διεκπεραίωση των ηλεκτρονικών συναλλαγών αλλά δεν εμπλέκονται, συνήθως, άμεσα σε αυτές είναι:

1. Έμπιστες Τρίτες Οντότητες (ΕΤΟ): αυτές είναι έμπιστες οντότητες οι οποίες δεν εμπλέκονται άμεσα στην συναλλαγή αλλά μπορούν να καταφύγουν οι εμπλεκόμενοι μιας συναλλαγής σε περιπτώσεις διενέξεων, για την επαλήθευση των στοιχείων της συναλλαγής. Τυπικό έργο των οντοτήτων αυτών είναι η έκδοση και διαχείριση ψηφιακών πιστοποιητικών (digital certificates). Οι ΕΤΟ συναντούνται στην βιβλιογραφία και με τον όρο Αρχές Πιστοποίησης (ΑΠ).

2. Λοιποί ενδιάμεσοι: αυτές είναι τυπικά οι Τράπεζες που εμπλέκονται στην εκκαθάριση των πληρωμών είτε αυτές πραγματοποιούνται με τεχνολογίες ψηφιακού χρήματος είτε με χρήση πιστωτικών καρτών.

Στην Ελλάδα το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 2774/99 (Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα) με τον οποίο η Αρχή Προστασίας Δεδομένων και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχουν αντίστοιχες αρμοδιότητες όπως ο νόμος αυτός ορίζει. Κάθε συλλογή και επεξεργασία στοιχείων των χρηστών του διαδικτύου (π.χ. ηλεκτρονική διεύθυνση αλληλογραφίας, διεύθυνση διαδικτύου κ.λ.π) εμπίπτουν στις διατάξεις των παραπάνω νόμων. Οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών όπως ορίζονται στο νόμο 2774/99 προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών. Η άρση του απορρήτου σε δημόσιες αρχές είναι επιτρεπτή μόνο για τους λόγους και υπό τους όρους και διαδικασίες που ορίζει ο Ν. 2225/94 όπως ισχύει.

Οι κίνδυνοι

Ο χώρος του ηλεκτρονικού εμπορίου κρύβει πολλούς κινδύνους για τον ανυποψίαστο χρήστη. Οι περιπτώσεις όπου διακριτά καταγράφονται προσωπικά δεδομένα διακρίνονται στις παρακάτω κατηγορίες:

1. Όταν με τη συγκατάθεσή του ο χρήστης δίνει τα προσωπικά του στοιχεία, όποτε για παράδειγμα επιθυμεί να αγοράσει κάποιο προϊόν /υπηρεσία ή να κατεβάσει (download) κάποιο πρόγραμμα στον προσωπικό του υπολογιστή ή και να εγγραφεί σε κάποια υπηρεσία του διαδικτύου. Προσωπικά δεδομένα, όπως στοιχεία ταυτότητας, στοιχεία επαγγελματικά, στοιχεία εκπαίδευσης ή και ακόμα οικονομικά στοιχεία όπως είναι ο αριθμός της πιστωτικής κάρτας.

2. Όταν χωρίς την συγκατάθεσή του χρήστη, συλλέγονται προσωπικά στοιχεία μέσω των λεγόμενων προγραμμάτων cookies τα οποία καταγράφουν και επεξεργάζονται την συμπεριφορά του χρήστη κατά την πλοήγησή του στο διαδίκτυο (πχ προτιμήσεις).

3. Όταν στα πλαίσια του παροχέα υπηρεσιών πρόσβασης στο Internet τηρείται αρχείο με τα προσωπικά στοιχεία του χρήστη και κατ΄ επέκταση στοιχεία των ηλεκτρονικών διευθύνσεων (ιστοσελίδες) τις οποίες επισκέπτεται, τον ακριβή χρόνο και τη διάρκεια της επίσκεψης.

5.1 Ασφάλεια προσωπικών δεδομένων

Άλλο ένα θεμελιώδες θέμα ασφαλείας συνίσταται στη διαφύλαξη του προσωπικού απορρήτου, το οποίο πλέον αποτελεί ένα ακανθώδες ζήτημα στο Internet. Ένας μεγάλος όγκος πληροφοριών μπορεί να συλλεχθεί σχετικά με τους χρήστες του Δικτύου και πολλές φορές δεν είναι ξεκάθαρο ποιος ή με ποιο τρόπο θα χρησιμοποιήσει αυτές τις πληροφορίες. Συγκεκριμένα, δύο από τις σημαντικότερες τεχνολογίες που σχετίζονται με το θέμα είναι: α) τα cookies και β) το Web tracking. Μέσω των Internet passports, διασφαλίζεται το προσωπικό απόρρητο του χρήστη, ενώ ταυτόχρονα επιτρέπεται στα Web sites να συλλέγουν πληροφορίες που χρειάζονται για να προσφέρουν εξειδικευμένες υπηρεσίες στους επισκέπτες τους. Η πιο κοινή χρήση των δεδομένων αυτών είναι η ‘διευκόλυνση’ της εισόδου των χρηστών σε Web sites που ζητούν όνομα χρήστη και password.

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

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

Άλλες μέθοδοι στηρίζονται στη χρήση ορισμένων προγραμμάτων λογισμικού, ονόματι sniffers, τα οποία εξετάζουν κάθε πακέτο που εισέρχεται ή εξέρχεται από ένα Web site. Για τη διαφύλαξη του ιδιωτικού απορρήτου έχουν αναπτυχθεί αρκετές τεχνολογίες και πρότυπα. Σε αυτά περιλαμβάνονται τα Platform for Privacy Preferences (P3P), Internet Content and Exchange standard (ICE) και Open Profiling Standard (OPS).

Οι τεχνολογίες αυτές ονομάζονται γενικά Internet passports. Τα Internet passports επιτρέπουν στους χρήστες να ελέγχουν ποιες προσωπικές πληροφορίες θα γίνουν διαθέσιμες στα Web sites, καθώς και τον τρόπο με τον οποίον αυτά θα τις χρησιμοποιήσουν. Επιτρέπουν, επίσης , στους χρήστες να ελέγχουν το είδος των πληροφοριών που θα συλλέξει το site κατά τη διάρκεια της πλοήγησής τους και το πώς θα τις χρησιμοποιήσει.

Με βάση αυτά ως δεδομένα διαπιστώνουμε ότι τελικά ακόμη και η ασφάλεια σε έναν χώρο όπως αυτός του Διαδικτύου, μπορεί να υπάρξει. Το Διαδίκτυο ξεκίνησε ως το απόλυτο εκφραστικό μέσο της ελευθερίας της επικοινωνίας των ανθρώπων. Σύντομα όμως πολλοί προσπάθησαν να εκμεταλευθούν αυτή την ελευθερία εις βάρος άλλων. Πλέον η τεχνολογία έχει φθάσει στο σημείο να μπορεί να μας εξασφαλίζει ότι οι συνδιαλλαγές μας στο Διαδίκτυο είναι ασφαλείς. Μπορούμε πλέον να αγοράζουμε οτιδήποτε από το χώρο αυτό με την ίδια ασφάλεια που θα ψωνίζαμε από το κατάστημα της γειτονιάς μας.

6 Στρατηγικές επένδυσης και απόδοσης για e-commerce

Το ηλεκτρονικό εμπόριο ως βασικό συστατικό της Νέας Οικονομίας είναι για όλες τις χώρες, τις αγορές και τις εθνικές οικονομίες μία εξαιρετικά σημαντική προοπτική. Ειδικά για τη χώρα μας η ανάπτυξή του οδηγεί σε περιορισμό του ρόλου της γεωγραφικής θέσης και της απόστασης. Έτσι, μέσω του ηλεκτρονικού εμπορίου και των σχετικών εφαρμογών της πληροφορικής συνδέονται οι ελληνικές επιχειρήσεις μεταξύ τους (business to business), με τις δημόσιες οικονομικές υπηρεσίες (business to public sector) και βέβαια με τους καταναλωτές του παγκόσμιου χωριού και όχι μόνο με τους τοπικούς (business to consumer). Το τμήμα ηλεκτρονικού εμπορίου μιας επιχείρησης ασχολείται όχι μόνο με το τεχνικό μέρος, αλλά και με το μάρκετινγκ (push technology, relationship marketing), αποφασίζει ποιες κινήσεις προσελκύουν περισσότερους αγοραστές, τι είδους προσφορές θα υπάρχουν, πότε θα γίνονται εκπτώσεις, τι προβλήματα αντιμετωπίζει ο καταναλωτής και πως αντιμετωπίζονται. Σε μία χώρα σαν την Ελλάδα που κυριαρχεί το μικρό και μεσαίο μέγεθος επιχείρησης, το ηλεκτρονικό εμπόριο συγκροτεί μία νέα ευκαιρία και μία δυνατότητα για άνοιγμα της αγοράς που οδηγεί με αξιώσεις τις εγχώριες επιχειρήσεις στα δεδομένα της νέας οικονομίας. Η έλλειψη ειδικευμένων στελεχών με την παράλληλη αίσθηση ανασφάλειας και αβεβαιότητας απέναντι στο τεχνολογικά και οικονομικά καινούριο βαθαίνει τη απόσταση που υπάρχει ανάμεσα στον επιχειρηματία που διστάζει ή φοβάται και σ' αυτόν που αντιλαμβάνεται τις εξελίξεις και προσαρμόζεται στην εποχή του.

6.1 Παγκοσμιοποίηση και Στρατηγικές Ανταγωνιστικότητας των Ελληνικών Επιχειρήσεων

Οποιαδήποτε θεώρηση στρατηγικών σχετικών με το ηλεκτρονικό εμπόριο δεν μπορεί να αφήνει αμέτοχη την έννοια της παγκοσμιοποίησης. Η έννοια αυτή αποδεικνύεται από τις σημαντικότερες στο συγκεκριμένο τομέα και θα συζητηθεί στη συνέχεια μέσα από το πρίσμα των στρατηγικών που πρέπει να εφαρμοστούν.

Πόσο έτοιμες είναι οι ελληνικές επιχειρήσεις για το μεγάλο άλμα προς ένα παγκόσμιο "Τόπο Δράσης"; Τι στρατηγικές πρέπει να ακολουθήσουν; Καθώς η παγκοσμιοποίηση προχωρεί, βρισκόμαστε μπροστά σε κρίσιμα διλήμματα και προβληματισμούς. Τι θα γίνει με τις ελληνικές επιχειρήσεις; Θα καταφέρουν να προσαρμοσθούν και να αξιοποιήσουν τις ευκαιρίες που ανοίγονται; Τι στρατηγικές πρέπει να ακολουθήσουν; Σήμερα η παγκοσμιοποίηση, περισσότερο

απ' ότι στο παρελθόν, κινείται από μικροοικονομικές δυνάμεις. Η προσοχή μας πρέπει να στραφεί στο επίπεδο της επιχείρησης. Στις αχανείς αγορές που αρχίζουν να διαμορφώνονται, το παιχνίδι θα κριθεί στη δυναμική και το ανταγωνιστικό πλεονέκτημα των επιχειρηματικών μας μονάδων και σχημάτων. Εκεί θα κριθεί πόσο βιώσιμη θα είναι η οικονομική ανάπτυξη.

Στη συνέχεια γίνεται μια συνοπτική αναφορά στην παγκοσμιοποίηση, στις δυνάμεις που την ωθούν, και στις επιπτώσεις της στις επιχειρήσεις. Στη συνέχεια παρουσιάζεται μία γενική εκτίμηση των προοπτικών των ελληνικών επιχειρήσεων και των κυρίων παραγόντων που δρουν ανασταλτικά στην ανταγωνιστικότητά τους στα πλαίσια των παγκοσμιοποιημένων αγορών. Τέλος, προτείνονται ορισμένες κατευθύνσεις στρατηγικής για τις ελληνικές επιχειρήσεις, οι οποίες θα μπορούσαν να

θεωρηθούν στο πλαίσιο της κάθε επιχείρησης. Το τμήμα αυτό της εργασίας στηρίζεται σε στοιχεία από μελέτες του ΟΟΣΑ, σε διεθνείς πηγές και σε έρευνες που έχουν γίνει στο ελληνικό περιβάλλον. Οι εκτιμήσεις και τα συμπεράσματα είναι υποκειμενικά και εκφράζουν σκέψεις και απόψεις οι οποίες θα πρέπει να τύχουν παραπέρα επεξεργασίας.

6.1.1 Παγκοσμιοποίηση και Επιχειρήσεις

Η παγκοσμιοποίηση είναι μία σύνθετη έννοια η οποία αναφέρεται στην ανάπτυξη οικονομικής δραστηριότητας σε πολυεθνική κλίμακα, που διατέμνει τα εθνικά σύνορα. Εκφράζεται με τη διακρατική μεταφορά προϊόντων και υπηρεσιών, κεφαλαίων, εργαζομένων, τεχνολογίας, γνώσης, και άϋλων πόρων σε ένα παγκόσμιο ορίζοντα. Αναπτύσσεται συνεχώς με νέες μορφές και συνδυασμούς επενδύσεων, εμπορίου και συνεργασίας μεταξύ επιχειρήσεων, που αλλάζουν τα μέχρι τώρα πρότυπα επιχειρηματικής δραστηριότητας. Γενικά η παγκοσμιοποίηση δεν είναι νέο φαινόμενο. Τα τελευταία 10 χρόνια έχουμε δει τρία κύματα παγκοσμιοποίησης:

1. Το πρώτο κύμα έλαβε χώρα πριν από τον Πρώτο Παγκόσμιο πόλεμο για μία περίοδο περίπου 50 χρόνων. Περιελάμβανε την ανάπτυξη εμπορίου, την αύξηση των ροών κεφαλαίου μεταξύ κρατών, και σημαντική μετακίνηση ατόμων.
2. Το δεύτερο κύμα αναπτύχθηκε κατά τη διάρκεια των δεκαετιών 1950 και 1960, με παραπέρα ανάπτυξη του εμπορίου, μείωση δασμών μεταξύ αναπτυγμένων χωρών (στο πλαίσιο συμφωνίας GATT), και σημαντική ανάπτυξη πολυεθνικών επιχειρήσεων.

3. Το τελευταίο κύμα το οποίο ζούμε τώρα, το τρίτο στον αιώνα μας, έχει αρχίσει από τη δεκαετία του 1980 και συνεχίζεται.

Το σημερινό όμως κύμα παγκοσμιοποίησης διαφέρει σημαντικά από τα προηγούμενα. Η κρίσιμη διαφορά είναι ότι αναπτύσσεται πλέον σε μικρο-επίπεδα, οδηγούμενο και διαμορφούμενο από τη διάδοση ευέλικτων μορφών οργάνωσης και συνεργασίας μεταξύ επιχειρήσεων.

Τα παραδοσιακά πρότυπα της ιεραρχικής οργάνωσης επιχειρηματικών και άλλων κοινωνικών δραστηριοτήτων αλλάζουν, καθώς υιοθετούνται νέα ευέλικτα σχήματα συνεργασίας και δικτύωσης μεταξύ ανεξάρτητων μονάδων. Τα τεϋλορικά πρότυπα μηχανιστικής οργάνωσης έχουν πλέον ξεπερασθεί και μάλιστα τα ίδια αποτελούν πλέον μία κύρια αιτία δομικών προβλημάτων στην προσαρμογή των επιχειρήσεων (oecd Development Centre, 1996). Στο άμεσο μέλλον αναμένεται μια ένταση στο σημερινό κύμα. Οι κυριότερες δυνάμεις που ωθούν αυτήν τη διαδικασία είναι οι εξής:

1. Οι πολιτικές μείωσης των εθνικών προστατευτικών εμποδίων στις επενδύσεις και το εμπόριο. Πέρα από τις πολιτικές διαμόρφωσης ενιαίας αγοράς στην Ευρωπαϊκή Ένωση, η ανάπτυξη του πολυμερούς συστήματος εμπορίου και επενδύσεων σε ευρύτερο επίπεδο θα έχει σημαντικές επιπτώσεις. Ιδιαίτερα σημαντική είναι η πολυμερής συμφωνία επενδύσεων (Multilateral Agreement on Investment), που προωθεί ο ΟΟΣΑ και αναμένεται να συμφωνηθεί σύντομα. Καθώς επίσης η εφαρμογή και σταδιακή επέκταση των πολιτικών του Διεθνούς Οργανισμού Εμπορίου. Με την ένταξη νέων χωρών στο πολυμερές σύστημα θα ενταθεί η παγκοσμιοποίηση.
2. Η προώθηση εγχώριων πολιτικών για το άνοιγμα των αγορών και αναμόρφωση των ρυθμίσεων στις αγορές προϊόντων, εργασίας και κεφαλαίου. Οι πολιτικές αυτές προωθούνται τόσο για εσωτερικούς λόγους καλής διαχείρισης και αποτελεσματικότητας όσο και για αύξηση της διεθνούς ανταγωνιστικότητας. Σχετικά είναι τα προγράμματα αναμόρφωσης ρυθμίσεων (regulatory reform) που προωθεί ο ΟΟΣΑ, το άνοιγμα των αγορών στον ανταγωνισμό στο πλαίσιο της Ευρωπαϊκής Ένωσης, καθώς και πολιτικές διεθνούς συνεργασίας για αποφυγή ανταγωνισμού μέσω φορολογίας, μειωμένων περιβαλλοντικών προτύπων (eco dumping), διαφορών στις εργασιακές πρακτικές, και μείωσης της διαφθοράς και των εθνικών διακρίσεων στις διεθνείς συναλλαγές.
3. Η αυξανόμενη δραστηριότητα συνεργασίας μεταξύ επιχειρήσεων σε διαφορετικά κράτη, η οποία εκφράζεται με διάφορες μορφές χαλαρών ή έντονων δεσμών και δικτύωσης. Το πλέγμα των

μεγάλων πολυεθνικών επιχειρήσεων, οι οποίες συνεχίζουν να αναπτύσσουν δίκτυα συνεργασιών και υπεργολαβικές σχέσεις, ακολουθείται τώρα από πολλές εθνικές επιχειρήσεις. Δικτυώσεις και συμμαχίες αλλάζουν πλέον τα κλασικά σύνορα των επιχειρήσεων και διαμορφώνουν ένα ενδογενές ρεύμα που οδηγεί σε παραπέρα ενίσχυση της παγκοσμιοποίησης.

4. Οι τεχνολογικές αλλαγές και διακίνηση γνώσης γενικότερα. Ιδιαίτερα σημαντική είναι η επίδραση των νέων τεχνολογιών επικοινωνίας και πληροφορικής στην παγκοσμιοποίηση, καθώς αναπτύσσονται δίκτυα που τέμνουν σύνορα, ηλεκτρονικό εμπόριο και επέκταση των συναλλαγών των επιχειρήσεων μέσω διεθνών δικτύων. Παράλληλα, η ανάπτυξη της γνώσης και καινοτομίας κινείται πιο εύκολα διασυνοριακά. Η κοινωνία που βασίζεται στη γνώση δεν έχει σύνορα. Το φαινόμενο της παγκοσμιοποίησης έχει λάβει τέτοια "δυναμική" που θεωρείται πλέον μη αναστρέψιμο.

Οι επιπτώσεις της παγκοσμιοποίησης στις επιχειρήσεις αναμένονται να είναι σημαντικές. Θα αυξηθούν οι ανταγωνιστικές πιέσεις καθώς όλο και περισσότερες επιχειρήσεις αναπτύσσουν δραστηριότητες σε άλλες χώρες[44]. Η παγκοσμιοποίηση έχει δύο πτυχές, μία "εξωστρεφή" και μία "ενδοστρεφή". Η πρώτη αναφέρεται στην επέκταση της επιχειρηματικής δραστηριότητας παγκοσμίως για αξιοποίηση ευκαιριών. Η δεύτερη στην είσοδο ξένων επιχειρήσεων στην εγχώρια αγορά και τους κινδύνους που συνεπάγεται για εγχώρια προσανατολισμένες επιχειρήσεις. Όλο και μεγαλύτερα τμήματα των αγορών θα καταλαμβάνονται από παγκοσμιοποιημένες επιχειρήσεις. Σε λίγα χρόνια, λίγες επιχειρήσεις θα μπορούν να παραμείνουν απρόσβλητες από το διεθνή ανταγωνισμό. Ακόμη και για τις μικρές ή μικρομεσαίες επιχειρήσεις, εθνικές ή όχι, θα περιορίσει το ζωτικό χώρο τους. Ιδιαίτερα έντονες θα είναι οι πιέσεις σε επιχειρήσεις μικρού, με διεθνή κριτήρια, μεγέθους όπως είναι συντριπτική πλειοψηφία των Ελληνικών Επιχειρήσεων.

Ενδιαφέροντα είναι τα αποτελέσματα μιας σχετικής μελέτης του ΟΟΣΑ για τις επιπτώσεις της παγκοσμιοποίησης στις Μικρο-Μεσαίες επιχειρήσεις (ΟΟΣΑ, 1997). Στη μελέτη αυτή εκτιμάται ότι το ποσοστό επιχειρήσεων που είναι λιγότερο εκτεθειμένες στην επίδραση από την παγκοσμιοποίηση είναι σήμερα λιγότερο από 40%. Το ποσοστό των επιχειρήσεων αυτών προβλέπεται να μειωθεί οτο 20% ή λιγότερο, μετά το 2006. Ένα μεγάλο ποσοστό επιχειρήσεων βρίσκεται σε κίνδυνο και θα αντιμετωπίσει προβλήματα προσαρμογής.

[44] OECD DEVELOPMENT CENTRE, The policy Challenges of Globalisation and Regionalisation (by C.Oman), 1996

Μόνο το 1/3 των επιχειρήσεων εκτιμάται ότι είναι ικανές να γίνουν διεθνώς ανταγωνιστικές και να αξιοποιήσουν την τάση της αυξανόμενης παγκοσμιοποίησης. Στη διεθνή συζήτηση έχει δοθεί έμφαση στην ανταγωνιστικότητα χωρών και στους κινδύνους από π.χ. τις αναδυόμενες αγορές των μεγάλων πέντε γρήγορα αναπτυσσόμενων χωρών (Κίνα, Ινδία, Ινδονησία, Βραζιλία, Ρωσία).

Καθώς όμως οι ίδιες οι επιχειρήσεις προσαρμόζονται στα δεδομένα των χωρών και επιχειρούν να αξιοποιήσουν τις ευκαιρίες σε παγκόσμιο επίπεδο, η προσοχή μας πρέπει να στραφεί πιο πολύ στο επίπεδο μιας επιχείρησης. Εξ' άλλου τα δεδομένα από το μικροεπίπεδο δείχνουν ότι οι διαφορές μεταξύ επιχειρήσεων μέσα οτην ίδια χώρα ή γεωγραφική περιοχή ή την ίδια αγορά είναι μεγαλύτερες απ' ό,τι οι διαφορές μεταξύ χωρών. Στο ίδιο περιβάλλον και με παρόμοια δραστηριότητα, άλλες επιχειρήσεις πετυχαίνουν και άλλες σβήνουν. Αυτό αναδεικύει τη σπουδαιότητα ενδογενών παραγόντων όπως η φύση της στρατηγικής, τα ανταγωνιστικά πλεονεκτήματα και οι ικανότητες της κάθε συγκεκριμένης επιχείρησης.

Οι δυνατότητες κρατικής στήριξης των επιχειρήσεων θα μειώνονται με την εξέλιξη της διαδικασίας παγκοσμιοποίησης. Αν οι προβλέψεις επαληθευτούν και επιβιώσουν κυρίως οι διεθνοποιημένες επιχειρήσεις, μικρές ή μεγάλες, τί πολιτικές θα μπορούσε να εφαρμόσει η κυβέρνηση; Τα οφέλη που θα παράγουν αυτές οι επιχειρήσεις είναι όλο και πιο δύσκολο να περιορισθούν εντός εθνικών ορίων. Θα κατανέμονται και σε άλλλες χώρες. Θα καταστεί πιο δύοκολο να ορισθεί ποια είναι "εθνική" επιχείρηση; Ποιό είναι το «εθνικό συμφέρον»; Η παγκοσμιοποίηση κάνει ασαφή τη διαφορά μεταξύ εγχωρίων και διεθνών πολιτικών. Αδυνατίζει τις παραδοσιακές κυβερνητικές πολιτικές στήριξης επιχειρήσεων, και θα απαιτήσει τη διαμόρφωση νέας βιομηχανικής πολιτικής πολυμερούς φύσης. Αλλά ειναι πολύ νωρίς να συζητήσουμε για τέτοιες πολιτικές σε διακρατικό επίπεδο. Όμως στο μεταξύ στο διακρατικό επίπεδο βλέπουμε πλέον την εφαρμογή τέτοιων πολιτικών μέσω στρατηγικών κοινοπραξιών και συμμαχιών σε παγκόσμιο πλαίσιο.

6.1.2 Ανασταλτικοί Παράγοντες και Προοπτικές Ελληνικών Επιχειρήσεων

Αν και υπάρχουν σημαντικές διαφορές μεταξύ επιχειρήσεων ως προς τις ανταγωνιστικές τους δυνατότητες, τις πρακτικές και το ιδιαίτερο τομεακό περιβάλλον στο οποίο

λειτουργούν, εν τούτοις υπάρχουν ορισμένα γενικά χαρακτηριστικά ή ανασταλτικοί παράγοντες που χαρακτηρίζουν την τυπική Ελληνική επιχείρηση. Τα κυριότερα χαρακτηριστικά είναι τα εξής[45]:

- το μικρό μέγεθος για το εξελισσόμενο, παγκοσμιοποιημένο περιβάλλον
- έντονος οικογενειακός έλεγχος σε πολλές επιχειρήσεις
- μικρή χρήση σύγχρονων τεχνικών μάνατζμεντ
- υστέρηση σε τεχνολογία και καινοτομία
- υστέρηση στο σχεδιασμό προϊόντων και το μάρκετινγκ
- ανταγωνιστική στρατηγική με εγχώρια και όχι διεθνή προοπτική.

'Οσον αφορά, στο ευρύτερο επιχειρησιακό περιβάλλον σημαντικές ελλείψεις υπάρχουν στις υποδοχέςκαι τη χρηματοδότηση, ενώ θεσμικά και γραφειοκρατικά εμπόδια εμποδίζουν την αποτελεσματική λειτουργία των επιχειρήσεων στην Ελλάδα. Βέβαια, αυτούς τους παράγοντες πρέπει να τους δούμε στο πλαίσιο της παγκοσμιοποίησης λαμβάνοντας υπόψη τη δυνατότητα των επιχειρήσεων να αξιοποιήσουν τυχόν ευνοϊκούς παράγοντες στο επιχειρησιακό περιβάλλον άλλων χωρών. Η εξάρτηση από το κράτος θα γίνεται όλο και λιγότερο σημαντική στο πλαίσιο αυτό.

6.1.2.1 Μέγεθος επιχειρήσεων

Το μικρό γενικά μέγεθος των ελληνικών επιχειρήσεων έχει επιπτώσεις στις δυνατότητές τους για ανάπτυξη. Για παράδειγμα, δεν μπορεί να στηρίξει μεγάλα προγράμματα έρευνας και ανάπτυξης, αξιοποίησης ευκαιριών και συνεργασιών σε ευρεία κλίμακα. Οι περισσότερες ελληνικές επιχειρήσεις λειτουργούν τοπικά και έχουν περιορισμένες δυνατότητες αύξησης του μεγέθους τους μέσω οργανικής ανάπτυξης ή εξαγωγών και συγχωνεύσεων. Κάτω από τις συνθήκες αυτές θα έχουν δυσκολίες να ανταγωνιστούν σε ίση βάση με πραγματικά παγκοσμιοποιημένες επιχειρήσεις, εκτός αν βρουν και εφαρμόσουν ειδικές στρατηγικές. Οι μεγάλοι ανταγωνιστές τους δαπανούν υψηλά ποσά για την ανάπτυξη νέων προϊόντων, τεχνολογία και έρευνα αγοράς. Ταυτόχρονα λόγω της διασποράς τους έχουν πρόσβαση σε πολλές αγορές και ανευρίσκουν καινοτομικές ιδέες μέσω της επαφής τους με πελάτες διαφορετικών απαιτήσεων και πολιτισμικών χαρακτηριστικών.

[45] Μακρυδάκης Σ., Παπαγιαννάκης Λ. Καλογήρου Γ., το Ελληνικό Μάνατζμεντ: Εξελίξεις, Τάσεις, Προοπτικές, ΕΑΣΕ, 1996

Υπάρχει όμως και η θετική άποψη ως προς τις προοπτικές των μικρών επιχειρήσεων. Με κατάλληλες στρατηγικές μπορούν να παγκοσμιοποιηθούν και να εισέλθουν στο ποσοστό αυτών που θα γίνουν διεθνώς ανταγωνιστικές. Και ήδη ορισμένες ελληνικές επιχειρήσεις έχουν αρχίσει πετυχημένα να αποκτούν αυτή τη μορφή. Σχετική είναι η έρευνα του H. Simon για τους «κρυφούς πρωταθλητές» της Γερμανίας: σχετικά μικρότερες επιχειρήσεις που έχουν γίνει πραγματικά παγκόσμιες, και αντιμετωπίζουν τις μεγάλες πολυεθνικές επιχειρήσεις πετυχημένα (Simon, 1996). Οι επιχειρήσεις αυτές, συγκεντρώνονται σε ειδικές αγορές, στενά ορισμένες, αλλά επεκτείνονται γεωγραφικά σε παγκόσμια κλίμακα. Οι πολυεθνικές αποφεύγουν να τις ανταγωνίζονται, είτε διότι η αγορά στην οποία επικεντρώνονται είναι πολύ μικρή γι' αυτές, διότι γνωρίζουν ότι θα χάσουν σε έναν ανοιχτό πόλεμο.

6.1.2.2 Οικογενειακός έλεγχος

Ιδιαίτερα σημαντικός είναι ο τρόπος άσκησης εταιρικού ελέγχου από τους ιδιοκτήτες των επιχειρήσεων. Η πλειοψηφία των Ελληνικών επιχειρήσεων είναι «οικογενειακού» τύπου. Το 57% των επιχειρήσεων ελέγχεται από τον ιδιοκτήτη και την οικογένειά του. Παρά το ότι πολλοί απόγονοι των ιδρυτών-ιδιοκτητών έχουν κάνει καλές σπουδές (MBA, κ.α.) και έχουν αποκτήσει εμπειρία, εν τούτοις ο οικογενειακός τύπος της επιχείρησης συχνά έχει αρνητικές επιπτώσεις. 'Οχι μόνο δεν επιτρέπει την αξιοποίηση επαγγελματιών μανατζερς, αλλά επηρεάζει τις επιλογές και τις επιδόσεις της επιχείρησης. Για παράδειγμα, ιδιοκτήτης-γενικός διευθυντής μπορεί να τοποθετήσει σε υψηλές θέσεις άτομα με τα οποία ξεκίνησε την επιχείρηση, αν και οι ικανότητες των ατόμων αυτών δεν είναι κατάλληλες ή έχουν απαρχαιωθεί. Καθώς στερούνται σύγχρονων συστημάτων ελέγχου, δίνει προτεραιότητα στην τοποθέτηση "εμπίστων" παρά επαγγελματιών μάνατζερς. Συνήθως, ο ιδιοκτήτης-γενικός διευθυντής δρα συγκεντρωτικά και πρακτικά εμπλέκεται σ. όλες τις αποφάσεις. Αν και νομίζει ότι έχει εκχωρίσει αρμοδιότητες και ότι επιθυμεί να ενισχύσει τις δυνατότητες λήψης αποφάσεων από τους συνεργάτες του, στην πράξη είναι δύσκολο να δεχθεί τις αποφάσεις τους. Μόνο 32% από τους ιδιοκτήτες-γενικούς διευθυντές επιθυμούν τέτοια εκχώρηση δικαιοδοσιών, ενώ το ποσοστό αυτό είναι 51% στις επιχειρήσεις με επαγγελματίες γενικούς διευθυντές, και ξεπερνά το 60% μεταξύ επιχειρήσεων της Δυτικής Ευρώπης, ΗΠΑ και Ιαπωνίας.

Ενδεικτική των επιπτώσεων είναι η χαμηλότερη παραγωγικότητα στις οικογενειακές επιχειρήσεις, όπως αυτή εκφράζεται με το δείκτη «πωλήσεις ανά υπάλληλο». Οι επιχειρήσεις με επαγγελματίες μάνατζερς υπερέχουν και φθάνουν στο ήμισυ περίπου της παραγωγικότητας των

θυγατρικών πολυεθνικών στην Ελλάδα. Οι διαφορές αυτές γίνονται πιο έντονες τα τελευταία χρόνια.

6.1.2.3 Πρότυπα διοίκησης

Το ελληνικό μάνατζμεντ γενικά θα μπορούσε να θεωρηθεί ως μάνατζμεντ «δυτικού τύπου» που όμως δεν έχει ακόμα φθάσει ένα υψηλό επίπεδο εκσυγχρονισμού και εφαρμογής επιστημονικών μεθόδων και τεχνικών (Μπουραντάς και Παπαδάκης, 1997). Είναι ενδιαφέρον να επισημανθεί ότι ο Έλληνας μάνατζερ, αν και γνωρίζει τα σύγχρονα εργαλεία και τις τελευταίες τεχνικές μάνατζμεντ, υστερεί στην εφαρμογή τους.

Ιδιαίτερα σημαντική είναι η υστέρηση του οικογενειακού τύπου επιχειρήσεων. Σε σύγκριση με επιχειρήσεις στην Δυτική Ευρώπη, ΗΠΑ και Ιαπωνία, οι ελληνικές επιχειρήσεις υστερούν σημαντικά στην εφαρμογή τεχνικών και πρακτικών όπως: στρατηγικές συμμαχίες, ανταγωνιστική σύγκριση, ολική ποιότητα, μέτρηση ικανοποίησης πελατών, και επανασχεδιασμός διαδικασιών. Οι τεχνικές αυτές είναι απαραίτητες για το μετασχηματισμό τους σε πραγματικά παγκοσμιοποιημένες επιχειρήσεις. ’Ομως θα πρέπει να τονισθούν οι μεγάλες διαφορές που υπάρχουν στην άσκηση διοίκησης από επιχείρηση σε επιχείρηση. Σε πολλούς χώρους επικρατεί επαγγελματικό μάνατζμεντ που δεν έχει τίποτε να ζηλέψει από αυτό άλλων αναπτυγμένων χωρών, π.χ. της Αγγλίας, Γαλλίας ή των Ηνωμένων Πολιτειών. Σε άλλους επικρατούν ακόμη παραδοσιακά πρότυπα χωρίς σύγχρονη προσέγγιση, που συχνά επιβαρύνεται με ανασταλτικές μορφές οικογενειακού ελέγχου. ’Ομως, δεν πρέπει να παραγνωρίσουμε και τα θετικά σημεία των Ελλήνων μάνατζερς. Μια πρόσφατη έρευνα έχει δείξει ότι οι ’Ελληνες μάνατζερς γενικά δίνουν μεγαλύτερη σημασία στη δημιουργικότητα και αυτό αποτελεί πλεονέκτημα στη διαδικασία παγκοσμιοποίησης (βλέπε Πίνακα 3) .

’Ομως φαίνεται να είναι λιγότερο αναλυτικό, κυρίως στις οικογενειακές επιχειρήσεις. Επίσης, υπερτερούν στη συνεργασιμότητα, πράγμα που επίσης μπορεί να αποτελέσει δυνητικά αξιοποιήσιμο παράγοντα, αλλά υστερεί στην ανάληψη κινδύνου, γεγονός που μπορεί να οφείλεται σε εξωγενείς περιορισμούς, (χρηματοδότηση, ασφάλεια κινδύνων). Είναι σημαντικό πάντως να τονισθεί ότι οι προσδοκίες των Ελλήνων μάνατζερς σχετικά με το στιλ διοίκησης που επιθυμούν να εφαρμόσουν στο μέλλον, μετά από 10 χρόνια, συγκλίνουν πολύ με αυτές των άλλων χωρών. Αυτό δείχνει ότι θα υπάρξει κάποια τάση σύγκλισης με δυτικά πρότυπα στο μέλλον (Μακρυδάκης κ.α.,

1996, Bouraητas & Papadakis, 1997). Οι διεθνείς συνεργασίες και δικτυώσεις θα επιταχύνουν τη διαδικασία σύγκλισης.

6.1.2.4 Τεχνολογία και καινοτομία

Οι δυνατότητες της χώρας μας σε προϊόντα υψηλής τεχνολογίας είναι περιορισμένες. Αυτό φαίνεται και από τη σχετικά περιορισμένη συμμετοχή κλάδων υψηλής ή έστω ενδιάμεσης τεχνολογίας στη συνολική παραγωγή. 'Οπως αναφέρθηκε παραπάνω, λόγω του μικρού τους μεγέθους οι ελληνικές επιχειρήσεις δεν μπορούν να δαπανήσουν σημαντικά ποσά σε Έρευνα και Τεχνολογία ώστε να βελτιώσουν τα προϊόντα ή τις υπηρεσίες και να παράγουν νέα τεχνολογικά προηγμένα. Τα ποσά που μπορούν να συγκεντρώσουν είναι μικρά συγκρινόμενα με τα αντίστοιχα μεγάλων πολυεθνικών. 'Ενα παράδειγμα που δείχνει πόσο συγκεντρωμένη είναι η έρευνα σε διεθνές επίπεδο αποτελεί η IηteI, η οποία δαπανά για 'Ερευνα και Τεχνολογία πέντε φορές περισσότερο απ' ό, τι η Ελλάδα - δηλαδή όλες οι ελληνικές επιχειρήσεις, η κυβέρνηση, τα πανεπιστήμια και άλλα ερευνητικά ινστιτούτα.

Επιπλέον, υπάρχει και για τη χώρα μας το γνωστό πρόβλημα της Ευρώπης όπου οι τεχνολογικές καινοτομίες δύσκολα καταλήγουν σε εμπορική αξιοποίηση. Και αυτό σε αντίθεση με τις ΗΠΑ όπου η 'Ερευνα και Τεχνολογία πιο εύκολα οδηγείται σε εμπορικά αξιοποιήσιμα προϊόντα ή υπηρεσίες (Green Paper on Innovation, EC, 1995). Σημαντικά όμως ανασταλτικό παράγοντα αποτελεί και ο στενός προσανατολισμός της τεχνολογίας, δηλ. προς την τεχνολογία προϊόντος ή παραγωγής. Η έμφαση στην Ελλάδα είναι προς τεχνολογίες πυρήνα και όχι προς ευρύτερες καινοτομίες στη σύλληψη στρατηγικής σ' όλη την αλυσίδα αξίας και τις ιδιαίτερες απαιτήσεις συγκεκριμένων τμημάτων της αγοράς (ζήτησης). Δεδομένων και των περιορισμών μεγέθους, η έμφαση των Ελληνικών επιχειρήσεων πρέπει να δοθεί στην ικανότητα της επιχείρησης για απορρόφηση τεχνολογίας και εφαρμογή της σε καινοτομικούς τρόπους μέσω της επαφής με τους πελάτες και την αγορά, και σε διαφοροποιήσεις στην όλη παροχή υπηρεσιών. Δηλαδή, σε καινοτομίες που ωθούνται από την αγορά και δεν απαιτούν πρωτογενή 'Ερευνα και Ανάπτυξη. Με μια τέτοια προοπτική πρέπει να δούμε και τις διεθνείς συνεργασίες με άλλες μεγάλες επιχειρήσεις, καθώς επίσης το ρόλο των Ευρωπαϊκών Προγραμμάτων και της όλης δραστηριότητας που τροφοδοτείται απ' αυτά.

6.1.2.5 Σχεδιασμός προϊόντων και μάρκετινγκ

Χαρακτηριστική είναι η υστέρηση πολλών ελληνικών προϊόντων σε θέματα ποιότητας, σχεδιασμού, συσκευασίας και μάρκετινγκ. Ιδιαίτερα έντονη είναι η έλλειψη επώνυμων προϊόντων, καθώς και η σχετική αδυναμία μας να αξιοποιήσουμε διεθνώς ορισμένα παραδοσιακά χαρακτηριστικά των προϊόντων μας που τα κάνουν μοναδικά και θα μπορούσαν να στηρίξουν μια ανταγωνιστική στρατηγική σε παγκόσμιο επίπεδο . Το κενό αυτό καλύπτεται από απομιμήσεις όπως π.χ. στη Γαλλία το «Γιαούρτι ελληνικού τύπου» που προωθούν γαλλικές ή πολυεθνικές επιχειρήσεις, το ελληνικό μάρμαρο ή ελαιόλαδο που προωθείται με ιταλική προστιθέμενη αξία. Η εμπειρική ερευνα έδειξε ότι οι ελληνικές επιχειρήσεις αναγνωρίζουν την ποιότητα ως κύριο ανταγωνιστικό παράγοντα και ακολουθούν οι χαμηλότερες τιμές. ’Ομως ο ανταγωνισμός φέρνει το μέσο επίπεδο ποιότητας όλο και πιο ψηλά και για να διαφοροποιηθεί η επιχείρηση πρέπει διαρκώς να ξεπερνά τις προσδοκίες των πελατών σε χαρακτηριστικά σχεδίασης, εξατομίκευσης, υποστήριξης του πελάτη και καινοτομικών υπηρεσιών. Αυτή θα είναι η νέα μορφή ανταγωνισμού.

6.1.2.6 Ανταγωνιστική στρατηγική

Ο παραδοσιακός προσανατολισμός πολλών ελληνικών επιχειρήσεων σε τυποποιημένα προϊόντα ή υπηρεσίες, τα οποία συνδυάζουν συνήθως ένα μεσαίο επίπεδο ποιότητας και τιμών, δε θα μπορεί πλέον να αποτελεί πετυχημένη συνταγή. Οι αγορές των τυποποιημένων προϊόντων θα αποτελέσουν όλο και πιο πολύ το προνόμιο των μεγάλων παγκοσμιοποιημένων επιχειρήσεων, οι οποίες έχουν χαμηλό κόστος, αξιοποιούν τις δυνατότητες αναδιάταξης της παραγωγής σε χώρες χαμηλού κόστους και επενδύουν σημαντικά σε ’Ερευνα και Ανάπτυξη για βελτίωση των προϊόντων. Οι σύγχρονες τεχνολογίες προσφέρουν επίσης στις μεγάλες αυτές επιχειρήσεις τη δυνατότητα μαζικής παραγωγής προϊόντων προσαρμοσμένων στις ανάγκες ειδικών πελατών (mass customisation), περιορίζοντας έτσι την αγορά αυτών που είχαν στρατηγική εξειδίκευση στην ικανοποίησης ειδικών αναγκών (niche markets).

Αν επομένως εξαιρεθούν τυποποιημένα προϊόντα και υπηρεσίες (επώνυμα και μη-επώνυμα), καθώς και προϊόντα υψηλής τεχνολογίας, απομένει σε χώρες όπως η Ελλάδα ζωτικός χώρος για μη-τυποποιημένα προιόντα ή προϊόντα ή υπηρεσίες σε κλάδους όχι υψηλής τεχνολογίας. Οι στρατηγικές επομένως, πρέπει να κατευθυνθούν σε διαφοροποιήσεις και ειδικές αγορές όπου μπορεί να στηριχθεί ανταγωνιστικό πλεονέκτημα (niche markets). Πάντως, αφού διαμορφωθεί και εξειδικευθεί μία τέτοια στρατηγική κατεύθυνση, πρέπει να αξιοποιηθεί σε παγκόσμια κλίμακα,

ώστε να προκύπτουν οικονομίες έκτασης και να καταστεί δυνατή η συνεχής ανανέωση και διατήρηση ανταγωνιστικού πλεονεκτήματος. Χρειάζεται επομένως σφαιρικό πλαίσιο σκέψης με προσανατολισμό την παγκόσμια αγορά, έξω από τα νοητικά όρια της εγχώριας αγοράς, και κάποια δειλή επέκταση σε γειτονικές χώρες. Επίσης, θεώρηση του ανταγωνιστικού πλεονεκτήματος στο πλαίσιο αναπτυγμένων αγορών (όπως της Δυτικής Ευρώπης) και όχι στο πλαίσιο λιγότερο αναπτυγμένων αγορών όπως οι βαλκανικές αγορές, υποδομές στήριξης επιχειρήσεων και ρυθμιστικό πλαίσιο.

Το επιχειρηματικό περιβάλλον στην Ελλάδα έχει ορισμένες αδυναμίες σε σύγκριση με άλλες ευρωπαϊκές χώρες. Οι κυριότερες είναι:

• Ελλείψεις υποδομών, κυρίως στο χώρο χρηματοδότησης ΜΜΕ, επιχειρηματικού κεφαλαίου και παροχής εγγυήσεων έναντι κινδύνων στις διεθνείς αγορές.

• Ελλείψεις στις επιχειρηματικές σπουδές και την κατάρτιση. Αυτό φαίνεται και από το ρεύμα σπουδαστών που κάνουν MBA και άλλες σχετικές για τις επιχειρήσεις σπουδές στο εξωτερικό. Ιδιαίτερα στην Ελλάδα λείπουν τα πολλά διεθνούς επιπέδου και προσανατολισμού MBA, τα οποία θα μπορούσαν να δώσουν υψηλά καταρτισμένα στελέχη με διεθνή προσανατολισμό, και με ιδιαίτερη εστίαση στην προώθηση σπουδών προσαρμοσμένων στις ανάγκες των αναδυόμενων οικονομιών.

• Πολλαπλές ρυθμίσεις και γραφειοκρατικά εμπόδια τα οποία δημιουργούν κόστος στην ανάπτυξη της επιχειρηματικής δραστηριότητας και επιβραδύνουν την προσαρμογή των επιχειρήσεων στα νέα δεδομένα. Η χώρα μας θεωρείται από τις πιο έντονα ρυθμισμένες στην Ευρώπη, και χρειάζεται εντατικές πρωτοβουλίες ρυθμιστικού ανασχεδιασμού (Koedijk & Kremers, 1996).

Σύμφωνα με μελέτη του ΟΟΣΑ, δομικοί περιορισμοί κυρίως από την οργάνωση της αγοράς εργασίας περιορίζουν τις επιχειρήσειςκαι ουσιαστικά τις οδηγούν σε περιορισμένης έκτασης προσαρμογές εσωτερικά στην επιχείρηση (OECD, 1996). Παρά τις παραπάνω δυσκολίες, οι διεθνοποιημένες επιχειρήσεις μπορούν να αποκτήσουν προσβάσεις στους πόρους άλλων χωρών και έτσι να ξεπεράσουν πιο εύκολα τα προβλήματα των εγχωρίων περιορισμών.

6.1.3 Κατευθύνσεις Στρατηγικής για το Μέλλον

Στο πλαίσιο των εξελίξεων της διαδικασίας παγκοσμιοποίησης και των παραπάνω χαρακτηριστικών των Ελληνικών επιχειρήσεων θα μπορούσαν να υποστηριχθούν ορισμένες στρατηγικές κατευθύνσεις για το μέλλον[46]. Οι κατευθύνσεις αυτές φαίνονται καταρχήν ελκυστικές, αλλά θα πρέπει να προσαρμοσθούν στις ιδιαιτερότητες της κάθε επιχείρησης.

6.1.3.1 Συγκέντρωση σε ειδικές αγορές (niche markets)

- Επιλογή κάποιου ειδικού τμήματος αγοράς, στενά ορισμένου, και επέκταση σε διεθνή κλίμακα. Αποφυγή άλλων παραπλήσιων δραστηριοτήτων ή διαφοροποίησης σε άλλα προιόντα ή υπηρεσίες.
- Στενότερη επαφή και δεσμοί (με τους πελάτες στις διεθνείς αγορές) ώστε να εμβαθύνεται συνεχώς η γνώση των απαιτήσεών τους και η καινοτομική διαφοροποίησης ως προς μαζικούς τυποποιημένους ανταγωνιστές.
- Αποφυγή μαζικών τυποποιημένων προιόντων.

6.1.3.2 Καινοτομικά, επώνυμα προιόντα και υπηρεσίες

- Εστίαση σε παράγοντες πέρα από την ποιότητα και το κόστος όπως ολοκλήρωση υπηρεσιών, ευελιξία, σχεδίαση, εξατομίκευση, καινοτομικές εφαρμογές.
- Καινοτομίες στην εφαρμογή και προσαρμογή νέων τεχνολογιών στη βάση σχέσεων με τον πελάτη και την αγορά.
- Δημιουργία επώνυμων προιόντων που αυξάνουν την προστιθέμενη αξία.
- Αξιοποίηση των παραδοσιακών ιδιαζόντων χαρακτηριστικών της χώρας και της επιχείρησης για δημιουργία διαφοροποιημένων προϊόντων, κυρίως σε σχέση με πολιτισμικά και κοινωνικά χαρακτηριστικά σε τομείς όπως τα αγροτικά προϊόντα και υπηρεσίες τουρισμού και υγείας.

[46] Simon, H,. Hidden Champions: Lessons from 500 of the Worlds Best unknown Companies, Harvard Business School Press, Boston, 1996

6.1.3.3 Σφαιρικός προσανατολισμός προς παγκοσμιοποίηση

- Σχεδιασμός στρατηγικής σε παγκοσμιοποιημένο πλαίσιο. Επιδίωξη ανταγωνιστικού πλεονεκτήματος και αξιοποίηση αιχμών σε σύγκριση με ομοειδείς διεθνοποιημένες επιχειρήσεις.
- Ανάπτυξη της διεθνούς δραστηριότητας με στρατηγικές που θα περιλαμβάνουν επέκταση σε προηγμένες αγορές ώστε να αποκτηθεί εμπειρία (π.χ. Ευρώπη). Στρατηγική παρουσία σε αναπτυσσόμενες αγορές για απόκτηση μεριδίου αγοράς, με σχεδιασμό για μακροπρόθεσμη αποκομιδή κέρδους, και όχι ευκαιριακά.

6.1.3.4 Συνεργασίες,δικτύωση, στρατηγικές συμμαχίες

- Επιδίωξη συνεργασιών και αξιοποίηση δικτυώσεων με άλλους προηγμένους εταίρους για μάθηση, απόκτηση γνώσεων και απορρόφηση τεχνολογιών, σε τομείς που ενισχύουν τη βασική στρατηγική της επιχείρησης, όπως R&D, μάρκετινγκ, πωλήσεις και άλλες στρατηγικές λειτουργίες.
- Στρατηγικές συμμαχίες, με αυστηρή επιλογή εταίρων που έχουν ανταγωνιστικό πλεονέκτημα συμβατό με τη βασική στρατηγική της επιχείρησης, ώστε να μην αμβλύνεται η σαφήνεια στρατηγικής και να μη χάνεται ο έλεγχός της.
- Περιορισμός συνεργασιών με λοιπούς «μη-στρατηγικούς» εταίρους σε υποστηρικτικές λοιπές υπηρεσίες που δε θίγουν τον ανταγωνιστικό πυρήνα.

6.1.3.5 Μεταστρατηγική σε γεωπολιτικό επίπεδο.

- Αξιοποίηση γεωπολιτικών παραγόντων για ευρύτερη επιχειρηματική ανάπτυξη στις
- αναπτυσσόμενες αγορές (π.χ. Βαλκάνια, Ρωσία). Επιδίωξη δικτυώσεων στις αγορές αυτές σε επιχειρηματικό και μη επίπεδο.
- Συνεργασίες με προηγμένους εταίρους στις αγορές αυτές. Ανταλλαγή δυνατοτήτων πολιτισμικής προσέγγισης, πλεονεκτημάτων γεωγραφικές γειτνίασης και διαθεσιμότητας υποδομών με τεχνολογίες/τεχνογνωσία, παρουσία στην αγορά και μοίρασμα κινδύνου.
- Ανάπτυξη επιχειρηματικότητας και αξιοποίηση ευκαιριών πέραν των υπαρχόντων προϊόντων και επιχειρηματικών μονάδων. Τέλος, όσον αφορά την κυβερνητική πολιτική ενίσχυσης των ελληνικών επιχειρήσεων ώστε να καταστούν ανταγωνιστικές στο

αναδυόμενο παγκοσμιοποιημένο περιβάλλον, υψηλή προτεραιότητα πρέπει να δοθεί σε οριζόντιες πολιτικές όπως:

- Ενίσχυση των υποδομών, κυρίως χρηματοδότησης, επιχειρηματικού κεφαλαίου και παροχής εγγυήσεων έναντι των κινδύνων στις διεθνείς αγορές.
- Δημιουργία υποδομών που θα προωθούν και θα υποστηρίζουν τις προσπάθειες των επιχειρήσεων για διεθνή δικτύωση.
- Ενίσχυση των επιχειρηματικών σπουδών και της κατάρτισης, περιλαμβανόμενης της δημιουργίας ενός διεθνούς MBA ειδικευμένου σε αναδυόμενες οικονομίες.
- Οριζόντιο πρόγραμμα ρυθμιστικού ανασχεδιασμού (regulatory reform) σε τομείς απασχόλησης, αγοράς προϊόντων, κοινωνικών και διοικητικών ρυθμίσεων.

6.1.4 Ανάπτυξη επιχειρηματικής δραστηριότητας στο Internet: Επιχειρηματικά πλάνα και μοντέλα τιμολόγησης

Στη συνέχεια θα διερευνήσουμε μέσα από το στρατηγικό πρίσμα την επίσης πολύ βασική έννοια των "ηλεκτρονικών ενδιάμεσων". Θα θεωρήσουμε δηλαδή την υπό μελέτη επιχείρηση σαν ηλεκτρονικό ενδιάμεσο που δέχεται και παρέχει υπηρεσίες. Ειδικότερα θα δούμε τρία βασικά θέματα:

1. Το επιχειρηματικό μοντέλο των ενδιάμεσων φορέων,

2. Τη σύνταξη ενός business plan με αντικείμενο μια συγκεκριμένη μορφή ενδιάμεσου φορέα, και

3. Την εξέταση της τιμολογιακής πολιτικής που πρέπει να ακολουθούν οι ενδιάμεσοι φορείς, και γενικότερα οι επιχειρήσεις που προσφέρουν υπηρεσίες, στο Internet.

Οι ηλεκτρονικοί ενδιάμεσοι είναι παροχείς υπηρεσιών, που συνήθως χρησιμοποιούν το δίκτυο Internet, για την υποκατάσταση παλαιότερων γραφειοκρατικών, κατά κύριο λόγο, υπηρεσιών με αντίστοιχες ηλεκτρονικές. Ένα από τα κύρια χαρακτηριστικά τους είναι ότι διαθέτουν πηγές πληροφόρησης, οι οποίες δεν είναι εύκολα και ολοκληρωμένα προσβάσιμες από επιχειρήσεις και πολίτες. Οι πληροφορίες που προσφέρονται είναι συνήθως τριών ειδών:

- Ανταγωνιστικές (π.χ. χαρακτηριστικά και τιμές προϊόντων που προσφέρονται από διαφορετικούς προμηθευτές).

- Συμπληρωματικές (π.χ. συμπληρωματικά προϊόντα του ίδιου - ή άλλων - προμηθευτή).
- Υποστήριξης Αποφάσεων (η παρεχόμενη πληροφορία αποσκοπεί στην υποστήριξη λήψης μιας επιχειρηματικής απόφασης και όχι στην επίτευξη μιας συναλλαγής).

Στις ηλεκτρονικές αγορές δραστηριοποιούνται διάφοροι τύποι ηλεκτρονικών ενδιαμέσων όπως π.χ ηλεκτρονικές δημοπρασίες, ηλεκτρονική διεξαγωγή προμηθειών, ηλεκτρονικοί ενδιάμεσοι για εύρεση προϊόντων και υπηρεσιών, ηλεκτρονικοί κατάλογοι καταστημάτων, κ.λ.π. Παράλληλα, υπάρχουν ηλεκτρονικοί ενδιάμεσοι οι οποίοι λειτουργούν με σκοπό την υποστήριξη ενός συνόλου επιχειρήσεων, και με διάφορους άλλους στόχους, πλην του κέρδους. Μια τέτοια μορφή ενδιάμεσων φορέων αποτελούν και οι συλλογικοί φορείς. Από τον χώρο αυτό υπάρχουν πολλά παραδείγματα.

Ανάμεσα σε αυτά συγκαταλέγονται τα Ηλεκτρονικά Σημεία Εμπορίου, και το αντίστοιχο τους στον ελλαδικό χώρο, τα Ηλεκτρονικά Κέντρα Εμπορίου (ΗΚΕ). Ένα Ηλεκτρονικό Κέντρο Εμπορίου (ΗΚΕ) αποτελεί ουσιαστικά έναν ενδιάμεσο φορέα (σε φυσικό και εικονικό επίπεδο), ο οποίος συγκεντρώνει ένα σύνολο από τεχνολογίες και προηγμένες επιχειρηματικές πρακτικές, προσφέροντας υπηρεσίες Ηλεκτρονικού Εμπορίου στις Επιχειρήσεις (κυρίως μικρομεσαίες) που συνδέονται με αυτό. Πρόκειται δηλαδή για ένα ηλεκτρονικό (one stop) κέντρο διευκόλυνσης εμπορικών συναλλαγών, όπου κάθε ενδιαφερόμενος φορέας (επιχείρηση) μπορεί να συναλλαγεί με όλους τους παράγοντες που εμπλέκονται σε μια εμπορική πράξη (π.χ. πωλητές, αγοραστές, τελωνεία, μεταφορικές εταιρίες, τράπεζες, ασφαλιστικές εταιρίες κλπ). Όλοι οι συμμετέχοντες σε μια εμπορική πράξη, συγκεντρώνονται σε ένα φυσικό χώρο, κυρίως όμως σε ένα ιδεατό (virtual) σημείο, στο οποίο η συγκέντρωση επιτυγχάνεται .ηλεκτρονικά. μέσω τηλεπικοινωνιακών δικτύων (Internet).

Προκειμένου να καταστεί εφικτή η ομαλή και επιτυχημένη λειτουργία αυτού του ενδιάμεσου φορέα, θα πρέπει να συνταχθεί ένα επιχειρηματικό σχέδιο (Business Plan). Πρόκειται για ένα πλάνο, το οποίο καλύπτει όλους τους τομείς δράσης των Ηλεκτρονικών Κέντρων Εμπορίου. Σχεδιάζεται η στρατηγική που πρέπει να ακολουθήσει ένας ενδιάμεσος φορέας όπως τα ΗΚΕ, προκειμένου να εξασφαλίσει την οικονομική σταθερότητα και βιωσιμότητα του, αλλά και γενικότερα την επιτυχημένη λειτουργία του. Ένα επιχειρηματικό σχέδιο περιλαμβάνει την περιγραφή μιας επιχείρησης, καθώς και του περιβάλλοντος μέσα στο οποίο αυτή λειτουργεί. Στο

Business Plan πρέπει να καθορίζονται οι στόχοι τους οποίους θέτει η επιχείρηση, καθώς και να προσδιορίζεται ο τρόπος με τον οποίο αυτή θα πρέπει να λειτουργεί, προκειμένου να τους επιτύχει.

Οι βασικές ενότητες οι οποίες πρέπει να αποτελούν ένα business plan είναι[47]:

I. Το Executive summary

II. Περιγραφή της επιχείρησης

III. Περιγραφή των προϊόντων/ υπηρεσιών

IV. Περιγραφή και ανάλυση της αγοράς

V. Διαμόρφωση στρατηγικής προώθησης (Marketing Strategy)

VI. Περιγραφή της οργανωτικής δομής και της τεχνολογικής υποδομής

VII. Οικονομικό πλάνο

VIII. Παράρτημα

Για κάθε μια από αυτές αναφέρονται οι κρίσιμοι παράγοντεςεπιτυχίας. Η δυσκολία που υπάρχει στην σύνταξη του συγκεκριμένου επιχειρηματικού σχεδίου είναι η διαφοροποίηση που υπάρχει ανάμεσα στα παραδοσιακά Business Plans και τα Business Plans που αφορούν επιχειρήσεις οι οποίες δραστηριοποιούνται στον χώρο του Internet. Οι κυριότερες διαφορές εντοπίζονται: στην περιγραφή και ανάλυση της αγοράς, στον τρόπο διαμόρφωσης της στρατηγικής marketing και στην διαδικασία σύνταξης του οικονομικού πλάνου.

Ειδικά, για τα ΗΚΕ η δομή του επιχειρηματικού σχεδίου είναι η ακόλουθη. Αρχικά, δίνεται μια γενική περιγραφή της λειτουργίας του φορέα, παρουσιάζονται οι επιχειρηματικές ευκαιρίες που υπάρχουν στον ελλαδικό χώρο, οι κρίσιμοι παράγοντες επιτυχίας του φορέα, αλλά και τα υπάρχοντα επιχειρηματικά ρίσκα. Στην συνέχεια, παρουσιάζονται αναλυτικά οι προσφερόμενες υπηρεσίες από τα Κέντρα Εμπορίου. Αυτές είναι:

[47] Μακρυδάκης Σ., Παπαγιαννάκης Λ. Καλογήρου Γ., το Ελληνικό Μάνατζμεντ: Εξελίξεις, Τάσεις, Προοπτικές, ΕΑΣΕ, 1996

1) Υπηρεσίες πληροφόρησης και εκπαίδευσης,
2) Υπηρεσίες υποστήριξης των επιχειρηματικών διαδικασιών, και
3) Τεχνολογική και επιχειρηματική έρευνα.

Για την καλύτερη και ουσιαστικότερη κατανόηση του τρόπου λειτουργίας των ΗΚΕ είναι απαραίτητη η πραγματοποίηση μιας SWOT (Strengths-Weaknesses-Opportunities-Threats) ανάλυσης. Μια τέτοια ανάλυση έχει ως στόχο να προσδιορίσει παράγοντες που επηρεάζουν την λειτουργία και την επιτυχία των ΗΚΕ.

Ως επόμενο βήμα γίνεται μια ανάλυση της αγοράς. Για την ανάλυση του περιβάλλοντος δραστηριοποίησης των ΗΚΕ, χρησιμοποιείται το μοντέλο του Porter. Το μοντέλο αυτό, εξετάζει την επιρροή πέντε βασικών παραγόντων του περιβάλλοντος οι οποίοι αφορούν: την Υπάρχουσα Αγορά (Rivalry), τους Προμηθευτές (Suppliers), τους Πελάτες (Customers), τους Νέους Ανταγωνιστές (New Competitors), καθώς και τα Υποκατάστατα (Substitutes). Ιδιαίτερη έμφαση δίνεται στην ανάλυση των ανταγωνιστών. Εντοπίζονται διάφορες δομές, οι οποίες δρουν κατά τρόπο ανταγωνιστικό προς τα ΗΚΕ.

Παραδείγματα μεγάλων δομών ΗΚΕ αποτελούν τα portal sites, οι web hosts, τα ηλεκτρονικά εμπορικά κέντρα (shopping malls), τα ηλεκτρονικά καταστήματα (e-shops), οι ηλεκτρονικές εφημερίδες και τα συστήματα billing. Αυτά θεωρούνται ως ανταγωνιστές, με την έννοια ότι παρέχουν ένα υποσύνολο των υπηρεσιών που προσφέρονται από τα "καθαρόαιμα" ΗΚΕ. Η ανάλυση τους συντελεί στην καλύτερη κατανόηση του τρόπου λειτουργίας αυτών των επιχειρηματικών μοντέλων, και αποτελεί γνώση η οποία θα πρέπεινα χρησιμοποιηθεί από τα μικρότερα ΗΚΕ προκειμένου να διαφοροποιηθούν και να προσφέρουν εμπλουτισμένες υπηρεσίες.

Αφού ολοκληρωθεί η ανάλυση της αγοράς, ακολουθεί η διαμόρφωση της στρατηγικής παροχής και προώθησης αγοράς. Αρχικά προσδιορίζεται η αγορά στην οποία απευθύνεται η κάθε υπηρεσία. Το επόμενο βήμα είναι η ομαδοποίηση των υπηρεσιών, και η οργάνωση τους σε πακέτα. Η διαδικασία αυτή, καθώς και η τιμολόγηση του κάθε πακέτου, αποτελούν κρίσιμους παράγοντες επιτυχίας, και θα καθορίσουν την βιωσιμότητα των κέντρων. Η τιμολογιακή πολιτική σε συνδυασμό με την στρατηγική προώθησης αποτελούν τους πιο κρίσιμους παράγοντες για την επιτυχία μιας πρωτοβουλίας. Η στρατηγική προώθησης αφορά τις ενέργειες, οι οποίες θα πρέπει να πραγματοποιηθούν προκειμένου να γνωστοποιηθεί το έργο των ΗΚΕ, και τα οφέλη που θα προκύψουν από αυτό. Στην περίπτωση των ΗΚΕ επιλέγονται:

α) Γενικές Στρατηγικές Προώθησης όπως παραγωγή και διάθεση ενημερωτικών φυλλαδίων και CDs, δημοσίευση Αναφορών, αξιοποίηση των καναλιών επικοινωνίας που έχουν οι εμπλεκόμενοι φορείς, δημιουργία ειδικού web site για την προβολή του έργου, ημερίδες /συνέδρια/ παρουσιάσεις, σεμινάρια, Help Desk στις εγκαταστάσεις των Κέντρων, και προώθηση προς τον ΟΗΕ, και

β) Εξειδικευμένες Στρατηγικές Προώθησης στο Internet όπως τοποθέτηση της διεύθυνσης του site σε search engines, αγορά διαφημιστικών banners και τοποθέτηση links, σε sites γενικού ενδιαφέροντος, αγορά διαφημιστικών banners σε εξειδικευμένα sites (π.χ σχετικά με το ηλεκτρονικό εμπόριο), έκδοση e-mail Newsletter κ.λ.π.

Τέλος, εξετάζονται στρατηγικές συνεργασίες που θα συμβάλουν στην γνωστοποίηση της λειτουργίας των ΗΚΕ όπως συνεργασίες με συλλογικούς φορείς, τεχνολογικούς προμηθευτές και συμβούλους, παροχείς υπηρεσιών Internet, εφημερίδες και περιοδικά, διαφημιστικές εταιρείες, εκθεσιακούς φορείς, τράπεζες, κρατικούς φορείς κ.λ.π. Τέλος, η σύνταξη του επιχειρηματικού σχεδίου ολοκληρώνεται με τον σχεδιασμό του οικονομικού πλάνου και την παρουσίαση της οργανωτικής δομής των κέντρων.

Συνεπώς, έχουν συλλεχθεί όλα τα απαραίτητα στοιχεία και έχει διατυπωθεί ένα σχέδιο δράσης, το οποίο στοχεύει στην οικονομική σταθερότητα και βιωσιμότητα των ΗΚΕ. Στο Business Plan, αναφέρονται ορισμένα γενικά στοιχεία σχετικά με την τιμολόγηση. Η μεθοδολογία που ακολουθείται για την προσέγγιση του θέματος της τιμολόγησης, είναι η ακόλουθη:

1. Εξέταση γενικών θεμάτων σχετικά με την τιμολόγηση. Εξετάζονται ορισμένα ζητήματα που απορρέουν από την οικονομική θεωρία και αναφέρονται βασικές οικονομικές έννοιες. Παρουσιάζονται οι βασικές μέθοδοι τιμολόγησης και εξετάζονται τα κριτήρια που καθορίζουν την επιλογή της καθεμιάς.
2. Εξέταση της τιμολόγησης ανά επιχειρηματικό μοντέλο. Παρουσιάζονται ορισμένα βασικά μοντέλα τιμολόγησης που χρησιμοποιούνται σήμερα από τις επιχειρήσεις στο διαδίκτυο. Στην συνέχεια, προσδιορίζονται τα επιχειρηματικά μοντέλα που υπάρχουν στο Internet, και για κάθε μοντέλο περιγράφεται ο τρόπος δημιουργίας εσόδων.
3. Εξέταση της τιμολόγησης ανά υπηρεσία. Δεδομένου ότι οι επιχειρήσεις στην πλειονότητα τους δραστηριοποιούνται σε πολλά επίπεδα και προσφέρουν ένα ευρύ φάσμα υπηρεσιών, επιχειρείται και μια διαφορετική προσέγγιση. Εκτιμάται, ότι καλύτερη μελέτη του θέματος θα επιτευχθεί,

εφόσον μελετηθεί ο τρόπος τιμολόγησης, όχι με βάση το επιχειρηματικό μοντέλο στο οποίο ανήκει μια επιχείρηση, αλλά με βάση τις υπηρεσίες που προσφέρει. Επομένως, οι εναλλακτικοί τρόποι τιμολόγησης προσδιορίζονται σε επίπεδο υπηρεσίας. Δηλαδή, για κάθε βασική υπηρεσία που προσφέρεται στο διαδίκτυο, εξετάζονται οι διαφορετικοί τρόποι χρέωσης της, από διαφορετικές επιχειρήσεις.

Για την ορθότερη παρουσίαση των υπηρεσιών, κρίνεται σκόπιμη η κατηγοριοποίηση τους με βάση την πολυπλοκότητα τους, και τον βαθμό στον οποίο συμβάλλουν στην πραγματοποίηση του Ηλεκτρονικού Εμπορίου και την ολοκλήρωση μιας εμπορικής συναλλαγής. Στο πρώτο επίπεδο εντάσσονται οι υπηρεσίες πληροφόρησης (π.χ πληροφόρηση σε γενικά θέματα, εξειδικευμένη πληροφόρηση κ.λ.π.). Στο δεύτερο επίπεδο κατατάσσονται οι υπηρεσίες που βοηθούν μια επιχείρηση να αποκτήσει μια παρουσία στο διαδίκτυο (π.χ σχεδίαση site επιχείρησης, διαφημιστική προβολή κ.ο.κ.). Τέλος, στο τρίτο επίπεδο, εντάσσονται οι υπηρεσίες εκείνες, οι οποίες προσφέρονται σε e-commerce sites, δηλαδή εκείνα που πραγματοποιούν εμπορικές συναλλαγές. Οι υπηρεσίες αυτές είναι πιο πολύπλοκες υπό την έννοια ότι για να καταστεί εφικτή η προσφορά τους, απαιτείται και πιο εξελιγμένη τεχνολογική υποδομή. Ως αποτέλεσμα, δημιουργούνται πιο σύνθετα και ολοκληρωμένα μοντέλα τιμολόγησης. Στόχος είναι, τα συμπεράσματα που θα εξαχθούν να χρησιμοποιηθούν για την τιμολόγηση των υπηρεσιών και κατ' επέκταση για την εξασφάλιση της βιωσιμότητας των επιχειρήσεων και την αύξηση της αποδοτικότητας τους.

7 Στρατηγικές επιβίωσης απο την e-καταστροφή

Στον ταχύτατα αναπτυσσόμενο χώρο του Internet, όπου οι νέες επιχειρήσεις εμφανίζονται η μία μετά την άλλη, το ερώτημα πλέον δεν είναι αν μπορεί κανείς να ιδρύσει μία επιχείρηση που να δραστηριοποιείται στο e-business, αλλά το κατά πόσο η επιχείρηση αυτή θα μπορέσει να επιβιώσει[48]. Στην χώρα μας ο χώρος του Διαδικτύου είναι εν πολλοίς "παρθένος" με τους πρώτους μόλις ενδιαφερόμενους να διαγωνίζονται για μια θέση στη συγκεκριμένη αγορά, που αν και αναπτυσσόμενη, θεωρείται περιφερειακή και ως εκ τούτου περιορισμένη. Παρά τα μικρά μεγέθη ωστόσο, η επιχειρηματική δραστηριοποίηση στο Internet (πλατφόρμες, παροχή υπηρεσιών κ.τ.λ.) ή μέσω Internet (π.χ. ηλεκτρονικό εμπόριο για τις παραδοσιακές εταιρίες) αποτελεί πεδίο ενδιαφέροντος για τους εγχώριους παίκτες των τηλεπικοινωνιών, της πληροφορικής και των media.

[48] OECD DEVELOPMENT CENTRE, The policy Challenges of Globalisation and Regionalisation (by C.Oman), 1996

Από την άλλη πλευρά, είναι χαρακτηριστική η "στροφή" που επιχειρούν προς αυτήν την κατεύθυνση πολλές μεγάλες εταιρίες εισηγμένες και μη προκειμένου να προσελκύσουν νέα κεφάλαια, νέους πελάτες και κατ' επέκταση να αυξήσουν τα κέρδη τους. Την ίδια στιγμή στην άλλη άκρη του Ατλαντικού, οι Ηνωμένες Πολιτείες προσφέρουν ένα ζωντανό παράδειγμα του πόσο εύκολα μία επιχείρηση του e-business, που ξεκινά με τις καλύτερες προοπτικές, μπορεί να βρεθεί σε "βαθιά νερά" και είτε να αναγκαστεί να αναζητήσει κάποιον στρατηγικό συνεργάτη είτε να οδηγηθεί στην πτώχευση πριν προλάβει να "γευτεί" τους καρπούς των κόπων της.

Την άνοιξη του 2000 αρκετές επιχειρήσεις του Internet στις ΗΠΑ, είδαν τις μετοχές τους να καταρρέουν χάνοντας έως και πάνω από 60% των κερδών που κατέγραφαν μέχρι τότε, ενώ από την αρχή του έτους πάνω από 30 εταιρίες ακύρωσαν τις δημόσιες εγγραφές τους, σύμφωνα με την IPO Monitor. Παράλληλα δεκάδες άλλες αναβάλουν τις αυξήσεις κεφαλαίου που είχαν προαναγγείλει και μεταθέτουν τις ημερομηνίες των δημόσιων εγγραφών τους, προκειμένου να επανεξετάσουν τις επόμενες κινήσεις τους. Οι λεγόμενες εταιρίες καινοτομικών κεφαλαίων (venture capital companies) από την άλλη πλευρά παύουν να χρηματοδοτούν εκείνες τις εταιρίες που κινδυνεύουν

περισσότερο. Στο α' τρίμηνο μόνον το 5% της χρηματοδότησης των venture capitals αφορούσε νέες εταιρίες του e-commerce έναντι ποσοστού 12% που ήταν στο προηγούμενο τρίμηνο. Είναι πλέον εμφανές ότι η αγορά έχει γίνει πιο επιφυλακτική, γεγονός που καθιστά τις προοπτικές των πιο αδύναμων εταιριών αβέβαιες, ενώ υπάρχει μεγάλη πιθανότητα να προξενήσει προβλήματα ακόμη και σε επιχειρήσεις με αρκετά γερές βάσεις.

Όλα τα προαναφερθέντα μπορεί να ταλανίζουν τις εταιρίες των ΗΠΑ, ωστόσο για την Ελλάδα μπορούν να αποτελέσουν ένα καλό οδηγό για την αποφυγή λαθών που σε αρκετές περιπτώσεις έχουν κοστίσει ολόκληρες εταιρίες. Τι μπορεί λοιπόν να κάνει μία εταιρία του Internet προκειμένου να διαφυλάξει την ακεραιότητα της και να αυξήσει τις πιθανότητες επιβίωσης της;

7.1 Εναλλακτικές Πηγές Χρηματοδότησης

Τα κεφάλαια υψηλού επιχειρηματικού κινδύνου (venture capital) μπορεί να βρίθουν ρευστότητας, ωστόσο οι εταιρίες έχουν γίνει πιο επιλεκτικές στις τοποθετήσεις τους. Η παλαιότερη επιτυχία των επιχειρήσεων του Internet προσήλκυσε το ενδιαφέρον της "κοινότητας" των VCs και γενικά των επενδυτών, παρ' όλα αυτά η πτώση των μετοχών των e-businesses έχει οδηγήσει τις εν

λόγω εταιρίες στο να εξετάζουν πιο προσεκτικά τις μελλοντικές επενδύσεις τους και τους δευτερεύοντες ή μεσολαβητικούς "κύκλους" χρηματοδότησης.

Αν και οι πιο δυνατές επιχειρήσεις μπορούν να περιμένουν μέχρις ότου επιτύχουν μία καλύτερη συμφωνία χρηματοδότησης, υπάρχουν και οι πιο αδύναμες που ενδεχομένως να συμβιβαστούν ενισχύοντας τα αποθέματα ρευστότητας τους μέσω του λεγόμενου "flat round" ήτοι αποδεχόμενες χρηματοδότηση, που έχει την ίδια αποτίμηση με προηγούμενους "κύκλους" χρηματοδότησης. Παράλληλα υπάρχουν και οι πιο προβληματικές επιχειρήσεις οι οποίες θα αναγκαστούν να πάρουν χρήμα με χαμηλότερη αποτίμηση έναντι προηγούμενων "κύκλων", μέθοδος που ενδέχεται να αποδυναμώσει κατά πολύ το μετοχικό κεφάλαιο κάποιων πρώιμων επενδυτών, διευθυντικών στελεχών ή υπαλλήλων. Η μερική αποδυνάμωση, ωστόσο, μπορεί να είναι το τίμημα που καλείται να πληρώσει μία εταιρία, προκειμένου να επιβιώσει.

Βέβαια τα κεφάλαια υψηλού κινδύνου δεν είναι ο μόνος τρόπος χρηματοδότησης για μία εταιρία του Internet. Μία εκ των εναλλακτικών λύσεων είναι η προσέλκυση εταιρικών επενδυτών οι οποίοι, όχι μόνο θα παράσχουν ρευστότητα αλλά θα συμβάλλουν και στην δημιουργία μίας επιχείρησης με γερές βάσεις, όπως το παράδειγμα της εταιρίας γραφικής ύλης και ευχετήριων καρτών OurBeginning.com, η οποία πλέον στρέφεται σε εταιρικούς επενδυτές που δραστηριοποιούνται στον συγκεκριμένο τομέα και σύμφωνα με τον οικονομικό διευθυντή, Michael Budowski, αυτού του είδους οι επενδυτές μπορούν να βοηθήσουν την εταιρία μακροπρόθεσμα. Ακόμη ένα πρόβλημα είναι το γεγονός ότι η αγορά είναι πλέον "κλειστή" στις δευτερεύουσες δημόσιες προσφορές, στις οποίες καταφεύγουν συχνά οι εταιρείες προκειμένου να καλύψουν τις υποχρεώσεις τους. Ως επακόλουθο, οι εταιρίες που δεν μπορούν να προβούν σε αυξήσεις κεφαλαίου μέσω του χρηματιστηρίου, θα αναγκαστούν να δεχθούν τοποθετήσεις ιδιωτικών κεφαλαίων, εκτός του περιβάλλοντος και των όρων της κεφαλαιαγοράς. Σ’ αυτή την περίπτωση, οι ιδιωτικές τοποθετήσεις μπορεί να γίνουν με όρους επαχθέστερους και σε ύψος μικρότερο των απαιτήσεων αλλά και των προοπτικών των εταιρειών, αλλά αποτελούν μια κάποια λύση, έως ότου οι συνθήκες στις κεφαλαιαγορές γίνουν ευνοϊκότερες.

7.2 Κίνητρα Στους Εργαζομένους

Η δυνατότητα μίας επιχείρησης να καλύψει τα έξοδα πληρωμής των υπαλλήλων της δεν σημαίνει τίποτα εάν δεν είναι σε θέση να τους παρέχει προοπτική στην εργασία. Εάν τα δικαιώματα μελλοντικής αγοράς / πώλησης μετοχών "πέσουν" κάτω από την τιμή εξάσκησης ενός

δικαιώματος των υπαλλήλων, οι εργοδότες κινδυνεύουν να χάσουν κάποιους ταλαντούχους υπαλλήλους έναντι των ανταγωνιστών τους. Ένας υψηλός ρυθμός αποδυνάμωσης μπορεί παράλληλα να δημιουργήσει προβλήματα στις διαπραγματεύσεις των επιχειρήσεων κατά την αναζήτηση χρηματοδότη, όπως επίσης και να προσελκύσει επιθετικές προσφορές εξαγορών. Η προσφορά νέων δικαιωμάτων είναι ένας τρόπος για να δελεάσει μία εταιρία τους ανικανοποίητους υπαλλήλους ώστε να μην είναι τόσο πρόθυμοι να δεχθούν μία νέα προσφορά από κάποιον ανταγωνιστή. Χαρακτηριστικό είναι το παράδειγμα της εταιρίας Beyond.com η οποία πρόσφατα έδωσε σε όλους τους υπαλλήλους της επιπλέον μετοχές ως επίδομα, ενώ επιπλέον διένειμε 250.000 "κεκτημένα επιδόματα" (vested grants) τα οποία επιτρέπουν στους εργαζόμενους να συμμετάσχουν σε ένα συνταξιοδοτικό σχέδιο της επιχείρησης όταν συμπληρώσουν ένα ορισμένο χρονικό διάστημα εργασίας.

Οι μετοχές, ωστόσο, δεν είναι ο μόνος λόγος για τον οποίο δουλεύει κανείς. Έτσι η επιχείρηση θα πρέπει από την μία να παρέχει στους εργαζόμενους τη σιγουριά ότι η εταιρία τους έχει μακροπρόθεσμο ορίζοντα επιβίωσης και συγχρόνως από την άλλη να αναδιαμορφώσει το μοντέλο λειτουργία της δίνοντας τη δυνατότητα στους υπαλλήλους να ασχοληθούν με καινούργια πράγματα, αναζωπυρώνοντας έτσι το ενδιαφέρον τους για την εργασία τους.

7.3 Περικοπή Δαπανών

Οι δαπάνες μίας επιχείρησης είναι ένα από τα πιο σημαντικά κεφάλαια στην λειτουργία τους καθώς σε αρκετές περιπτώσεις ο προγραμματισμός τους βασίζεται και σε προσδοκώμενα κέρδη ανάλογα με την πορεία μίας επιχείρησης. Όταν όμως παρουσιαστούν προβλήματα, από το "γύρισμα" της αγοράς, την κακή εκτίμηση μία επένδυσης ή την αποτυχία μίας συνεργασίας, η επιχείρηση πρέπει να είναι σε θέση να αναδιοργανωθεί το συντομότερο δυνατό και να εξοικονομήσει ρευστότητα ώστε να μπορεί να κινηθεί πιο ευέλικτα. Προκειμένου να γίνει αυτό λοιπόν, είναι σε αρκετές περιπτώσεις αναγκαία η περικοπή κάποιων δαπανών και η επανατοποθέτηση αυτών των χρημάτων σε πιο προσοδοφόρα προγράμματα.

Ένας από τους βασικούς τομείς στους οποίους μπορεί να γίνει περικοπή δαπανών είναι το κόστος διαφήμισης μίας εταιρίας, το οποίο σε αρκετές περιπτώσεις μπορεί να είναι δυσανάλογο σε σχέση με τα αποτελέσματα που προσδοκώνται. Για παράδειγμα η εταιρία Ashford.com. αναγκάστηκε να επανεξετάσει την διαφημιστική της καμπάνια, όταν οι μετοχές της άρχισαν να υποχωρούν σημαντικά. Ως αποτέλεσμα περιέκοψε τον διαφημιστικό προϋπολογισμό

της από τα 7,33 εκ. δολ., στα 5,87 εκ. δολ., γεγονός που της παρείχε τη δυνατότητα να εξασφαλίσει πόρους για την αγορά εξοπλισμού χωρίς να χρειαστεί να προσφύγει στα ρευστά αποθέματα της. Χαρακτηριστικό της κατάστασης που επικρατεί, τουλάχιστον στις ΗΠΑ, είναι το γεγονός ότι πολλές εταιρίες του Internet προχωρούν σε περικοπές προσωπικού ενώ παράλληλα άλλες μειώνουν τις διαφημίσεις τους στον χώρο της τηλεόρασης και στρέφονται προς την διαφήμιση μέσω μηνυμάτων από το Διαδίκτυο.

Οι εταιρίες έχουν αρχίσει να συνειδητοποιούν ότι το να ξοδεύει κανείς οποιοδήποτε ποσό προκειμένου να αποκτήσει πελάτες δεν μπορεί να λειτουργήσει μακροπρόθεσμα, γι' αυτό και καταφεύγουν σε άλλους τρόπους προσέλκυσης του ενδιαφέροντος των καταναλωτών όπως η έκπτωση για τις πρώτες αγορές ή για συγκεκριμένες κατηγορίες προϊόντων. Η εταιρία εκπαιδευτικών παιχνιδιών SmarterKids.com που δραστηριοποιείται στον τομέα του λιανικού εμπορίου, έχει να αντιμετωπίσει ένα αρκετά ανταγωνιστικό περιβάλλον, ενώ ήδη υπάρχει το παράδειγμα της εταιρίας toysmart.com., που υποστηριζόταν από την Disney, η οποία τον Μάϊο πτώχευσε. Καθώς λοιπόν η μετοχή της εταιρίας σημείωσε υποχώρηση πάνω από 80% από τα υψηλότερα επίπεδα όπου βρισκόταν, ο οικονομικός της διευθυντής, David Blohm στο α' τρίμηνο περιέκοψε την δαπάνη της εταιρίας για απόκτηση πελατών κατά 75%, ενώ οι "οικονομίες" της εταιρίας ενισχύθηκαν και από τη μείωση των διαφημίσεων στην τηλεόραση. Μία εταιρία, ωστόσο, βασίζεται περισσότερο στους σταθερούς πελάτες της και όχι τόσο σε εκείνους που θα την προτιμήσουν μόνο κάθε φορά που έχει κάποια ειδική προσφορά. Γι' αυτό το λόγο εκτός από την περικοπή των δαπανών, η οποία εκτός από την διαφημιστική καμπάνια, θα πρέπει να επεκταθεί και σε λογαριασμούς τηλεφώνων, υπέρογκους μισθούς υπαλλήλων, εξοπλισμό γραφείου, αλλά και σε εκπτώσεις ή προσφορές στην αποστολή κάποιων προϊόντων, ενώ αντίστοιχα τα χρήματα που θα εξοικονομηθούν θα πρέπει να διοχετευτούν σε τομείς που θα αυξήσουν τις πωλήσεις.

7.4 Αλλαγή Προσανατολισμού

Όταν η περικοπή των εξόδων δεν αποφέρει τα προσδοκώμενα, οι εταιρίες του Internet προκειμένου να ενισχύσουν τα έσοδα τους στρέφονται στην παροχή νέων υπηρεσιών και αγαθών, ή επιχειρούν την είσοδο τους σε νέους τομείς οι οποίοι δεν είναι τόσο κορεσμένοι. Ένα παράδειγμα αλλαγής του επαγγελματικού προσανατολισμού αποτελεί η εταιρία OpenAuto.com., με έδρα την Καλιφόρνια, η οποία εγκατέλειψε τα αρχικά σχέδια της που την ήθελαν να είναι μία ακόμη εταιρία επικεντρωμένη στο εμπόριο αυτοκινήτων μέσω του Διαδικτύου. Πλέον η εταιρία στρέφεται στον

χώρο παροχής υπηρεσιών όσον αφορά την κατασκευή, πωλώντας την τεχνογνωσία της σε άλλες εταιρίες αυτοκινήτων. Με το ίδιο σκεπτικό η εταιρία MyWay.com που ιδρύθηκε από την CMGI, αρχικά προσπάθησε να ακολουθήσει τα βήματα των Yahoo!, και Excite, δημιουργώντας ένα portal με επίκεντρο τους καταναλωτές. Ωστόσο απέτυχε καταλήγοντας στο να απολύσει 27 υπαλλήλους και να επαναπροσαρμόσει την λειτουργία της σε ένα μικρό επιχειρηματικό portal. Βέβαια εκτός από το λιανεμπόριο που στοχεύει κυρίως στους καταναλωτές οι εταιρίες του Internet στρέφονται και στον χώρο του business-to-business, που αφορά κυρίως την πώληση υπηρεσιών και αγαθών από μία εταιρία σε κάποια άλλη. Ωστόσο και σε αυτήν την περίπτωση οι αναλυτές διατηρούν κάποιες επιφυλάξεις, καθώς υφίσταται και το θέμα του ανταγωνισμού που μπορεί να σταθεί εμπόδιο στην περίπτωση δύο επιχειρήσεων με το ίδιο αντικείμενο, ενώ γενικότερα η αλλαγή του μοντέλου λειτουργίας μιας επιχείρησης είναι ριψοκίνδυνη όταν αυτή βρίσκεται ήδη σε δύσκολη θέση.

Σύμφωνα με τον αναλυτή της Forrester, Seema Williams, είναι σχεδόν αναπόφευκτο μία επιχείρηση να στραφεί σε νέες αγορές, ειδικά όταν δραστηριοποιείται σε έναν χώρο με χαμηλές εγγυήσεις. Αντιπροσωπευτικό είναι το παράδειγμα του Jeff Bezos από το Amazon.com ο οποίος σχετικά νωρίς συνειδητοποίησε τα παραπάνω και ήταν σε θέση να ξοδέψει αρκετά ώστε να επεκταθεί σε αγορές όπως αυτές των CDs, των προγραμμάτων υπολογιστών, των επίπλων κουζίνας κ.τ.λ., μία πολυτέλεια την οποία δεν μπορούν να απολαύσουν πολλοί.

7.5 Εξαγορές-Συγχωνεύσεις-Συνεργασίες

Κάποιες εταιρίες του Internet δεν θα είναι ποτέ επικερδείς, όσες λειτουργικές και οργανωτικές αλλαγές και αν κάνουν. Πολλές εταιρίες στο χώρο του λιανικού εμπορίου κινδυνεύουν να βρεθούν σε προβληματική θέση, εάν πωλούν εμπορεύματα ευρείας κλίμακας όπως βιβλία, μουσική ή λουλούδια, τα οποία δεν διαφοροποιούνται σε τίποτα εκτός από την τιμή. Οι χαμηλές τιμές σημαίνουν μικρά περιθώρια κέρδους και οι αναπτυσσόμενες εταιρίες (startups) δεν είναι πλέον δυνατόν να έχουν την απαίτηση από τους επενδυτές να "υπομένουν" μαζικές απώλειες με την προσδοκία μελλοντικής αύξησης μεριδίου και ταχύτερων ρυθμών ανάπτυξης. Στην περίπτωση αυτή ορισμένες επιχειρήσεις θα αναγκαστούν να αναζητήσουν στρατηγικούς συνεταίρους ή ακόμη χειρότερα θα εξαγοραστούν από ανταγωνιστές ακόμη και έναντι μίας πολύ χαμηλής τιμής. Ωστόσο ακόμη και οι συγχωνεύσεις που γίνονται για λόγους επιβίωσης ενδέχεται

να μην έχουν μακροπρόθεσμα αποτελέσματα, καθώς δύο μικρές και προβληματικές επιχειρήσεις δεν δημιουργούν μία υγιή.

Για να εκτιμήσει κανείς την βιωσιμότητα μίας εταιρίας πρέπει να εξετάσει την κατάσταση πέρα από την προσωρινή της εικόνα, θέτοντας έναν χρονικό ορίζοντα 3 έως 5 ετών. Παράλληλα, με την παρουσία τόσων πολλών εταιριών του Internet των οποίων οι μετοχές πιέζονται και με δεδομένο το ενδιαφέρον των ιδιωτικών εταιριών για την ανεύρεση χρηματοδότησης, οι μεγαλύτεροι παίκτες της αγοράς και ειδικότερα οι παραδοσιακές εταιρίες θα μπορούν εύκολα να αποκτήσουν τις εν λόγω εταιρίες σε ιδιαίτερα χαμηλές τιμές. Για παράδειγμα η ολλανδική αλυσίδα σούπερ μάρκετ Royal Ahold απέκτησε την εταιρία πώλησης λαχανικών στο Internet, Peapod.com. έναντι μόνον 2,12 δολαρίων ανά μετοχή. Επιπλέον, καθώς οι μεγαλύτερες επιχειρήσεις συνενώνουν τις δυνάμεις τους όπως η Healtheon/Web MD, η οποία τον περασμένο χρόνο εξαγόρασε 3 online ανταγωνίστριες εταιρίες, μία επιχείρηση η οποία δεν έχει κάποιον σημαντικό υποστηρικτή ή συνεργάτη, θα είναι δύσκολο να ανταγωνιστεί με αυτά που θα προσφέρουν οι υπόλοιποι από την πελατειακή της βάση μέχρι το δίκτυο διανομής. Κατ' επέκταση οι εταιρίες θα πρέπει να γνωρίζουν τη θέση που κατέχουν έναντι των ανταγωνιστών τους και κυρίως τους τομείς στους οποίους υστερούν έναντι αυτών.

Οι επιχειρήσεις που δεν μπορούν να περικόψουν τους ρυθμούς ανάπτυξης των δαπανών τους χωρίς να πληγούν τα υπόλοιπα θεμελιώδη οικονομικά στοιχεία τους όπως τα ρευστά αποθέματα, τα έσοδα κ.τ.λ. δεν έχουν πολλές επιλογές εκτός από το να αναζητήσουν έναν αγοραστή ή συνεργάτη, προτού καταστρέψουν τα περιουσιακά τους στοιχεία, καθώς θα πρέπει να έχουν κάποια αξία για τους υποψήφιους αγοραστές. Οι εταιρίες του Internet θα πρέπει επίσης να υπολογίσουν την κατάσταση της γεωγραφικής τους θέσης στην αγορά προκειμένου να καθορίσουν και περαιτέρω τη θέση τους ως υποψήφιες προς πώληση.

7.6 Προφυλάξεις

Εκτός όμως από όλα όσα προαναφέραμε μία εταιρία θα πρέπει να φροντίζει να χρησιμοποιεί και την υπάρχουσα νομοθεσία προκειμένου να προστατευθεί. Στο παράδειγμα των ΗΠΑ, με την αγορά να πλημμυρίζει από ρευστότητα και αισιοδοξία, τουλάχιστον μέχρι πρόσφατα, λίγες ήταν εκείνες οι επιχειρήσεις του Internet οι οποίες είχαν επιλέξει να καταφύγουν στο λεγόμενο Κεφάλαιο 11 του καταστατικού τους το οποίο τις προστατεύει από την πτώχευση, λειτουργώντας σαν ένα εμπόδιο ανάμεσα στην επιχείρηση και τους πιστωτές, ενώ παράλληλα

μπορεί να τις καταστήσει ιδιαίτερα ελκυστικές για τους υποψήφιους αγοραστές, οι οποίοι εξαγοράζοντας τες αποκτούν τα περιουσιακά τους στοιχεία, όχι όμως και τα χρέη τους. Επιπλέον ακόμη και με το Κεφάλαιο 11, (ειδική ρύθμιση με ισχύ στις ΗΠΑ) οι επιχειρήσεις χρειάζονται αρκετά ρευστά διαθέσιμα ώστε να συνεχίσουν να λειτουργούν, αλλιώς κινδυνεύουν να οδηγηθούν στο δικαστήριο το οποίο θα επιβάλει ρευστοποίηση όλων των περιουσιακών τους στοιχείων.

8. ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναμφίβολα, το Διαδίκτυο επέφερε ένα μαζικό αντίκτυπο στον τρόπο που οι ναυτιλιακές εταιρίες επικοινωνούν και συλλέγουν πληροφορίες. Τα τηλέφωνα και το ηλεκτρονικό ταχυδρομείο είναι τα σημαντικότερα και πιο εύχρηστα μέσα επικοινωνίας στη ναυτιλιακή βιομηχανία. Όπως προτάθηκε στη βιβλιογραφία, κεφάλαιο τρίτο, οι εταιρίες δεν αποστέλλουν και λαμβάνουν απλά μηνύματα ηλεκτρονικού ταχυδρομείου, αλλά ενεργά δημιουργούν καινούριες σχέσεις ή διατηρούν τις ήδη υπάρχουσες καθώς αλληλεπιδρούν μεταξύ τους και με αυτόν τον τρόπο εμπλουτίζουν τις πληροφορίες και καλλιεργούν την επικοινωνία. Η αρχική υπόθεση ότι η τεχνολογική πρόοδος στη ναυτιλία θα μπορούσε να καταστρέψει τις καλές σχέσεις που έχουν δημιουργηθεί με το πέρασμα του χρόνου έχουν αρχίσει να εξαφανίζονται.

Σε αντίθεση με τα προηγούμενα, η διαπροσωπική επαφή και το telex είναι τα λιγότερα σημαντικά επικοινωνιακά και πληροφοριακά μέσα. Το telex, δεν είναι πλέον η μόνη απόδειξη επικοινωνίας που δέχεται ο νόμος, αλλά και το ηλεκτρονικό ταχυδρομείο αποτελεί πλέον νομική τεκμηρίωση. Το φωνητικό ταχυδρομείο και η τηλεδιάσκεψη δεν έχουν ακόμη διαδοθεί ως μέσα επικοινωνίας, κυρίως γιατί η τεχνολογία δεν έχει φθάσει στο επιθυμητό ακόμα επίπεδο.

Οι περισσότερες ναυτιλιακές εταιρίες έχουν συνειδητοποιήσει την ανάγκη δημιουργίας και διατήρησης ιστοσελίδας. Οι περισσότερες εταιρίες διαθέτουν ήδη ιστοσελίδα και αυτές που δεν έχουν σκέφτονται να αποκτήσουν στο άμεσο μέλλον. Για οποιοδήποτε λόγο και αν τις χρησιμοποιούν, είτε ως μέσο συλλογής και διανομής πληροφοριών, είτε για τις δραστηριότητες προβολής τους, είναι πλέον μια ανάγκη για αυτές. Και αυτό γιατί τα web sites είναι περισσότερο αλληλεπιδραστικά και ενημερωμένα (up to date), από ότι τα φυλλάδια.

Σχεδόν το σύνολο των ναυτιλιακών εταιριών έχουν προσδιορίσει σημαντικούς πόρους τα προηγούμενα δύο έτη από δραστηριότητες ηλεκτρονικού εμπορίου. Αυτό συμβαίνει απλά διότι αντιλαμβάνονται το ηλεκτρονικό εμπόριο ως την αναγκαία ζήτηση που απαιτούν οι πελάτες και οι συνεργάτες τους. Οι Pisanias και Willcocks[49] το εξηγούν αυτό λέγοντας ότι η ζήτηση των χρηστών

[49] N. Pisanias & L. Willccocks, “Understanding Slow Internet Adoption: Infomediation in Ship-Broking Markets”, 1999

προσδιορίζει τον τρόπου που η τεχνολογία χρησιμοποιείται. Ο δεύτερος λόγος είναι ότι οι εφαρμογές ηλεκτρονικού εμπορίου μειώνουν το κόστος λειτουργίας των επιχειρήσεων.

Ακόμη, εμπόδια όπως νομικά ζητήματα, ασφάλεια και κοινά πρότυπα, η υιοθέτηση του Διαδικτύου δεν θεωρούνται τα σημαντικότερα εμπόδια. Τα σημαντικότερα εμπόδια αποτελούν η έλλειψη προτύπων, η έλλειψη ασφάλειας και η ανασφάλεια αναφορικά με τις χρηματικές συναλλαγές.

Κλείνοντας, ο μελλοντικός ρόλος των ναυλομεσιτών είναι ότι θα ενεργούν ως σύμβουλοι και ειδικοί και θα παρέχουν ταυτόχρονα ηλεκτρονικές και παραδοσιακές υπηρεσίες. Όπως είδαμε στο δεύτερο και τρίτο κεφάλαιο, ο σκοπός των άμεσων διαπραγματεύσεων είναι να περικόψουν το κόστος και να εξαλείψουν τις αναποτελεσματικότητες που προκαλούνται πολλές φορές από τους διαμεσολαβητές. Ο αριθμός των άμεσων διαπραγματεύσεων και υπογραφής ναυλοσύμφωνων ανάμεσα σε πλοιοκτήτες και ναυλωτές θα αυξηθεί. Τέλος, οι άμεσες διαπραγματεύσεις είναι πιθανό να αυξηθούν σε μια πιο ξεκάθαρη, ανοικτή και λιγότερο τεμαχισμένη αγορά.

Η μελέτη ξεκάθαρα καταδεικνύει ότι οι παραδοσιακοί ναυλομεσίτες θα πρέπει να διαφοροποιήσουν τις υπηρεσίες που προσφέρουν – παρέχουν, χρησιμοποιώντας τους πόρους του Internet. Θα πρέπει επίσης, να συνεχίσουν να προσφέρουν τις ήδη υπάρχουσες υπηρεσίες, καθώς και να τις επεκτείνουν (online υπηρεσίες). Έτσι, θα διατηρήσουν καλές πιθανότητες να παραμείνουν και να είναι χρήσιμοι στην αγορά.

Οι ηλεκτρονικές πλατφόρμες παροχής υπηρεσιών ναύλωσης επιτρέπουν στις μικρομεσαίες επιχειρήσεις να συμμετέχουν σε ανοικτά δίκτυα πληροφοριών στο βαθμό που το κάνουν και οι μεγάλοι οργανισμοί. Επιπρόσθετα, οι πλατφόρμες αυτές είναι πιθανό να μειώσουν το κόστος διεκπεραίωσης συναλλαγής και να αυξήσουν την αποδοτικότητα – αποτελεσματικότητα των οργανισμών με την ηλεκτρονική παρακολούθηση και έλεγχο των εγγράφων.

Παρόλο που η πλειοψηφία των ενδιαφερομένων πιστεύει πως το ηλεκτρονικό εμπόριο θα οδηγήσει σε τυποποίηση των όρων του ναυλοσυμφώνου, εντούτοις ένα μεγάλο μέρος διαφωνεί. Τελειώνοντας, λαμβάνοντας υπόψη τις πρόσφατες αποτυχίες ορισμένων ηλεκτρονικών ναυτιλιακών πλατφόρμων, δεν προκαλεί έκπληξη το γεγονός ότι η ναυτιλιακή κοινότητα επιζητά να δει τη μακροχρόνια αντοχή και σταθερότητά τους, πριν εμπλακεί στις διαδικασίες αυτές.

Παρόλο που τα web – based ηλεκτρονικά συστήματα δεν έχουν υιοθετηθεί ευρέως, η γενική τάση στις ηλεκτρονικές ναυλώσεις είναι προς αυτή την κατεύθυνση. Οι ναυτιλιακές εταιρίες αρχίζουν να συνειδητοποιούν τη δυναμική των τεχνολογιών πληροφορικής και επικοινωνίας. Καθώς η αγορά του ηλεκτρονικού εμπορίου περνάει στο στάδιο ωρίμανσης, διαφαίνεται ότι ολοένα και περισσότεροι οργανισμοί πρόκειται να εμπλακούν στο χώρο του e- επιχειρήν.

Επιπλέον, οι υπάρχουσες ηλεκτρονικές πλατφόρμες ναύλωσης προσφέρουν ποικίλες υπηρεσίες. Διαφορετικές υπηρεσίες πιθανώς θα συναντήσουν διαφορετικές απαιτήσεις πελατών – χρηστών. Μερικές τέτοιες πλατφόρμες επιτρέπουν να συνδιαλέγονται οι πλοιοκτήτες και ναυλωτές άμεσα, ενώ άλλες όχι. Από την άποψη των ανταγωνιστικών συνθηκών της αγοράς και των απαιτήσεων των πελατών είναι πράγματι αναπόφευκτο ότι οι ναυλομεσίτες θα αναθεωρήσουν το ρόλο τους, θα επεκτείνουν τις παρεχόμενες υπηρεσίες τους και θα προσφέρουν ταυτόχρονα και online υπηρεσίες.

Οι περισσότερες επιχειρήσεις, που πραγματοποιούν ηλεκτρονικές συναλλαγές δηλώνουν ότι ο σημαντικότερος παράγοντας για να κάνεις ηλεκτρονικό εμπόριο είναι οι απαιτήσεις των πελατών. Καθώς οι ηλεκτρονικές πλατφόρμες ωριμάζουν και αποδεικνύουν τη μακροχρόνια αντοχή και σταθερότητά τους, παρέχοντας ασφαλείς, ανταγωνιστικές και φερέγγυες υπηρεσίες και εφαρμογές, φαίνεται ότι το ηλεκτρονικό εμπόριο θα είναι αναπόφευκτη πραγματικότητα.

Έτσι, είναι πιθανό να υφίστανται διαφορετικά κανάλια επικοινωνίας και συναλλαγών ανάμεσα στα εμπλεκόμενα μέρη, είτε δηλαδή άμεσα, είτε μέσω των ηλεκτρονικών πλατφόρμων είτε μέσω των διαφοροποιημένων ναυλομεσιτών. Το ερώτημα που γεννάται είναι ποιος θα χρησιμοποιεί κάθε κανάλι και σε ποιο βαθμό. Η απάντηση στο ερώτημα αυτό δεν είναι εύκολη, αλλά θα μπορούσαμε να πούμε ότι εξαρτάται από πολλούς παράγοντες, όπως από τις συνθήκες της αγοράς, την αποτελεσματικότητα των ναυλομεσιτών, την ικανότητα περικοπής του κόστους και αντικατάστασης των παραδοσιακών υπηρεσιών με ηλεκτρονικές, τις κυβερνητικές πολιτικές.

Παρόλο που η παρούσα μελέτη αποκάλυψε πολλά ενδιαφέροντα ζητήματα σχετικά με το ηλεκτρονικό εμπόριο στη ναυτιλία, εντούτοις πολλά ερωτήματα παραμένουν ανοικτά. Η ναυτιλία είναι μια πολυδιάστατη βιομηχανία και έτσι, οφείλουμε να την αντιμετωπίσουμε κατά αυτόν τον τρόπο και να λάβουμε υπόψη μας όλες τις διαστάσεις προκειμένου να συνάγουμε χρήσιμα συμπεράσματα.

9. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Drewry, “Recent Development in Web-Based Maritime Services”, Digital Ship & Drewry Shipping Consultants Ltd. 2000.
2. Frost D., 1999, http://www.emaconnect.com/archive/MarketC/0599market.html
3. Gray P., Igbaria M., “Virtual Organizations and E-Commerce”, 2000
4. King D., “Intranets: An Internet inside the Organization”, 2000
5. Lloyd’s List, 12/05/1999, “Quarterpoints: Are shipbrokers complete Luddites?”
6. Lloyd’s List, 23/10/1999, “Technology: Changing the Structure of Dry Cargo Shipping: IT maters”
7. Lloyd’s List, 20/1o/2000, “Seavantage Teams up Online with Ariba”
8. Lloyd’s List, 20/11/2000, “Bumper Year Predicted for Korean dot-coms”
9. Lloyd’s List, 08/01/2001, “Bunker News, Fujarah demand Strongest”
10. Lloyd’s List, 31/01/2001, “Internet Competition set to Force Market Consolidation”
11. Lloyd’s List, 08/02/2001, “Silja Line Takes Purchasing Portal Onboard”
12. Lloyd’s List, 14/02/2001, “Email Pioneer SpecTec can Build on its Credentials”
13. Lloyd’s List, 13/03/2001, “The Ups and Downs of Maritime e-Commerce”
14. Lloyd’s List, 21/05/2001, “Summer Launch Still on for Baltic dotcom site”
15. Lloyd’s List, 19/06/2001, “Approaching the Point of Delivery”
16. Malone T., Yates J. & Benjamin R., “Electronic Markets and Electronic Hierarchies”, Communications of ACM, Vol. 30, No. 6, 1987
17. N. Pisanias & L. Willccocks, “Understanding Slow Internet Adoption: Infomediation in Ship-Broking Markets”, 1999, http://www.templeton.ox.ac.uk/web/site/research/workingpapers/00-8.pdf
18. H. Oldendorff, “E-Shipping, Why and How Will it work?”, http://www.oldendorff.com
19. The Baltic Exchange Web Site: http://www.thebaltic.com
20. Timers Paul Electronic Commerce “Strategies and Models for Business-to-Business Trading”, Jony Wiley & Sons Ltd., Chichester, 1999
21. C. Bauer, “Requirements and Infrastructure for Modelling of Electronic Market Transactions”, 1999, http://www.collecter.org/coll99/bauer.pdf

22. M. Bichler, A. Segev, C. Beam, “An Electronic Broker for Business to Business Electronic Commerce on The Internet”, 1998,
23. M. Bloch, Y. Pigneur, A. Sefev, “On the Road of Electronic Commerce – A Business Value Framework, Gaining Competitive Advantage and Some Research Issues”, 1996, http://www.stern.nyu.edu/~docs/roadtoec/ec.htm
24. CIO Magazine, “Not all e-Signatures are Equal”. 15/01/2001, http://www.cio.com/archive/011501/fine.html
25. The Economist Intelligence Unit, “E-business Transformation”, 2000
26. International Transport Journal, “Shipbrokers Cautiously Optimistic”, 20/03/2001
27. J. Ricker, D. Munro & D. Hopeman, “XML and EDI: Peaceful Co-Existence”, 2000, http://www.xmls.com/resourches/whitepapers/XMLSolutions_Peaceful_Co-Existence.pdf
28. Y. Shee, Daniel & Tang, Tzung-I, “Modeling the Supply-Demand Interaction in Electronic Commerce”, 2000, http://www.csulb.edu/web/journals/jeer/issues/20002/paper4.htm
29. M. Strobel, “On Auctions as the Negotiation Paradigm of Electronic Markets”, Electronic Markets volume 10 number 2000
30. Κ. Γκιζιάκης, Α. Παπαδόπουλος, Ε. Πλωμαρίτου, “Εισαγωγή στις Ναυλώσεις”, εκδόσεις Σταμούλης, Αθήνα 2002
31. K.C. Laudon, J.P. Laudon, “Management Information Systems”, εκδόσεις Κλειδάριθμος, 2002
32. "E-Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή " Κωνσταντίνος Μουλίνος , Κωνσταντίνα Καμπουράκη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
33. Η προστασία του καταναλωτή ως ασθενέστερου, Η προστασία του ασθενέστερου στο δίκαιο Αλεξανδρίδου Ελίζα (εκδόσεις Σάκκουλα, 1997)
34. Β΄Γνωμοδοτήσεις – Μελέτες «Η πρόταση της οδηγίας της ΕΕ για το ηλεκτρονικό εμπόριο και προστασία του καταναλωτή» Αλεξανδρίδου Ελίζα (περιοδικό «Δίκαιο Επιχειρήσεων & Εταιριών» έτος 6ο, αρ. τεύχους 58, σ. 113)
35. Εισαγωγή στο Δίκαιο του Ηλεκτρονικού Εμπορίου Θεόδωρος Γ. Σιδηρόπουλος (εκδόσεις Αδελφών Κυριακίδη Α.Ε.) α.ε.
36. Ηλεκτρονικό Εμπόριο Αρσένης Πασχόπουλος και Παναγιώτης Σκαλτσάς Εκδόσεις Κλειδάριθμος.
37. The World Wide Web Security FAQ: http://www.w3.org/Security/faq/wwwsf1.html

38. e-Επιχειρείν Πλήρης Οδηγός Ανάλυσης Τεχνικών Και Εμπορικών Θεμάτων Εκδότης Μ. Γκιούρδας 2001 McGraw Hill Companies.
39. Web Commerce Technology Handbook Daniel Minoli –Emma Minoli McGraw Hill Series
40. PC Magazine , "Secure Sockets Layer –SSL 3.0 ", May 26, 1998
41. Pc Magazine, "S/Mime keeps e-mail communication secure-usually", September 1 ,1998
42. PGP FAQ: http://www.cam.ac.uk.pgp.net/pgpnet/pgp-faq/
43. An Overview of SSL : http://www.homeport.org./~adam/ssl.html
44. Cryptography –An Overview : http://www.hack.gr/users/dij/crypto/
45. SHTTP: The Protocol : http://cis.nyu.edu./xiaodong/security/protocol.html
46. Visa Security FAQ: http://www.visa.com/nt/ecomm/faq.html
47. The World Wide Web Security FAQ : http://www.w3.org/Security/faq/wwwsf1.html
48. OECD DEVELOPMENT CENTRE, The policy Challenges of Globalisation and Regionalisation (by C.Oman), 1996
49. OECD Globalisation and Small-and-Medium Enterprises (SMEs), Vol.l and 2, 1997
50. Simon, H,. Hidden Champions: Lessons from 500 of the Worlds Best unknown Companies, Harvard Business School Press, Boston, 1996.
51. Μακρυδάκης Σ., Παπαγιαννάκης Λ. Καλογήρου Γ., το Ελληνικό Μάνατζμεντ: Εξελίξεις, Τάσεις, Προοπτικές, ΕΑΣΕ, 1996.

ΠΑΡΑΡΤΗΜΑ

Πίνακας 1

Ενδοδίκτυα Χρηματοοικονομικής Διοίκησης & Λογιστηρίου	
Οργανισμός	**Εφαρμογή Ενδοδικτύου**
Charles Schwad	Η εφαρμογή αναφορών και ανάλυσης SMART εφοδιάζει τα στελέχη του οργανισμού με μια περιεκτική προβολή των οικονομικών δραστηριοτήτων του, στην οποία περιλαμβάνεται ένα υπόδειγμα αξιολόγησης κινδύνου που βοηθάει τα στελέχη να αξιολογήσουν εννέα κατηγορίες επιχειρηματικών κινδύνων. Το ενδοδίκτυο της SCHWAD περιέχει επίσης και το σύστημα αναφορών γενικού καθολικού FinWeb, μέσω δικτύου σε μορφή εύκολα κατανοητή.
U.S. Department of Argiculture. Rural Development	Το ενδοδίκτυο διαθέτει πληροφορίες για τα προγράμματα δανείων και επιδοτήσεων για μικρές κοινότητες στους 7.200 υπαλλήλους του οργανισμού. Οι υπάλληλοι μπορούν να χρησιμοποιούν φυλλομετρητές Ιστού (Web Browsers) για να εντοπίζουν τα έργα που έχουν χρηματοδοτηθεί σε διάφορες περιοχές.
Pacific Northwest National Laboratory	Το σύστημα αναφορών Ιστού μέσω ενδοδικτύου παρέχει οικονομικές στατιστικές για τις δραστηριότητες του εργαστηρίου, στις οποίες περιλαμβάνονται το τρέχον κόστος που χρεώνεται σε κάθε έργο, ο αριθμός ωρών που αναλώθηκαν σε κάθε έργο από κάθε υπάλληλο και η σύγκριση του πραγματικού κόστους με αυτό που προϋπολογίστηκε. Οι υπάλληλοι του εργαστηρίου μπορούν να πραγματοποιούν και έκτατα ερωτήματα για οικονομικά στοιχεία με τη βοήθεια φυλλομετρητών Ιστού.

Πίνακας 2

Ενδοδίκτυα για τους Ανθρώπινους Πόρους	
Οργανισμός	**Εφαρμογή Ενδοδικτύου**
Sandia National Laboratories	Στο ενδοδίκτυο Tech Web δημοσιεύεται κάθε εβδομάδα ένα ειδησεογραφικό δελτίο και ένας κατάλογος των υπαλλήλων. Το προσωπικό μπορεί να χρησιμοποιεί το δίκτυο για υπολογισμούς χρόνου και εξόδων και επίσης για τη διαχείρις των έργων.
Public Service & Gas Co. of New Jersey	Το προσωπικό μπορεί να χρησιμοποιεί ένα ενδοδίκτυο για να βρίσκει πληροφορίες για τα συνταξιοδοτικά προγράμματα της εταιρίας, να ανατρέχει σε στατιστικές απόδοσης και να ανακατανέμει κεφάλαια στα προγράμματα συνταξιοδότησης αφού μελετήσει τα μοντέλα κατανομής ενεργητικού για να πάρει αποφάσεις. Οι υπάλληλοι έχουν επίσης τη δυνατότητα, μέσω αυτού του δικτύου, να επιλέξουν ένα πρόγραμμα υγειονομικής περίθαλψης, αφού πρώτα δουν αναφορές για τους Υγειονομικούς οργανισμούς που θα τους βοηθήσουν στην επιλογή τους και να διαλέξουν ακόμη και τους γιατρούς τους.
Sun Healthcare	Το ενδοδίκτυο SunWeb περιέχει εικονικές περιηγήσεις των εγκαταστάσεων για τους νέοπροσληφθέντες. Επιπρόσθετα, διαθέτει προγράμματ εκπαίδευσης για το νοσηλευτικό και το υπόλοιπο προσωπικό, που συμπεριλαμβάνουν και videos. Μια τρισδιάστατη φιγούρα με την επωνυμία “Sunny” καθοδηγεί το προσωπικό στις σελίδες του δικτύου και περιγράφει τα διαθέσιμα εκπαιδευτικά προγράμματα.

Πίνακας 3

Ενδοδίκτυα για τις Πωλήσεις & το Μάρκετινγκ	
Οργανισμός	**Εφαρμογή Ενδοδικτύου**
Haworth Inc.	Προσάρμοσε το ERoom, ένα εργαλείο συνεργασίας που βασίζεται στον Παγκόσμιο Ιστό, για την υποστήριξη του προσωπικού πωλήσεών της. Το ERoom περιλαμβάνει τοποθεσίες συνεργασίας, στις οποίες μπορούν να αποθηκεύονται έγγραφα και λογικές ακολουθίες συζητήσεων. Η εταιρία δημιούργησε εικονικούς χώρους εργασίας αποκλειστικά για αναφορές πωλήσεων, ανάπτυξη στρατηγικής πωλήσεων, προβλέψεις πωλήσεων, διεργασίες εξωτερικών πωλήσεων και εκπαίδευση και επιμόρφωση. Το σύστημα διευκολύνει τη συνεργασία μεταξύ πωλητών σε πολλές διαφορετικές χώρες, σε περιπτώσεις πολυεθνικών πελατών.
Case Corp.	Το ενδοδίκτυό της υποστηρίζει τις ομάδες πωλήσεων και μάρκετινγκ με εργαλεία συνεργασίας για διαχείριση επαφών, φόρουμ συζητήσεων, διαχείριση εγγράφων και ημερολόγια.
Marketsmarter LLC	Η εταιρία αναπτύσσει εξειδικευμένες εφαρμογές ενδοδικτύων για προσωπικό μάρκετινγκ και πωλήσεων, οι οποίες βασίζονται σε μια ιδιόκτητη διεργασία που ονομάζεται PRAISE (Purpose, Research, Analyze, Implement, Strategize and Evaluate). Οι εφαρμογές αυτές διευκολύνουν την κοινή χρήση πληροφοριών για τους ανταγωνιστές, για την ανάπτυξη νέων προϊόντων και ερευνητικών εργασιών και περιλαμβάνει δυνατότητες αξιολόγησης αποτελεσμάτων σε πραγματικό χρόνο.

Πίνακας 4

Ενδοδίκτυα στη Βιομηχανική Παραγωγή	
Οργανισμός	**Εφαρμογή Ενδοδικτύου**
Nortel Technologies	Στο ενδοδίκτυο δημοσιεύονται τρισδιάστατα μοντέλα και κινούμενα σχέδια για γρηγορότερη διερεύνηση ιδεών, καλύτερη αναπληροφόρηση και συντομότερους κύκλους ανάπτυξης. Η εφαρμογή μειώνει τα προβλήματα επικοινωνίας μεταξύ των μηχανικών διεργασιών και της μονάδας παραγωγής επειδή τα κινούμενα σχέδια απεικονίζουν τον τρόπο με τον οποίο συναρμολογούνται τα διάφορα εξαρτήματα.
Sony Corporation	Το ενδοδίκτυο παρέχει οικονομικές πληροφορίες στο προσωπικό παραγωγής έτσι ώστε να τα παρακολουθεί και να έχει τη δυνατότητα να προσαρμόζει τη γραμμή παραγωγής ανάλογα με τα αποτελέσματα. Επίσης, στο δίκτυο συμπεριλαμβάνονται δεδομένα μετρήσεων ελέγχου ποιότητας, όπως ελαττώματα και απορρίψεις, καθώς και προγράμματα συντήρησης και εκπαίδευσης.
Duke Power	Το ενδοδίκτυο παρέχει άμεση πρόσβαση σε ένα ηλεκτρονικό εργαλείο για την ανάκτηση σχεδίων κατασκευής εξοπλισμού και προδιαγραφών λειτουργίας, το οποίο επιτρέπει στο προσωπικό να επιθεωρεί κάθε σημαντικό σύστημα της εγκατάστασης σε διάφορα επίπεδα λεπτομέρειας. Διαφορετικά υποσύνολα συστημάτων μπορούν να μορφοποιηθούν μαζί για να δημιουργήσουν μια προβολή ολόκληρου του εξοπλισμού σε έναν ορισμένο χώρο. Οι τεχνικοί συντήρησης, οι μηχανικοί της εγκατάστασης και το προσωπικό λειτουργίας είναι σε θέση να χρησιμοποιούν αυτό το εργαλείο με ελάχιστη εκπαίδευση.