Τ.Ε.Ι. ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο)
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ»

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ :
ΛΑΖΟΣ ΑΛΕΞΑΝΔΡΟΣ Α.Μ:3530
ΛΙΟΝΤΟΣ ΛΑΜΠΡΟΣ Α.Μ:3531

ΠΕΡΙΕΧΟΜΕΝΑ

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ :
ΛΑΖΟΣ ΑΛΕΞΑΝΔΡΟΣ Α.Μ:3530
ΛΙΟΝΤΟΣ ΛΑΜΠΡΟΣ Α.Μ:3531

ΕΙΣΑΓΩΓΗ

Ο αγγλικός όρος “security”, φέρεται να είναι Λατινικής προέλευσης , αφού προέρχεται από της αντίστοιχες λατινικές λέξεις “se” που σημαίνει “χωρίς ” και “cura” που σημαίνει “φροντίδα ”. Δηλαδή η έννοια της ασφάλειας σε ένα σύστημα μπορεί και να ειδωθεί ως μια επιθυμητή ιδιότητα – κατάστασή του , κατά την οποία οι χρήστες του απαλλάσσονται κάθε έγνοιας και φροντίδας ως της τη σωστή λειτουργία του.Παρόλο που ο όρος ασφάλεια φαίνεται να έχει μια προφανή σημασία , χρειάζεται να καταβληθεί σημαντική προσπάθεια προκειμένου να καταγραφεί το ακριβές της νόημα .

Αντικείμενο της εργασίας αυτής είναι η ασφάλεια στο ηλεκτρονικό εμπόριο . Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Εξετάζονται οι κίνδυνοι που πηγάζουν από την αθρόα και απρόσωπη διεξαγωγή συναλλαγών που αφορούν το ηλεκτρονικό εμπόριο .

Στη συνέχεια γίνεται αναφορά στους τρόπους με τους οποίους κάποιος μπορεί να προφυλαχθεί από αυτές τις απειλές που καραδοκούν στο διαδίκτυο . Τέτοιοι τρόποι είναι *η κρυπτογράφηση , οι ψηφιακές υπογραφές , τα ψηφιακά πιστοποιητικά* αλλά και η *χρησιμοποίηση πρωτοκόλλων* όπως το SSL και το SET . Τα τελευταία μάλιστα αποδεικνύονται ιδιαίτερα χρήσιμα στις ηλεκτρονικές πληρωμές .

Το κρισιμότερο σημείο κάθε εμπορικής συναλλαγής είναι η πληρωμή. Εμπόριο χωρίς χρήμα δεν έχει νόημα. Το Internet παρουσιάζει την ιδιομορφία να μην υπάρχει προσωπική επαφή μεταξύ του εμπόρου και του πελάτη, ιδιαίτερα στις λιανικές συναλλαγές. Κατά συνέπεια το θέμα των πληρωμών είναι το σημαντικότερο κομμάτι του ηλεκτρονικού εμπορίου.

Στη συνέχεια γινεται μία αναφορά στα *Firewalls* καθώς και επιχειρείται προσπάθεια ερμηνείας της λειτουργίας τους . Το επόμενο θέμα αφορά την προστασία που είναι δυνατόν να παρασχεθεί σε ένα χρήστη όσον αφορά την *ηλεκτρονική του αλληλογραφία* και τους *ιούς* που κινούνται ανεξέλεγκτα στο διαδίκτυο . Τέλος , ένα αντικείμενο μελέτης της εργασίας αυτής είναι η σχέση του ηλεκτρονικού εμπορίου με *τα προσωπικά δεδομένα* κάθε χρήστη καθώς και ποια θα πρέπει να είναι *η πολιτική ασφάλειας* για την καλύτερη αντιμετώπιση των κινδύνων που πηγάζουν από το ηλεκτρονικό εμπόριο .

Σκοπός της εργασίας μας είναι να προσφέρει μια συνοπτική εικόνα σχετικά με την Ασφάλεια στο Ηλεκτρόνικο Εμπόριο.

ΚΕΦΑΛΑΙΟ 1

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Ο όρος Ηλεκτρονικό Εμπόριο (ΗΕ) χρησιμοποιείται για να περιγράψει την χρήση τηλεπικοινωνιακών μέσων (κυρίως δικτύων) για κάθε είδους εμπορικές συναλλαγές ή επιχειρηματικές δραστηριότητες μεταξύ επιχειρήσεων και ιδιωτών. Με άλλα λόγια, κάθε "εμπορική" δραστηριότητα που πριν από μερικά χρόνια ήταν δυνατή, μόνο χάρη στην φυσική παρουσία και μεσολάβηση ανθρώπων ή υλικών μέσων (π.χ. εμπορική αλληλογραφία), σήμερα μπορεί να επιτευχθεί αυτόματα, ηλεκτρονικά και εξ' αποστάσεως.

Βλέπουμε λοιπόν, ότι το ΗΕ δεν αποτελεί μία και μόνη τεχνολογία. Πρόκειται περισσότερο για ένα συνδυασμό τεχνολογιών ανταλλαγής δεδομένων ,πρόσβασης σε δεδομένα και αυτόματης συλλογής δεδομένων. Το ΗΕ προσπαθεί να αναπτύξει την εκτέλεση των επιχειρησιακών συναλλαγών μέσα από διάφορα δίκτυα. Αυτές οι αναπτύξεις αναφέρονται σε μεγαλύτερη απόδοση (καλύτερη ποιότητα, μεγαλύτερη ικανοποίηση πελατών και καλύτερη λήψη αποφάσεων), μεγαλύτερη οικονομική χρησιμότητα (χαμηλότερο κόστος) και πιο γρήγορες συναλλαγές (μεγάλη ταχύτητα, αλληλεπίδραση πραγματικού χρόνου).

Το όραμα όσων ασχολούνται με το ΗΕ είναι η ομογενοποίηση (χάρη στην εφαρμογή νέων τεχνολογιών) όλων των οικονομικών λειτουργιών των επιχειρήσεων και οργανισμών με τέτοιο τρόπο που κάθε δραστηριότητα να μπορεί :

- **να εκτελείται σε ηλεκτρονική μορφή**
- **να μεταφέρεται εύκολα από τον ένα συναλλασόμενο στον άλλο (π.χ. ένα ψηφιακό τιμολόγιο από τον πωλητή στον αγοραστή)**
- **να είναι προσιτή σε κάθε μέλος της ηλεκτρονικής οικονομικής κοινότητας (π.χ. να μπορεί οποιοσδήποτε να βρει τον τιμοκατάλογο ή τα τεχνικά χαρακτηριστικά των προϊόντων μου άμεσα και με δικές τους ενέργειες, χωρίς να χρειαστεί δική μου μεσολάβηση π.χ. να μου τα ζητήσει και να του τα στείλω).**

Συνοψίζοντας, ένας πιθανός ορισμός του Η.Ε. είναι : "Το Η.Ε. είναι οποιαδήποτε μορφή επιχειρησιακής συναλλαγής, οι συντελεστές της οποίας αλληλεπιδρούν με ηλεκτρονική μορφή περισσότερο παρά με φυσικές συναλλαγές ή διαμέσου φυσικής επικοινωνίας".

1.1 Κίνδυνοι στο Ηλεκτρονικό Έμποριο

Σε ένα συνεχώς διευρυνόμενο μέσο όπως το διαδίκτυο με τα κεφάλαια για επενδύσεις στην ιδέα του ηλεκτρονικού επιχειρείν να ρέουν άφθονα και συνεχώς ,

υπάρχει μεγάλο περιθώριο για κέρδος αλλά και για … χάσιμο . Μέσα σ ’ αυτό το κλίμα , όπου αυξάνονται και οι ευκαιρίες για (ηλεκτρονική) απάτη , οι επιτήδειοι δεν λείπουν ποτέ .

Οι επιθέσεις περιληπτικά

Κατηγορία	Πηγή	Στόχος	Επικινδυνότητα	Κίνδυνοι	Αναμετώπιση
Επιθέσεις σε διακομιστές και εταιρικά δίκτυα	Κράκερ από το Internet	Διακομιστές	Υψηλή	Απώλεια δεδομένων, διακοπή υπηρεσιών	Εγκατάσταση firewall, χρήση κωδικών πρόσβασης, επιτήρηση λογισμικού
Μη εξουσιοδοτημένη πρόσβαση	Τοπικό δίκτυο, Internet	Όλοι οι χρήστες	Υψηλή	Κατάληψη μηχανημάτων, παραβίαση του απορρήτου, μηχανήματα εκτίθενται στο τοπικό δίκτυο	Εγκατάσταση firewall, σειδωτή χρήση των κοινόχρηστων φακέλων και εκτυπωτών, χρήση «καλών» κωδικών
Ιοί, σκουλήκια (worms) και δούρειοι ίπποι (Trojan horses)	Ηλεκτρονική αλληλογραφία, λογισμικά που κατεβάζουμε από το Internet	Όλοι οι χρήστες	Μέτρια έως και υψηλή	Παρακολούθηση ενεργειών, απώλεια δεδομένων	Χρήση «αντιβιοτικών» και firewall
Παρακολούθηση e-mail	Κράκερ από το Internet ή το τοπικό δίκτυο	Όλοι οι χρήστες	Μέτρια έως και υψηλή	Μη εξουσιοδοτημένοι χρήστες μπορούν να διαβάζουν το e-mail από ενδιάμεσους διακομιστές	Κρυπτογράφηση μηνυμάτων, χρήση «καλών» κωδικών, περιορισμός της φυσικής πρόσβασης σε μηχανήματα
Παρακολούθηση πληκτρολόγησης	Δούρειοι ίπποι, χρήστες που έχουν φυσική πρόσβαση στο μηχάνημα	Όλοι οι χρήστες	Υψηλή	Παρακολουθείται οτιδήποτε πληκτρολογείται, έτσι γίνονται γνωστοί διάφοροι κωδικοί πρόσβασης	Χρήση προγραμμάτων για τον εντοπισμό δούρειων ίππων, έλεγχος της φυσικής πρόσβασης

Πίνακας 1.1: Κίνδυνοι στο ηλεκτρονικό εμπόριο

Ένα χαρακτηριστικό παράδειγμα επίθεσης σε διαδικτυακό σύστημα ειναι το παρακάτω:

Η Βρετανικη εταιρία Argos,που πραγματοποιεί πωλήσεις καταλόγου μέσω ταχυδρομείου εγκαινίασε την άνοιξη ιστοσελίδες στο διαδίκτυο(internet) μέσω των οποίων άρχισε να πραγματοποιεί ηλεκτρονικές πωλήσεις.Τον περασμένο Σεπτέμβριο όμως, κινδύνεψε να πληρώσει πολύ ακριβά το πρώτο ‘μάθημα’ στο ηλεκτρονικό εμπόριο.

Ένα λάθος στο πρόγραμμα εμφάνισης των τιμών στο διαδίκτυο,έφερε μια τηλεόραση sony 21 ιντσών αξίας 299,99 λιρών Αγγλίας(περίπου 150000 δρχ.) να πωλείται προς 3 λίρες Αγγλίας (περίπου 1500 δρχ.Το πρόβλημα εντοπίστηκε στην στρογγυλοποίηση του ποσού και στην αποκοπή μετά των 2 μηδενικών όχι από το δεκαδικό μέρος, αλλά από το ακέραιο!

Οι καταναλωτές γρήγορα αντιλήφθησαν την προσφορά και έσπευσαν να προχωρήσουν σε παραγγελίες.Πολλοί μάλιστα προέβησαν σε πολλαπλές παραγγελίες.Μέχρι να αντιληφθούν το λάθος στην εταιρεία Argos , είχαν γίνει εκατοντάδες παραγγελίες συνολικής αξίας περισσοτέρου του 1 εκ. Λιρών (περίπου 500 εκ. Δρχ.)Μάλιστα ένας πελάτης παρήγγειλε 1700 τηλεοράσεις.

Η εταιρεία τελικά αποφάσισε να μήν ικανοποιήσει τις παραγγελίες που έλαβε.Η απόφαση όμως αυτή μπορεί να οδηγήσει σε μια από τις πρώτες υποθέσεις εμπορίου επάνω από το διαδίκτυο,που θα φτάσει στα δικαστήρια.Η Argos ανακοίνωσε ότι για την απόφασή της αυτή συμβουλεύτηκε πρώτα την Αρχή για τον έλεγχο των διαφημίσεων της Αγγλίας και ότι δεν έχει καταρτισθεί σύμβαση μεταξύ εταιρείας και πελάτη,εφόσον η εταιρέια δεν επιβεβαίωσε τις παραγγελίες.

Ο Terry Duddy ,γενικός διευθυντής της εταιρείας,συμπλήρωσε ότι οι σελίδες μας στο διαδίκτυο δέχονται περισσότερες από 100000 επισκέψεις τον μήνα και έχουν καταπληκτικές προσφορές,αλλά όχι για τηλεοράσεις των 1500 δρχ.Προφανώς έγινε ένα λάθος ,το οποίο το διορθώσαμε πολύ γρήγορα.Θα επικοινωνήσουμε προσωπικά με κάθε πελάτη που παρήγγειλε την τηλεόραση για να του ζητήσουμε συγνώμη και να του εξηγήσουμε γιατί δεν μπορούμε να δεχτούμε αυτές τις παραγγελίες.

Παρόλα αυτά ορισμένοι δικηγόροι,που εξέτασαν τις σελίδες της εταιρείας στο διαδίκτυο είπαν ότι δεν υφίσταται προφανής λόγος ούτε υπάρχει σχετική σημείωση της εταιρείας με την οποία να απαλάσσεται από την υποχρέωση να πουλάει τα είδη της στις τιμές που αναγράφει.

Όπως εξηγεί ο δικηγόρος του BBC,Joshua Rozenberg στις σχετικές σελίδες με το θέμα αυτό στο διαδίκτυο η περίπτωση είναι ανάλογη με το εξής:

Ένας καταστηματάρχης βάζει στην βιτρίνα του καταστήματος του μια τηλεόραση προς πώληση και αναρτά και μια ταμπέλα με την τιμή της.Ένας πελάτης βλέπει την τηλεόραση και προτείνει να την αγοράσει.Ο καταστηματάρχης δεν υποχρεούτε να την πωλήσει αν δεν το επιθυμεί.Στην φάση αυτη δεν υπάρχει σύμβαση μεταξύ του καταστηματάρχη και του πελάτη,γιατί ο καταστηματάρχης απλά προσκαλεί τον πελάτη να κάνει μια προσφορά.Συνεπώς ο πελάτης δεν μπορεί να επιμείνει στην πώληση στην προκαθορισμένη τιμή και αν ο καταστηματάρχης έβαλε πολύ χαμηλή τιμή από λάθος,δεν υποχρεούται να πραγματοποιήσει την πώληση.

Όμως,αν μια εταιρεία αποδεχθεί ηλεκτρονικά την πώληση τότε μπορεί να θεωρηθεί ότι υπάρχει σύμβαση.Ο πελάτης που έδωσε στην Argos τον αριθμό της πιστωτικης του κάρτας και έλαβε τον ‘μοναδικό κωδικό παραγγελίας’ ως επιβεβαίωση, μπορεί να θεωρηθεί ότι έχει σύμβαση με την εταιρεία για την πώληση ακόμα και αν η εταιρεία σημειώσει στην επιβεβαίωση οτι ‘ισχύει εφόσον επαρκούν τα αποθέματα’.

Επίσης είναι δυνατόν τα δικαστήρια να θεωρήσουν άκυρη την σύμβαση τη σύμβαση πώλησης εφόσον έχει γίνει πραγματικό λάθος.Σύμφωνα με τον νόμο προστασίας των καταναλωτών της Βρετανίας είναι παράνομο να δίνεται παραπλανητική ένδειξη τιμής στα προιόντα.

Οι καταστηματάρχες μάλιστα μπορεί να τιμωρηθούν με πρόστιμο μέχρι 5000 λίρες για κάθε παραπλανητική ένδειξη τιμής.Αν φτάσει μια υπόθεση για παραπλανητική ένδειξη τιμής στα δικαστήρια, θα πρέπει ο καταστηματάρχης να αποδείξει οτι έδρασε με προσοχή και οτι έλαβε κάθε δυνατή προφύλαξη για να αποφύγει την παραπλάνηση του καταναλωτή.

Η εταιρεία Argos όμως ,αν η υπόθεση αυτή φτάσει τελικά στα δικαστήρια, δεν αρκεί απλά να πει οτι έκανε λάθος.Θα πρέπει να αποδείξει οτι έχει εγκαταστήσει αξιόπιστα συστήματα τα οποία σχεδιάστηκαν έτσι ώστε να αποφεύγονται αυτά τα λάθη.Το γεγονός ότι το Argos δημοσίευσε τις τιμές στο διαδίκτυοκαι όχι σε έντυπο δεν μεταβάλλει καθόλου το γεγονός.Ο νόμος για την προστασία του καταναλωτή δεν επιτρέπει την με ‘οποιονδήποτε τρόπο’ καταχώρηση παραπλανητικών τιμών.

Μένει λοιπόν να δούμε πως θα τελειώσει η υπόθεση αυτή, που αν τελικά φθάσει στα δικαστήρια θα είναι μία από τις πρώτες υποθέσεις ηλεκτρονικού εμπορίου για την οποία θα πρέπει να αποφανθεί η δικαιοσύνη.

1.2 Στόχοι Ασφάλειας στο Ηλεκτρονικό Εμπόριο

- *Εμπιστευτικότητα (confidentiality):* Διασφάλιση της προσπελασιμότητας της πληροφορίας μόνο από όσους έχουν τα απαραίτητα δικαιώματα .

- *Ακεραιότητα (integrity):* Διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής .

- Δ*ιαθεσιμότητα (availability):* Διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται .

- *Έλεγχος αυθεντικότητας (authentication):* Εξακρίβωση της ταυτότητας του χρήστη είτε με passwords είτε με προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers - PIN's) και διάφορα άλλα .

- *Μη αποποίηση της ευθύνης (non – repudiation):* Ολοκλήρωση συναλλαγής όπου κάποιος μετά δεν μπορεί να ισχυρισθεί ότι δεν συμμετείχε σ ' αυτήν .

- *Εξουσιοδότηση (authorization):* Παραχώρηση δικαιωμάτων στο χρήστη από τον Ιδιοκτήτη.

ΚΕΦΑΛΑΙΟ 2

ΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΔΙΑΔΙΚΤΥΟΥ

Το *διαδίκτυο (Internet*), είναι το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων *(internet of internets*) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη . Επιτυγχάνει τη διασύνδεση ετερογενών δικτύων Η /Υ *(INTERnetworking NETworks*). Ο ιδιαίτερος χαρακτήρας του προκύπτει από την ανοχή που διαθέτει σε αναξιόπιστες συνδέσεις . Σχεδιάστηκε έτσι ώστε να υποστηρίζει πολλαπλές συνδέσεις μεταξύ των υπολογιστών με αποτέλεσμα να διατηρεί τη λειτουργικότητά του ακόμα και με κατεστραμμένους κλάδους .

Πραγματικά είναι πολύ σημαντική η ικανότητά του κάθε υπολογιστή να μπορεί να στέλνει μηνύματα στους άλλους ακολουθώντας οποιοδήποτε διαθέσιμο δρόμο και όχι κάποιο σταθερό και προκαθορισμένο .

Η ομάδα πρωτοκόλλων *TCP/IP (Transmission Control Protocol / Internet Protocol*), είναι αυτή που κατά κανόνα χρησιμοποιείται ως η προσυμφωνημένη μέθοδος επικοινωνίας και διαμεταγωγής δεδομένων στο Internet, και η οποία καθιέρωσε τη λογική του «πακέτου »: στον κόμβο του αποστολέα το μήνυμα μετάδοσης τεμαχίζεται σε μικρά τμήματα σταθερού μεγέθους τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου . Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγησή του (όπως πχ . η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο . Στον κόμβο του παραλήπτη τα πακέτα θα συναρμολογηθούν για να σχηματιστεί το αρχικό μήνυμα . Φυσικά η όλη διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο διαδίκτυο έχει και τη δική του διεύθυνση επικοινωνίας *(IP address*).

Με τον τρόπο αυτό , επιτεύχθηκε η δημιουργία *κατανεμημένων δικτύων (distributed networks*) τα οποία δεν εξαρτώνται από ένα κέντρο οργάνωσης – ελέγχου και άρα δεν χρειάζεται να στηρίζονται σε ένα μεμονωμένο κεντρικό υπολογιστή - οικοδεσπότη *(single centralized host*). Το σημείο αυτό , ενοχλητικό για πολλούς , είναι που εξηγεί και την άναρχη δομή του Internet: κάθε υπολογιστής -οικοδεσπότης είναι ομότιμος μέσα στο δίκτυο χωρίς να υπάρχει κεντρική διαχείριση .

Το διαδίκτυο αποτελεί σήμερα τη θεμέλια βάση για την παγκοσμίου κλίμακας επικοινωνία και πρόσβαση απομακρυσμένων πόρων που απολαμβάνουν εκατομμύρια χρήστες υπολογιστών . Τα πλεονεκτήματα που προέκυψαν για την παγκόσμια κοινότητα από τη χρήση του Internet, είναι διαθέσιμα και στις επιχειρήσεις μέσω των *intranets*, δηλαδή των ιδιωτικών δικτύων υπολογιστών που χρησιμοποιούν το λογισμικό και τα πρότυπα του διαδικτύου αλλά δεν προσφέρουν ελεύθερη προσπέλαση σε όλους τους χρήστες .

Ένα *intranet*, χρησιμοποιεί το πρωτόκολλο TCP/IP τόσο για τοπικής εμβέλειας όσο και για ευρείας εμβέλειας μεταφορά πληροφοριών . Χρησιμοποιεί ακόμη τα πρωτόκολλα *HTTP, SMTP* και άλλα «ανοικτά » διαδικτυακά πρότυπα , για να μεταφέρει πληροφορίες ανάμεσα στους πελάτες και τους διανομείς , προσανατολισμένο αυστηρά σε χρήστες που ανήκουν στην επιχείρηση ή έχουν κάποια συνεργασία μαζί της . Στη δικτυακή αρχιτεκτονική μιας τέτοιας επιχείρησης , συνήθως περιλαμβάνεται μια σειρά από υπολογιστές -διανομείς (πχ . *web server, SQL server, application server* και *database* server), οι οποίοι είναι συνδεδεμένοι μεταξύ τους , όχι απαραίτητα μέσω ενός τοπικού δικτύου .

Υπάρχουν όμως ακόμη , θέματα σχετικά με την ασφάλεια στο Internet που κάνουν τους χρήστες να το αποφεύγουν για τη διακίνηση ευαίσθητων δεδομένων . Κλασικό παράδειγμα η εισαγωγή του αριθμού πιστωτικής κάρτας για την προμήθεια αγαθών ή υπηρεσιών μέσω διαδικτύου . Είναι γενικά αποδεκτό ότι ο σημαντικότερος παράγοντας που επηρεάζει τη περαιτέρω διάδοση της χρήσης του Internet, είναι αυτός
της δημιουργίας κλίματος μεγαλύτερης εμπιστοσύνης και αξιοπιστίας σε αυτό .

Σύμφωνα με την επισκόπηση *"Third Annual Ernst & Young/Information Week Information Security Survey*", όπως σημειώνεται στον Ahuja, το 87% αυτών που χρησιμοποιούν το διαδίκτυο , το 66% αυτών που δεν το χρησιμοποιούν ακόμη και το 83% αυτών που σκοπεύουν να συνδεθούν μέσα σε ένα χρόνο , δηλώνουν ότι θα χρησιμοποιούσαν το Internet για εμπορικές συναλλαγές αν διευρυνόταν σημαντικά η παρεχόμενη ασφάλεια του .

2.1 Βασικοί Χειρισμοί ασφαλείας στο Διαδίκτυο

Σε γενικές γραμμές τα πρωτόκολλα του Internet, δίνουν τη δυνατότητα σε ένα τρίτο μέρος να παρέμβει με τους ακόλουθους τρόπους στην επικοινωνία δυο νόμιμων μερών :

- *Κρυφάκουσμα (eavesdropping*): Οι πληροφορίες παραμένουν ανέγγιχτες , αλλά παραβιάζεται η εμπιστευτικότητά τους . Π .χ . η καταγραφή μιας ιδιωτικήςσυζήτησης .

- *Παραποίηση (tampering*): Οι πληροφορίες κατά τη μεταφορά τους μεταβάλλονται ή τροποποιούνται και στη συνέχεια στέλνονται στον αποδέκτη
. Π .χ . η αλλαγή μιας *αίτησης χρήστης (user's request)* ή μιας *απάντησης συστήματος (system's response*).

- *Πλαστοπροσωπία (impersonation*): Οι πληροφορίες πηγαίνουν σε ένα πρόσωπο που παριστάνει το νόμιμο αποδέκτη . Χρησιμοποιείται και ο όρος *προσποίηση (spoofing)* για τη περιγραφή της κατάστασης όπου κάποιος ή κάτι επιχειρεί να φανεί σαν κάποιος ή κάτι άλλο . Π .χ . ένας χρήστης μπορεί να ισχυρίζεται ότι έχει μια συγκεκριμένη διεύθυνση e-mail, ή ένας δικτυακός τόποςμπορεί να αυτό -προσδιορίζεται ως μια συγκεκριμένη *URL (Uniform Resource Locator) διεύθυνση ,* χωρίς τίποτε από αυτά να ισχύει στη πραγματικότητα .

Συνεπώς , οι *χειρισμοί ασφάλειας (security controls)* στο διαδίκτυο κινούνται σε τρεις κυρίως κατευθύνσεις :

- Αρχικά , είναι η προστασία της *ιδιωτικότητας των δεδομένων* με βασικό όπλο τους μηχανισμούς κρυπτογράφησης .

- Στη συνέχεια είναι η προστασία στα επικοινωνούντα μέρη του ενός από το άλλο , δηλαδή του αποστολέα από το παραλήπτη , και αντίστροφα . Αυτό σημαίνει την προστασία της *ακεραιότητας των δεδομένων* από τότε που έφυγαν από τον αποστολέα , αλλά και την *υποστήριξη αδυναμίας απάρνησης ενεργειών* για τα δυο μέρη . Μηχανισμοί σχετικοί με ψηφιακές υπογραφές χρησιμοποιούνται ευρύτατα για τέτοιες λειτουργίες .

- Τέλος , είναι ο *έλεγχος γνησιότητας* της *ταυτότητας* των χρηστών , των προγραμμάτων ή των μηχανημάτων (μέσω κυρίως συνθηματικών και ψηφιακών πιστοποιητικών) καθώς *και* των *εξουσιοδοτήσεων* που διαθέτουν για τη προσπέλαση των προστατευμένων πόρων του συστήματος (μέσω μηχανισμών ελέγχου προσπέλασης).

2.2 Απαιτήσεις και Λειτουργίες Ασφάλειας στο Internet

Πιο αναλυτικά , η *διαχείριση ασφάλειας (security management)* οφείλει να υποστηρίξει τις ακόλουθες *υπηρεσίες ασφάλειας (security services)* γνωστές και ως *λειτουργίες ασφάλειας (security functions):*

- *Εμπιστευτικότητα δεδομένων (data confidentiality):* Η προστασία ενάντια σε μη -εξουσιοδοτημένες αποκαλύψεις πληροφοριών .Η τεχνολογία της *κρυπτογράφησης (encryption* or *cryptography)* είναι σχεδόν συνώνυμη της λειτουργίας αυτής , λόγω του κυρίαρχου ρόλου της . Υπάρχει όμως και μια ειδική κατηγορία απειλών εμπιστευτικότητας που απαιτεί ειδικά μέτρα αντιμετώπισης :

- *Εμπιστευτικότητα ροής δεδομένων (traffic flow confidentiality*): Πολλές φορές όχι το περιεχόμενο , αλλά απλά η ύπαρξη κάποιων μηνυμάτων αποτελεί ευαίσθητη πληροφορία και άρα χρειάζεται προστασία . Και αυτός ο κίνδυνος διαρροής πληροφοριών γίνεται σοβαρότερος στις περιπτώσεις που κάποιος εισβολέας έχει καταφέρει να δημιουργήσει ένα *κρυφό κανάλι (covert channel)* στο δίκτυο , από όπου καταγράφοντας την εμφάνιση σποραδικών bits μπορεί να εξάγει συμπεράσματα σχετικά με την επικοινωνία που παρακολουθεί . Οι απόπειρες υποκλοπής εδώ , εκδηλώνονται με επιθέσεις τύπου *traffic analysis* και μπορούν να εξουδετερωθούν με δυο κυρίως *μεθόδους ελέγχου κίνησης δικτύου (traffic controls*):

1. *Παρεμβολές στη κίνηση (traffic pad*): Ο διαχειριστής ασφάλειας εισάγει «θόρυβο » στο δίκτυο , δηλαδή πλαστά μηνύματα , με σκοπό να διαταραχθεί η κανονική ροή των πληροφοριών και να συγκαλύψει τις πραγματικές ποσότητες στη κυκλοφορία των δεδομένων .
2. *Έλεγχος δρομολόγησης (routing control*): Ο διαχειριστής προσπαθεί να επέμβει ενεργά στη διαδρομή που ακολουθούν τα μηνύματα . Έτσι περιοδικά , καθυστερεί πακέτα δεδομένων , αλλάζει τους ενδιάμεσους κόμβους που επισκέπτονται ή ακόμη και σβήνει ορισμένα (δεν υπάρχει πρόβλημα , αφού το TCP/IP έχει ανοχές αρκετές ώστε να ξαναζητάει από τους διανομείς τα χαμένα πακέτα δεδομένων).

- *Ακεραιότητα δεδομένων (data integrity*): Η δυνατότητα εντοπισμού παραποίησης και ανάκτησης των δεδομένων . Για την προστασία της εγκυρότητας των δεδομένων εκτός της κρυπτογράφησης , χρησιμοποιούνται μηχανισμοί δημιουργίας *περιλήψεων μηνυμάτων (message digests)* και *ψηφιακών υπογραφών (digital signatures).*

- *Αδυναμία απάρνησης (non-repudiation*): Η προστασία από την μη -ανάληψη ευθύνης ενός αποστολέα ότι αυτός έστειλε συγκεκριμένα δεδομένα *(non-repudiation*

of origin), καθώς και από την άρνηση ενός παραλήπτη ότι παρέλαβε κάποια δεδομένα *(non-repudiation of delivery).* Χρησιμοποιούνται οι προαναφερθέντες μηχανισμοί προστασίας ακεραιότητας δεδομένων , μαζί με υποδομές υποστήριξης και διακίνησης *ψηφιακών πιστοποιητικών (X.509 certificates*). *Εποπτείες* ή *Αρχές Πιστοποίησης (Certification Authorities)* αναλαμβάνουν την ευθύνη , ως *τρίτες έμπιστες συμβολαιογραφικές αρχές (3 rd party trusted notaries)* για την δημιουργία κλίματος εμπιστοσύνης στα επικοινωνούντα μέρη .

- *Αναγνώριση και πιστοποίηση (identification and authentication*): Η απαίτηση πληροφοριών πιστοποίησης , οι οποίες διακινούνται συνήθως κρυπτογραφημένα , και οι οποίες μπορούν να επιβεβαιώνουν την ταυτότητα των μερών που επικοινωνούν Ο έλεγχος αυθεντικότητας αφορά δυο διακεκριμένες περιπτώσεις :

- την ταυτότητα των χρηστών *(user* or *entity authentatio*n). Συνήθως συμβαίνει στην αρχή μιας τοπικής σύνδεσης *(local logon)* και οι μηχανισμοί που χρησιμοποιούνται ονομάζονται *πρωτόκολλα αυθεντικότητας(authentication protocols).* Παραδείγματα τέτοιων μηχανισμών είναι η χρήση *αναγνωριστικού και συνθηματικού (user-ID & password), οι τεχνικές πρόκλησης -απόκρισης (challenge-response techniques)* και άλλες μορφές *διαπιστευτηρίων (credentials*).

- την ταυτότητα των συστημάτων ως αφετηρίες – πηγές προέλευσης μηνυμάτων *(origin authentatio*n). Χρησιμοποιείται και ο όρος *πιστοποίηση κατανεμημένων συστημάτων (authentication of distributed systems*). Η λειτουργία αυτή έχει συναφές έργο με την λειτουργία της αδυναμίας απάρνησης αποστολέα *(non-repudiation of origi*n) και συνεπώς στηρίζεται στις μηχανισμούς *ψηφιακών υπογραφών – πιστοποιητικών* και αξιοποίησης *έμπιστων τρίτων μερών (trusted third parties).*

- *Έλεγχος προσπέλασης (access control) και εξουσιοδοτήσεις (authorizations*): Η προστασία ενάντια σε μη -εξουσιοδοτημένη χρήση των πόρων , είτε είναι υλικό (δικτυακό υλικό , μονάδες επεξεργασίας – αποθήκευσης κλπ .), είτε λογισμικό (κώδικας που εκτελείται ή πρόκειται να εκτελεστεί), είτε δεδομένα . Μηχανισμοί όπως οι *λίστες ελέγχου προσπέλασης (Access Control Lists-ACLs)* και οι *ετικέτες ασφάλειας (security labels*), χρησιμοποιούνται για το περιορισμό στη προσπέλαση των πόρων . Γενικότερα , υποστηρίζουν πολιτικές ασφάλειας που παρέχουν μια *πολλαπλών επιπέδων* και διαφοροποιημένη *προσπέλαση πόρων (supporting different levels of resource access)* στους χρήστες ανάλογα με το επίπεδο εμπιστοσύνης που μπορούν να τεκμηριώσουν . Τα *δικαιώματα προσπέλασης (access rights)* είναι οι απαραίτητες πληροφορίες που συσχετίζουν ένα σύστημα πελάτη με ένα σύστημα διανομέα και καθορίζουν αν ο πελάτης θα αποκτήσει συγκεκριμένου τύπου προσπέλαση σε ένα συγκεκριμένο πόρο του διανομέα . Να τονιστεί εδώ , ότι στην περίπτωση του Internet πολύ συχνά και ανάλογα με τη χρονική στιγμή , οι ρόλοι αλλάζουν και ένας διανομέας λειτουργεί προσωρινά ως πελάτης και το αντίστροφο . Οπότε η ασφάλεια πρέπει κάθε φορά να «βλέπει » και προς τις δυο κατευθύνσεις ροής των πληροφοριών .

Επιπλέον σημαντικές παράμετροι για την διαχείριση ασφάλειας στο διαδίκτυο , αποτελούν οι μηχανισμοί :

- *Επίβλεψης (auditing) και υπευθυνότητας (accountability*): Καταγράφουν τις δηλώσεις ταυτότητας και τις ενέργειες των χρηστών (αλλά και των συστημάτων) που αποκτούν πρόσβαση σε προστατευμένους πόρους .

- *Ελέγχου αποδοτικότητας δικτύου (efficiency controls):* Πρόκειται για μηχανισμούς που καταγράφουν και παρακολουθούν τη συνολική απόδοση του συστήματος και την κίνηση του δικτύου , με σκοπό την *αποτροπή καταστάσεων άρνησης εξυπηρέτησης* (*prevention of Denial of Service*).

- *Υποστήριξης συνεργασίας των υπηρεσιών ασφάλειας που προσφέρονται από εφαρμογές (callable security services from applications):* Οι εφαρμογές που εκτελούνται στο διαδίκτυο , διαθέτουν ενδεχομένως χαρακτηριστικά ασφάλειας που πρέπει να μπορούν να κληθούν και να λειτουργούν με ενιαίους τρόπους . Η βασική έννοια της υποστήριξης ενός βασικού πλαισίου συνεργασίας ασφαλών εφαρμογών *(Security Application Program Interface)* προωθείται μέσω των τεχνολογιών *Generic Security Service A*PI, *Generic Cryptographic Service API* και *Generic Audit Service A*PI.

2.3 Επισυμάνσεις-Συμπεράσματα

Η ασφάλεια των πληροφοριακών συστημάτων , ως κλάδος της επιστήμης της Πληροφορικής , έχει αντικείμενο την πρόληψη μη-εξουσιοδοτημένων ενεργειών των χρηστών ενός πληροφοριακού συστήματος καθώς και την ανίχνευση και την κατάλληλη αντίδραση στις περιπτώσεις εκδήλωσής τους . Τα δίκτυα μπορεί να ειδωθούν ως κάποιες περισσότερο σύνθετες περιπτώσεις πληροφοριακών συστημάτων , και έτσι είναι ουσιαστικά οι γνώριμες απειλές εμπιστευτικότητας , ακεραιότητας και διαθεσιμότητας οι οποίες εκδηλώνονται και σε αυτά αλλά με πολύ περισσότερους και διαφορετικούς τρόπους . Σε ένα μάλιστα ανοικτό δικτυακό περιβάλλον , όπως αυτό του Internet, οι κίνδυνοι πολλαπλασιάζονται λόγω της έλλειψης εμπιστοσύνης προς οποιαδήποτε εξωτερική , ως προς το υπό προστασία σύστημα , οντότητα.

Ο τρόπος αντιμετώπισης των προβλημάτων ασφάλειας στηρίζεται σε τρεις θεμελιώδεις αρχές . Σύμφωνα με την "αρχή της ευκολότερης διείσδυσης ", ένας επίδοξος "εισβολέας " θα χρησιμοποιήσει τον ευκολότερο για αυτόν τρόπο επίθεσης . Για αυτό το λόγο όλες οι αδυναμίες ενός πληροφοριακού συστήματος πρέπει να προφυλαχθούν στον ίδιο βαθμό . Ακόμη περισσότερο , πρέπει τα ζητήματα ασφάλειας , από κάθε άποψη , να μελετηθούν και να απαντηθούν ως ένα ενιαίο σύνολο , έτσι ώστε να είναι δυνατή η επίτευξη ενός ομοιόμορφου επιπέδου ασφάλειας σε όλα τα συστατικά μέρη του πληροφοριακού συστήματος ή δικτύου . Σύμφωνα με τη δεύτερη "αρχή της κατάλληλης προστασίας ", τα μέρη ενός συστήματος πρέπει να προστατεύονται πάντα σε ένα βαθμό ανάλογο και συνεπή ως προς την αξία τους .Τέλος , σημαντικό ρόλο διαδραματίζει και η τρίτη "αρχή της αποτελεσματικότητας ", η οποία ορίζει ως προϋποθέσεις αποτελεσματικότητας των μέτρων προστασίας , την ευχρηστία , την επάρκεια και την καταλληλότητά τους , έτσι ώστε αυτά να είναι όντως σε ισχύ όταν εκδηλωθούν τα προβλήματα ασφάλειας .

Στη συνέχεια , θα παρουσιαστούν οι σημαντικότερες από τις διαθέσιμες τεχνολογίες διασφάλισης στο διαδίκτυο , οι οποίες αποτελούν πολύ χρήσιμα εργαλεία υποστήριξης μέτρων προστασίας . Η κατάλληλη διαμόρφωση και εφαρμογή τους , πρέπει να γίνεται πάντοτε με γνώμονα τις θεμελιώδεις προαναφερθείσες αρχές , έτσι ώστε αυτές να οδηγούν στο υψηλότερο δυνατό επίπεδο ασφάλειας .

ΚΕΦΑΛΑΙΟ 3

ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι' αυτό άτομα (*εμπιστευτικότητα*). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (*ακεραιότητα*).

Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (*αυθεντικότητα*). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον Χ. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (*μη αποποίηση ευθύνης*).

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

3.1 Κρυπτογράφηση (Encryption)

Η ανάγκη για εμπιστευτικότητα στις ηλεκτρονικές συναλλαγές ικανοποιείται με την κρυπτογραφηση. Ο αποστολέας, χρησιμοποιώντας συγκεκριμένη μαθηματική συνάρτηση, μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης, έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, ωσότου αποκρυπτογραφηθεί.

Οι διάφορες μέθοδοι κρυπτογράφησης βασίζονται στη χρήση ενός "κλειδιού", ενός μαθηματικού δηλαδή κώδικα - αλγόριθμου, ο οποίος διασφαλίζει το μη "αναγνώσιμο" από τρίτους, και χρησιμοποιείται στην κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε αλγόριθμος παίρνει την ονομασία του από τον αριθμό που μεταλλάσσεται και πρέπει να βρεθεί με μια σειρά μαθηματικών πράξεων.

Αρχικά το κλειδί κρυπτογράφησης ήταν το ίδιο με το κλειδί αποκρυπτογράφησης, δηλαδή αποστολέας και παραλήπτης χρησιμοποιούσαν το ίδιο συμμετρικό κρυπτογραφικό σύστημα (symmetric cryptosystem). Το σύστημα αυτό

χρησιμοποιήθηκε κυρίως σε κλειστά συστήματα και εφαρμόστηκε τη δεκαετία του '80 για τη μεταφορά τραπεζικών δεδομένων. Αργότερα η εξέλιξη οδήγησε στη χρησιμοποίηση δύο κλειδιών, ενός ιδιωτικού και ενός δημόσιου (ασύμμετρο κρυπτογραφικό σύστημα - asymmetric or public key cryptosystem). Το ιδιωτικό κλειδί (private key) χρησιμοποιείται για το σφράγισμα του ηλεκτρονικού μηνύματος και είναι απόρρητο, ενώ το δημόσιο κλειδί (public key) αντιστοιχεί στο πρώτο, χρησιμοποιείται για την αποσφράγιση του μηνύματος και δεν είναι απόρρητο.

Συνεπώς, το πρώτο κλειδί το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο, ενώ το δεύτερο το γνωστοποιεί σε κάθε συναλλασσόμενό του για να μπορεί να αποκρυπτογραφεί/διαβάζει τα μηνύματα του πρώτου.

3.2 Τι είναι η ψηφιακή υπογραφή

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της.

Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!!

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα).

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

3.2.1 Δημιουργία και επαλήθευση ψηφιακής υπογραφής

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

3.2.1.1 Αποστολέας

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

2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

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

3.2.1.2 Παραλήπτης

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

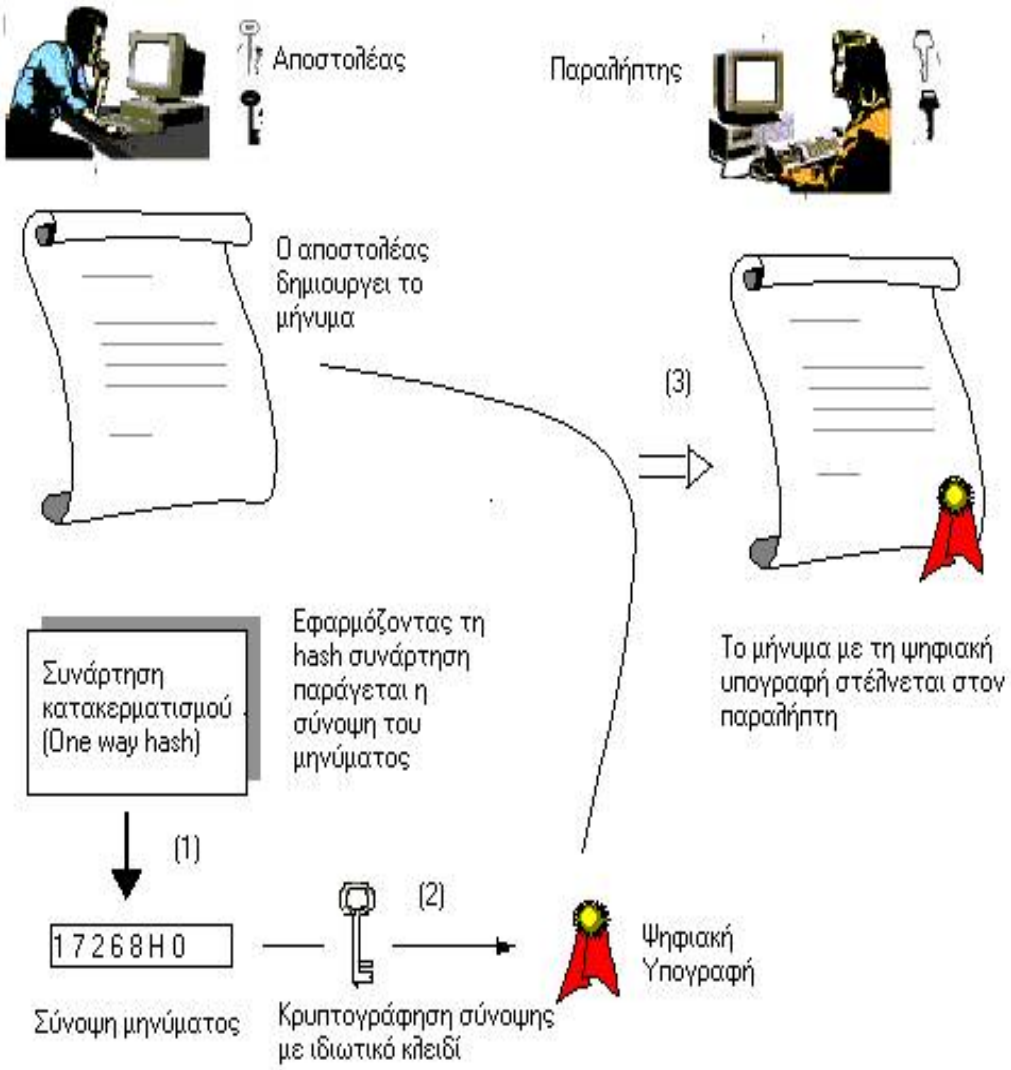
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

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

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

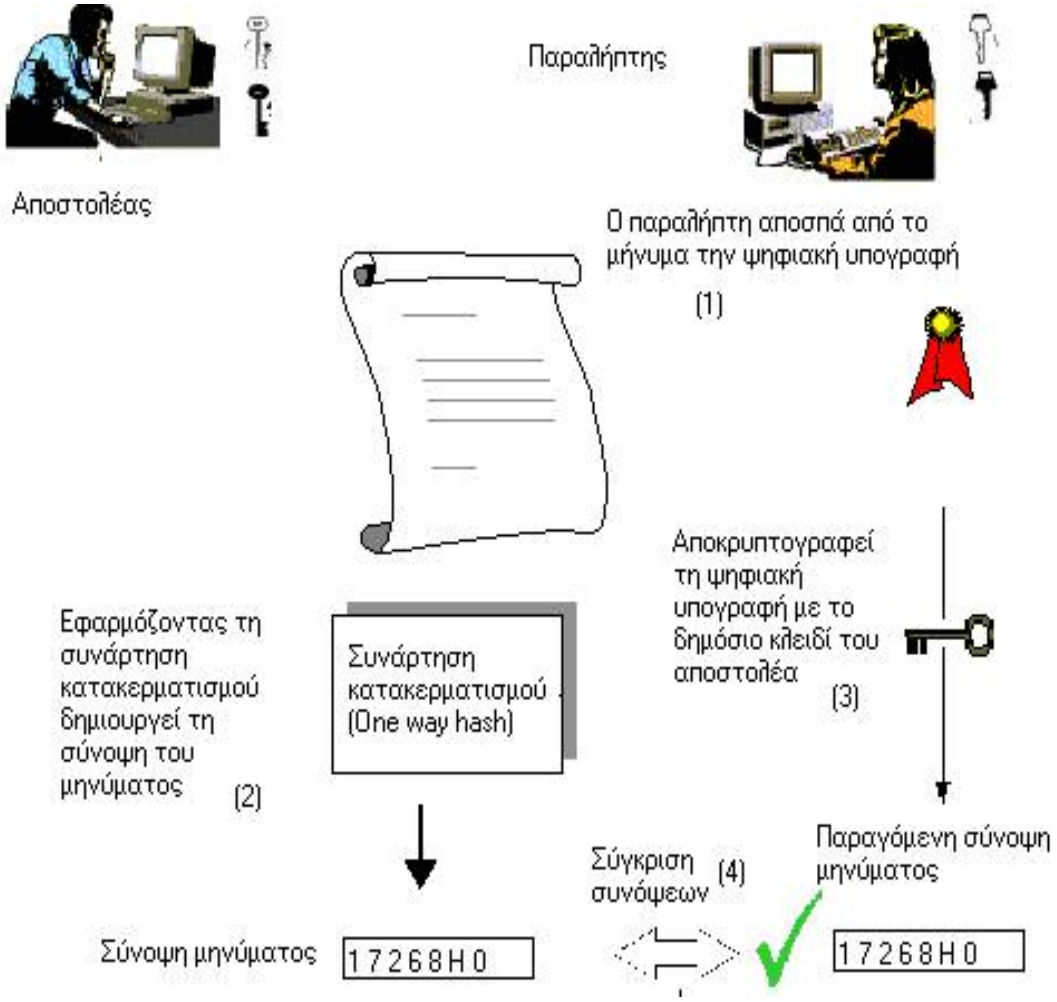
θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.

Δημιουργία ψηφιακής υπογραφής



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

Επαλήθευση ψηφιακής υπογραφής



3.3 Ψηφιακά πιστοποιητικά

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που

ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (*μη αποποίηση*).

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

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

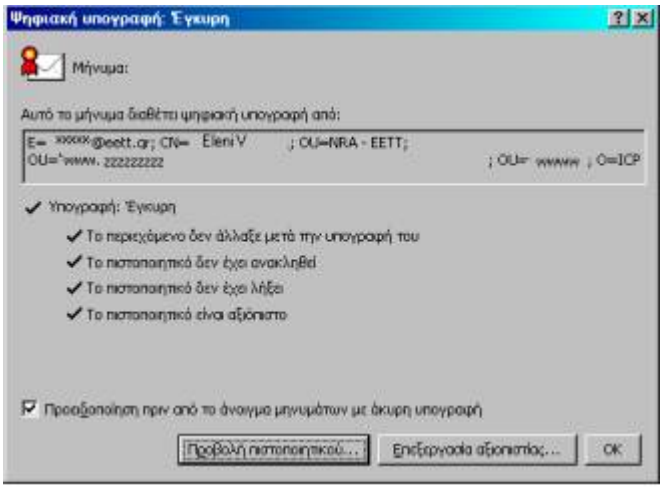
Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο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

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

Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Παράδειγμα προβολής πιστοποιητικού

Ένδειξη ψηφιακής υπογραφής σε μήνυμα με πιστοποιητικό



Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς

τα στοιχεία της ταυτότητάς του κ.λπ), τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.

3.4 Νομικό πλαίσιο ηλεκτρονικών συναλλαγών

ΔΕΝ υπάρχει νομικό κενό

- Οι πωλήσεις μέσω διαδικτύου θεωρούνται πωλήσεις εξ'αποστάσεως.
- Υπάγονται στις διατάξεις του νόμου 2251 της 16 Νοεμβρίου 1994 (Φ.Ε.Κ.: Α191) για την προστασία των καταναλωτών.

Κάθε εξ' αποστάσεως αγορά θεωρείται άκυρη όταν ο καταναλωτής δεν έχει ενημερωθεί για τα παρακάτω:

1. Ταυτότητα προμηθευτή
2. Τα ουσιώδη χαρακτηριστικά του προιόντος
3. Την τιμή,την ποσότητα και τις δαπάνες μεταφοράς
4. Τον τρόπο πληρωμής και παράδοσης
5. Τη διάρκεια ισχύος της πρότασης για σύναψη σύμβασης

Το δικαίωμα υπαναχώρησης

Υπαναχώρηση από τον πελάτη μπορεί να γίνει:

1. Αναιτιολογήτως μέσα σε 10 εργάσιμες ημέρες από την ημερομηνία παραλαβής του αγαθού ή υπηρεσίας αν δεν έχει συμφωνηθεί ΜΕΓΑΛΥΤΕΡΗ διάρκεια υπαναχώρησης
2. Το αγαθό πρέπει να επιστραφεί στην αρχική του κατάσταση με μοναδική επιβάρυνση τα έξοδα επιστροφής.

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΕΙΑ ΣΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΩΜΩΝ

Το κρισιμότερο σημείο κάθε εμπορικής συναλλαγής είναι η πληρωμή. Εμπόριο χωρίς χρήμα δεν έχει νόημα. Το Internet παρουσιάζει την ιδιομορφία να μην υπάρχει προσωπική επαφή μεταξύ του εμπόρου και του πελάτη, ιδιαίτερα στις λιανικές συναλλαγές. Κατά συνέπεια το θέμα των πληρωμών είναι το σημαντικότερο κομμάτι του ηλεκτρονικού εμπορίου.

Το μεγαλύτερο μέρος της παρακάτω συζήτησης θα αναφέρεται κυρίως στις πληρωμές λιανικών πωλήσεων, οι οποίες έχουν και το σημαντικότερο πρόβλημα καθώς τις περισσότερες φορές η επαφή πελάτη-εμπόρου είναι πολύ σπάνια ή και μοναδική (λ.χ. η αγορά ενός ασφαλιστηρίου συμβολαίου από έναν πράκτορα που διαπραγματεύεται πολλές εταιρείες) . Οι πληρωμές του χονδρικού εμπορίου έχουν διαφορετική λογική και άλλα μέσα (λ.χ. εγγυητικές επιστολές, φορτωτικές κλπ) και δεν έχουν τα ίδια προβλήματα.

Η ύπαρξη παραστατικών που τα απαιτούν οι αρχές, κάνει δύσκολη τη δημιουργία νέων κόλπων από κακοπληρωτές ή την διείσδυση νέου τύπου απατεώνων. Αν η κύρια χρήση του δικτυακού σας τόπου είναι το χονδρεμπόριο, τότε λίγα πράγματα θα αλλάξουν από πλευράς πληρωμών. Απλά θα υπάρχει ακόμα ένα κανάλι διανομής στο οποίο η επιχείρηση πρέπει να χρησιμοποιήσει την τακτική της συγκεκριμένης αγοράς.

Δύο πράγματα πάντως θα πρέπει να παρακολουθεί κάποιος. Πρώτον, το θέμα της νομικής υπόστασης της ηλεκτρονικής ανταλλαγής εγγράφων, κατά πόσο δηλαδή είναι δυνατόν να θεωρηθεί κάποιας μορφής ηλεκτρονική ανταλλαγή ως νόμιμο αντίστοιχο λ. χ. του τιμολογίου. Αυτό προσπαθεί να το κάνει η Κοινότητα, οπότε μπορεί να θεσμοθετηθεί απότομα. Το άλλο είναι το γεγονός ότι οι αυτόματες διαδικασίες πολλές φορές είναι δύσκολο να παρακολουθούνται με τους παραδοσιακούς τρόπους γι' αυτό καλό θα ήταν να μελετηθούν προσεκτικά τα πιστωτικά όρια και μετά να αυτοματοποιηθούν.

4.1 Internet Banking

Υπάρχει μία γκάμα πιθανών μεθόδων πληρωμής που χρησιμοποιείται στο Internet. Η πιο συνήθης είναι η χρήση πιστωτικής κάρτας. Δεδομένου ότι αυτή είναι η μόνη ώριμη μέθοδος στην Ελλάδα, θα επικεντρωθούμε σε αυτή. Οι άλλες που υπάρχουν είναι τεχνολογικά ανώριμες ή δεν έχουν φτάσει στην Ελλάδα. Στις τεχνολογικά ανώριμες περιλαμβάνεται το e-cash και σε αυτές που δεν έχουν έρθει στην Ελλάδα περιλαμβάνονται οι ηλεκτρονικές επιταγές. Τέλος η ταχύτητα εξελίξεων

στο διαδίκτυο είναι τέτοια που πάντα θα πρέπει κάποιος να θεωρεί ότι πάντα θα υπάρχουν μέθοδοι πληρωμών που δεν τις ξέρει, άρα θα πρέπει να ψάχνει συνέχεια.

4.2 E-cash

Με αυτή την μέθοδο υπάρχει μία "τράπεζα" εκδίδει "νόμισμα", στην πραγματικότητα ηλεκτρονικές εγγραφές σε υπολογιστές που λέγονται tokens και οι αγοροπωλησίες
γίνονται με ανταλλαγή των tokens. Με άλλα λόγια αγοράζει κάποιος κάτι και μία εγγραφή φεύγει από τον υπολογιστή του και πάει στον υπολογιστή του πωλητή, από όπου μπορεί να φύγει προς ένα τρίτο για μία άλλη συναλλαγή, κοκ. Ο κεντρικός πυρήνας αυτής της τεχνολογίας είναι η κρυπτογραφία ασύμμετρου κλειδιού.

Ουσιαστικά τα tokens είναι ένα είδος λογιστικών εγγραφών που επιβεβαιώνονται από την «εκδοτική αρχή» του «νομίσματος» μέσω της κρυπτογραφικής αυτής μεθόδου. Αυτό τον καιρό είμαστε στον δεύτερο κύκλο προσπαθειών γιά δημιουργία e-cash.
Ο πρώτος απέτυχε κυρίως γιά εμπορικούς λόγους, αλλά και λόγω εχθρότητας των κεντρικών τραπεζών.

Μολονότι το e-cash είναι τεχνικά εφικτό, τα διάφορα γενικότερα προβλήματα που δημιουργούνται είναι τεράστια. Είναι η προβληματικότερη μορφή πληρωμών στο Διαδίκτυο. Τα προβλήματα, εκτός από τα τεχνικά, είναι και γενικότερης κοινωνικής και πολιτικής φύσεως. Για τους ανθρώπους που ασχολούνται παραγωγικά με το ηλεκτρονικό εμπόριο, το μόνο που ενδιαφέρει είναι να παρακολουθούν τις εξελίξεις, καθώς η γενική εντύπωση είναι ότι μόλις αρχίσει να λειτουργεί θα είναι απαραίτητο.

4.3 Ηλεκτρονικές επιταγές

Οι ηλεκτρονικές επιταγές είναι ένα σύστημα ηλεκτρονικών πληρωμών το οποίο χρησιμοποιείται τον τελευταίο καιρό σε χώρες με παράδοση χρήσης επιταγών. Μία επιταγή έχει μία σειρά από νούμερα τα οποία καθιστούν την κάθε επιταγή μοναδική . Ο αγοραστής εισάγει αυτά τα νούμερα, η τράπεζα ειδοποιείται και ακυρώνει την συγκεκριμένη επιταγή, αν το επιτρέπει το υπόλοιπο του λογαριασμού του. Η μέθοδος είναι αποτελεσματική, αλλά μάλλον ακατάλληλη για την Ελλάδα. Δεδομένης της ανυπαρξίας λιανικών συναλλαγών με επιταγή η αξία αυτής της διαδικασίας είναι μάλλον ακαδημαϊκή στην Ελλάδα. Αν όμως έχετε σημαντικό αριθμό πελατών από Αγγλοσαξονικές Κυρίως χώρες, θα πρέπει να μελετήσετε το θέμα προσεκτικά με τελικό στόχο την υλοποίηση.

4.4 Πιστωτικές κάρτες

Ο πλέον διαδεδομένος τρόπος πληρωμής στο internet βασίζεται στο γεγονός ότι το νούμερο της κάρτας είναι μυστικό και όσοι το χρήσιμοποιούν (εστιατόρια, διάφορα μαγαζιά) είναι μέρος του συστήματος ασφαλείας. Δεδομένου ότι είναι ο μόνος τρέχων τρόπος στην Ελλάδα όταν θα αναφερόμαστε στο θέμα της ασφάλειας

πληρωμών θα εννοούμε πληρωμές με πιστωτικές κάρτες, εκτός αν γίνεται ρητή αναφορά σε άλλη μέθοδο. Αυτός ο οποίος αναλαμβάνει την διαδικασία της πληρωμής είναι συνήθως μία τράπεζα. Αν γιά κάποιο λόγο δεν είναι δυνατή η συνεργασία με μία ελληνική τράπεζα τότε κάποιος θα πρέπει να δοκιμάσει μερικούς ειδικούς οργανισμούς πληρωμών όπως το CCBILL ή το IBILL (και τα δύο στις ΗΠΑ) ή κάτι παρόμοιο.

Αυτό ήδη γίνεται από μερικούς τόπους στην Ελλάδα, έχει δε κάποια πλεονεκτήματα όπως της εμπειρίας του οργανισμού, της καλύτερης εξυπηρέτησης λόγω του ανταγωνιστικού διεθνούς περιβάλλοντος αλλά και της διεθνούς εμβέλειας αυτών των εταιρειών. Από την άλλη πλευρά, Θα χρειαστεί πολύ καλή γνώση Αγγλικών, πιθανόν συμβόλαια με χώρα επίλυσης διαφορών τις ΗΠΑ κλπ. Είναι βέβαια θέμα επιλογής της κάθε εταιρείας, αλλά ένα ψάξιμο στο διαδίκτυο αμέσως πριν την απόφαση και μία έστω αρχική επαφή με κάποιους ξένους οργανισμούς πληρωμών είναι μία καλή τακτική κίνηση, ειδικά αν αναμένονται σκληρές διαπραγματεύσεις με την τράπεζα.

4.5 SECURE SOCKET LAYER (SSL)

Αν ο μέσος χρήστης έπρεπε να καταλάβει πώς να χρησιμοποιεί κρυπτογράφηση , ψηφιακά πιστοποιητικά , ψηφιακές υπογραφές κλπ , τότε θα υπήρχαν λίγες ασφαλείς συναλλαγές και συνεπώς θα γίνονταν λίγες αγορές στο Web.
Ευτυχώς , όλα αυτά τα θέματα τα διαχειρίζονται με ένα διαφανή τρόπο τα προγράμματα πλοήγησης και οι Web servers. Αυτό γίνεται κυρίως μέσω ενός ειδικού πρωτοκόλλου , που καλείται **secure socket layer (SSL**), που κρυπτογραφεί επικοινωνίες ανάμεσα σε προγράμματα πλοήγησης και servers.

Κάποια εποχή υπήρχε ένα εναλλακτικό πρωτόκολλο με όνομα S-HTTP . Για αρκετούς λόγους το S-HTTP δεν υποστηρίχτηκε πολύ . Σήμερα , η έκδοση 3.0 του SSL έχει υιοθετηθεί από την Netscape και από την Microsoft.

Το secure socket layer είναι ένα πρωτόκολλο που λειτουργεί στο επίπεδο TCP /IP. Αυτό σημαίνει ότι κάθε εφαρμογή που βασίζεται στο TCP /IP όπως το Web (HTTP), οι ομάδες ειδήσεων UseNet (NNTP), και το e-mail (SMTP) μπορούν να διασφαλιστούν από το SSL. Το secure socket layer υποστηρίζει διάφορους αλγόριθμους κρυπτογράφησης και μεθόδους πιστοποίησης .
Ο συνδυασμός αλγορίθμων και μεθόδων καλείται *σειρά* κρυπτογράφησης . Οταν ένας πελάτης έρχεται σε επαφή με ένα server, οι δύο τους διαπραγματεύονται την σειρά κρυπτογράφησης ,επιλέγοντας την δυνατότερη σειρά που είναι κοινή και για τους δύο . Για ιστοσελίδες ,η διαδικασία διαπραγμάτευσης ξεκινά όταν ο χρήστης κάνει κλικ σε ένα δεσμό , το URL του οποίου αρχίζει με https αντί του http (π .χ ., https:// www.ups.com,/ σε αντίθεση με το http://www.ups.com/). Από εκεί και ύστερα , όλες οι επικοινωνίες τους είναι κρυπτογραφημένες .

4.5.1 Ασφάλεια

Ο μεγαλύτερος κίνδυνος ασφαλείας με το Secure Sockets Layer είναι ότι οι έμποροι που χρησιμοποιούν το πρωτόκολλο πρέπει να κρατήσουν τους servers

ασφαλείς έτσι ώστε οι αριθμοί πιστωτικών καρτών να παραμείνουν ασφαλείς . Κατά συνέπεια ο πελάτης πρέπει να εμπιστευθεί όχι μόνο τον έμπορο και τους υπαλλήλους του , αλλά και την διορατικότητα του τεχνικού στην ασφάλεια υπολογιστών . Η κλοπή 20.000 αριθμών πιστωτικών καρτών από την Netcom στις αρχές της δεκαετίας του '90 διευκρινίζει ότι η επέκταση αυτής της εμπιστοσύνης είναι μια προβληματική πρόταση .

Εάν οι υπάλληλοι ενός εμπόρου είναι ανέντιμοι , οι οργανωτικές διαδικασίες ασφάλειάς του ανεπαρκείς , ή η εγκατάσταση του λογισμικού του ελαττω ματικού , ο καταναλωτής διατρέχει τον κίνδυνο για την απάτη πιστωτικών καρτών .
Ακόμα κι αν ο έμπορος είναι τίμιος , οι υπάλληλοί του μπορούν να παρουσιάσουν ένα πρόβλημα ασφάλειας . Οι επανειλημμένες επιθέσεις είναι εύκολο
να ξεκινήσουν για έναν ανέντιμο υπάλληλο που δεν έχει την πρόσβαση στις πληροφορίες που παρέχονται στον έμπορο .

4.5.2 Μυστικότητα

Το Secure Sockets Layer μπορεί να μην παρέχει οικονομικές υπηρεσίες , αλλά σίγουρα προσφέρει το λογισμικό για να δημιουργήσει κάποιος μια εξασφαλισμένη κρυπτογράφηση για σύνδεση μέσω του διαδικτύου . Η μη απευθείας σύνδεση με τράπεζα είναι ο οικονομικός φορέας παροχής υπηρεσιών , και ο Netscape είναι μόνο ο προμηθευτής λογισμικού ασφάλειας μ ετάδοσης , δεν παρέχει κανένα κρυπτογραφικό πιστοποιητικό και δεν παρέχει καμία έγκριση οικονομικής συναλλαγής .

Ο Netscape δεν λαμβάνει ούτε διατηρεί οποιεσδήποτε πληροφορίες για οποιαδήποτε συναλλαγή που διευθύνεται χρησιμοποιώντας το Secure Sockets Layer. Ο πίνακας 5.1 παρουσιάζει τις διαθέσιμες πληροφορίες για τα διάφορα συμβαλλόμενα μέρη σε μια συναλλαγή που χρησιμοποιεί το Secure Sockets Layer. Η πληροφορία ταυτότητας (identity information) είναι διαθέσιμη όπως άλλωστε φαίνεται στον πίνακα 5.1 διότι τα πιστοποιητικά για την πιστοποίηση του καταναλωτή και του εμπόρου στέλνονται χωρίς κρυπτογράφηση .

	Information				
Party	Merchant	Customer	Date	Amount	Item
Merchant	Full	Full	Full	Full	Full
Customer	Full	Full	Full	Full	Full
Law enforcement with warrant	Full	Full	Full	Full	Full
Netscape	None	None	None	None	None
Bank	Full	Full	Full	None	Full
Observer	Full	Full	Full*	None	None

** Ο παρατηρητής μπορεί να αποφασίσει μόνο όταν η επικοινωνία έγινε μεταξύ εμπόρου και καταναλωτή*

Πίνακας 5.1: Διαθέσιμες πληροφορίες στα συμβαλλόμενα μέρη σε μια συναλλαγή που χρησιμοποιεί SSL

4.5.3 Διοίκηση

Το Secure Sockets Layer φτιάχνει ασφαλείς συνδέσεις μέσω ενός ανοικτού δικτύου . Ο Netscape σαν μία οντότητα δεν έχει καμία πληροφορία για το ποια δεδομένα έχουν περάσει μέσα από μια ασφαλή Sockets σύνδεση , έτσι δεν υπάρχει κεντρική αποθήκη πληροφοριών για διοίκηση .

Σχήματα ασφάλειας υιοθετούνται σε πρωτόκολλα σαν το SSL και το SET. Αυτή η ενότητα εξηγεί το πρωτόκολλο γενικής χρήσης SSL.Επειδή το SET έχει καθοριστεί επάνω στο SSL, η κατανόηση του SSL είναι η βάση για την κατανόηση του SET . Το πρωτόκολλο Secure-HTTP (S-HTTP) εφαρμόζει το SSL ανά μ εσα σε Web servers και σε προγράμματα πλοήγησης , που επικοινωνούν με το πρωτόκολλο HTTP.
Το πρωτόκολλο SSL κάνει ανταλλαγή μηνυμάτων όπως φαίνεται στον Πίνακα 5.2.

Υποθέστε ότι ο αποστολέας είναι η Sally και ο παραλήπτης είναι ο Richard. Τα βήματα της διαδικασίας αντιστοιχούν στους αριθμούς στον Πίνακα 5.2.

1. Στον δικτυακό τόπο της Sally, το μήνυμα προς αποστολή κόβεται στο προηγουμένως σταθερό μήκος για σύνοψη μηνύματος .

2. Η σύνοψη μηνύματος κρυπτογραφείται με το κλειδί ιδιωτικής υπογραφής της Sally χρησιμοποιώντας ένα αλγόριθμο RSA, και η έξοδος είναι μια ψηφιακή υπογραφή .

3. Η ψηφιακή υπογραφή και το πιστοποιητικό της Sally προσαρτώνται στο αρχικό μήνυμα . Στο μεταξύ , ένα μυστικό κλειδί , που χρησιμοποιεί τον αλγόριθμο DES στον υπολογιστή της Sally, κρυπτογραφεί την δέσμη με το κλειδί .

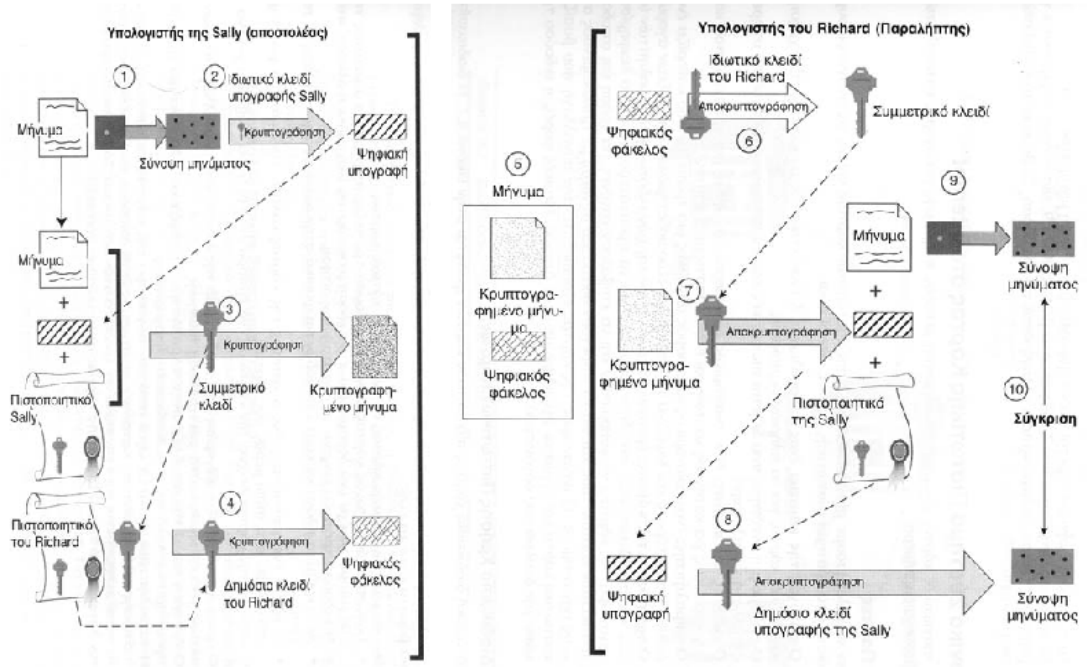
4. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του Richard, που βρίσκεται στο πιστοποιητικό του Richard, το οποίο έχει ληφθεί εκ των προτέρων . Το αποτέλεσμα είναι ένας ψηφιακός φάκελος .

5. Το κρυπτογραφημένο μήνυμα και ο ψηφιακός φάκελος μεταδίδονται στον υπολογιστή του Richard μέσω του Internet.

6. Ο ψηφιακός φάκελος αποκρυπτογραφείται με το ιδιωτικό κλειδί ανταλλαγής του Richard.

7. Χρησιμοποιώντας το επαναφερθέν μυστικό κλειδί , το παραληφθέν μήνυμα αποκρυπτογραφείται στο μήνυμα , στην ψηφιακή υπογραφή και στο πιστοποιητικό της Sally.

8. Για επιβεβαίωση της ακεραιότητας , η ψηφιακή υπογραφή αποκρυπτογραφείται από το δημόσιο κλειδί της Sally (που βρίσκεται στο πιστοποιητικό της Sally), λαμβάνοντας την σύνοψη μηνύματος .



Πίνακας 5.2: Σχήματα ασφαλούς μετάδοσης στα πρωτόκολλα SSL και SET

4.6 SECURE ELECTRONIC TRANSACTIONS (SET)

Το SSL, κάνει δυνατή την κρυπτογράφηση αριθμών πιστωτικών καρτών που στέλνονται από το πρόγραμμα πλοήγησης ενός καταναλωτή στον δικτυακό τόπο ενός εμπόρου . Υπάρχουν όμως πολύ περισσότερα πράγματα όταν γίνεται μια αγορά στο Web από το απλό πέρασμα ενός αριθμού πιστωτικής κάρτας σε ένα έμπορο . Ο αριθμός πρέπει να ελεγχθεί για την εγκυρότητα του , η τράπεζα του καταναλωτή πρέπει να εξουσιοδοτήσει την κάρτα , και πρέπει να γίνει η επεξεργασία της αγοράς .

Το SSL δεν έχει σχεδιαστεί να διαχειρίζεται κανένα από αυτά τα βήματα , πέρα από την μετάδοση του αριθμού της κάρτας . Ένα πρωτόκολλο κρυπτογράφησης που έχει σχεδιαστεί για να χειρίζεται την πλήρη συναλλαγή είναι το **secure electronic transaction (SET**), που έχει αναπτυχθεί από κοινού από τις Visa, Mastercard , Netscape και Microsoft.Το πρωτόκολλο SET παρέχει πιστοποίηση ,εμπιστευτικότητα ακεραιότητα μηνύματος και σύνδεση , βασίζεται σε δημόσια και ιδιωτικά κλειδιά για τον καταναλωτή και τον έμπορο και υποστηρίζει τα παρακάτω χαρακτηριστικά (Stein 1998):

•εγγραφή κατόχου κάρτας

•εγγραφή εμπόρου

•αιτήσεις αγοράς

•εξουσιοδότηση πληρωμής

•σύλληψη πληρωμής

•επιστροφές χρεώσεων

•πιστώσεις

•αντιστροφή πίστωσης

•συναλλαγές χρεωστικής κάρτας

Τα μόνα εμπορικά προϊόντα που παρέχουν σήμερα συναλλαγές SET είναι η εφαρμογή Wallet της Verifone Corporation για καταναλωτές και η επέκταση vPOS για τον Merchant Web Server της Microsoft. Στο μέλλον , τα προγράμματα πλοήγησης της Netscape και της Microsoft θα παρέχουν υποστήριξη για SET.

4.6.1 Ασφάλεια

Η πιο δραματική βελτίωση του Secure Electronic Transaction Protocol πέρα από το πρωτόκολλο διαταγής τηλεφώνων και ταχυδρομείου για Mastercard είναι ότι ο έμπορος παίρνει μόνο αρκετές πληροφορίες για μόνο μια αγορά . Οι έμποροι δεν μπορούν να χρησιμοποιήσουν το Secure Electronic Transaction Protocol για τις επαναλαμβανόμενες επιθέσεις .

Το Secure Electronic Transaction Protocol δεν περιλαμβάνει διαπραγμάτευση ή εξακρίβωση της παράδοσης της πληροφορίας αγαθών . Η μη αποποίηση της ευθύνης έχει περιορισμένη δύναμη όταν η υπόσχεση μπορεί να εξακριβωθεί αλλά η ολοκλήρωση της υπόσχεσης δεν μπορεί .

Η έλλειψη ατομικότητας των αγαθών που διέπει το Secure Electronic Transaction Protocol δημιουργεί εύφορο έδαφος για απάτες . Επίσης το πρωτόκολλο αυτό εμπεριέχει την δυνατότητα χρησιμοποίησης ψευδωνύμου όσον αφορά τον αριθμό λογαριασμού .

Η διεύθυνση του καταναλωτή (customer) και τα δεδομένα παραγγελίας προσφέρονται στους εμπόρους (merchants) σε ένα ξεχωριστό κανάλι από το Secure Electronic Transaction Protocol μέσω των πελατών . Γι ’ αυτό το λόγο αυτή η πληροφορία είναι διαθέσιμη στους παρατηρητές (observers).

4.6.2 Μυστικότητα

Ο Πίνακας 5.3 παρουσιάζει τις διαθέσιμες πληροφορίες σε μια συναλλαγή χρησιμοποιώντας το Secure Electronic Transaction Protocol.Το ασφαλές ηλεκτρονικό πρωτόκολλο συναλλαγής (Secure Electronic Transaction Protocol) παρέχει περισσότερη μυστικότητα από τις τυποποιημένες συναλλαγές πιστωτικών καρτών έξω από το διαδίκτυο , δεδομένου ότι ο πελάτης μπορεί να επιλέξει έναν ψευδώνυμο αριθμό λογαριασμού . Αυτό υπονοεί ότι η ικανότητα για τη χρησιμοποίηση των

ψευδωνύμων χτίζεται στο ασφαλές ηλεκτρονικό πρωτόκολλο συναλλαγής , αν και δεν είναι την συγκεκριμένη στιγμή σαφής .

Σημειώστε ότι το γεγονός ότι οι οικονομικές πληροφορίες είναι κρυμμένες από τον έμπορο αυξάνει την ασφάλεια και όχι την μυστικότητα .Ένας ηλεκτρονικός παρατηρητής μπορεί να λάβει την πλήρη γνώση για μια συναλλαγή χρησιμοποιώντας το ασφαλές ηλεκτρονικό πρωτόκολλο συναλλαγής επειδή τα πιστοποιητικά που περιέχουν τις πληροφορίες ταυτότητας των συμβαλλόμενων μερών συναλλαγής διαβιβάζονται εκτός (in the clear).

	Information				
Party	Merchant	Customer	Date	Amount	Item
Merchant	Full	Partial	Full	Full	Full
Customer	Full	Full	Full	Full	Full
Law enforcement with warrant	Full	Full	Full	Full	Full
Bank	Full	Full	Full	Full	Full
Observer	Full	Full	Full	Full	Full

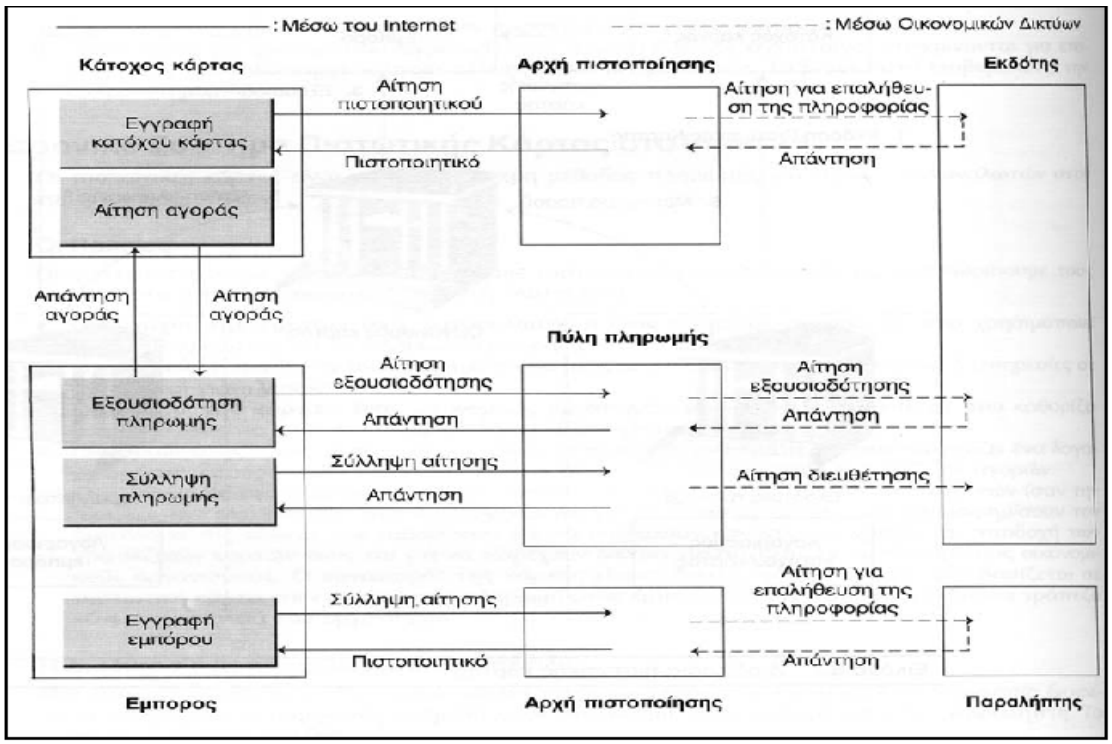
Πίνακας 5.3: Διαθέσιμες πληροφορίες στα συμβαλλόμενα μέρη σε μια συναλλαγή πρωτοκόλλου SET

4.6.3 Διοίκηση

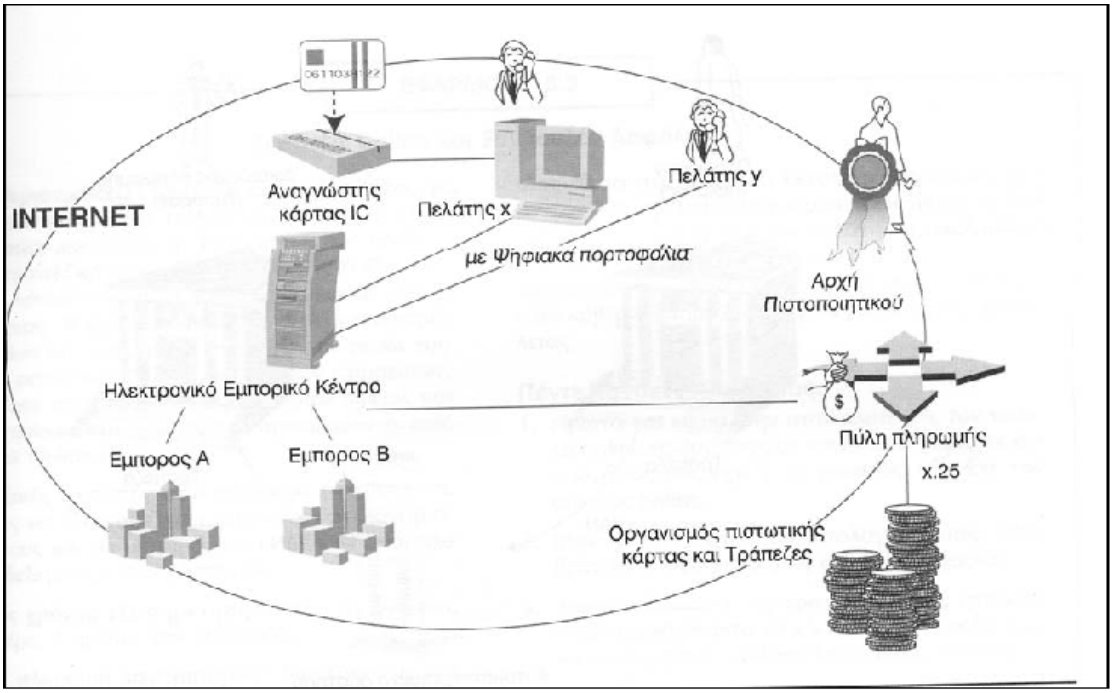
Το Secure Electronic Transaction Protocol είναι ένα ανοικτό πρότυπο που παρέχει όλες τις απαραίτητες πληροφορίες για ρυθμιστικούς λόγους . Το Secure Electronic Transaction Protocol δεν βελτιστοποιείται πρώτιστα για τη μυστικότητα δεδομένου ότι το όνομα και η διεύθυνση του πελάτη απαιτούνται από τον έμπορο για την επαλήθευση . Με τη χρήση των πιστοποιητικών και των δημόσιων κλειδιών , το πλεονέκτημα ασφάλειας που αποκομίζεται με την απαίτηση του συνυπολογισμού τέτοιων πληροφοριών είναι αμφισβητήσιμο για τα στοιχεία που δεν απαιτούν τη φυσική παράδοση . Στην πραγματικότητα , η χρήση ενός πιστοποιητικού με ψευδώνυμο χωρίς τις φυσικές πληροφορίες πελατών δεν θα απαιτούσε καμία αλλαγή στα πρωτόκολλα και θα πρόσφερε μια απέραντη βελτίωση στην καταναλωτική ιδιωτικότητα .

Το *SET* ορίζει την μορφή του μηνύματος , την μορφή του πιστοποιητικού και την διαδικασία της ανταλλαγής μηνύματος , όπως παρουσιάζεται στην Εικόνα 5.4. Στο πρωτόκολλο SET, υπάρχουν τέσσερις οντότητες : κάτοχος κάρτας , έμπορος , αρχή πιστοποίησης (Certificate Authority-CA) και πύλη πληρωμής , όπως φαίνεται στην

Εικόνα 5.5. Οι ρόλοι του εκδότη , του παραλήπτη και του οργανισμού είναι πέρα από τις προδιαγραφές του πρωτοκόλλου S ET . Ο ρόλος της πύλης πληρωμής είναι να συνδέει το Internet με τα ιδιωτικά δίκτυα τραπεζών . Κάθε συμμετέχουσα οντότητα χρειάζεται το δικό της πιστοποιητικό . Για να κρατείται το πιστοποιητικό του καταναλωτή στον προσωπικό του υπολογιστή ή κάρτα (Identification Card-IC), απαιτείται λογισμικό που καλείται **ηλεκτρονικό πορτοφόλι** ή *ψηφιακό πορτοφόλι* . Για να συνδεθεί το ψηφιακό πορτοφόλι με διάφορους εμπόρους , η διαλειτουργικότητα είναι ένα πολύ σημαντικό χαρακτηριστικό που πρέπει να ικανοποιείται .



Πίνακας 5.4: Επισκόπηση των κύριων μηνυμάτων στο SET



Πίνακας 5.5: Οντότητες του πρωτοκόλλου SET στις κυβερνοαγορές

4.7 First Virtual

Η First Virtual (FV) (http://www.fv.com/) υλοποίησε και ανέπτυξε ένα από τα πρώτα ηλεκτρονικά συστήματα πληρωμών , το First Virtual Internet Payment System, τον Οκτώβριο του 1994. Όλως περιέργως , το FV δεν χρησιμοποιεί κρυπτογραφία ή ασφαλή μέσα επικοινωνίας . Αντίθετα μάλιστα , το σύστημα της πληρωμής βασίζεται στην ανταλλαγή e-mail μηνυμάτων και στην εντιμότητα των καταναλωτών .

Το First Virtual παίζει το ρόλο του μεσολαβητή στις συναλλαγές πιστωτικών καρτών μεταξύ καταναλωτών και εμπόρων . Ένας καταναλωτής πρέπει πρώτα να εγκαταστήσει έναν λογαριασμό με FV. Ο λογαριασμός ασφαλίζεται με πιστωτικές κάρτες Visa ή MasterCard. Μετά την υπογραφή με FV, παρέχεται ο καταναλωτής με ένα ψηφιακό κωδικό πρόσβασης (Virtual PIN). Το Virtual PIN παίζει το ρόλο του πληρεξούσιο για το νούμερο της πιστωτικής κάρτας , το οποίο κρατιέται από την FV. Ένα ετήσιο ποσό 2$ χρεώνεται στους καταναλωτές με πιστωτική κάρτα .

Τα πλεονεκτήματα της First Virtual και τα οποία παρέχουν ασφάλεια ενάντια σε απάτες βασίζονται σε τρεις επιχειρηματικές πρακτικές :

•Τα νούμερα της πιστωτικής κάρτας δεν μεταφέρονται ποτέ μέσω Internet

•Επανειλλημένες επιθέσεις δεν είναι πιθανές

•Ένας έμπορος που είναι απλήρωτος για online παράδοση πληροφοριών για αγαθά παθαίνει αμελητέες ζημιές .

Παρ ’ όλα αυτά αν ένας πελάτης που έχει δώσει την ηλεκτρονική του διεύθυνση δεν ζητήσει να αποκλειστεί (excluded) η αθετημένη (default) αξία θα ξαναεπανέλθει για επανάληψη πληρωμής .

4.8 Digicash

Στην Digicash (Chaum 1985), οι καταναλωτές κρατάνε τη νομισματική αξία μέσα σε μία φόρμα ηλεκτρονικών εμβλημάτων (tokens). Καταναλωτές και έμποροι ανταλλάσσουν εμβλήματα (tokens) και αυτά τα εμβλήματα επιβεβαιώνονται από μία τράπεζα . Η τράπεζα επιβεβαιώνει ότι οι υπογραφές πάνω στα εμβλήματα (token) είναι έγκυρες και ότι αυτά τα εμβλήματα (token) δεν έχουν ήδη ξοδευτεί .

Η Digicash παρέχει μόνο ένα μηχανισμό για ηλεκτρονική πληρωμή . Τα πρωτόκολλα της Digicash δεν παρέχουν μηχανισμούς για ανακάλυψη , διαπραγμάτευση , παράδοση ή ανάλυση σύγκρουσης (conflict resolution). Ο σκοπός της Digicash είναι μαζί η δύναμη και η αδυναμία της . Το πλεονέκτημά της είναι ότι παρέχει ένα κομψό και απλό πρωτόκολλο . Το μειονέκτημα της είναι ότι δεν μπορεί να προσφέρει μείωση του κόστους που σχετίζεται με την συλλογή και αμφισβήτηση ανάλυσης .

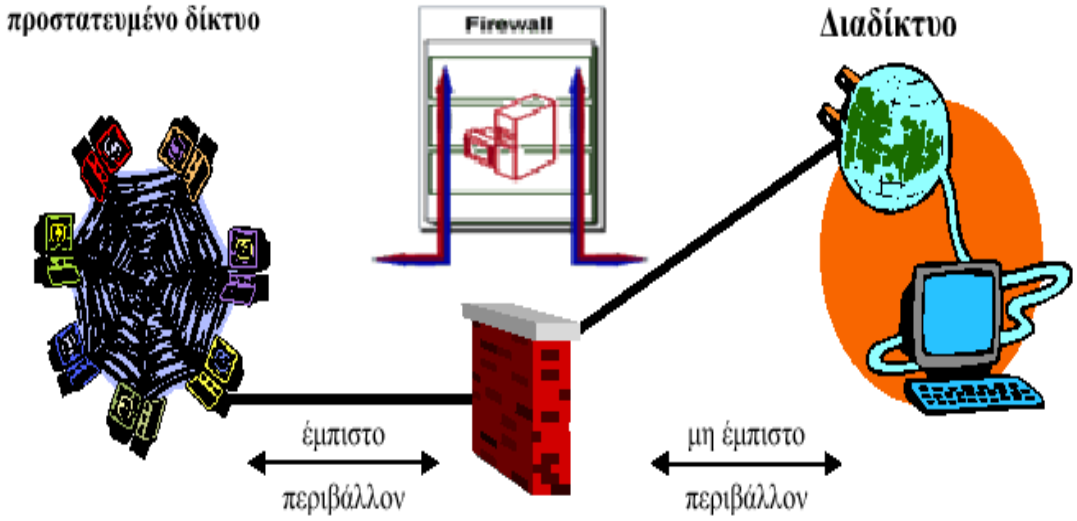
Η Digicash είναι ένα υψηλά ασφαλές σύστημα .Ο έμπορος που σε μια συναλλαγή χρησιμοποιεί Digicash έχει την απαραίτητη πληροφόρηση μόνο για να διασφαλίσει την πληρωμή ενώ η τράπεζα σε μια συναλλαγή έχει την απαραίτητη πληροφόρηση μόνο για να πιστώσει και να χρεώσει ένα λογαριασμό .

ΚΕΦΑΛΑΙΟ 5

ΑΣΦΑΛΕΙΑ ΔΙΑΚΟΜΙΣΤΗ

Ο διακομιστής που συνδέει την εταιρεία κάποιου με το Internet και το Internet με την εταιρεία είναι ένας σταθερός κίνδυνος . Είναι σημαντικό να έχει κάποιος μία σαφή ιδέα ποιοι είναι οι κίνδυνοι που περιβάλλουν τον διακομιστή και τι μέτρα ασφαλείας πρέπει να πάρει για να τον προστατεύσει . Ένα τέτοιο μέτρο είναι τα λεγό μενα φράγματα **firewalls.**

5.1 Τεχνολογίες Firewalls - Περιμετρική ή συνοριακή άμυνα (border defense)



Σχήμα 3.6 - Σύστημα Firewall

Μόλις ένα δίκτυο αποκτήσει σύνδεση στο Internet, ένα κανάλι αμφίδρομης επικοινωνίας ανοίγει :οι χρήστες του δικτύου *(insider*s) αποκτούν επαφή με τον έξω κόσμο αλλά ταυτόχρονα και οι *outsiders,* δηλαδή οι εξωτερικοί χρήστες ως προς αυτό το δίκτυο , αποκτούν πλέον δυνατότητα πρόσβασης . Ο τρομακτικός ρυθμός αύξησης του μεγέθους του διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά *(private*) δίκτυα που συνδέονται μαζί του .

Για τη προστασία τους από παρακολουθήσεις , εισβολές και άλλες διαδικτυακές απειλές απαιτείται ένα κατάλληλο φράγμα . Ο φράκτης αυτός που καλείται *firewall,*

πρέπει να είναι ικανός να αναχαιτίζει όλη τη κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet.

Στη πραγματικότητα ένα σύστημα firewall ανορθώνει ένα εξωτερικό τοίχο ασφάλειας , οριοθετώντας μια περίμετρο προστασίας . Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο εσωτερικό δίκτυο ενός οργανισμού (το οποίο θεωρείται ασφαλές και έμπιστο) και στο εξωτερικό διαδίκτυο (το οποίο θεωρείται μη ασφαλές και μη έμπιστο).

Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο διαδίκτυο και στο υπό προστασία δίκτυο , επιτρέπει τη προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο , μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά .Έτσι ένα τυπικό σύστημα firewall μπορεί να επιτρέπει επιλεκτικά τη πρόσβαση στους εξωτερικούς χρήστες , βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε *ονόματα επικρατειών (domain names).*

Αυτός είναι ο κύριος σκοπός του : να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευμένο περιβάλλον . Επιπλέον , είναι σε θέση να ρυθμίσει και τις παρεχόμενες διαδικτυακές υπηρεσίες για τους εσωτερικούς χρήστες . Για τη λειτουργία του αυτή δεν εξετάζει μόνο χαρακτηριστικά των χρηστών , αλλά και στοιχεία σχετικά με το προορισμό των αιτήσεων προσπέλασής τους . Ένα σύστημα λοιπόν firewall έχει σαν στόχο να ελέγχει και να καταγράφει τη πρόσβαση σε προστατευμένες υπηρεσίες , που προέρχονται και από το εσωτερικό και από το εξωτερικό του δικτύου ενός οργανισμού , με το να επιτρέπει , να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του .

Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μ ηχανισμών που ο ένας μπλοκάρει τη κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή τους . Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της *πολιτικής (policy*) ελέγχου που αυτό υποστηρίζει και εξαρτάται από τη διαμόρφωσή του *(firewall configuratio*n). Πραγματικά , ένα σύστημα firewall δεν είναι απλά ένας *δρο μολογητής (route*r), ένας *διανομέας* ή *διακομ ιστής* ή εξυπηρετητής *(serve*r), ένας *οικοδεσπότης (hos*t) ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα .

Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη έμπιστες επικράτειες . Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων *(network access control policy)* γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, όπου αποτελούν αντικείμενο εξέτασης και καταγραφής .

5.2 Γιατί είναι αναγκαία τα firewalls

Όταν τοπικά δίκτυα *(local network*s) συνδέονται στο Internet, αποτελεί ζήτημα μεγάλης σημασίας η διασφάλιση της κανονικής λειτουργίας τους από τους νόμιμους και παράνομους χρήστες τους . Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο ενός οργανισμού και το διαδίκτυο , εγκαθιστά δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη διαδικτυακή σύνδεση *(internet lin*k) προστατεύοντας στον οργανισμό :

• τους πόρους του (υλικό , λογισμικό , δεδομένα) από φθορά , κατάχρηση , κλοπή και κατάχρηση .

• την υπόληψή του από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου του .

• την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του διαδικτύου από τους εργαζομένους του .

Ο πιο συνηθισμένος πάντως λόγος ύπαρξης ενός συστήματος firewall σε έναν οργανισμό είναι η παροχή ενός μηχανισμού *ελέγχου προσπέλασης (access contro*l), πρώτου επιπέδου , για τον *Web Serve*r. Ένα *firewall* πρέπει να ελέγχει και να καταγράφει την ροή των επικοινωνιών που διέρχονται μέσα από τον *διακομ ιστή We*b.Δηλαδή πρέπει να παρεμβάλλεται και να αποκόβει όλη την κίνηση των δεδομένων ανάμεσα στον *Web server* και το Internet. Έτσι είναι σε θέση να προστατεύει τα δεδομένα που δημοσιεύονται από ανεπιθύμητες αλλαγές και να ελέγχει τη πρόσβαση στον διακομιστή Web, αποκλείοντας τους μη εξουσιοδοτημένους χρήστες από ευαίσθητους πόρους του δικτύου .

Ακόμη , ένας οργανισμός μπορεί να χρησιμοποιήσει ένα firewall για να απομονώσει τις επικοινωνίες ανάμεσα στα δίκτυα των επιμέρους τμημάτων του . Για παράδειγμα ένα νοσοκομείο ενδεχομένως να θελήσει να διαχωρίσει το δίκτυο διακίνησης των δεδομένων των ασθενών από το δίκτυο των οικονομικών στοιχείων του . Ένα ή περισσότερα firewalls *(intranet firewalls)* μπορούν να χρησιμοποιηθούν για να παρέχουν απομόνωση και ελεγχόμενη προσπέλαση ανάμεσα στα διάφορα μέρη ενός οργανισμού .

Ένα σύστημα firewall λοιπόν μπορεί να αποτελέσει μια διάταξη δρομολόγησης *(route*r), ένας προσωπικός υπολογιστής , ένας διακομιστής , ή ένα σύνολο από διακομιστές , διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία *(site*) ή ένα υποδίκτυο *(subne*t) από πρωτόκολλα και υπηρεσίες (πχ . υπηρεσίες FTP, HTTP, e-mail κλπ .) οι οποίες μπορούν να προσβληθούν από διακομιστές εκτός του υποδικτύου . Η συνηθισμένη θέση του είναι ως πύλη υψηλού επιπέδου ακριβώς στο σημείο σύνδεσης ενός οργανισμού με το Internet. Όπως όμως έχει ήδη αναφερθεί , μπορεί να τοποθετηθούν και ως πύλες χαμηλότερων επιπέδων πρόσβασης , με σκοπό τη προστασία επιμέρους τμημάτων ενός υποδικτύου .

5.3 Πλεονεκτήματα και περιορισμοί από τη χρήση firewalls

Ένα firewall σε λειτουργία , δεν είναι ένα απλό συστατικό του δικτύου αλλά αποτελεί την υλοποίηση μιας στρατηγικής για την προστασία των συνδεδεμένων στο διαδίκτυο πόρων ενός οργανισμού . Εξασφαλίζει ότι όλες οι επικοινωνίες από και προς το Internet είναι σύμφωνες με την προκαθορισμένη πολιτική ασφάλειας του οργανισμού. Πρόκειται για την πρώτη και σημαντικότερη ωφέλεια . Όμως σπουδαίες είναι και οι υπόλοιπες επιμέρους ωφέλειες που παρέχει ένα σύστημ α firewall. Αναλυτικά :

• Επιτρέπει αποτελεσματικά την *υλοποίηση* και *διαχείριση* μέρους της *πολιτικής*

*ασφάλειας (policy enforcemen*t) που θέλουμε να εφαρμόσουμε στο σύστημά μας . Η διαμόρφωση παραμετροποίηση που υποστηρίζει μας βοηθά να ορίσουμε ποιος χρήστης θα έχει πρόσβαση σε ποιο πόρο . Παράλληλα μέσω των διαθέσιμων εργαλείων του για καταγραφή και επίβλεψη , έχουμε μια πλήρη εικόνα των προσπαθειών (επιτυχών και ανεπιτυχών) σύνδεσης η οποία θα χρησιμεύσει στη συντήρηση ή και μετατροπή της πολιτικής ασφάλειας ειδικότερα πάνω σε χρήστες με «ύποπτη » συμπεριφορά . Χωρίς firewalls, η εφαρμογή της πολιτικής εξαρτάται από τη διάθεση συνεργασίας των χρηστών , αφού η ασφάλεια ενός δικτύου αντιμετωπίζεται ξεχωριστά από το κάθε τμήμα του . Βέβαια , η ασφάλεια ενός οργανισμού λίγο πολύ εξαρτάται από τους χρήστες του και τη συμμόρφωσή τους στους προβλεπόμενους κανόνες , αλλά με κανένα τρόπο δεν πρέπει να εξαρτάται από τους εξωτερικούς χρήστες του διαδικτύου .

• *Προστατεύει από ευπαθείς υπηρεσίες δικτύων (protecting from vulnerable services*). Είναι γνωστό ότι τα πρωτόκολλα επικοινωνίας του διαδικτύου παρουσιάζουν εγγενή προβλήματα ασφάλειας . Η εγκαθίδρυση ενός συστήματος firewall προσφέρει δυνατότητες φιλτραρίσματος που ελαχιστοποιούν τους κινδύνους . Ακόμη μπορεί και καλύπτει γνωστές ρωγμές ασφαλείας (όπως οι επιθέσεις αδυναμίας εξυπηρέτησης) στο κατώτερο επίπεδο των λειτουργικών συστημάτων . Έτσι , κάποια αδύνατα σημεία για την ασφάλεια του δικτύου , που έχουν ήδη εκμεταλλευτεί διάφοροι βάνδαλοι , έρχεται να προστατέψει και να οχυρώσει το firewall.

• Αποτελεί μέσο *καταγραφής* και *δημ ιουργίας στατιστικών στοιχείων* για τη *χρήση και κατάχρηση του δικτύου (logging-alarming & statistics of network use/misuse*). Πρόκειται για πολύτιμες πληροφορίες που λόγω της θέσης του firewall ως το μοναδικό σημείο σύνδεσης με το έξω δίκτυο , είναι ακριβείς και αξιόπιστες . Η χρησιμότητά τους είναι μεγάλη . Τεκμηριώνουν την ικανότητα ή όχι του ίδιου του firewall για αποτροπή των επιθέσεων που συνέβησαν και κρίνουν την καταλληλότητα της πολιτικής ασφάλειας που εφαρμόζεται . Επιπλέον , τα στατιστικά χρήσης του δικτύου είναι χρήσιμα και στις διαδικασίες *ανάλυσης επικινδυνότητας (risk analysis)* και *ανάλυσης απαιτήσεων δικτύου (network requirement analysis*). Ένα firewall μπορεί ακόμη με τις δυνατότητες επεξεργασίας των πληροφοριών αυτών που διαθέτει , να εντοπίσει ύποπτες δραστηριότητες και να αντιδράσει με προαποφασισμένες ενέργειες όπως το κλείσιμο της σύνδεσης ή η ενημέρωση του διαχειριστή ασφάλειας με e-mail.

• Επιβάλλει *ελεγχόμενη προσπέλαση (controlled access)* στους πόρους ενός εσωτερικού δικτύου . Για παράδειγμα , κάποιοι διακομιστές ενδέχεται να προσφέρονται για επικοινωνία με το Internet, ενώ άλλοι όχι .

• Προσφέρει *διευρυμένη ιδιωτικότητα (enhanced privac*y). Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου . Έτσι , οι εξωτερικοί εισβολείς *(intruder*s) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν » από τα όρια χρήσης του δικτύου που εμείς τους ορίσαμε . Γενικότερα , υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς , περιέχουν σημαντικά στοιχεία για έναν επιδέξιο χρήστη που θέλει να επιχειρήσει επίθεση . Έτσι , μέσω του firewall, πολλοί οργανισμοί σταματούν υπηρεσίες όπως η *Finger* και η *DNS (Domain Name Servic*e). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου , όπως το πότε συνδέθηκαν

για τελευταία φορά , αν διαβάσανε το ηλεκτρονικό τους ταχυδρομείο κλπ . Έτσι όμως διαρρέουν πληροφορίες στους εισβολείς σχετικές με το πόσο συχνά ένα σύστημα χρησιμοποιείται ή αν εκείνη τη στιγμή υπάρχουν συνδεδεμένοι ενεργοί χρήστες . Η υπηρεσία DNS από την άλλη , παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος , όπως τα ονόματα των τόπων και οι IP διευθύνσεις του . Η μη δημοσιοποίησή τους στο διαδίκτυο , αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα επιβουλεύονται .

• *Συγκεντρώνει υπηρεσίες ασφάλειας* σε μια καλά ορισμένη και οχυρωμένη περιοχή *(concentrated security).* Ελαχιστοποιεί τη ζώνη κινδύνου *(zone ris*k) ενός οργανισμού εφόσον η ευρεία περιοχή των μηχανημάτων του παύει να απειλείται άμεσα . Ουσιαστικά το ίδιο το firewall αποτελεί τη μοναδική ζώνη κινδύνου για τον οργανισμό . Άμεση συνέπεια του γεγονότος αυτού , είναι η ευκολία διαχείρισης ασφάλειας και γενικότερα μια οικονομία κλίμακας αφού δεν χρειάζεται κάθε φορά που χρειάζονται ρυθμίσεις επειδή κάτι αλλάζει στο λογισμικό των εφαρμογών ή της ασφάλειας , να απαιτούνται επεμβάσεις σε όλους τους διακομιστές . Η ενημέρωση συντήρηση αφορά κυρίως το σύστημα firewall. Για παράδειγμα η εγκατάσταση πρόσθετου λογισμικού πιστοποίησης (όπως τα συστήματα συνθηματικών μιας χρήσης "authentication using one-time password systems"), δεν χρειάζεται να γίνει σε κάθε διακομιστή ξεχωριστά , αλλά να γίνει μια φορά στο firewall.

• Αρκετά σύγχρονα συστήματα firewall προσφέρουν ως μια επιπλέον λειτουργία τους και τις υπηρεσίες τους ως *πύλες κρυπτογράφησης (encrypting gateways*). Δηλαδή έχουν ταυτόχρονα δυνατότητες *κρυπτογράφησης* στις επικοινωνίες μεταξύ των διακομιστών που προστατεύουν . Ακόμη και εξωτερικά συστήματα μπορούν να συνομιλήσουν σε κρυπτογραφημένη μορφή , αρκεί να εγκαταστήσουν το ανάλογο λογισμικό πελάτη και να παρουσιάσουν τα σχετικά διαπιστευτήρια που προέρχονται από το διαχειριστή του firewall. Ένας τέτοιος λογικός διαχωρισμός των δικτύων μέσω firewalls και τεχνικών κρυπτογράφησης δημιουργεί τα λεγόμενα *εικονικά ιδιωτικά δίκτυα (VPN – Virtual Private Networks).* Η κρυπτογράφηση μπορεί να είναι επιλεκτική , ανάλογα με την αιτούμενη από το διαδίκτυο υπηρεσία και η διαχείρισή της είναι ενσωματωμένη με τα υπόλοιπα χαρακτηριστικά του firewall, έτσι ώστε να είναι δυνατή η εκμετάλλευση όλων των βοηθημάτων που υποστηρίζονται για την κατασκευή των κανόνων ελέγχου προσπέλασης , την καταγραφή παρακολούθηση των ενεργειών κλπ .

Τα συστήματα firewalls δεν αποτελούν πανάκεια για τα προβλήματα ασφάλειας στο διαδίκτυο .Υπάρχουν κίνδυνοι που ξεφεύγουν από τις δυνατότητές τους :

1. Δεν προστατεύουν από τους εσωτερικούς χρήστες (πχ . από τους υπάλληλους του οργανισμού). Εφόσον ένα εσωτερικό μηχάνημα μπορεί να επικοινωνήσει με ένα άλλο , κάνοντας χρήση πρωτοκόλλου Internet, χωρίς να «περάσει » μέσα από το firewall, οποιαδήποτε ζημιά μπορεί να προκληθεί χωρίς να γίνει αντιληπτό από αυτό . Απαιτούνται επιπλέον μηχανισμοί πιστοποίησης και ελέγχου προσπέλασης για τους χρήστες και τις δραστηριότητες των συστημάτων τους .Φυσικά , τα intranet firewalls ελαχιστοποιούν ανάλογους κινδύνους ,παρακολουθώντας την κυκλοφορία ανάμεσα στα διάφορα τμήματα ενός οργανισμού .

2. Μπορούν να προστατεύσουν ένα περιβάλλον , μόνον όταν ελέγχουν πλήρως την περίμετρό του . Δηλαδή δεν πρέπει να υπάρχουν συνδέσεις (πχ . μέσω modem) που να μην διοχετεύονται μέσω του firewall. Έστω και αν ένας εσωτερικός διακομιστής αποκτήσει τέτοια εξωτερική σύνδεση , ολόκληρο το εσωτερικό δίκτυο τίθεται σε κίνδυνο .

3. Δεν είναι εντελώς άτρωτα , μπορούν να διαπεραστούν . Οι κατασκευαστές των συστημάτων firewalls τα κρατούν μικρά και απλά έτσι ώστε ο πιθανός εισβολέας να μην αποκτήσει στη συνέχεια τον έλεγχο επικίνδυνων εργαλείων όπως τα *προγράμματα μεταγλώττισης (compiler*s), τα *προγράμματα σύνδεσης (linkers)* κλπ . Όμως σε καμιά περίπτωση δεν πρέπει να θεωρείται ότι είναι ικανά μόνα τους να εξασφαλίσουν την απόκρουση όλων των εξωτερικών επιθέσεων . Πρέπει να θεωρούνται απλώς σαν μια ισχυρή πρώτη γραμμή άμυνας .

4. Αποτελούν για έναν οργανισμό , το πιο ορατό σημείο του προς τον έξω κόσμο .Έτσι μοιραία είναι και ο πιο ελκυστικός στόχος επίθεσης . Απαραίτητη λοιπόν και πάλι η οργάνωση άμυνας εις βάθος , με επιπλέον επίπεδα προστασίας .

5. Διαθέτουν από περιορισμένο έως ελάχιστο έλεγχο πάνω στο περιεχόμενο των εισερχομένων μηνυμάτων . Έτσι σε επιθέσεις όπως αυτές των ιών και παρόμοιου επικίνδυνου κώδικα χρειάζονται επιπλέον μέτρα προστασίας .

6. Απαιτούν σωστή εγκατάσταση , προσεκτικές ρυθμίσεις και συνεχείς ενημερώσεις στη διαμόρφωσή τους ανάλογα με τις αλλαγές που παρουσιάζουν το εσωτερικό δίκτυο και οι συνδέσεις τους με τον έξω κόσμο . Ακόμη πρέπει να μελετώνται οι εγγραφές των αρχείων καταγραφής για τον έλεγχο της απόδοσής τους και για τον εντοπισμό πιθανών δυσλειτουργιών τους . Αλλιώς δημιουργείται μια εσφαλμένη αίσθηση ασφάλειας με αποτέλεσμα μια σχετικά εύκολη διείσδυση να αφήνει απροστάτευτους τους θεωρούμενους ασφαλείς εσωτερικούς πόρους .

5.4 Αποδεκτή λειτουργικότητα στα συστήματα firewalls

Ένα σύστημα firewall θα πρέπει να ικανοποιεί τις ακόλουθες προϋποθέσεις :

- Να απορρίπτει κάθε πακέτο που ρητά κάποιος κανόνας δεν το επιτρέπει . Είναι η *εξ ' ορισμού (default*) άλλωστε ρύθμιση για τα περισσότερα firewalls, και επιβάλλει στο διαχειριστή τους να διευκρινίσει ποιες ακριβώς επικοινωνίες είναι αποδεκτές .

- Να κρατάει τους εξωτερικούς χρήστες έξω από το προστατευμένο δίκτυο . Αν για παράδειγμα πρέπει κάποια αρχεία να γίνουν προσιτά μέσω διαδικτύου , τότετο πιο σίγουρο – αλλά όχι και απαραίτητο – είναι αυτά να τοποθετηθούν έξω από

το firewall. Εναλλακτικά απαιτούνται ισχυροί μηχανισμοί *πιστοποίησης (authentatio*n) σε επίπεδο εφαρμογών πια , για την παρεμπόδιση των μη εξουσιοδοτημένων χρηστών .

- Να διαθέτει προηγμένα εργαλεία καταγραφής , επίβλεψης και *πρόκλησης συναγερμού (alarm generation),* ικανά να δημιουργούν και να αναλύουν τις πραγματοποιημένες συναλλαγές με σκοπό την εξαγωγή συμπερασμάτων σχετικά με το είδος και τη φύση των επιθέσεων και τη συνακόλουθη προσαρμογή της υφιστάμενης πολιτικής ασφάλειας .

Συνοπτικά , ένα firewall πρέπει να είναι ικανό να προσφέρει υπηρεσίες ασφάλειας *ελέγχου προσπέλασης (access control*), συνδυάζοντας μηχανισμούς *αυθεντικοποίησης (authentication), εξουσιοδότησης (authorization), επίβλεψης (auditing)* και όπου είναι δυνατόν και *κρυπτογράφησης (encryption).*

5.5 Τεχνολογίες – συστατικά μέρη των Firewalls

Αρχικά , δυο ήταν οι τύποι *firewal*l, που εναλλακτικά μπορούσαν να υλοποιηθούν για τη προστασία ενός εσωτερικού δικτύου από ένα άλλο εξωτερικό δίκτυο . Η πύλη φιλτραρίσματος πακέτων *(packet filtering gatewa*y) ή δρομολογητής φιλτραρίσματος *(screening router)* και η πύλη επιπέδου εφαρμογής *(proxy ή application level gateway).* Σήμερα , ένα ολοκληρωμένο σύστημα firewall, συνδυάζει τις τεχνολογίες αυτές οι οποίες λειτουργούν άλλωστε και σε διαφορετικά κανάλια της επικοινωνίας : η πρώτη στο χαμηλό επίπεδο των πακέτων δεδομένων ενώ η άλλη στο υψηλό επίπεδο εφαρμογής .

5.6 Φίλτρα Πακέτων *(packet filter*s)

Πραγματοποιούν ελέγχους στα IP πακέτα *(Internet Protocol packet*s). Ένα πακέτο είναι μια μικρή μονάδα επικοινωνίας , συνήθως μερικές εκατοντάδες bytes, και ένας δρομολογητής *(route*r) μπορεί να διοχετεύσει χιλιάδες πακέτα σε ένα δευτερόλεπτο . Σαν τεχνολογία είναι η πρώτη που εμφανίστηκε ως συνοδευτικό εργαλείο λογισμικού για την υποστήριξη επιπλέον ρυθμίσεων στον αρχικά απλό εξοπλισμό των διατάξεων ή συσκευών δρομολόγησης που δεν είχαν δυνατότητες φιλτραρίσματος των πακέτων .Το φίλτρο πακέτων διενεργεί τον έλεγχο εφαρμόζοντας ένα σύνολο κανόνων *(rule*s), οι οποίοι έχουν οριστεί από το διαχειριστή του firewall κατά τη διαμόρφωσή του και οι οποίοι υλοποιούν μια προαποφασισμένη πολιτική ασφάλειας . Κάθε κανόνας έχει δυο βασικά τμήματα : το πεδίο της ενέργειας και το πεδίο των κριτηρίων επιλογής .

Οι δυνατές ενέργειες είναι δύο : *επιτρέπω (permit, allow)* ή *σταματώ (block, deny).* Τα κριτήρια επιλογής των πακέτων για τα οποία θα ισχύσει η αντίστοιχη ενέργεια ,βασίζονται στις ακόλουθες παραμέτρους :

- Δ*ιεύθυνση προέλευσης και προορισμού :* Για τις IP διευθύνσεις μπορούν να χρησιμοποιηθούν και μάσκες διευθύνσεων *(address masks)* που ομαδοποιούν τις διευθύνσεις .

- *Αριθμός θυρίδας προέλευσης και προορισμού :* Σε κάθε διακομιστή , οι εκτελούμ-ενες εφαρμογές καταλαμβάνουν συγκεκριμένους αριθμούς θυρίδας επικοινωνίας *(port numbers).*

- *Πρωτόκολλο* : Για παράδειγμα TCP *(Transfer Control Protocol),* ICMP *(Internet Control Message Protocol)* ή UDP *(User Datagram Protoco*l).

- *Κατεύθυνση* : Ανάλογα με το αν εισέρχεται το πακέτο στο ιδιωτικό δίκτυο ή αν εξέρχεται από αυτό .

Από απόψεως αρχιτεκτονικής δικτύου , ο χώρος δράσης του είναι τα χαμηλότερα στρώματα *(network – transport layer*s) για αυτό και είναι πολύ γρήγορο . Είναι ικανό επίσης να ελέγχει την κυκλοφορία και βάσει συγκεκριμένης εφαρμογής *(by applicatio*n) αφού η διεύθυνση που ελέγχει ένας δρομολογητής , μπορεί να είναι συνδυασμός διεύθυνσης δικτύου και αριθμού θυρίδας εφαρμογής (π .χ . το 21 για εφαρμογές FTP, το 25 για εφαρμογές SMTP κλπ).

Η τεχνολογία φιλτραρίσματος πακέτων παρουσιάζει όμως και αρκετούς περιορισμούς :

- Ο έλεγχος που πραγματοποιούν αυτά τα firewalls, αφορά κυρίως το είδος της κυκλοφορίας του δικτύου , αφού εξετάζονται μόνο οι IP-επικεφαλίδες κάθε πακέτου . Εκεί υπάρχουν οι πληροφορίες δρομολόγησης (όπως η προέλευση και ο προορισμός του κάθε πακέτου). Το περιεχόμενο του κάθε πακέτου ΔΕΝ εξετάζεται , γι ’ αυτό και η τεχνολογία αυτή είναι κατάλληλη για απλές σχετικά πολιτικές ασφαλείας .

- Δεν προσφέρει επαρκείς μηχανισμούς *επίβλεψης (auditin*g) και *ειδοποίησης κινδύνου (alertin*g).

- Δεν υποστηρίζει εύκολη διαχείριση γιατί υπάρχει περιορισμένος αριθμός κανόνων οι οποίοι μάλιστα απαιτούν κατανόηση των ιδιαιτεροτήτων των πρωτοκόλλων επικοινωνίας . Έτσι είναι αρκετά σύνθετο και δύσκολο έργο η ορθή διαμόρφωσή τους για την εφαρμογή μιας πολιτικής ασφάλειας . Βέβαια διατίθενται κάποια εργαλεία υποστήριξης του έργου των διαχειριστών , που ελέγχουν τη σύνταξη των κανόνων , κάνουν λιγότερο άβολο το περιβάλλον επικοινωνίας *(interfac*e) κλπ .

- Δεν διαθέτουν συνήθως *μηχανισμούς πιστοποίησης σε επίπεδο χρήστη (user level authenticatio*n).

- Δεν προστατεύουν από επιθέσεις πλαστογραφίας σε IP και DNS διευθύνσεις *(IP & DNS address spoofing*). Η βασική αδυναμία των μηχανισμών φιλτραρίσματος πακέτων είναι ότι στηρίζονται στις IP διευθύνσεις , οι οποίες όμως δεν είναι απόλυτα ασφαλείς γιατί συνήθως δεν προστατεύονται .

Σε γενικές γραμμές το επίπεδο ασφάλειας που προσφέρουν είναι χαμηλού επιπέδου . Από την άλλη μεριά πάλι , είναι απλοί , ταχύτατοι , ευέλικτοι και χαμηλού κόστους . Έτσι θεωρούνται ιδανικοί για περιβάλλοντα χαμηλής επικινδυνότητας *(low-risk environments*). Βεβαίως οι υπηρεσίες που προσφέρουν είναι σημαντικότατες για αυτό και θεωρούνται αναπόσπαστο τμήμα ενός ολοκληρωμένου συστήματος firewall.

5.7 Πύλες επιπέδου εφαρμογής *(application level gateway*s)

Λειτουργούν στο υψηλότερο στρώμα επικοινωνίας , στο επίπεδο εφαρμογής *(application layer*). Έτσι έχουν πρόσβαση σε περισσότερες πληροφορίες από ότι τα συστήματα με απλό φιλτράρισμα πακέτων και μπορούν να προγραμματιστούν πιο έξυπνα , κάνοντας τα ικανά να υποστηρίξουν σύνθετες πολιτικές ασφάλειας . Όλα τα IP-πακέτα που φτάνουν ή που πρέπει να φύγουν , εξετάζονται πρώτα ως προς το περιεχόμενό τους και ανάλογα προωθούνται ή απορρίπτονται .

Χρησιμοποιούνται προγράμματα που εκτελούνται σαν εφαρμογές , οι οποίες ονομάζονται *proxie*s. Κάθε TCP/IP υπηρεσία που θέλουμε το firewall να ελέγχει , έχει το δικό του *proxy* δηλαδή μια *υπηρεσία διαμεσολαβητή (middleman servic*e). Για παράδειγμα ένας χρήστης προερχόμενος από το Internet, για να αποκτήσει πρόσβαση στην υπηρεσία FTP ενός μηχανήματος του προστατευμένου δικτύου , θα πρέπει πρώτα να συνδεθεί με την αντίστοιχη proxy εφαρμογή , να ακολουθήσει η αναγνώριση πιστοποίησή του και στη συνέχεια αν η πολιτική ασφάλειας του firewall περιέχει για το συγκεκριμένο και αναγνωρισμένο χρήστη τις κατάλληλες εξουσιοδοτήσεις , θα προωθηθεί η σύνδεση με την υπηρεσία FTP που ζήτησε .

Κάθε υπηρεσία *proxy*, είναι ένα λογισμικό δυο κατευθύνσεων που δρα ταυτόχρονα και σαν *διανομέας (server)* και σαν πελάτης *(client*): στους εσωτερικούς χρήστες απαντάει σαν να είναι η εξωτερική σύνδεση που ζήτησαν . Ενώ στους εξωτερικούς χρήστες αποκρίνεται σαν να είναι η εσωτερική υπηρεσία που θα χρειαστούν . Στην πραγματικότητα δηλαδή , ένα τέτοιου τύπου firewall ή συστατικό ενός firewall, τρέχοντας ψευδόεφαρμογές , εισέρχεται στη μέση της ανταλλαγής πρωτοκόλλων και έτσι ελέγχει τη νομιμότητα των επικοινωνιών .

Οποιαδήποτε άλλη υπηρεσία δεν μπορεί να στείλει ή να λάβει δεδομένα .Αυτός είναι άλλωστε και ο ρόλος του συστήματος firewall, ως ένα τείχος ασφαλείας ισχυρό αλλά και ικανό να προσαρμόζεται εύκολα στις ανάγκες επικοινωνίας του δικτύου μας .Η τεχνολογία αυτή προσφέρει ολοκληρωμένη ασφάλεια με τους ισχυρούς μηχανισμούς *πιστοποίησης χρηστών και συστημάτων (entity and origin authentication*),*επίβλεψης (logging)* και *υποστήριξης υπευθυνότητας (accounting)* που διαθέτει .

Επιπλέον , προσφέρει πολύ ευκολότερη διαχείριση , αφού οι κανόνες που απαιτεί για τον έλεγχο μιας εφαρμογής είναι πολύ πιο απλοί από αυτούς που θα χρειαζόταν ένα firewall τύπου φίλτρου πακέτων . Αξίζει να σημειωθεί ότι επιπλέον μπορεί σαν μια από τις υπηρεσίες της , να ελέγχει την κυκλοφορία των δεδομένων μέσω IP επικεφαλίδων ,δηλαδή μπορεί να παίξει και το ρόλο ενός *φίλτρου πακέτων δεδομένων* , αλλά με χαμηλότερες επιδόσεις στη ταχύτητα ελέγχου των πακέτων .

5.8 Σύγχρονες τεχνολογίες Firewalls – Υβριδικές πύλες *(Hybrid gateways)*

Ο όρος *υβριδικές* ή *σύνθετες πύλες (hybrid or complex gateways)* χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα firewall που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών -τύπων , προχωρούν ακόμη ένα βήμα παραπέρα . Παρατηρείται μια τάση υιοθέτησης της σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστήματος firewall για *περιβάλλοντα μεσαίας έως υψηλής επικινδυνότητας (medium-to-high risk environments).*

Είναι γενική αίσθηση των διαχειριστών firewalls, ότι για ολοκληρωμένη προστασία απαιτείται η συνδυασμένη δράση των τεχνολογιών επιπέδου πακέτων και επιπέδου εφαρμογής . Δύο είναι οι σύγχρονες εναλλακτικές υλοποιήσεις :

5.8.1 Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών

Έχει ήδη τονιστεί ότι ο σχετικά πρωτόγονος έλεγχος αποκλειστικά των IP-επικεφαλίδων , είναι μια λειτουργία που κάθε firewall χρειάζεται , γιατί σε αρκετές περιπτώσεις αυτός είναι ο πιο κατάλληλος και πιο γρήγορος τρόπος ελέγχου . Έτσι ακόμη και τα καθαρά *proxy firewalls* διαθέτουν λογισμικό που προσομοιώνει έναν δρομολογητή φιλτραρίσματος . Επειδή όμως αυξάνει κατά πολύ η ασφάλεια ενός συστήματος όταν δεν είναι συγκεντρωμένη η άμυνά του σε ένα μοναδικό σημείο,πολλές φορές ένα proxy-based σύστημα firewall συνδυάζεται με μια επιπλέον διάταξη φίλτρου πακέτων .

Το υβριδικό αυτό σύστημα , αποκτά παράλληλα πιο γρήγορο και πιο αξιόπιστο φιλτράρισμα πακέτων , αφού είναι επιπέδου hardware. Η σύνδεσή τους πρέπει φυσικά να γίνει εν σειρά έτσι ώστε οι επικοινωνίες να διέρχονται και από τα δύο αυτά συστατικά μέρη του firewall.

5.8.2 Τεχνολογία Stateful Inspection: Δυναμικό φιλτράρισμα πακέτων *(dynamic packet filtering)*

Πρόκειται για μια νέα τεχνολογία , κατηγορίας *packet filtering*. Όμως εδώ επεκτείνεται το απλό IP φιλτράρισμα δίνοντας δυνατότητα να εξετάζεται το κάθε πακέτο στο εσωτερικό του και μάλιστα όχι το κάθε ένα ξεχωριστά και απομονωμένα αλλά ο έλεγχος να γίνεται σε σχέση με προηγούμενες επικοινωνίες . Δημιουργείται δηλαδή μια εσωτερική βάση δεδομένων με πληροφορίες προηγούμενων πακέτων που συνεχώς ενημερώνεται . Μπορεί λοιπόν να γνωρίζει *πληροφορίες κατάστασης (state information)* και *συναφείς πληροφορίες (context information)* για κάθε επικοινωνία ,

οπότε είναι σε θέση να επιτρέπει ή να απαγορεύει μια επικοινωνία με δυναμικό τρόπο ,συμβουλευόμενο τη συνεχώς εξελισσόμενη βάση δεδομένων του .

Ο χώρος δράσης ενός τέτοιου «έξυπνου -*intelligent*» *firewall* εκτείνεται και στα χαμηλά επίπεδα δικτυακής επικοινωνίας , όπου φιλτράρονται τα πακέτα αλλά και στο επίπεδο εφαρμογής . Σ ' αυτό το επίπεδο γίνεται η διαχείριση και ο καθορισμός της πολιτικής ασφαλείας μέσω πάλι proxy υπηρεσιών , διαφορετικής όμως κατασκευής από τα firewalls τύπου application gateway. Αυτός ο συνδυασμός δράσης προσφέρει υπεροχή , αφού συγκεντρώνονται τα πλεονεκτήματα των δύο βασικών τεχνολογιών . Όπως και στα προηγούμενου τύπου firewalls, η εγκατάσταση μιας ξεχωριστής διάταξης δρομολόγησης έχει νόημα μόνο σαν διασπορά των σημείων αμύνης .

5.9 Σύγκριση : Τα υπέρ και τα κατά

Ο όρος *firewall* αναφέρεται πλέον στις δυο νεότερες τεχνολογίες , αυτές που ξεφεύγουν από ένα απλό *(stateles*s) φιλτράρισμα πακέτων . Η σύγκριση λοιπόν αφορά σήμερα τα συστήματα τύπου *application gateway* και *τύπου stateful inspection.*

Το μειονέκτημα των πρώτων είναι ότι πρέπει να γραφεί ένα εξειδικευμένο πρόγραμμα *(proxy*) για κάθε εφαρμογή που πρέπει να διαπερνά το firewall. Βέβαια κάθε τέτοιο firewall έρχεται με έναν αριθμό ήδη έτοιμων εφαρογών για την εξυπηρέτηση των πιο συνηθισμένων υπηρεσιών (όπως FTP, HTTP κλπ .). Πάντως η ανάπτυξη μιας εφαρμογής *proxy* για μια νέα υπηρεσία είναι μια χρονοβόρα και δύσκολη υπόθεση .

Αυτό το μειονέκτημα έρχονται να καλύψουν τα *firewalls* δυναμικού φιλτραρίσματος . Η προσθήκη υποστήριξης νέων υπηρεσιών , γίνεται εδώ πιο εύκολα μέσω μιας πανίσχυρης και υψηλού επιπέδου γλώσσας προγραμματισμού *(Inspect Languag*e) η οποία έχει τη δυνατότητα να επεμβαίνει στο κέντρο της λειτουργίας του firewall, την αποκαλούμενη *Inspect Engin*e. Έτσι , διαθέτουν πολύ σημαντική επεκτασιμότητα *(system extensibilit*y).

Επιπλέον , η τεχνολογία αυτή *stateful inspection* (και μόνον αυτή) προσφέρει δυνατότητα φιλτραρίσματος για πρωτόκολλα *UDP (User Datagram Protocol)* και *RPC (Remote Procedure Call*). Τα πρωτόκολλα αυτά του *Internet* είναι stateless, δηλαδή κάθε μονάδα δεδομένων ταξιδεύει ανεξάρτητη , εφοδιασμένη με πληροφορίες πηγής και προορισμού . Αυτό όμως δυσκολεύει τη δουλειά ενός κλασσικού firewall, γιατί δεν γνωρίζει για το κάθε πακέτο σε ποια επικοινωνία εντάσσεται . Η *Inspect Engine* είναι ικανή να δημιουργεί και να αποθηκεύει «συμφραζόμενα » *(context dat*a), για να προσφέρει έλεγχο και σε τέτοιες επικοινωνίες .

Υπάρχει τίμημα για όλα αυτά . Είναι η ευκολία εισχώρησης λαθών κατά τη συντήρηση ενός firewall με *stateful inspectio*n. Ο διαχειριστής ενός τέτοιου firewall, πρέπει να είναι πολύ προσεκτικός γιατί έχει στη διάθεσή του ισχυρά εργαλεία που αν δεν χρησιμοποιηθούν σωστά , θα επιτρέπονται επικίνδυνες υπηρεσίες να διαπερνούν το σύστημα , κάνοντάς το πιο ευάλωτο . Δεν είναι λοιπόν τυχαίο ότι για τους επίδοξους *εισβολείς (intruders, hackers κλπ .)* τα συστήματα δυναμικού φιλτραρίσματος πακέτων ,αποτελούν τον αγαπημένο τους στόχο .

Προφανώς θεωρούνται πιο δύσκολα για την πραγματοποίηση επιτυχημένων επιθέσεων , αν έχουν διαμορφωθεί σωστά , και έτσι η διακύβευσή τους αποτελεί αναγνώριση στους κύκλους τους , των ικανοτήτων παραβίασης και της επιδεξιότητας

που έχουν . Όμως ακόμη ένας λόγος προτίμησής τους , και μάλιστα ο πιο συνηθισμένος , είναι το ότι μια ακατάλληλη διαμόρφωση των firewalls, δηλαδή ένας ακατάλληλος διαχειριστής τους , προσφέρει διευκολύνσεις εισχώρησης .

5.10 Επίλογος

Η υλοποίηση ενός συστήματος firewall, δεν είναι μια αυτοματοποιημένη διαδικασία αλλά μια δέσμη ενεργειών αναλύσεων , σχεδιασμών και ρυθμίσεων που πρέπει να υποστηρίζουν μια σωστή λειτουργικότητα στο υπό προστασία περιβάλλον . Δεν είναι όλα ρόδινα με τα συστήματα firewalls. Μπορούν να προκαλέσουν προβλήματα *αποδοτικότητας (performanc*e) σε χρήστες καθώς και περιορισμούς σε προγράμματα εφαρμογών ώστε να μην μπορούν αυτά να λειτουργούν όπως πρέπει κάτω από ορισμένες προϋποθέσεις . Σε πολλές περιπτώσεις είναι απαραίτητος ένας ειδικευμένος τεχνικός για τη σωστή ρύθμιση των παραμέτρων εγκατάστασης ενός firewall.

Από την άλλη μεριά , τα firewalls είναι πολύ χρήσιμα : Η ανησυχητική πραγματικότητα στο διαδίκτυο , είναι ότι κυκλοφορούν μη -ασφαλείς εφαρμογές και υπηρεσίες πολύ γρηγορότερα από ότι οι τρόποι προστασίας και αντιμετώπισής τους .Για όποιους το Internet αποτελεί σημαντικό μέρος των δραστηριοτήτων τους , αυτό είναι ένα αναμφισβήτητο γεγονός , που είναι αποδεκτό κατ ’ ανάγκη , και το οποίο απαιτεί την υιοθέτηση προχωρημένων μηχανισμών ασφάλειας .

ΚΕΦΑΛΑΙΟ 6

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Τεχνολογίες ασφάλειας των πληροφοριών και προστασίας της ιδιωτικότητας τείνουν να είναι άμεσα συνδεδεόμενες με ένα επιτυχημένο περιβάλλον ηλεκτρονικού επιχειρείν. Τόσο οι πηγές όσο και οι αποδέκτες των υπηρεσιών του ηλεκτρονικού εμπορίου πρέπει να εφαρμόζουν τα αντίστοιχα τεχνικά και διαδικαστικά μέτρα για την εξασφάλιση του απορρήτου μιας ηλεκτρονικής συναλλαγής.

Στα πλαίσια της συνεχούς εξέλιξης των τεχνολογιών λειτουργίας του ηλεκτρονικού εμπορίου, όλα τα εμπλεκόμενα μέρη οφείλουν να ενημερώνονται συνεχώς σε θέματα προστασίας της ιδιωτικότητας τόσο σε τεχνικό όσο και σε νομικό επίπεδο .Αν πιστεύετε ότι κανείς δεν μπορεί να μάθει τι κάνετε καθημερινά με τον υπολογιστή σας, κάνετε μεγάλο λάθος. Κάθε σας βήμα παρακολουθείται και καταγράφεται, είτε από τα Windows είτε από τα προγράμματα που χρησιμοποιείτε. Μολονότι αυτό γίνεται για προσωπική σας διευκόλυνση, μπορεί τελικά να αποδειχθεί μοιραίο, αν, για παράδειγμα, το έτερον ήμισυ ανακαλύψει τις ροζ ιστοσελίδες που κατά λάθος επισκεφθήκατε στην προσπάθειά σας να εντοπίσετε κάποιο "σπαστήρι".

Στην περίπτωση τώρα που ο άνθρωπος ο οποίος σας παρακολουθεί είναι υποψιασμένος και γνωρίζει από προσωπικούς υπολογιστές, βρίσκεστε σε πολύ δύσκολη θέση και καλό είναι να αρχίζετε να συνηθίζετε την ιδέα του Internet Cafe... Το δυσάρεστο όμως είναι ότι ακόμα και αν το μόνο που ξέρει είναι να γράφει διευθύνσεις και να πατά το Enter, ακόμα και τότε η διαδικτυακή σας "ζωή" και δραστηριότητα κινδυνεύουν άμεσα αποκαλυφθούν, αν δεν έχετε φροντίσει να λάβετε τα μέτρα σας,.

6.1 Μέτρα αντιμετώπισης

Ας εξετάσουμε την πρώτη εκδοχή. Είναι γεγονός ότι οποιοσδήποτε έχει πρόσβαση στο PC σας και έχει βασικές γνώσεις υπολογιστή, μπορεί να ανακαλύψει σχεδόν όλες σας τις δραστηριότητες, on-line και μη. Με μεγάλη ευκολία θα δει, για παράδειγμα, πότε και ποιες ιστοσελίδες επισκεφθήκατε, τα τραγούδια και τα βίντεο που αναπαραγάγατε, τα έγγραφα και τις φωτογραφίες που ανοίξατε. Επιπλέον, θα διαβάσει τα μηνύματα που ανταλλάξατε στα κανάλια ή στα προγράμματα επικοινωνίας, π.χ., IRC, ICQ κ.λπ.

Εάν ο/η σύντροφός σας ανήκει στη δεύτερη κατηγορία, θα εντοπίσει επίσης εύκολα τους προορισμούς των κυβερνοταξιδιών σας. Αν, δηλαδή, πληκτρολογήσει ένα δικτυακό τόπο που το πρώτο του γράμμα είναι το "S" (και για κακή σας τύχη σταματήσει την πληκτρολόγηση), αυτόματα θα εμφανιστεί η μπάρα του Explorer (ή του Netscape), όπου θα περιλαμβάνονται αναλυτικά όλοι οι δικτυακοί τόποι που

ξεκινούν από το γράμμα "S" το οποίο δεν χρειάζεται να θυμίσουμε με ποιες λέξεις και δικτυακούς τόπους συνδέεται.

Η κατάσταση θα γίνει πιο δυσάρεστη για εσάς αν η λειτουργία απομνημόνευσης κωδικών είναι ενεργοποιημένη, διότι επιτρέπει στον "αδιάκριτο" που γνωρίζει μόνο το όνομα χρήστη να αποκτήσει πρόσβαση σε πιο ευαίσθητα προσωπικά δεδομένα, όπως οι λογαριασμοί e-mail ή άλλες υπηρεσίες που παρέχονται μέσω Web. Θα σκεφτείτε, βέβαια (και δεν θα έχετε άδικο), ότι χάρη στα κατάλληλα "σπαστήρια" όποιος έχει πρόσβαση στον υπολογιστή σας μπορεί να αποκρυπτογραφήσει οποιονδήποτε κωδικό από τον κωδικό της τηλεφωνικής σύνδεσης (dialup) μέχρι τον κωδικό των Windows, των εγγράφων και των συμπιεσμένων αρχείων.

Ωστόσο, το θέμα της ασφάλειας αντιμετωπίζεται συνήθως με την εισαγωγή ενός κωδικού πρόσβασης στο σύστημα (μέσω BIOS) ή/και στο λειτουργικό σύστημα, απαγορεύοντας έτσι την πρόσβαση σε τρίτους.

Τι συμβαίνει όμως στην περίπτωση που μοιράζεστε τον υπολογιστή με άλλους και εκ των πραγμάτων δεν έχετε τη δυνατότητα να ενεργοποιήσετε τέτοιου είδους δικλίδες ασφαλείας;

Η δημιουργία διαφορετικών λογαριασμών χρηστών (user accounts) θεωρείται οπωσδήποτε μια καλή και αρκετά ασφαλής λύση, εντούτοις πολλές φορές δεν ενδείκνυται για πρακτικούς λόγους, όπως, π.χ., εάν ο υπολογιστής χρησιμοποιείται από όλη την οικογένεια και υπάρχει ανάγκη να μοιράζονται κάποιοι πόροι.

Τη λύση εδώ προσφέρουν τα ειδικά προγράμματα "καθαρισμού", τα οποία αναλαμβάνουν να εξαφανίσουν όλες τις λίστες ιστορικού των Windows, να αδειάσουν τον κάδο ανακύκλωσης, να σβήσουν τα αρχεία αναφοράς και γενικά να καταστρέψουν όλα τα στοιχεία και τα δεδομένα που ενδέχεται να σας βάλουν σε περιπέτειες.

Εναλλακτικά, έχετε την ευχέρεια να εξαφανίσετε και οι ίδιοι τα ίχνη σας, αρκεί να γνωρίζετε ορισμένα βασικά πραγματάκια για τα αρχεία αναφοράς και τις λίστες των Windows, καθώς και τον τρόπο διαγραφής τους. Με τη χειροκίνητη διαγραφή έχετε "τζάκποτ", αφού μπορείτε αφενός να προστατευθείτε και αφετέρου να ελέγξετε τις δραστηριότητες του ανθρώπου που χρησιμοποιεί τον υπολογιστή σας. Ας δούμε τι πρέπει να προσέξετε για να μη βρεθείτε ηλεκτρονικά εκτεθειμένοι.

Εξίσου σημαντική λίστα ιστορικού είναι και αυτή που διατηρούν τα προγράμματα περιήγησης, καταγράφοντας τις τοποθεσίες του Internet που έχετε επισκεφθεί. Είναι γνωστό ότι πατώντας από τη γραμμή εργαλείων του Internet Explorer το κουμπί "History" ("Ιστορικό") θα δείτε τις σελίδες που επισκεφθήκατε τις τελευταίες μέρες.

Σκεφτείτε όμως τι θα συμβεί εάν έχετε ενεργοποιήσει την αυτόματη συμπλήρωση κωδικού (Auto Complete) στις υπηρεσίες Web που χρησιμοποιείτε, όπως, για παράδειγμα, σε ένα διακομιστή ηλεκτρονικού ταχυδρομείου Web (Yahoo!, Hotmail κ.λπ.). Αυτό με απλά λόγια σημαίνει ότι ο υπολογιστής καταγράφει αυτόματα τον κωδικό (password) και ο χρήστης πρέπει απλώς να γράψει το όνομα χρήστη (user name) που είναι ευκολότερο να το θυμάται, αφού συνήθως το χρησιμοποιεί και σε άλλες περιπτώσεις. Έτσι, ο επιτήδειος που θα προσπαθεί να ανακαλύψει τις ψηφιακές σας κινήσεις, το μόνο που έχει να κάνει είναι να μεταβεί από τη λίστα ιστορικού στην ιστοσελίδα της υπηρεσίας που χρησιμοποιείτε, π.χ., στο Yahoo!, και πληκτρολογώντας μόνο το όνομα χρήστη (το οποίο μπορεί να αποκτήσει σχετικά εύκολα, ειδικά αν είναι άτομο του στενού οικογενειακού-φιλικού σας περιβάλλοντος), να έχει πρόσβαση στο λογαριασμό σας.

Αν έχετε ενεργοποιημένη τη λειτουργία της αυτόματης συμπλήρωσης κωδικού ή την απομνημόνευση των στοιχείων, τότε δεν είναι καθόλου δύσκολο για τον αδιάκριτο να αποκτήσει πρόσβαση στην υπηρεσία Web που χρησιμοποιείτε, όπως, για παράδειγμα, σε ένα λογαριασμό ταχυδρομείου.

Ηλεκτρονικό δίδαγμα λοιπόν: Διαγράφετε τακτικά τη λίστα ιστορικού του Internet Explorer και δεν επιτρέπετε στα Windows να καταγράφουν τους κωδικούς σας. Μπορεί αυτά να μην κάνουν άνετη τη ζωή σας στο σερφάρισμα, εντούτοις σας προστατεύουν από τις κακοτοπιές.

Γι' αυτό λοιπόν, κατά την εισαγωγή σας σε κάποια υπηρεσία Web που τα Windows θα σας ρωτήσουν αν θέλετε να απομνημονεύσουν τον κωδικό στον υπολογιστή, απαντάτε αρνητικά και τσεκάρετε το πλαίσιο "Don't offer to remember any more passwords".

6.2 Τα αρχεία αναφοράς και οι λίστες ιστορικού

Τα αρχεία αναφοράς (log files) δημιουργούνται από τα Windows ή από τις εφαρμογές και έχουν κατάληξη ".log". Πρόκειται τις περισσότερες φορές για απλά αρχεία κειμένου στα οποία οι εφαρμογές καταγράφουν αναφορές για λειτουργίες που επιτελούν.

Εξ ορισμού αρχείο αναφοράς, για παράδειγμα, δημιουργεί το Scandisk (βρίσκεται στο c:\scandisk.log) κάθε φορά που ελέγχει το δίσκο για σφάλματα, σημειώνοντας την ώρα και την ημερομηνία ελέγχου, αλλά και τα λάθη που εντοπίστηκαν στο δίσκο. Παρόμοια αρχεία φτιάχνουν πολλά προγράμματα. Κάνοντας μια απλή αναζήτηση θα βρείτε στο δίσκο σας δεκάδες ή και εκατοντάδες αρχεία αναφοράς. Ασφαλώς, σας ενδιαφέρουν μόνο όσα έχουν γίνει από συγκεκριμένα προγράμματα και τα οποία άμεσα ή έμμεσα μαρτυρούν αυτά που θέλετε να κρατήσετε μυστικά.

Σημειώστε ότι τα **Windows 98/Me** διατηρούν σε έναν κρυφό φάκελο με το όνομα "**Applog**" (Application log files) αρχεία αναφοράς που έχουν κατάληξη ".lgc", ".lgd", ".lge" κ.ο.κ. Ποιος είναι ο ρόλος αυτών των αρχείων; Το πρόγραμμα TaskMon παρακολουθεί τη δραστηριότητα του σκληρού δίσκου, καταγράφοντας σε αρχεία αναφοράς πληροφορίες για τη θέση των προγραμμάτων στο δίσκο και για το πόσο συχνά αυτά φορτώνονται. Όταν αργότερα ζητήσετε από τα Windows να αποκερματίσουν (defrag) το δίσκο σας, το πρόγραμμα αποκερματισμού (Disk Defragmenter) θα χρησιμοποιήσει τα αρχεία αναφοράς του καταλόγου "Applog" για να βελτιστοποιήσει το σύστημά σας, τοποθετώντας στην ίδια περιοχή του δίσκου τα αρχεία-πληροφορίες που χρειάζεται κάθε πρόγραμμα για να εκτελεστεί. Δεν υπάρχει λόγος να ασχοληθείτε μαζί τους, αλλά ούτε φυσικά και να τα διαγράψετε (αν και δεν θα συμβεί τίποτα).

Όσον αφορά στις **λίστες ιστορικού**, δημιουργούνται κυρίως από το λειτουργικό σύστημα, προκειμένου ο χρήστης να έχει άμεση πρόσβαση και να μην απαιτείται η εκ νέου αναζήτησή τους. Η σημαντικότερη λίστα ιστορικού των Windows είναι η "**Documents**" ("Έγγραφα" στην ελληνική έκδοση), η οποία ονομάζεται και **MRU (Most Recently Used List).** Εμφανίζεται κάνοντας κλικ στο "Start*Documents" ("Έναρξη*Έγγραφα") και περιλαμβάνει όσα αρχεία κειμένου, βίντεο και φωτογραφιών ανεξαρτήτως κατάληξης έχετε ανοίξει, π.χ., ".txt", ".doc", ".avi", ".mov" κ.ά. Πρόκειται για την πρώτη λίστα που θα ελέγξει ο εισβολέας στον υπολογιστή σας προσπαθώντας να ανακαλύψει όλα όσα θέλετε να κρατήσετε μακριά από τα αδιάκριτα μάτια...

6.3 Η ώρα των "εκκαθαρίσεων"

Εφόσον γνωρίζετε τα επίμαχα σημεία που ενδέχεται να προδώσουν τις κινήσεις σας, χρειάζεται να μάθετε τον τρόπο με τον οποίο θα τα εξαφανίσετε. Μπορείτε, βέβαια,όπως ήδη είπαμε, να χρησιμοποιήσετε κάποιο πρόγραμμα καθαρισμού, ωστόσο, καλό είναι να ξέρετε να κάνετε όλη τη δουλειά χειροκίνητα, αφού τη δύσκολη στιγμή ίσως να μην έχετε αυτά τα όπλα στα χέρια σας.

Κατ' αρχάς, δεν πρέπει να ξεχνάτε να αδειάζετε τον κάδο ανακύκλωσης**,** ειδικά όταν διαγράφετε προσωπικά αρχεία.

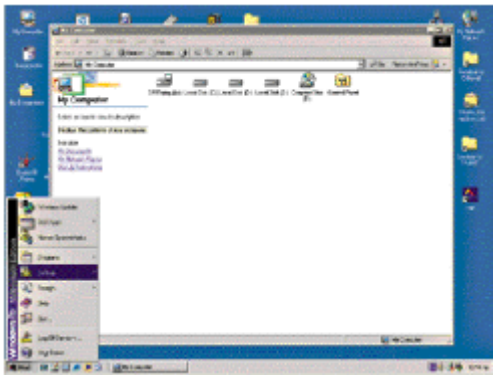
Επίσης, να φροντίζετε να διαγράφετε τακτικά τα περιεχόμενα του προσωρινού (Temp) καταλόγου των Windows. Τη λίστα ιστορικού "**Documents**" μπορείτε να τη διαγράψετε από το "Start **Settings*Taskbar and Start Menu" και πατώντας το κουμπάκι "clear" από την καρτέλα "Advanced". Από τον Internet Explorer κάνετε κλικ στο "Tools*Internet Options" και πατάτε στο "**Clear History**" για να διαγράψετε τη λίστα ιστορικού. Από το ίδιο μενού έχετε επίσης τη δυνατότητα να διαγράψετε τα cookies και τα προσωρινά αρχεία Internet (συνιστάται), να επιλέξετε το μέγεθος του αποθηκευτικού χώρου που θα παραχωρήσετε στο πρόγραμμα για τα αρχεία αυτά, καθώς και να καθορίσετε πόσες μέρες θα διατηρεί τις σελίδες το πρόγραμμα στο ιστορικό.

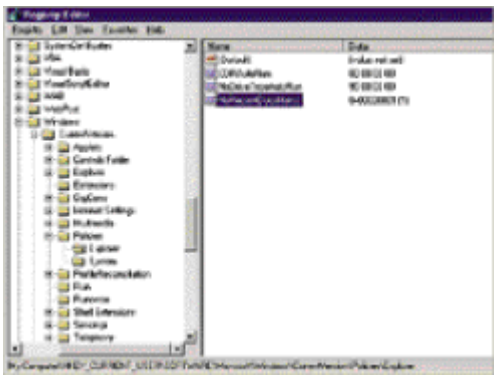
Δύο λιγότερο σημαντικές λίστες ιστορικού είναι η λίστα εκτέλεσης προγραμμάτων **(Run History)**, στην οποία καταγράφονται τα αρχεία, οι φάκελοι κ.ά. που ανοίγετε με την επιλογή Run (Start*Run), και η λίστα της αναζήτησης αρχείων (Find Files History). Επειδή τα Windows δεν παρέχουν κάποια σχετική επιλογή, θα τις διαγράψετε από το μητρώο συστήματος (registry), χρησιμοποιώντας το πρόγραμμα Regedit.

Για τη λίστα εκτέλεσης προγραμμάτων ανατρέχετε στο πεδίο "HKEY_CURRENT_USER\ SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" και από τη λίστα που παρουσιάζεται δεξιά διαγράφετε τις καταχωρίσεις που θέλετε.

Το ίδιο κάνετε και για το ιστορικό της αναζήτησης, ανατρέχοντας στο πεδίο "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars\{C4EE31F3-4768-11D2-BE5C-00A0C9A83DA1}\FilesNamedMRU".

6.3.1Πώς θα απαλλαγείτε από τη λίστα Documents





Αν θέλετε να απαλλαγείτε μια και καλή από τη λίστα "Documents", φορτώστε το Regedit και, αφού μετακινηθείτε στο πεδίο "HKEY_CURRENT_USER\SOFTWARE\Microsoft \Windows\CurrentVersion\Policies\Explorer", κάντε κλικ στο "Edit*New*DWORD

Value" και δώστε ως όνομα το "NoRecentDocsMenu" και τιμή 1. Προσοχή, η παραπάνω καταχώριση στο μητρώο συστήματος δεν διαγράφει τα περιεχόμενα της λίστας, απλώς δεν επιτρέπει την πρόσβαση από το μενού "Start". Παρατηρήστε στη δεξιά φωτογραφία (μετά την καταχώριση και την επανεκκίνηση του υπολογιστή) ότι η λίστα "Documents" δεν εμφανίζεται πλέον στο μενού "Start".

6.3.2 Οι προδοσίες των προγραμμάτων άμεσης επικοινωνίας και συζητήσεων

Ας εξετάσουμε τώρα τις εφαρμογές άμεσων μηνυμάτων (Instant Messenger) και τα προγράμματα συνομιλιών (chat). Η κατάσταση εδώ είναι κάπως περίπλοκη. Άλλα προγράμματα καταγράφουν τις συνομιλίες, ενώ κάποια άλλα όχι. Το ICQ, για παράδειγμα, καταγράφει τα πάντα, ακόμα και τα αρχεία που στέλνετε ή λαμβάνετε. Μάλιστα, οι συνομιλίες αποθηκεύονται σε κρυπτογραφημένη μορφή και όχι ως απλό κείμενο. Για να απενεργοποιήσετε τη λειτουργία καταγραφής των συνομιλιών, κάντε κλικ στο κουμπί ICQ (Main), επιλέξτε "Preferences*Events" και μαρκάρετε την επιλογή "**Do Not Log Event History**". Να επισημάνουμε ότι το ICQ σάς δίνει τη δυνατότητα να επιλέξετε με ποιους χρήστες δεν θα καταγράφεται η συνομιλία σας.

Αντίθετα από το ICQ, ο MSN Messenger της Microsoft δεν διατηρεί αρχεία αναφοράς. Άπαξ και κλείσετε το ενεργό παράθυρο συνομιλιών, εξαφανίζεται και η τελευταία λέξη που πληκτρολογήσατε.

Όσον αφορά τέλος στο mIRC που χρησιμοποιείται για κουβέντα στο IRC, κρατά και αυτό ημερολόγιο, σημειώνοντας τα κανάλια που επισκέπτεστε και τις συνομιλίες σας. Κάντε κλικ στο "File* Options", επιλέξτε "IRC*Logging" και από τη λίστα "**Automatic Log**" διαλέξτε "None".

Εκτός από τα δεκάδες εμπορικά ή ελεύθερης διανομής προγράμματα καθαρισμού που κυκλοφορούν, τα Windows περιλαμβάνουν στα εργαλεία τους το **Disk Cleanup**, το οποίο αναλαμβάνει να καθαρίσει τα προσωρινά αρχεία που συσσωρεύονται από τα προγράμματα ή τον Internet Explorer, ορισμένα αρχεία αναφοράς, να αδειάσει τον κάδο ανακύκλωσης και γενικά να απαλλάξει το σύστημα από τα περιττά βάρη.

Όπως όμως θα διαπιστώσετε, μετά την ενεργοποίησή του αφήνει ανέπαφη τη λίστα "Documents", καθώς και τις λίστες ιστορικού της εκτέλεσης προγραμμάτων και της αναζήτησης. Ενεργοποιήστε το από το "Start* Programs*Accessories*System Tools", επιλέξτε την κατάτμηση ή το δίσκο που θέλετε να καθαρίσετε και μαρκάρετε τις κατηγορίες αρχείων που επιθυμείτε να διαγράψετε. Σε ορισμένες κατηγορίες μην ξεχάσετε να εκμεταλλευτείτε τη δυνατότητα προβολής των προσωρινών αρχείων, ώστε να δείτε πού βρίσκονται, τι μέγεθος έχουν και πώς ονομάζονται.

6.4 Προστασία της ιδιωτικότητας των πληροφοριών που διακινεί ένας χρήστης του διαδικτύου (Internet).

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.

6.5 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.

Είναι γεγονός, ότι σε όλες τις παραπάνω περιπτώσεις, η συλλογή και επεξεργασία προσωπικών δεδομένων μπορεί να οδηγήσει σε παραβίαση της ιδιωτικής και προσωπικής ζωής του χρήστη όταν αυτή δεν εφαρμόζεται σύμφωνα με τις οικείες διατάξεις. Αποτελέσματα δημοσκοπήσεων, έχουν δείξει ότι η έλλειψη προστασίας της ιδιωτικότητας στις επικοινωνίες είναι ο κύριος λόγος αποχής των δυνητικών χρηστών από την χρήση των υπηρεσιών του διαδικτύου. Οι χρήστες θεωρούν ότι η έλλειψη ιδιωτικότητας στις επικοινωνίες είναι ο σημαντικότερος παράγοντας που εμποδίζει την ανάπτυξη του ηλεκτρονικού εμπορίου και τη θεωρούν σημαντικότερη από άλλους παράγοντες όπως το κόστος πραγματοποίησης ηλεκτρονικών συναλλαγών, οι δυσκολίες χρήσης του τεχνολογικού εξοπλισμού και η παραλαβή ανεπιθύμητων ηλεκτρονικών διαφημιστικών μηνυμάτων.

6.6 Τα μέτρα προφύλαξης

Το αντίδοτο στην παραβίαση της προσωπικής ζωής είναι η δημιουργία καναλιών επικοινωνίας που δεν αποκαλύπτουν την ταυτότητα των επικοινωνούντων μερών. Για το λόγο αυτό οι πολίτες της χώρας χρειάζονται τεχνολογίες που θα προστατεύουν την ασφάλεια των επικοινωνιών τους ενώ παράλληλα θα εξασφαλίζουν τα πρωταρχικά τους δικαιώματα σε σχέση με την ελευθερία έκφρασης και την ιδιωτικότητα των πληροφοριών που σχετίζονται με την προσωπική τους ζωή και γίνονται αντικείμενο επεξεργασίας από διάφορους φορείς (τρίτοι). Η εξέλιξη στις τεχνολογίες πληροφορικής σήμερα, δίνει τη δυνατότητα σε οργανισμούς να επεξεργάζονται απλά ή/ και ευαίσθητα προσωπικά δεδομένα, έτσι όπως αυτά νοούνται στο ν.2472/97 με μεγάλη ταχύτητα.

6.6.1 Τεχνολογίες Ασφάλειας Πληροφορίων και Τεχνολογίες Προστασίας Ιδιωτικότητας

Για τους παραπάνω λόγους έχουν αναπτυχθεί τεχνολογίες οι οποίες βοηθούν τους χρήστες του διαδικτύου να αυξήσουν αφενός την ασφάλεια των συνδέσεων που πραγματοποιούν με χρήση του διαδικτύου και αφετέρου να διατηρήσουν το δικαίωμα της ανωνυμίας των διακινούμενων πληροφοριών που τους αφορούν. Οι μεν πρώτες είναι γνωστές ως τεχνολογίες ασφάλειας πληροφοριών, ΤΑΠ, (Infromation Security Technologies, IST) οι δε δεύτερες ως τεχνολογίες αύξησης ιδιωτικότητας, ΤΑΙ (Privacy Enhancing Technologies, PETs). Πολλές από τις ΤΑΠ μπορούν να χρησιμοποιηθούν για την αύξηση της ιδιωτικότητας. Η έμφαση όμως στο κείμενο αυτό δίνεται στις ΤΑΙ.

6.6.1.1 Μέτρα προφύλαξης του χρήστη

Οι χρήστες που χρησιμοποιούν υπηρεσίες ηλεκτρονικού εμπορίου θα πρέπει να έχουν γνώση και να ενημερώνονται σχετικά με τις εξελίξεις τόσο στις ΤΑΠ όσο και στις ΤΑΙ. Για τους παραπάνω λόγους θα πρέπει να:

1. Χρησιμοποιούν όλα τα διαθέσιμα μέσα για να προστατεύουν τα δεδομένα που τους αφορούν τ και ις επικοινωνίες, όπως τα νόμιμα διαθέσιμα τεχνολογικά εργαλεία κρυπτογράφησης δεδομένων, ηλεκτρονικού ταχυδρομείου, κωδικών πρόσβασης κ.λ.π.
2. Είναι προσεκτικοί σε σχέση με τις πληροφορίες που μεταβιβάζουν σε κάθε επίσκεψή τους στις ιστοσελίδες ενός δικτυακού τόπου, κατά την πραγματοποίηση μιας ηλεκτρονικής σύνδεσης και γενικότερα μιας επικοινωνίας με χρήση του διαδικτύου. Οι προσωπικές πληροφορίες που μεταβιβάζονται ποικίλλουν και αφορούν σε:

- Πληροφορίες που μεταβιβάζονται εις γνώσιν του χρήστη π.χ. ονοματεπώνυμο, ταχυδρομική διεύθυνση κ.λ.π.

- Πληροφορίες που μεταβιβάζονται εν αγνοία του χρήστη π.χ. IP διεύθυνση, το όνομα του υπολογιστή κ.λ.π. Τις περισσότερες φορές η μεταβίβαση αυτών των πληροφοριών είναι αναγκαία για λόγους επίτευξης της επικοινωνίας και επιβάλλεται από την φύση της σχεδίασης των επικοινωνιακών πρωτοκόλλων.

3. Αναζητά και να του παρέχονται, στο βέλτιστο βαθμό, τεχνολογίες που του εξασφαλίζουν την ανωνυμία στο βαθμό εκείνο που δεν θίγονται άλλοι νόμοι και αρχές που θεωρούνται ανώτερες από την προσωπική ζωή π.χ. δημόσιο συμφέρον κ.λ.π. Ο καλύτερος τρόπος διασφάλισης της ιδιωτικότητας είναι η ανώνυμη πρόσβαση και χρήση επικοινωνιών καθώς επίσης και οι τεχνολογίες πραγματοποίησης ανώνυμων πληρωμών.

4. Επιδιώκει τη χρήση ψευδωνύμων, σε περιπτώσεις που είναι νομικά αδύνατη η παροχή παντελούς ανωνυμίας έτσι ώστε η πραγματική ταυτότητα να είναι αποκαλύψιμη μόνο στον φορέα εκείνο που διατηρεί την αντιστοίχηση μεταξύ ψευδωνύμου τ και αυτότητας φυσικού προσώπου.

5. Αποκαλύπτει μόνο τα δεδομένα εκείνα που είναι απαραίτητα για την επίτευξη των σκοπών που επιδιώκονται μέσω της συγκεκριμένης επικοινωνίας ή συναλλαγής. Ιδιαίτερη προσοχή πρέπει να δοθεί στην περίπτωση αποκάλυψης αριθμών πιστωτικών καρτών, στοιχείων τραπεζικών λογαριασμών, ευαίσθητων δεδομένων κ.λ.π. Σε αυτές τις περιπτώσεις συστήνεται η χρήση τεχνολογιών διασφάλισης εμπιστευτικότητας πληροφοριών. Μια τέτοια τεχνολογία είναι η χρήση του πρωτοκόλλου επικοινωνίας Secure Socket Layer, SSL. Το πρωτόκολλο αυτό χρησιμοποιείται συχνά σε συνδυασμό με το

πρωτόκολλο HTTP για την παροχή ασφαλών διμερών επικοινωνιών με χρήση υπηρεσιών WWW. Τυπικά, ο χρήστης μπορεί να αναγνωρίσει την ενεργοποίηση αυτού του πρωτοκόλλου αναζητώντας τα αρχικά https:// στην τοποθεσία της ηλεκτρονικής σελίδας με την οποία έχει συνδεθεί.

6. Πραγματοποιεί προσεκτική μεταβίβαση της ηλεκτρονικής διεύθυνσης αλληλογραφίας (e-mail address). Η ηλεκτρονική διεύθυνση αλληλογραφίας αποτελεί προσωπικό στοιχείο π και ροστατεύεται όπως και τα λοιπά προσωπικά στοιχεία. Για το λόγο αυτό θα πρέπει να αποφεύγεται η συμμετοχή σε λίστες με ηλεκτρονικές ταχυδρομικές διευθύνσεις που δεν κάνουν γνωστό τον σκοπό για τον οποίο συλλέγονται, την διάρκεια της επεξεργασίας, τους πιθανούς αποδέκτες των στοιχείων και επίσης δεν παρέχουν έναν ρητό τρόπο διαγραφής τους από αυτές.

7. Δίνει ιδιαίτερη προσοχή στα προγράμματα τα οποία "κατεβαίνουν" (download) από το διαδίκτυο διότι μπορεί να επεξεργάζονται προσωπικά δεδομένα και να τα αποστέλλουν σε δικτυακούς τόπους τους οποίους δεν γνωρίζει ο χρήστης. Τεχνολογικά εργαλεία ενεργού περιεχομένου (active content) π.χ. Java, ActiveX, Javascript, μπορούν να χρησιμοποιηθούν για την, εν αγνοία του χρήστη, συλλογή και επεξεργασία προσωπικών στοιχείων.

8. Αποφεύγει την εγκατάσταση cookies στον υπολογιστή του. Τα cookies είναι αρχεία τα οποία αποστέλλονται από την πλευρά του δικτυακού τόπου που συνδέεται ο χρήστης και εγκαθίστανται στον υπολογιστή του χρήστη. Τα αρχεία αυτά μπορούν να χρησιμοποιηθούν για την αποθήκευση προσωπικών στοιχείων, στοιχείων συμπεριφοράς πλοήγησης κατά την διάρκεια παραμονής στο δικτυακό τόπο κ.λ.π., έτσι ώστε την επόμενη φορά που ο χρήστης θα συνδεθεί με το δικτυακό τόπο από το οποίο εγκαταστάθηκε το cookie, ο εξυπηρετητής (server) του δικτυακού τόπου να παρέχει στον χρήστη εξυπηρέτηση προσαρμοσμένη στις καταναλωτικές του ανάγκες. Η εγκατάσταση των αρχείων cookies θα πρέπει να αποφεύγεται γιατί κατ' αυτόν τον τρόπο δημιουργούνται καταναλωτικά προφίλ χρηστών. Ο χρήστης έχει τη δυνατότητα να απαγορεύσει την εγκατάσταση των cookies στον υπολογιστή του από τις ρυθμίσεις ασφάλειας του προγράμματος πλοήγησης (web browser).

9. Ζητά από τους Παροχείς Υπηρεσιών Διαδικτύου (ΠΥΔ) και τους Παροχείς Τελικών Υπηρεσιών (ΠΤΥ) το κείμενο της ενημέρωσης του κοινού για την τήρηση αρχείου προσωπικών ή/ και ευαίσθητων δεδομένων έτσι όπως αυτό απορρέει από τις υποχρεώσεις των υπεύθυνων επεξεργασίας έναντι της Πολιτείας βάσει του ν.2472/97. Τα στοιχεία που κατ' ελάχιστον θα πρέπει να συμπεριλαμβάνονται στο κείμενο αυτό θα πρέπει να είναι εκείνα που

ορίζονται στο άρθρο 11 του ν.2472/97 και τον κανονισμό 1/1999 (ΦΕΚ 555/6.5.1999) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Επίσης μπορεί να ζητήσει από τους ΠΥΔ και ΠΤΥ τον αριθμό πρωτοκόλλου της γνωστοποίησης ή/ και άδειας τήρησης αρχείου ευαίσθητων δεδομένων προς την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

10. Ενημερώνεται σχετικά με τις εξελίξεις και αλλαγές στην Ελληνική νομοθεσία που σχετίζεται με θέματα προστασίας της προσωπικής ζωής και των επικοινωνιών (ν.2472/97, ν. 2774/99). Επίσης μπορεί να λαμβάνει σχετικές πληροφορίες για τις αποφάσεις και οδηγίες της Αρχής Προστασίας Δεδομένων από την ηλεκτρονική διεύθυνση http://www.dpa.gr.

6.6.1.2 Μέτρα προστασίας Παροχέων Υπηρεσιών Διαδικτύου

Οι Παροχείς Υπηρεσιών Διαδικτύου θα πρέπει να:

1. Χρησιμοποιούν λογισμικό ή/ και υλικό το οποίο έχει πιστοποιηθεί σχετικά με την ποιότητά του, και εξασφαλίζει την ασφάλεια των μεταδιδόμενων πληροφοριών. Οι ΠΥΔ θα πρέπει να ενημερώνουν και να διευκολύνουν, αν είναι δυνατόν, τους χρήστες στην απόκτηση τέτοιου είδους λογισμικού. Για παράδειγμα οι ΠΥΔ θα μπορούσαν να εγκαταστήσουν έναν Secure Shell Server (SSH) και να διευκολύνουν τους συνδρομητές τους στην απόκτηση του ssh client. Το πρόγραμμα αυτό στηρίζεται στην χρήση κρυπτογραφίας δημόσιου κλειδιού για την διασφάλιση της ιδιωτικότητας των μεταδιδόμενων πληροφοριών. Με την χρήση του προγράμματος αυτού ο χρήστης μπορεί να εγκαταστήσει ασφαλείς συνδέσεις με χρήση διαφόρων πρωτοκόλλων π.χ. telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP).

2. Εκπονούν μελέτη ασφάλειας επικινδυνότητας και στην συνέχεια να αναπτύσσουν και να καταγράφουν την πολιτική ασφάλειας του οργανισμού σχετικά με το Πληροφοριακό τους σύστημα. Η πολιτική ασφάλειας θα πρέπει να τηρείται στο μέγιστο βαθμό από ολόκληρο τον οργανισμό. Με τον τρόπο αυτό θα εξασφαλίζεται η φυσική λ και ογική ασφάλεια του επικοινωνιακού εξοπλισμού που χρησιμοποιεί ο ΠΥΔ σύμφωνα με το άρθρο 10 του Ν.2472/97.

3. Να συντάσσουν ένα κώδικα δεοντολογίας για την προστασία των προσωπικών δεδομένων ο οποίος θα στηρίζεται στις διατάξεις και στο πνεύμα του Ν.2472/97 και το οποίο θα κοινοποιούν στην διεύθυνση και σε όλο το προσωπικό.

4. Ενημερώνουν τους χρήστες και διευκολύνουν την πρόσβασή τους σε πόρους σχετικά με την ασφάλεια πληροφοριών και την προστασία της ιδιωτικής τους ζωής. Για παράδειγμα θα πρέπει σε όλα τα έντυπα που μοιράζουν στους συνδρομητές τους να τους ενημερώνουν σχετικά με το δικαίωμα αντίρρησης τους στην συλλογή προσωπικών ή/ και ευαίσθητων δεδομένων που τους αφορούν, με τους αποδέκτες των δεδομένων που έχουν εις γνώσει των υποκειμένων συλλέξει, τους κινδύνους που απορρέουν από την δημιουργία καταναλωτικών προφίλ κ.λ.π.

5. Ανακοινώνουν μέσω των ηλεκτρονικών σελίδων τους, σε εμφανή σημεία (στην πρώτη σελίδα), πολιτικές διασφάλισης της ιδιωτικότητας (privacy policies) που απορρέουν από τον ν.2472/97. Μια πολιτική διασφάλισης της ιδιωτικότητας θα πρέπει να περιλαμβάνει τουλάχιστον τα στοιχεία που περιλαμβάνονται στο άρθρο 11 του ν.2472/97 και τον κανονισμό 1/1999 (ΦΕΚ 555/6.5.1999) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

6. Συλλέγουν τα στοιχεία των συνδρομητών με διαφανή τρόπο. Αυτό πρακτικά σημαίνει ότι θα πρέπει να αποφεύγεται η χρήση των cookies και των τεχνολογιών ενεργού περιεχομένου. Η μέθοδος που συνίσταται είναι η χρήση ηλεκτρονικών φορμών. Τα στοιχεία που θα συλλέγονται θα πρέπει να είναι ακριβώς εκείνα που απαιτούνται για την κατάρτιση της σύμβασης μεταξύ συνδρομητή και ΠΥΔ. Ο ΠΥΔ μπορεί να επιθυμεί να συλλέξει επιπρόσθετα στοιχεία. Τα στοιχεία αυτά θα πρέπει με κάποιο τρόπο (π.χ. την ύπαρξη ενός αστερίσκου ή την αλλαγή στο χρώμα εμφάνισης της γραμματοσειράς στο όνομα του πεδίου) να σημειώνονται ως μη υποχρεωτικά προς συμπλήρωση και να υπάρχει ρητή ένδειξη για τον σκοπό της συλλογής τους.

7. Μην υποβιβάζουν τη λειτουργικότητα που προσφέρεται σε έναν χρήστη σε περίπτωση που ο τελευταίος απέφυγε την παροχή προσωπικών δεδομένων που δεν είναι απαραίτητα για την εκπλήρωση της σύμβασης μεταξύ συνδρομητή και ΠΥΔ. Για παράδειγμα δεν θα πρέπει να περιορίζεται το υλικό που εμφανίζεται στις HTML σελίδες του φυλλομετρητή (browser) ενός χρήστη επειδή αρνήθηκε την εγκατάσταση ενός cookie στον δίσκο του υπολογιστή του. Επιπλέον δεν θα πρέπει να μειώνονται οι επιλογές πρόσβασης σε περίπτωση που ο χρήστης απέφυγε να συμπληρώσει τα πεδία με προσωπικά δεδομένα τα οποία έχουν μαρκαριστεί ως προαιρετικά στην περίπτωση που τα

στοιχεία για την κατάρτιση της σύμβασης υποβάλλονται με χρήση ηλεκτρονικών φορμών.

8. Σε σχέση με την παραπάνω παράγραφο, τονίζεται ότι δεν θα πρέπει σε καμία περίπτωση να πριμοδοτούν με οποιονδήποτε τρόπο (αύξηση παροχών, διαφημιστικά δώρα κ.λ.π) τη συγκατάθεση του χρήστη στην συλλογή στοιχείων που δεν είναι απαραίτητα για την κατάρτιση της σύμβασης μεταξύ συνδρομητή και ΠΥΔ.

9. Παρέχουν εξασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων που απαιτούνται για την κατάρτιση της σύμβασης όταν αυτά υποβάλλονται ηλεκτρονικά. Στις περιπτώσεις αυτές συνιστάται η χρήση ΤΑΠ που εκμεταλλεύονται τα πλεονεκτήματα της κρυπτογραφίας δημόσιου κλειδιού. Μια τέτοια πρόσφορη τεχνολογία είναι τα ψηφιακά πιστοποιητικά (digital certificates). Ευρεία χρήση των ψηφιακών πιστοποιητικών γίνεται σε συνδυασμό με την χρήση του πρωτοκόλλου SSL. Προτείνεται στους ΠΥΔ, η απόκτηση ενός ή περισσότερων ψηφιακών πιστοποιητικών και η εγκατάστασή τους στους εξυπηρετητές που διατηρούν. Κατ' αυτόν τον τρόπο προτείνεται να εξασφαλίζεται η σύνδεση των χρηστών, τουλάχιστον, στις σελίδες όπου φιλοξενούνται οι φόρμες συλλογής προσωπικών δεδομένων που απαιτούνται για την κατάρτιση της σύμβασης μεταξύ των χρηστών και των ΠΥΔ.

10. Αποφεύγουν τη μεταβίβαση των προσωπικών ή/ και ευαίσθητων σε χώρες εκτός ΕΕ ή τρίτες χώρες που δεν παρέχουν επίπεδο ασφάλειας ανάλογο με αυτό που παρέχεται από Ευρωπαϊκές χώρες. Για το λόγο αυτό θα πρέπει να αποφεύγεται η απόκτηση ψηφιακών πιστοποιητικών από χώρα που δεν παρέχει ικανοποιητικό επίπεδο ασφάλειας εκτός αν:

- Δεν απαιτείται η αυθεντικοποίηση του χρήστη με χρήση ψηφιακών πιστοποιητικών στις υπηρεσίες που παρέχει ο ΠΥΔ.

- Η Εκδούσα Αρχή του πιστοποιητικού, έχει συμπεριλάβει στην αλυσίδα πιστοποίησης της κάποια Εκδούσα Αρχή που λειτουργεί σε χώρα εντός ΕΕ ή σε χώρα όπου παρέχει ικανοποιητικό επίπεδο ασφάλειας για τα προσωπικά δεδομένα η οποία δεσμεύεται για την μη μεταβίβαση των προσωπικών δεδομένων σε χώρες εκτός ΕΕ.

11. Ενθαρρύνουν και να παρέχουν τα κατάλληλα τεχνολογικά μέσα που απαιτούνται για την επίτευξη ανώνυμων επικοινωνιών. Για παράδειγμα συστήνεται η διατήρηση από κάθε ΠΥΔ ενός ανώνυμου εξυπηρετητή ηλεκτρονικού ταχυδρομείου (anonymous re-mailer). Σε περιπτώσεις όπου είναι νομικά αδύνατη η πλήρης ανωνυμία, ο ΠΥΔ θα πρέπει να διατηρεί ένα

αρχείο ψευδωνύμων. Το αρχείο αυτό τυπικά θα πρέπει να παρέχει την ένα προς ένα αντιστοίχηση φυσικών προσώπων και ψευδωνύμων. Οι αντιστοιχήσεις αυτές δεν θα πρέπει να αποκαλύπτονται σε τρίτους.

12. Αποφεύγεται η παρακολούθηση και καταγραφή των επικοινωνιών των χρηστών παρά μόνο σε περιπτώσεις όπου αυτό είναι απαραίτητο για την τιμολόγηση τους. Σε περιπτώσεις όπου η τιμολόγηση δεν εξαρτάται από τους πόρους (πχ payload) που χρησιμοποιεί ο χρήστης, θα πρέπει να αποφεύγεται η καταγραφή των συνδέσεων του χρήστη με χρήση των στοιχείων που παρέχουν τα πρωτόκολλα βάσει των οποίων υλοποιούνται οι υπηρεσίες του διαδικτύου. Για παράδειγμα, δεν πρέπει να καταγράφονται οι IP διευθύνσεις των χρηστών σε συνδυασμό με τα ονόματα των χρηστών (usernames) που επικοινωνούν με τον ΠΥΔ.

13. Σε περιπτώσεις όπου η καταγραφή των επικοινωνιών είναι απαραίτητη για την εξυπηρέτηση του χρήστη π.χ χρήση τεχνολογίας proxy για την μείωση του κόστους σύνδεσης με δικτυακούς τόπους όπου ο χρήστης επισκέπτεται συχνά, θα πρέπει να γίνονται γνωστοί στον χρήστη οι κίνδυνοι που απορρέουν από μια τέτοια υπηρεσία και να ζητείται η ρητή συγκατάθεσή του για την συμμετοχή του σε τέτοιου είδους υπηρεσίες.

14. Είναι υπεύθυνοι για τα διαφημιστικά λογότυπα (banners) που φιλοξενούνται από τις σελίδες τους και για τις προσωπικές πληροφορίες που μπορούν να υποκλαπούν σε περίπτωση ενεργοποίησης ενός τέτοιου λογότυπου όταν ο χρήστης πιέσει το ποντίκι του υπολογιστή του πάνω σε αυτό.

6.6.1.3 Μέτρα προστασίας Παροχέων Τελικών Υπηρεσιών

Οι Παροχείς Τελικών Υπηρεσιών εκτός των παραγράφων 1 έως 10, 12 και 14 που ισχύουν για τους ΠΥΔ θα πρέπει να:

1. Κατά την διάρκεια του προσυμβατικού σταδίου θα πρέπει να εξασφαλίζουν την συμφωνία του χρήστη σχετικά με την συναλλαγή που πρόκειται να εκτελεσθεί. Στην περίπτωση της επί γραμμής (on line) συμφωνίας χρήστη θα πρέπει να ισχύουν τα παρακάτω:

- Να είναι ευκρινής

- Να είναι όσο το δυνατόν περισσότερο κατανοητή από τον χρήστη
- Να μην είναι μακροσκελής
- Να μην δίνεται η δυνατότητα πραγματοποίησης της συναλλαγής αν δεν αποσπάται η ρητή αποδοχή της από τον χρήστη
- Να δίνεται η δυνατότητα στον χρήστη να αποσυρθεί σε οποιοδήποτε στάδιο της, ακόμα και αν έχει συμφωνήσει σε προηγούμενα στάδια

Τέλος, θα πρέπει να δίνεται η δυνατότητα στον χρήστη να προμηθευθεί (download) την συμφωνία, να την διαβάσει και στην συνέχεια να την υποβάλλει στον ΠΤΥ έτσι ώστε να συνεχισθεί η εκτέλεση της συναλλαγής.

2. Θα πρέπει να υπάρχει η ρητή συγκατάθεση του χρήστη για την εγγραφή του στις ηλεκτρονικές ταχυδρομικές λίστες που διατηρούνται από τον ΠΤΥ και αποσκοπούν στην προώθηση των προϊόντων του με χρήση του ηλεκτρονικού ταχυδρομείου ή που διατηρούνται από συνεργάτες ή άλλους συναλλασσομένους με τον ΠΤΥ.

3. Θα πρέπει να υπάρχει μια σαφής και ευκολόχρηστη διαδικασία διαγραφής του χρήστη (opt-out) από μια ηλεκτρονική ταχυδρομική λίστα. Η διαδικασία αυτή θα πρέπει να είναι πάντα στην διάθεση του χρήστη. Η αρχική αποστολή ενός ηλεκτρονικού ταχυδρομικού μηνύματος προς τον χρήστη από την πλευρά του ΠΤΥ που περιλαμβάνει οδηγίες διαγραφής από την ηλεκτρονική ταχυδρομική λίστα που διατηρεί ο ΠΤΥ δεν θα πρέπει είναι ο μοναδικός τρόπος διαγραφής του χρήστη διότι το μήνυμα αυτό μπορεί να χαθεί. Για το λόγο αυτό θα πρέπει να διατηρείται με κάποια μορφή, π.χ. υπερ-συνδέσμου (hyperlink), σε ευκρινές σημείο, στις κεντρικές σελίδες του ΠΤΥ η διαδικασία διαγραφής από την ηλεκτρονική ταχυδρομική λίστα που διατηρεί ο ΠΤΥ.

4. Σε περίπτωση που ο ΠΤΥ έχει αποστείλει την ηλεκτρονική ταχυδρομική διεύθυνση του χρήστη για εγγραφή σε συνεργάτες ή άλλους συναλλασσομένους με τον ΠΤΥ, αποτελεί ευθύνη του ΠΤΥ για την διαγραφή του από όλες τις λίστες που έχει εγγραφεί ο χρήστης έ και χουν ως πηγή της ταχυδρομικής ηλεκτρονικής διεύθυνσης του χρήστη τον ΠΤΥ.

6.6.1.4 Μέτρα προστασίας Έμπιστων Τρίτων Οντοτήτων

Οι Έμπιστες Τρίτες Οντότητες θα πρέπει να:

1. Συμπεριλαμβάνουν την πολιτική ιδιωτικότητας που ακολουθούν εντός του κειμένου Δήλωσης Πρακτικών Πιστοποίησης που ανακοινώνουν στους χρήστες.

2. Διατηρούν λογισμικό ή/ και υλικό το οποίο να δίνει την δυνατότητα στον συνδρομητή τους σχετικά με το υπολογιστικό σύστημα το οποίο θα δημιουργήσει το ιδιωτικό κλειδί που θα χρησιμοποιείται για την κρυπτογράφηση και την ψηφιακή υπογραφή των μηνυμάτων. Οι παρούσες τεχνολογίες παρέχουν δύο δυνατότητες:
   α) Δημιουργία του ιδιωτικού κλειδιού του συνδρομητή από λογισμικό που είναι εγκατεστημένο στο υπολογιστικό σύστημα του συνδρομητή. Σε αυτή την περίπτωση η ΕΤΟ απλά πιστοποιεί το δημόσιο κλειδί του συνδρομητή.

   β) Δημιουργία του ιδιωτικού κλειδιού του συνδρομητή από λογισμικό που είναι εγκατεστημένο σε υπολογιστικό σύστημα που διατηρεί η ΕΤΟ. Σε αυτή την περίπτωση η ΕΤΟ παραδίδει το πιστοποιητικό μαζί με το ιδιωτικό κλειδί στον συνδρομητή σε ένα μεταφέρσιμο αποθηκευτικό μέσο.Η αποθήκευση του ιδιωτικού κλειδιού στην ΕΤΟ, για λόγους συντήρησης ενός αντιγράφου ασφαλείας, θα πρέπει να αποτελεί μια επιπρόσθετη από την ΕΤΟ υπηρεσία που θα αφήνεται στην διακριτική ευχέρεια του συνδρομητή.

3. Είναι σε θέση να εκδίδουν ανώνυμα πιστοποιητικά για την διενέργεια ανώνυμων συναλλαγών. Στις περιπτώσεις αυτές οι ΕΤΟ είναι υπεύθυνες για την διατήρηση της μυστικότητας της μονοσήμαντης αντιστοίχησης μεταξύ συνδρομητή και ψευδωνύμου που αυτός χρησιμοποιεί. Οι πρακτικές που η ΕΤΟ ακολουθεί για την διατήρηση αυτής της μυστικότητας θα πρέπει να συμπεριλαμβάνονται στην πολιτική προστασίας της ιδιωτικότητας.

6.7 Συμπέρασμα

Η προστασία των προσωπικών δεδομένων στα πλαίσια λειτουργίας του ηλεκτρονικού εμπορίου αποτελεί κρίσιμο παράγοντα για την επιτυχημένη εκπλήρωση των στόχων του στην Κοινωνία της Πληροφορίας. Οι κίνδυνοι προσβολής της προσωπικότητας μπορούν να προστατευθούν με την εφαρμογή των κατάλληλων μέτρων προστασίας κάθε εμπλεκομένου φορέα σε μια ηλεκτρονική συναλλαγή. Μέτρα μπορούν να εφαρμοστούν σε επίπεδο χρήστη, παροχέα υπηρεσιών διαδικτύου, παροχέα τελικών υπηρεσιών, έμπιστων τρίτων οντοτήτων και άλλων ενδιαμέσων. Τεχνικές που στοχεύουν στην ανωνυμοποίηση των καναλιών επικοινωνίας, η κρυπτογράφηση, οι υπηρεσίες έμπιστων τρίτων οντοτήτων λειτουργούν προς αυτήν την κατεύθυνση.

ΚΕΦΑΛΑΙΟ 7

ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ(E-MAIL)

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών.

Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι σημαντικό να διαχειριζόμαστε τη διεύθυνση της ηλεκτρονικής μας αλληλογραφίας με την ίδια προσοχή που διαχειριζόμαστε τον αριθμό του τηλεφώνου μας.

7.1 Πλεονεκτήματα ηλεκτρονικού ταχυδρομείου

Τα πλεονεκτήματα του ηλεκτρονικού ταχυδρομείου είναι η ταχύτητα,η εξοικονόμηση χρόνου και χρήματος και η ευελιξία:

- Μπορείτε να στέλνετε τα μυνήματά σας σε πολλούς παραλήπτες ταυτόχρονα.
- Τα μυνήματα φθάνουν σε οποιοδήποτε μέρος του κόσμου σε δευτερόλεπτα.
- Το κόστος αποστολής των μυνημάτων είναι μικρότερο από μια τοπική μονάδα τηλεφωνικής συνδιάλεξης ανά λεπτό,σε οποιοδήποτε μέρος του κόσμου κι αν πηγαίνει το μύνημα.
- Μπορείτε να στέλνετε και να λαμβάνετε τα μυνήματά σας από οποιονδήποτε υπολογιστή στον κόσμο, αρκεί αυτός να έχει σύνδεση με το διαδίκτυο.
- Μπορείτε να στέλνετε και να λαμβάνετε τα μυνήματά σας από οποιοδήποτε κινητό τηλέφωνο,αρκεί να έχετε σύνδεση με το διαδίκτυο.

7.2 Προβλήματα στο ηλεκτρονικό ταχυδρομείο

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

1. Ιοί

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

Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του email.

Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (στο outlook express επιλέξτε Προβολή->Διάταξη->απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»).

Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

2. Ενοχλητική αλληλογραφία(spam mail)

Είναι το λεγόμενο spam ή junk mail, δηλαδή μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ.ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

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

καρτέλες στο μενού του προγράμματος.

Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

3. Μηνύματα απατηλού περιεχομένου (hoaxes)

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

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

2. «Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται

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

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος.

Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

7.3 Προστασία προσωπικών δεδομένων

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού email .

Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail , οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

7.4 Μέτρα αντιμετώπισης

Αν και το ηλεκτρονικο ταχυδρομειο(e-mail) ήταν **,**είναι και ,όπως όλα δείχνουν , θα συνεχίσει να είναι η δολοφονική εφαρμογή (killer application) του διαδικτύου , ακόμα και σήμερα τα περισσότερα προγράμματα αποστολής και λήψης e-mail δεν εγγυώνται σε καμία περίπτωση τη διασφάλιση του προσωπικού απορρήτου του χρήστη ούτε και την ακεραιότητα της λειτουργίας του συστήματός του .Εξάλλου , ακόμα και ένας μέσος κράκερ γνωρίζει πολύ καλά ότι η υποκλοπή των ηλεκτρονικών μηνυμάτων υπό συγκεκριμένες συνθήκες είναι εξαιρετικά εύκολη υπόθεση . Για να κατανοήσει κάποιος το πώς είναι εφικτό κάτι τέτοιο ,αξίζει να αναφερθούμε συνοπτικά στον τρόπο διακίνησης της ηλεκτρονικής αλληλογραφίας .

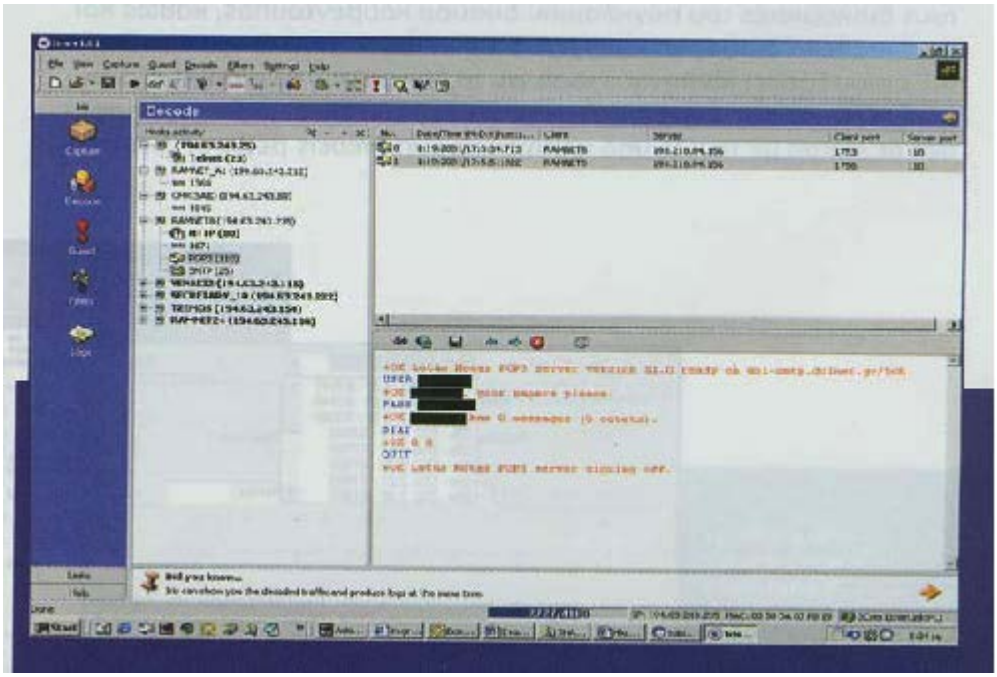
Κύριος φορέας των μηνυμάτων e-mail είναι το πρωτόκολλο επικοινωνίας SMTP (Simple Mail Transfer Protocol). Το SMT P αναλαμβάνει τη μεταφορά μηνυμάτων από το μ ηχάνημα του χρήστη σε ένα διακομιστή αλληλογραφίας (mail server), καθώς και την προώθηση του από έναν mail server σε κάποιον άλλο . Κάθε εταιρεία παροχής ιντερνετικών υπηρεσιών (Internet Provide Server) διαθέτει έναν ή περισσότερους διακομιστές αλληλογραφίας , οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την αποστολή των μηνυμάτων . Όταν ένας χρήστης συνδέεται τηλεφωνικά (dialup) με τον ISP του , μπορεί να «κατεβάσει » την αλληλογραφία του από τον mail server του ISP στον υπολογιστή του , με τη βοήθεια του πρωτοκόλλου POP (Post Office Protocol) ή του IMAP (Internet Access Protocol)

Το ζήτημα της ασφάλειας που προκύπτει από τον τρόπο ανταλλαγής του e-mail, έγκειται στο γεγονός ότι τα πακέτα SMTP , τα οποία διέρχονται το δίκτυο του ιντερνετικού φορέα ή ένα εταιρικό δίκτυο , είναι δυνάμει προσπελάσιμα από οποιονδήποτε έχει πρόσβαση στο εκάστοτε δίκτυο και χρησιμοποιεί ένα εργαλείο ανάλυσης δικτύων (network diagnostics tool ή αλλιώς sniffer). Εργαλεία του είδους είναι διαθέσιμα στο διαδίκτυο και μάλιστα οποιοσδήποτε μπορεί να τα βρει σχετικά εύκολα

Βασική λειτουργία των sniffer είναι η σύλληψη των πακέτων που διέρχονται έναν κό μβο ενός οποιουδήποτε δικτύου . Ένας υπέρ το δέον αδιάκριτος χρήστης μπορεί

να επιδοθεί στο «ευγενές » άθλημα της υποκλοπής ηλεκτρονικής αλληλογραφίας , κοινώς e-mail snooping, χρησιμοποιώντας ένα πρόγραμμα για «sniffing».

Ένας εκπρόσωπος της κατηγορίας των sniffer είναι το πρόγραμμα Iris της εταιρείας eEye Digital Security, για την πλατφόρμα των Windows.
Το πρόγραμμα είναι ικανό να συλλαμβάνει όλα τα πακέτα δεδομένων τα οποία περνούν μια δεδομένη
στιγμή από το τμήμα του δικτύου στο οποίο είναι συνδεδεμένος ο υπολογιστής που το φιλοξενεί .



Εικόνα 8.1: Το πρόγραμμα Iris εν δράσει .Διακρίνονται τα πακέτα POP που απεστάλησαν όταν επιχειρήθηκε το «κατέβασμα » των e-mail από το διακομιστή αλληλογραφίας . Εκτός από το περιεχόμενο των e-mail που ελήφθησαν , τα περιεχόμενα των πακέτων POP αποκαλύπτουν τον κωδικό πρόσβασης (password), καθώς και το όνομα χρήστη (username), που χρησιμοποιούνται για την πρόσβαση στον εν λόγω διακομιστή .

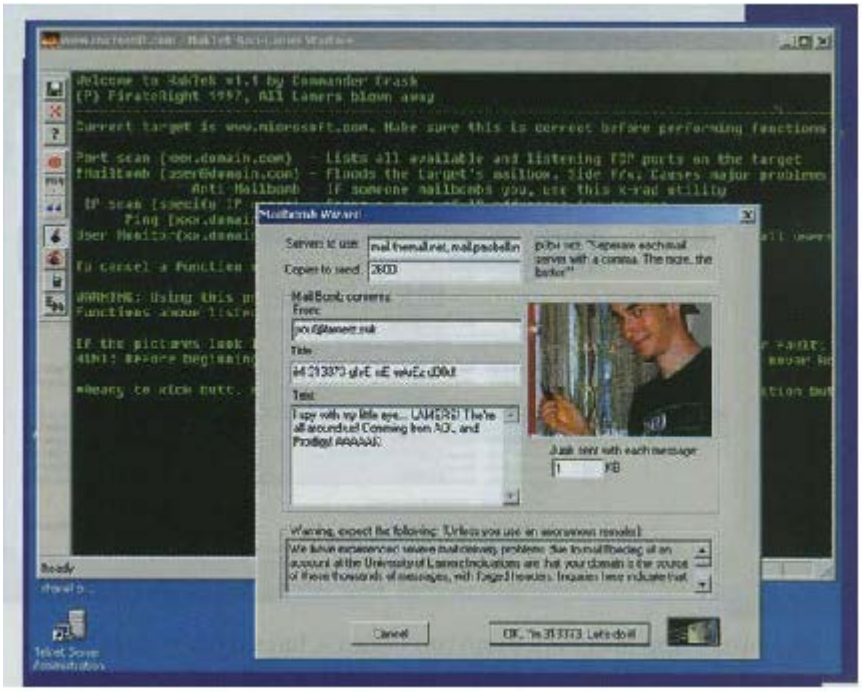
Δυστυχώς , η υποκλοπή δεδομένων μέσω sniffer δεν αποτελεί το μόνο κίνδυνο για την αποστολή και τη λήψη ηλεκτρονικού ταχυδρομείου .Μια ιδιαίτερα προσφιλής πρακτική για όλους τους χαιρέκακους θαμώνες του διαδικτύου είναι το λεγόμενο e-mail bombing. Η λογική του εν λόγω «βομβαρδισμού » είναι εξαιρετικά απλή και συνίσταται στην αποστολή μεγάλου αριθμού e-mail στο λογαριασμό ενός χρήστη .Οι περισσότεροι από εμάς θα έχουν παρατηρήσει πόσο χρονοβόρο και επίπονο είναι το κατέβασμα ενός e-mail, το μέγεθος του οποίου υπερβαίνει τα 3 ή 4 MB , ιδιαίτερα στις αργές συνδέσεις dialup.

Εύκολα , λοιπόν , μπορεί κάποιος να φανταστεί τι θα συμβεί στην περίπτωση που κάποιος μας έχει αποστείλει μηνύματα e-mail, το συνολικό μέγεθος των οποίων είναι γύρω στα 50,100 ή και 500 MB(!).Ο λογαριασμός του χρήστη καθίσταται ουσιαστικά άχρηστος αφού , προκειμένου να κατεβάσει το ηλεκτρονικό του ταχυδρομείο ,

οφείλει να κατεβάσει και ολόκληρα Mmegabyte «σκουπιδιών », που του έχει αποστείλει ο ανώνυμος «βομβιστής ». Συνήθως , ο υπαίτιος του βομβαρδισμού φροντίζει να καλύπτει τα ίχνη του , εξαπολύοντας την επίθεση του από έναν κλεμμένο λογαριασμό ή μεταμφιέζοντας την ηλεκτρονική του διεύθυνση (IP spoofing).

Αν και οι επιθέσεις γίνονται συνήθως με χρήση ειδικών προγραμμάτων - σεναρίων (scripts), υπάρχει ένα πλήθος εξαιρετικά εύχρηστων προγραμμάτων στο διαδίκτυο , τα οποία επιτρέπουν ακόμα και σε αδαείς να πραγματοποιούν ... βομβαρδισμούς .

Ένα από αυτά είναι το Hacktek (Εικόνα 8.2).



Εικόνα 8.2: Το πρόγραμμα Hacktek παρέχει τη δυνατότητα πραγματοποίησης επιθέσεων “mail bombing”, αποκρύπτοντας ταυτόχρονα την πηγή της επίθεσης . Ο συγγραφέας του προγράμματος δεν δίστασε να ενσωματώσει και μια δική του φωτογραφία .

Μετά το mail bombing έρχεται ένα άλλο «ing», το spamming. Αν και δεν είναι καταστροφικό σαν το πρώτο , είναι σίγουρα άκρως εκνευριστικό . Ο όρος spamming αποδίδεται στην αυθαδέστατη τακτική που ακολουθούν πολλοί ιντερνετικοί τόποι , οι οποίοι ενοχλούν κατ ' εξακολούθηση τους χρήστες με κάθε λογής διαφημιστικά μηνύματα και προσφορές , χωρίς προηγουμένως να έχουν λάβει την έγκριση τους . Οι ενοχλητικοί διαφημιστές συνήθως χρησιμοποιούν προγράμματα αυτόματης αναζήτησης ηλεκτρονικών διευθύνσεων (spambots), για να ανασύρουν ηλεκτρονικές διευθύνσεις από διάφορους δικτυακούς τόπους .

Αν και οι κίνδυνοι από όλες τις προαναφερθείσες «μάστιγες » είναι όντως υπαρκτοί , σε καμία περίπτωση δεν είναι αναπόφευκτοι , αρκεί να λαμβάνονται ορισμένα απλά ακόμη και στοιχειώδη μέτρα προστασίας .

7.4.1 Κρυπτογράφηση e-mail

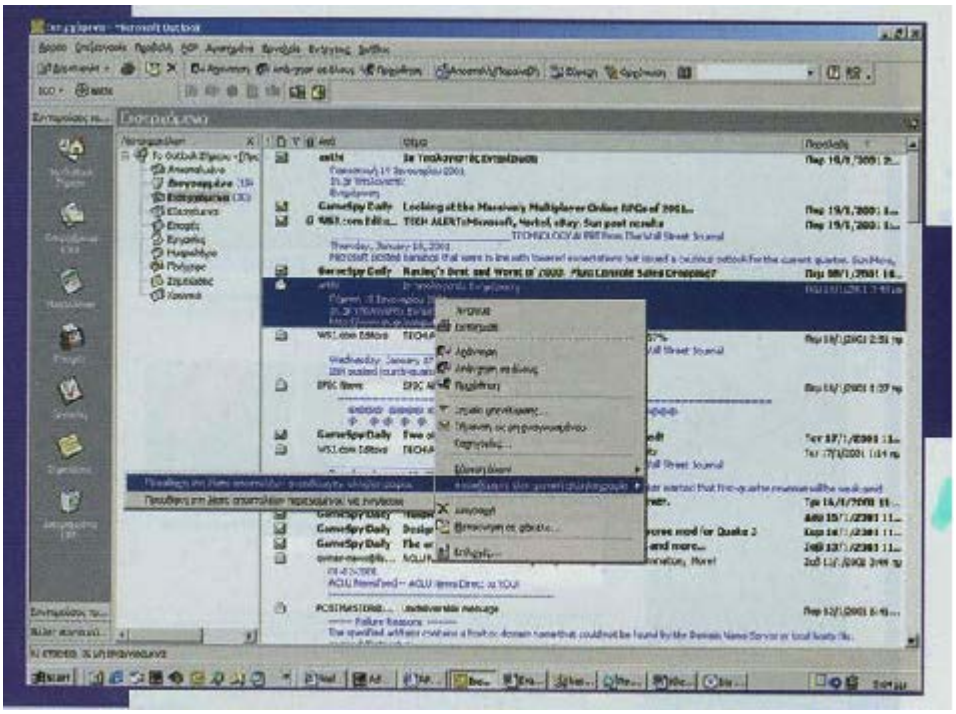
Πολλά είναι τα προγράμματα αποστολής ηλεκτρονικού ταχυδρομείου , τα οποία υποστηρίζουν κάποια μορφή κρυπτογράφησης δεδομένων . Τα πακέτα που αποστέλλονται κρυπτογραφημένα είναι πρακτικά άχρηστα για τους χρήστες των sniffer, αφού ακόμα και μετά τη «συναρμολόγηση » τους δεν προκύπτει νόημα από τη μορφή τους . Η καλύτερη λύση για την κρυπτογράφηση μηνυμάτων , καθώς και αρχείων οποιασδήποτε μορφής , προσφέρεται από το γνωστό , δωρεάν προσφερόμενο και πανίσχυρο σύστημα κρυπτογράφησης , το PGP (Pretty Good Privacy).

7.4.2 Αντιμετώπιση του spamming

Συνήθως ,ο παραλήπτης spam από ένα συγκεκριμένο δικτυακό τόπο , έχει τη δυνατότητα να διαγραφεί από μια σχετική λίστα παραληπτών , αρκεί να στείλει ένα e-mail με συγκεκριμένη μορφή σε κάποια ηλεκτρονική διεύθυνση που αναγράφεται στο τέλος του spam-mail (π .χ ., ίσως πρέπει να στείλει ένα e-mail με τη λέξη «Unsubscribe» στη θυρίδα του θέματος -Subject). Στην περίπτωση , όμως , που δεν προσφέρεται η συγκεκριμένη δυνατότητα , τότε ο χρήστης μπορεί να καταφύγει στις δυνατότητες φιλτραρίσματος του προγράμματος ηλεκτρονικής αλληλογραφίας που χρησιμοποιεί . Ο χρήστης του Outlook, για παράδειγμα , θα κάνει δεξί «κλικ » επάνω στο ανεπιθύμητο e-mail, θα επιλέξει «Ανεπιθύμητη ηλεκτρονική αλληλογραφία » και θα προσθέσει τη διεύθυνση του αποστολέα στη λίστα των ανεπιθύμητων (Εικόνα 8.3).

7.4.3 Αναζητώντας καταφύγια

Η αντιμετώπιση του e-mail bombing είναι μια υπόθεση , η οποία (πρέπει να) απασχολεί πρώτιστα τους διαχειριστές κάθε ιντερνετικού φορέα και όχι τον ίδιο το χρήστη . Οι μεγαλύτεροι ISP μπορούν να εφοδιάσουν τους διακομιστές αλληλογραφίας μ ε λογισμικό αυτόματης αντιμετώπισης τέτοιου είδους επιθέσεων όπως π .χ . το e-Safe Gateway της εταιρείας Alladin



Εικόνα 8.3: Ο χρήστης του Outlook μπορεί να απαλλαγεί μια για πάντα από τα ανεπιθύμητα μηνύματα , προσθέτοντάς τα στη λίστα αποστολέων ανεπιθύμητης αλληλογραφίας του προγράμματος .

ΚΕΦΑΛΑΙΟ 8

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΙΟΥΣ

8.1 Προγράμματα προσβολής ενός υπολογιστή

8.1.1. Ιός

Ο ιός του υπολογιστή είναι ένα κομμάτι προγράμματος, το οποίο αντιγράφει τον εαυτό του και επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα. Όταν το μολυσμένο πρόγραμμα εκτελεστεί (το λεγόμενο «άνοιγμα μολυσμένου αρχείου»), κάτω από ορισμένες συνθήκες, προσπαθεί να μολύνει και άλλα προγράμματα, να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Η ύπαρξη ιών είναι ένα από τα σημαντικότερα προβλήματα του Διαδικτύου. Υπάρχουν σήμερα χιλιάδες διαφορετικοί ιοί, οι οποίοι προσβάλλουν εκατομμύρια υπολογιστών σε όλον τον κόσμο. Πολλοί έχουν τη δυνατότητα να μεταλλάσσονται και να διαφέρουν σε μεγάλο βαθμό από τον αρχικό ιό. Σε περίπτωση που μιλάμε για υπολογιστές δικτύων, η καταστροφή έχει ακόμα μεγαλύτερες διαστάσεις, καθώς μολύνονται και καταρρέουν αρχεία εταιρειών, πανεπιστημίων, υπουργείων, ακόμα και κυβερνήσεων.

8.1.2 Δούρειος Ίππος (Trojan horse)

Πρόκειται για ένα είδος προγράμματος, το οποίο δεν αναπαράγεται και δρα «υπογείως», χωρίς ο χρήστης του υπολογιστή να αντιλαμβάνεται αρχικά την ύπαρξή του. Το πρόγραμμα αυτό ενεργεί ως μέσο μεταφοράς άλλων μορφών επιβλαβούς λογισμικού (malware), ενεργοποιείται σε συγκεκριμένο χρόνο και δημιουργεί ένα αντίγραφο του αυθεντικού προγράμματος που χρησιμοποιείται από το χρήστη, το οποίο θα δουλεύει κανονικά, σα να ήταν το αυθεντικό. Όταν ο χρήστης εκτελέσει το συγκεκριμένο πρόγραμμα χρησιμοποιεί την έκδοση του Δούρειου Ίππου, ο οποίος δρα καταστροφικά.

8.1.3 Σκουλήκια (worms)

Πρόκειται για προγράμματα υπολογιστών τα οποία αντιγράφουν τον εαυτό τους σε δίκτυα Η/Υ. Χρησιμοποιούν το Internet ως μέσο διάδοσής τους (emails, irc chat κ.ά.). Αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα σφάλματα των λειτουργικών προγραμμάτων των υπολογιστών. Οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονται από αντίγραφα του «σκουληκιού» και δε μπορούν να λειτουργήσουν.

8.2 Τρόποι μετάδοσης

- Από μολυσμένη δισκέτα ή μολυσμένο cd
- Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων του υπολογιστή
- Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων που επισυνάπτονται σε μηνύματα ηλεκτρονικής αλληλογραφίας
- Από άνοιγμα ή ανάγνωση αγνώστων μηνυμάτων ηλεκτρονικής αλληλογραφίας που περιέχουν καταστροφικό κώδικα (malicious code)
- Από άνοιγμα ή ανάγνωση μολυσμένων ιστοσελίδων .htm και .html

8.3 Τρόποι προστασίας

- Επιλογή ενός καλού αντιβιοτικού προγράμματος
- Τακτική ανίχνευση όλου του δίσκου με το αντιβιοτικό σας πρόγραμμα
- Συνεχής ανανέωση (update) του αντιβιοτικού προγράμματος
- Έλεγχος κάθε δισκέτας/cd με το αντιβιοτικό σας πρόγραμμα πριν την ανοίξετε.
- Τήρηση αντιγράφων ασφαλείας όλων των αρχείων σας σε cd ή δισκέτα.
- Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού σας.
- Ανίχνευση μέσω του αντιβιοτικού κάθε νέου αρχείου που «κατεβάζετε» από το Internet.
- Αν χρησιμοποιείτε irc chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.
- Επιλέξτε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσετε το

αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.

- Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.
  Εδώ πρέπει να επισημανθεί πως όσο πιο αυστηρές ρυθμίσεις ασφαλείας ενεργοποιείτε στον υπολογιστή σας, τόσο πιο δύσκολα έχετε πρόσβαση σε σελίδες του Διαδικτύου. Η συνήθης ρύθμιση ασφαλείας στους φυλλομετρητές είναι η «μεσαία».

ΚΕΦΑΛΑΙΟ 9

ΝΕΕΣ ΤΕΧΝΙΚΕΣ ΠΩΛΗΣΕΩΝ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΕΙΣΑΓΩΓΗ

Το ηλεκτρονικό εμπόριο αποτελεί σήμερα το δεύτερο πιο δημοφιλές αντικείμενο συζήτησης μεταξύ των στελεχών επιχειρήσεων και των κρατικών αξιωματούχων στην Ελλάδα (πρώτο παραμείνει ακόμη το Χρηματιστήριο). Κάθε τόσο ακούμε κυβερνητικές και ευρωπαϊκές εξαγγελίες για μέτρα ενθάρρυνσης των επενδύσεων σε αυτό το χώρο, ενώ ο τύπος δημοσιεύει συνεχώς μελέτες σύμφωνα με τις οποίες η επιχειρηματική δραστηριότητα μετακομίζει στο δίκτυο και σύντομα όλες οι εργασίες και οι αγοραπωλησίες θα γίνονται μέσα από αυτό.

Όπως είναι φυσικό, υπάρχει μια ισχυρή δόση υπερβολής σε όλες αυτές τις προβλέψεις (μέχρι σήμερα σχεδόν καμία νέα τεχνολογία δεν αντικατέστησε εντελώς τις προηγούμενες). Είναι όμως γεγονός πως βρισκόμαστε μπροστά σε μια πραγματική επανάσταση.

Μέσα σε αυτόν τον κυκεώνα προφητειών, ιδεών και προειδοποιήσεων, κάθε επενδυτής καλείται να προβλέψει ποια είναι εκείνα τα δεδομένα που θα μεταβληθούν στο άμεσο ή το απώτερο μέλλον και ποιες από τις παρουσιαζόμενες ως επαναστατικές αλλαγές θα αποδειχθούν επιτυχημένες και δεν θα προστεθούν στο WAIS, τις Push Technologies, τα e-malls και τα άλλα πολυδιαφημισμένα εργαλεία του δικτύου τα οποία τελικά αποδείχθηκαν άχρηστα και παραδόθηκαν στον Καιάδα των αποτυχημένων τεχνολογιών μαζί με τα εκατομμύρια δολάρια που δαπανήθηκαν για την ανάπτυξή τους.

Δυστυχώς, αυτό το άγχος για την καλύτερη κατανόηση και πρόβλεψη της εξέλιξης των τεχνολογιών Internet μας κάνει συχνά να ξεχνάμε πως η επιχειρηματική δραστηριότητα στο δίκτυο έχει τις ίδιες απαιτήσεις ανάλυσης, σχεδιασμού, κοστολόγησης, οικονομικής διαχείρισης, έρευνας αγοράς και διαφήμισης με κάθε ανάλογη προσπάθεια στην "παραδοσιακή" οικονομία.

Πριν από κάθε επένδυση απαιτείται η σύνταξη μιας σοβαρής μελέτης βιωσιμότητας η οποία θα περιλαμβάνει μεταξύ άλλων ρεαλιστικές εκτιμήσεις για τα απαιτούμενα έξοδα και τα προβλεπόμενα έσοδα της επένδυσης αυτής. Όσο και αν φαίνεται αντιτεχνολογικό λοιπόν η δημιουργία ενός ηλεκτρονικού καταστήματος ξεκινάει πάντοτε από ένα φύλλο λευκό χαρτί. Πάνω σε αυτό το απλό παραδοσιακό μέσο ο επίδοξος "δικτυοεπιχειρηματίας" πρέπει να γράψει τα ακόλουθα ερωτήματα μαζί με τις απαντήσεις τους: Ποιος, Τι, Πώς;

Ποιος;

Όπως σε κάθε επιχείρηση πώλησης, έτσι και σε ένα ηλεκτρονικό κατάστημα (e-store) η πρώτη ερώτηση που πρέπει να απαντηθεί είναι: "Σε ποια αγορά απευθύνεται

το κατάστημα;. Ποιο είναι το κοινό το οποίο προσδοκούμε πως θα επισκέπτεται αυτό το χώρο για να αγοράσει προϊόντα ή να παραγγείλει υπηρεσίες;"

Για να απαντήσει μια ελληνική επιχείρηση στο ερώτημα αυτό θα πρέπει να ξεκαθαρίσει τα ακόλουθα θέματα:

1. Εθνικότητα, Τόπος Κατοικίας, Γλώσσα

Το ηλεκτρονικό κατάστημα μπορεί να απευθύνεται μόνο στους Ελλαδίτες (κατοίκους Ελλάδος) χρήστες του Internet, στους Έλληνες του εξωτερικού, τους κατοίκους μιας συγκεκριμένης χώρας, σε ολόκληρο τον κόσμο ή σε ένα συνδυασμό όλων των παραπάνω.

Αντίθετα απ' ό,τι συμβαίνει στις ΗΠΑ, στην Ευρώπη και στην Ελλάδα οι περισσότερες επενδύσεις στο χώρο των ηλεκτρονικών καταστημάτων γίνονται από επιχειρήσεις οι οποίες δραστηριοποιούνται ήδη στο χώρο αυτό μέσω παραδοσιακών μορφών εμπορίου (π.χ. αλυσίδες βιβλιοπωλείων, ή καταστημάτων πώλησης Η/Υ). Για τον λόγο αυτό, συνήθως οι επιχειρήσεις αυτές προσεγγίζουν την παρουσία τους στο δίκτυο ως ένα ακόμη υποκατάστημα και σπάνια αναγνωρίζουν ότι το Internet τους δίνει πρόσβαση και σε άλλες, μεγαλύτερες και πιο προσοδοφόρες αγορές.

Έτσι, πολύ συχνά, όταν το ηλεκτρονικό κατάστημα ξεκινήσει τις εργασίες του, είτε χάνει σημαντικές αγορές, είτε υποχρεώνεται να επανασχεδιαστεί από την αρχή, επεκτείνοντας τις δυνατότητες του συστήματος χρέωσης και διανομής και καλύπτοντας όσες ανάγκες ή προκλήσεις εμφανίστηκαν στην πορεία.

Χαρακτηριστικό παράδειγμα τέτοιας ανάγκης αποτελεί η πώληση σε Έλληνες του εξωτερικού οι οποίοι πολλές φορές αποδεικνύονται πολύ σημαντικότεροι πελάτες απ' ό,τι αναμενόταν, ακόμη και για "απρόβλεπτα" προϊόντα όπως τα αθλητικά σουβενίρ ή τα ελληνικά γλυκά. Αξίζει επίσης να σημειωθεί πως η Ελλάδα και τα ελληνικά προϊόντα παρουσιάζουν ενδιαφέρον ακόμη και για Έλληνες δεύτερης, τρίτης ή τέταρτης γενεάς οι οποίοι είτε δεν γνωρίζουν ελληνικά είτε δεν έχουν εγκαταστήσει το απαραίτητο λογισμικό στον Η/Υ τους για την απεικόνιση ελληνικών χαρακτήρων.

2. Δημογραφικά Χαρακτηριστικά

Η ηλικία, το μορφωτικό επίπεδο και η οικογενειακή κατάσταση του κοινού στο οποίο απευθύνεται το κατάστημα παίζουν σημαντικό ρόλο στη δημιουργία του. Η γλώσσα που θα χρησιμοποιηθεί (τεχνική με πολλούς ειδικούς όρους σε ένα site για επαγγελματίες ή απλή καθημερινή σε ένα site για το ευρύ κοινό), η σχεδίαση η οποία θα επιλεγεί (σοβαρή, χαρούμενη, παιδική, ξένοιαστη κ.λπ.), οι τεχνικές δυνατότητες που θα παρέχονται (εξειδικευμένες εφαρμογές για power users ή απλές φόρμες παραγγελίας) κ.λπ. αποτελούν θέματα τα οποία πρέπει να έχουν καθοριστεί πολύ πριν αρχίσει η κατασκευή του καταστήματος.Όπως συμβαίνει σε όλες τις ανθρώπινες δραστηριότητες, έτσι και εδώ η πρόληψη κοστίζει πάντοτε πολύ λιγότερο από τη θεραπεία.

3. Αγοραστικές συνήθειες

Κάθε κοινό έχει τις δικές του ιδιαίτερες προτιμήσεις οι οποίες πρέπει να γίνουν σεβαστές από τους δημιουργούς ηλεκτρονικών καταστημάτων. Για παράδειγμα, οι μεγαλύτεροι σε ηλικία άνθρωποι προτιμούν να πληρώνουν μετρητοίς και όχι με πιστωτικές κάρτες, ενώ τα παιδιά δεν έχουν κάρτες, αλλά βάζουν τους γονείς τους να αγοράζουν για λογαριασμό τους, γι' αυτό και η πιστωτική κάρτα είναι ένας καλός τρόπος πληρωμής γι' αυτή την κατηγορία αγοραστών.

Ανάλογες ιδιαιτερότητες υπάρχουν και στον τομέα της συσκευασίας και αποστολής των προϊόντων. Οι χρήστες του Internet αρχίζουν σιγά σιγά να συνειδητοποιούν πως το κόστος λήψης μιας μικρής παραγγελίας είναι υπερβολικά υψηλό, ενώ μειώνεται σημαντικά όσο μεγαλώνει ο όγκος της (τα ταχυδρομικά έξοδα αποστολής ενός μικρού δέματος δεν είναι πολύ μικρότερα από τη δαπάνη αποστολής ενός μεγάλου). Για να αποφύγουν λοιπόν τα υψηλά έξοδα παράδοσης, οι πελάτες συνηθίζουν να αγοράζουν πολλά πράγματα μαζί ή να προμηθεύονται μεγάλες ποσότητες σε αραιά χρονικά διαστήματα.

Ένα ηλεκτρονικό κατάστημα πρέπει να έχει προβλέψει αυτή τη συμπεριφορά (καθώς και άλλες παρόμοιες), προσαρμόζοντας ανάλογα την εμπορική του πολιτική (π.χ. "οικογενειακές" συσκευασίες, επιπρόσθετα κίνητρα για παραγγελίες μεγαλύτερες από ένα ποσό κ.λπ.).

4. Επιχειρήσεις ή ιδιώτες;

Λόγω της μεγάλης απήχησης που έχουν στο ευρύ κοινό οι επιχειρήσεις πώλησης καταναλωτικών προϊόντων (Amazon, CDnow κ.λπ.), οι περισσότεροι άνθρωποι έχουν την τάση να συνδέουν το ηλεκτρονικό εμπόριο με τις πωλήσεις καταναλωτικών προϊόντων (Business to Consumer Commerce). Ωστόσο, μέσα στο δίκτυο το 90% των συναλλαγών στις ΗΠΑ, και το 70% στην Ευρώπη, διεξάγεται μεταξύ επιχειρήσεων (Business to Business Commerce).

Η διαφορά μεταξύ B2B (Business to Business) και B2C (Business to Consumer) γίνεται ακόμη μεγαλύτερη αν συγκρίνουμε την κερδοφορία αυτών των δύο αγορών. Στο B2B πραγματοποιείται μικρός αριθμός παραγγελιών μεγάλης αξίας (ακριβά προϊόντα ή μεγάλες ποσότητες) από μικρό αριθμό πελατών (επιχειρήσεις), ενώ στο B2C πραγματοποιείται μεγάλος αριθμός παραγγελιών σχετικά μικρής αξίας (καταναλωτικά προϊόντα σε μικρές ποσότητες) από έναν πολύ μεγάλο αριθμό πελατών (ιδιώτες).

Όπως είναι φυσικό, οι δαπάνες εξυπηρέτησης χιλιάδων μικρών παραγγελιών από ένα B2C ηλεκτρονικό κατάστημα επιβαρύνουν σημαντικά το κόστος λειτουργίας του και περιορίζουν τα περιθώρια κέρδους όλων των καταστημάτων αυτής της μορφής. Γι' αυτό και, ενώ υπάρχουν ήδη χιλιάδες κερδοφόρα sites B2B, οι περισσότερες επιχειρήσεις B2C είναι ακόμη ζημιογόνες και συντηρούνται μόνο χάρη στην υψηλή χρηματιστηριακή τους αξία (οι μετοχές τους βρίσκονται σε εξαιρετικά υψηλά

επίπεδα, καθώς όλοι προσδοκούν πως όταν γίνουν κερδοφόρα θα αποκτήσουν δεσπόζουσα θέση στο χώρο του ηλεκτρονικού εμπορίου).

Αυτά τα οικονομικά δεδομένα πρέπει να ληφθούν σοβαρά υπ' όψιν από κάθε επιχείρηση η οποία σχεδιάζει την είσοδό της στο χώρο του ηλεκτρονικού εμπορίου. Θα πρέπει επίσης να μελετηθούν από πολλές επιχειρήσεις οι οποίες μέχρι σήμερα διστάζουν να κινηθούν δυναμικά στο Internet, θεωρώντας λανθασμένα πως δεν υπάρχει ιδιαίτερο ενδιαφέρον για τα προϊόντα τους (π.χ. πώληση υπηρεσιών φασόν, πρώτων υλών, υπηρεσιών εκπαίδευσης κ.λπ.)

Τι;

Θεωρητικά, τα πάντα θα μπορούσαν να πουληθούν μέσω του Internet. Ωστόσο, η μέχρι σήμερα εμπειρία έχει δείξει πως ορισμένα προϊόντα δεν προσφέρονται ιδιαίτερα για πωλήσεις μέσω δικτύου, ενώ άλλα γίνονται πολύ πιο εύκολα δεκτά από τους χρήστες του Internet. Τα κύρια χαρακτηριστικά των προϊόντων τα οποία έχουν αποδειχθεί δημοφιλή μεταξύ των αγοραστών του δικτύου είναι:

Πολλά είδη

Το δίκτυο αποτελεί τον ιδανικό χώρο για την πώληση προϊόντων τα οποία έχουν πάρα πολλά είδη (βιβλία, CD, εξαρτήματα Η/Υ, αλλά ακόμη και πιο ασυνήθιστα προϊόντα όπως ανταλλακτικά αυτοκινήτων, αντίκες, είδη γραφείου και άλλα).Ένα ηλεκτρονικό κατάστημα με τέτοια προϊόντα υπερέχει σημαντικά έναντι των παραδοσιακών καταστημάτων σε ποικιλία και ευχρηστία, καθώς σε αυτό ο πελάτης μπορεί να βρει 24 ώρες το 24ωρο πολύ περισσότερα είδη απ' όσα διαθέτει οποιοδήποτε κλασικό (bricks and mortar κατά την αγγλική ορολογία) κατάστημα.Το ηλεκτρονικό κατάστημα λοιπόν έχει ένα ισχυρό Unique Selling Proposal (παρέχει υπηρεσίες που είναι δύσκολο ή αδύνατο να παρασχεθούν από ένα κοινό κατάστημα.)

Εξειδικευμένα προϊόντα

Η μεγάλη δημοτικότητα του δικτύου ενθαρρύνει την πώληση προϊόντων τα οποία είναι πολύ ειδικά για να καταστήσουν οικονομικά βιώσιμο ένα παραδοσιακό κατάστημα. Για παράδειγμα, αν ένα κατάστημα χρειάζεται 1000 πελάτες το χρόνο για να καλύψει τα έξοδά του, αυτοί θα βρεθούν πολύ πιο εύκολα στο παγκόσμιο κοινό του Internet (όπου οι 1000 πελάτες αποτελούν το 0,0000036% των 276 εκατομμυρίων χρηστών του δικτύου) παρά στην Αθήνα όπου οι 1000 πελάτες αποτελούν το 0,005% των 200.000 ανθρώπων οι οποίοι απέχουν 20 λεπτά από το κατάστημα (έρευνες έχουν δείξει πως αν απαιτούνται περισσότερα από 20 λεπτά, με οποιοδήποτε μέσο μεταφοράς, για να φθάσει κανείς σε ένα κατάστημα, τότε οι πιθανότητες να γίνει πελάτης του μειώνονται δραματικά).

Αυτή η ιδιαιτερότητα ανοίγει τον δρόμο για τη δημιουργία πολλών νέων καταστημάτων αφιερωμένων σε πολύ εξειδικευμένα προϊόντα για τα οποία ποτέ κανείς δεν θα φανταζόταν ότι θα ήταν δυνατή η αυτόνομη πώλησή τους.Χαρακτηριστικό παράδειγμα καταστήματος αυτής της μορφής είναι το Boxers-etcetera (http://www.boxers-etcetera.com) το οποίο είναι αφιερωμένο αποκλειστικά σε προϊόντα για σκυλιά ράτσας boxer. Σε καμία περιοχή του κόσμου δεν υπάρχουν αρκετοί ιδιοκτήτες τέτοιων σκυλιών. Μέσα στο δίκτυο όμως υπάρχουν τόσοι πολλοί

ώστε εξασφαλίζουν άνετα την επιβίωση αυτού του καταστήματος, αλλά και πολλών άλλων παρόμοιων εξειδικευμένων (niche market) εγχειρημάτων.

Υπηρεσίες μεσολάβησης

Σύμφωνα με μια ριζοσπαστική θεώρηση, τα ηλεκτρονικά καταστήματα δεν πρέπει να αποκαλούνται καταστήματα, αλλά μεσίτες προϊόντων διότι σπανίως έχουν στην αποθήκη τους τα προϊόντα που πουλάνε. Το Amazon.com για παράδειγμα δεν είχε μέχρι πρόσφατα κανένα βιβλίο στις αποθήκες του. Διατηρούσε όμως μια εξαιρετική βάση δεδομένων με όλα τα βιβλία που διέθεταν οι εκδότες βιβλίων στην αγγλική γλώσσα και φρόντιζε να προμηθεύεται από αυτούς ό,τι ζητούσαν οι πελάτες του.

Αντίστοιχες επιχειρηματικές πρωτοβουλίες μπορούν να αναληφθούν για μια μεγάλη ποικιλία προϊόντων ή υπηρεσιών (π.χ. πώληση εισιτηρίων ή μεταχειρισμένων αυτοκινήτων, μεσιτείες, πλειστηριασμοί, αγγελίες κ.λπ.). Η αγορά αυτή είναι ακόμη αναξιοποίητη και παρέχει πολλές ευκαιρίες σε ανθρώπους με φαντασία και όραμα. Για παράδειγμα θα μπορούσε να δημιουργηθεί ένα κατάστημα το οποίο θα πωλούσε πακέτα βραδινής εξόδου στην Αθήνα (π.χ. εισιτήρια για το θέατρο Χ και μετά δείπνο στο εστιατόριο Ψ με προκαθορισμένο μενού).

Χαμηλές τιμές

Οι χρήστες του Internet γνωρίζουν πως η δημιουργία και η συντήρηση ενός ηλεκτρονικού καταστήματος είναι φθηνότερη από εκείνη ενός παραδοσιακού χώρου πωλήσεων. Για τον λόγο αυτό προσδοκούν πως και οι τιμές πώλησης θα είναι σημαντικά χαμηλότερες.

Αν και αυτή η εκτίμηση δεν ανταποκρίνεται πάντοτε στην πραγματικότητα (ένα ηλεκτρονικό κατάστημα χρειάζεται πολύ περισσότερο χρόνο από ένα παραδοσιακό, για να αποκτήσει πιστή και πολυάριθμη πελατεία), υπάρχουν προϊόντα τα οποία μπορούν να διατεθούν μέσω Internet σε σημαντικά χαμηλότερες τιμές, λόγω της πολύ φθηνότερης διαχείρισής τους μέσω δικτύου.

Για παράδειγμα, ένα πρακτορείο ταξιδίων έχει πολύ υψηλό κόστος διαχείρισης ανά πελάτη λόγω αλλεπάλληλων τηλεφωνημάτων, διαβουλεύσεων, εξηγήσεων κ.λπ. ("Εξηγήστε μου ποια πτήση είναι καλύτερη" "Πείτε μου αν είναι καλό καράβι το Σκυλοπνίχτης ΙΙ" κ.α.). Μια Internet only υπηρεσία πώλησης εισιτηρίων θα ορθολογοποιούσε το σύστημα πωλήσεων του πρακτορείου, χρεώνοντας χαμηλότερη προμήθεια σε όσους αγοράζουν online και υψηλότερη σε όσους απασχολούν προσωπικό τηλεφωνικά.

Εξοικονόμηση χρόνου

Σύμφωνα με έρευνες που έχουν διεξαχθεί σε πολλές ανεπτυγμένες χώρες, οι άνθρωποι σήμερα παραπονούνται περισσότερο για την έλλειψη χρόνου παρά για την έλλειψη χρημάτων. Τα online καταστήματα είναι ανοιχτά όλο το εικοσιτετράωρο και μπορούν να αποδειχθούν πολύ χρήσιμα σε χρονικά πιεσμένες κατηγορίες ανθρώπων όπως οι νοικοκυρές, οι εργένηδες κ.λπ.

Στις ΗΠΑ γίνεται σήμερα μια μεγάλη προσπάθεια για να καλυφθεί αυτό το κενό από ηλεκτρονικά σουπερμάρκετ, φαρμακεία και άλλα καταστήματα στα οποία ο χρήστης του Internet μπορεί να ψωνίσει online. Αξίζει πάντως να σημειωθεί πως ο παράγοντας της εξοικονόμησης χρόνου λειτουργεί μόνο για καταστήματα ειδών πρώτης ανάγκης. Όταν τα ψώνια δεν αποτελούν αγγαρεία ή αναγκαίο κακό (π.χ. η αγορά ρούχων συνδυασμένη με πρωινή βόλτα) τότε το ηλεκτρονικό κατάστημα πρέπει να βασιστεί σε κάποιο άλλο κίνητρο για να προσελκύσει τους πελάτες του (χαμηλές τιμές, εξειδικευμένα προϊόντα κ.λπ.).

Πώς;

Ο τρόπος υλοποίησης ενός καταστήματος καθορίζεται από πολλούς παράγοντες. Αναφερθήκαμε είδη στους δύο πιο σημαντικούς από αυτούς (ποια προϊόντα και σε ποιο κοινό). Ο δημιουργός ενός ηλεκτρονικού καταστήματος όμως θα πρέπει να λάβει επίσης υπ' όψιν του τον ανταγωνισμό, καθώς επίσης και τις οικονομικές και τεχνικές δυνατότητές του.

Ένα ηλεκτρονικό κατάστημα αντιμετωπίζει ανταγωνισμό από τρεις πλευρές:

- Αλλα ηλεκτρονικά καταστήματα
- Παραδοσιακά καταστήματα
- Μελλοντικούς ανταγωνιστές

Τα άλλα ηλεκτρονικά καταστήματα αποτελούν ίσως τον "ευκολότερο αντίπαλο". Βρίσκονται βέβαια ήδη στο δίκτυο και πιθανώς να έχουν αποκτήσει ένα καλό όνομα και μια αξιόλογη πελατεία. Ωστόσο, ο μελλοντικός ανταγωνιστής τους μπορεί να μελετήσει με μεγάλη ευκολία τον τρόπο λειτουργίας τους, να αντιγράψει τα θετικά τους σημεία και να αποφύγει τα μειονεκτήματά τους. Αν γίνει αυτό τότε είναι βέβαιο πως το νέο κατάστημα θα αποδειχθεί πολύ πιο φιλικό προς το χρήστη και γι' αυτό σύντομα θα γίνει ιδιαίτερα δημοφιλές (τα νέα μεταξύ των χρηστών του δικτύου διαδίδονται πολύ γρήγορα και συνήθως οι πελάτες των ηλεκτρονικών καταστημάτων δεν τους είναι ιδιαίτερα πιστοί).

Δυσκολότερο αντίπαλο για το νέο ηλεκτρονικό κατάστημα αποτελούν τα παραδοσιακά καταστήματα τα οποία διαθέτουν ένα ισχυρό όνομα (brand name) και μια μεγάλη και πιστή πελατεία. (Υπάρχουν πελάτες οι οποίοι έχουν συνηθίσει να αγοράζουν για δεκαετίες από το ίδιο κατάστημα. Γι' αυτό και συνήθως αλλάζουν τις συνήθειές τους πολύ πιο δύσκολα απ' ό,τι οι πιο πρόσφατοι, και γι' αυτό πιο κινητικοί, πελάτες ενός άλλου ηλεκτρονικού καταστήματος).

Τα πλεονεκτήματα των παραδοσιακών καταστημάτων έγιναν κατανοητά από τους επενδυτές του Internet μόλις πριν από λίγους μήνες. Έτσι, σήμερα πολλά νέα ηλεκτρονικά καταστήματα (αλλά και μερικά από τα "παλαιότερα") αναπροσαρμόζουν τις εργασίες τους και συνάπτουν στρατηγικές συμμαχίες με επιχειρήσεις της "παλαιάς οικονομίας", προσπαθώντας να συνδυάσουν τον δυναμισμό του Internet με το καλό όνομα, την εμπειρία και τη μεγάλη πελατεία των παραδοσιακών επιχειρήσεων.

Τα καταστήματα αυτά έχουν καταλάβει πολύ καλά πως γάμοι ή συνεργασίες αυτής της μορφής είναι επωφελείς για όλους. Οι εκτός δικτύου επιχειρήσεις αποκτούν πρόσβαση στο χώρο όπου αργά ή γρήγορα θα "μετακομίσουν" οι πελάτες τους, ενώ οι επιχειρήσεις του δικτύου αυξάνουν την πελατεία τους και αποκτούν δεσπόζουσα θέση στην αγορά. Γι' αυτό και σήμερα ελάχιστα νέα ηλεκτρονικά καταστήματα ξεκινούν τις εργασίες τους, χωρίς να έχουν εξασφαλίσει εκ' των προτέρων τη συνεργασία ενός τουλάχιστον παραδοσιακού εταίρου.

Ωστόσο, ο μεγαλύτερος κίνδυνος για μια επιχείρηση δεν βρίσκεται ούτε στους ήδη υπάρχοντες ανταγωνιστές της ούτε στις συνεργασίες τους (ή στην απουσία δικών της συνεργασιών) με παραδοσιακά καταστήματα.

Ο κίνδυνος προέρχεται από τον μελλοντικό ανταγωνισμό ο οποίος διαθέτει το ίδιο πλεονέκτημα που είχε αρχικά το νέο κατάστημα έναντι των παλαιότερων. Ο νέος ανταγωνιστής μπορεί να μελετήσει τους άλλους "δικτυοπωλητές" και να διδαχθεί από τα λάθη τους. Επίσης, επειδή ξεκινά αργότερα, μπορεί να επωφεληθεί από την τελευταία λέξη της, ταχύτατα εξελισσόμενης, τεχνολογίας του Internet.

Θεωρητικά βέβαια, ένα παλαιό κατάστημα στο Internet μπορεί και αυτό να κάνει το ίδιο. Στην πράξη όμως η ανάγκη να αποσβεσθούν οι μέχρι τώρα επενδύσεις και η δυσκολία να αλλαχθούν οι ήδη υπάρχουσες διαδικασίες (τις οποίες έχουν συνηθίσει τόσο οι τακτικοί πελάτες όσο και το προσωπικό του καταστήματος) κάνουν πολύ δύσκολη τη μετατροπή της δομής και του παλαιού τρόπου λειτουργίας του (γι' αυτό και έχει τόσο μεγάλη σημασία η ορθή και ευέλικτη αρχική σχεδίαση του καταστήματος).

Ένας άλλος κίνδυνος, ο οποίος θα ελλοχεύει πάντοτε σε ένα χώρο τόσο ρευστό όσο το Internet, είναι εκείνος της εμφάνισης μιας νέας τεχνολογίας ή ενός καινούριου μοντέλου επιχειρηματικής δραστηριότητας το οποίο θα καταστήσει ασύμφορη τη χρήση του καταστήματος από τους σημερινούς ή τους μελλοντικούς πελάτες του.

Δεν μπορούμε φυσικά να προβλέψουμε ποια θα είναι αυτά τα καινούρια μοντέλα ή οι νέες τεχνολογίες οι οποίες θα αλλάξουν τόσο δραστικά το ηλεκτρονικό εμπόριο. Ένα καλό παράδειγμα όμως μπορεί να δει κανείς αν επισκεφθεί το site http://www.addall.com Το Addall είναι μια μηχανή αναζήτησης για ηλεκτρονικά καταστήματα η οποία χρησιμοποιεί agents (bots) για να αναζητεί προϊόντα και να συγκρίνει τις τιμές τους. Για παράδειγμα, ο χρήστης του Addall δηλώνει ποιο βιβλίο τον ενδιαφέρει και το σύστημα ερευνά μια σειρά από καταστήματα για να του παρουσιάσει έναν πλήρη συγκριτικό πίνακα με τις τιμές πώλησης κάθε καταστήματος.

Υπάρχει λοιπόν η πιθανότητα μετά από δύο ή τρία χρόνια να μην υπάρχουν πλέον ηλεκτρονικά καταστήματα (τουλάχιστον για τα προϊόντα στα οποία είναι εφικτές οι συγκρίσεις), αλλά απλώς βάσεις δεδομένων προϊόντων προς πώληση. Έτσι, όσοι έχουν δημιουργήσει ηλεκτρονικά καταστήματα για τα προϊόντα αυτά θα βρεθούν γρήγορα εκτός αγοράς.

Θα τελειώσουμε την παρουσίαση αυτή με μια αναφορά στις οικονομικές και τις τεχνικές δυνατότητες του υποψήφιου επενδυτή. Η μέχρι σήμερα εμπειρία έχει δείξει πως το κόστος εκμάθησης και υλοποίησης εφαρμογών τεχνολογίας αιχμής και

παροχής υπηρεσιών υψηλής ποιότητας είναι εξαιρετικά μεγάλο και σε καμία περίπτωση δεν εξασφαλίζει στους επενδυτές σίγουρα κέρδη. Όπως αναφέρθηκε ήδη, υπάρχει πάντα ο κίνδυνος εμφάνισης μιας νέας δυναμικής εταιρείας η οποία θα αξιοποιήσει ακόμη νεότερες ιδέες και τεχνολογίες, ανατρέποντας προς όφελός της το υπάρχον σκηνικό.

Ακόμη λοιπόν και για τους επιτυχημένους επενδυτές, η ζωή στο δίκτυο μοιάζει με την πορεία ενός ποδηλάτη: Είναι υποχρεωμένος να προχωρεί συνεχώς επενδύοντας, κάνοντας πειράματα, ανοίγοντας νέες αγορές κ.λπ. Αν σταματήσει για να απολαύσει τα όσα κέρδισε μέχρι σήμερα θα πέσει και οι άλλοι θα τον προσπεράσουν. Γι' αυτό και μακροπρόθεσμα στο χώρο του Internet επιζούν μόνο όσες επιχειρήσεις έχουν ισχυρή κεφαλαιακή υποστήριξη. (Μέχρι σήμερα μόνο μερικά εργαλεία αναζήτησης όπως το Yahoo! έχουν καταφέρει να παρουσιάσουν κέρδη.)

Για όλους αυτούς τους λόγους καμία επιχείρηση δεν θα πρέπει να επενδύει στο χώρο του ηλεκτρονικού εμπορίου και ειδικότερα στη δημιουργία ηλεκτρονικών καταστημάτων αν δεν έχει σταθμίσει προσεκτικά τις δυνατότητές της και τις απαιτήσεις της αγοράς, καθώς και τις δικές της αντοχές.

Τα παραπάνω αποτελούν τα σημαντικότερα θέματα που πρέπει να γνωρίζει κάθε υποψήφιος επενδυτής στο χώρο των ηλεκτρονικών καταστημάτων

9.1 Από το εμπόριο στο Ηλεκτρονικό εμπόριο

Στις μέρες μας, το πρόθεμα 'e-' (ηλεκτρονικό, στα ελληνικά) χρησιμοποιείται σαν πρώτο συνθετικό σε διάφορες λέξεις για να δοθεί η 'ηλεκτρονική' διάσταση στο νόημά της και για να καταδειχθεί οτιδήποτε γίνεται διαμέσου ή πάνω από το Internet. Έτσι, λέξεις όπως εμπόριο, επιχείρηση και επιχειρείν έχουν μετατραπεί σε ηλεκτρονικό εμπόριο (e-commerce), ηλεκτρονική επιχείρηση (e-enterprise) και ηλεκτρονικό επιχειρείν (e-business).

Η ονομαζόμενη ηλεκτρονική μετάλλαξη στην οποία πρέπει να προβεί μια επιχείρηση για να αδράξει τις ευκαιρίες που παρουσιάζονται και να αναπτύξει επικερδείς δραστηριότητες στον 21ο αιώνα αφορά:

- την οργανωτική της δομή τον τρόπο λειτουργίας της
- τις σχέσεις της με τις συνεργαζόμενες επιχειρήσεις
- τις σχέσεις της με τους εργαζόμενους και τον τρόπο συνεργασίας με αυτούς
- την στρατηγική της

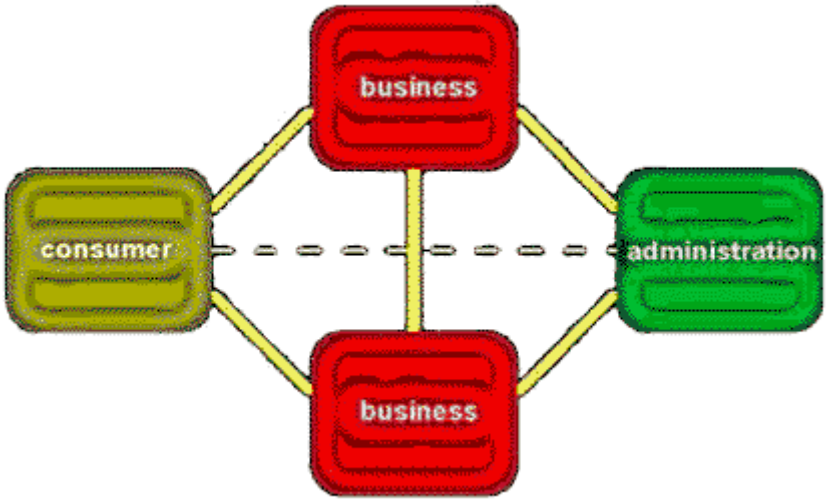
Με τον όρο "Ηλεκτρονικό Εμπόριο (Electronic Commerce)" εννοούμε τη χρήση υπολογιστών και τηλεπικοινωνιακών συστημάτων και τεχνολογιών για την διεκπεραίωση μίας πλήρους εμπορικής συναλλαγής. Μία τέτοια τυπική συναλλαγή μπορεί να περιλαμβάνει :

- την παρουσίαση των εμπορευμάτων
- την προσέλκυση των πελατών (διαφήμιση, marketing)
- την αλληλεπίδραση με τον πελάτη (κατάλογοι εμπορευμάτων, πωλήσεις)
- τη διεκπεραίωση παραγγελιών-πωλήσεων (καταγραφή παραγγελιών, πληρωμές)
- την υποστήριξη των πελατών (after sales support, order tracking)
- την επικοινωνία με τους προμηθευτές

9.1.1 Κατηγορίες Ηλεκτρονικού Εμπορίου

Όπως φαίνεται στην εικόνα 1 το Ηλεκτρονικό Εμπόριο μπορεί να υποδιαιρεθεί σε 4 κατηγορίες :

- **επιχείρηση - επιχείρηση**
- **επιχείρηση - καταναλωτής**
- **επιχείρηση - δημόσια διοίκηση**
- **καταναλωτής - δημόσια διοίκηση**



Εικόνα 1 Κατηγορίες ηλεκτρονικού εμπορίου

επιχείρηση - επιχείρηση

Είναι μια επιχείρηση που χρησιμοποιεί ένα δίκτυο για τις παραγγελίες της από προμηθευτές, που λαμβάνει τιμολόγια και κάνει πληρωμές. Αυτή η κατηγορία έχει κατοχυρωθεί αρκετά χρόνια, ειδικά με την χρησιμοποίηση του EDI σε κλειστά ή διεθνή δίκτυα.

επιχείρηση - καταναλωτής

Εξομοιώνεται με την ηλεκτρονική λιανική πώληση. Αυτή η κατηγορία έχει αναπτυχθεί με την εκτόξευση του World Wide Web. Οι καταναλωτές μαθαίνουν για τα προϊόντα μέσα από ηλεκτρονικές εκδόσεις, αγοράζουν προϊόντα με "ψηφιακό" χρήμα και άλλα ασφαλή συστήματα πληρωμής. Υπάρχουν τώρα "καταστήματα" σε όλο το Internet, που προσφέρουν κάθε είδος προϊόντων, από κέικ και κρασιά, μέχρι Η/Υ και αυτοκίνητα.

επιχείρηση - δημόσια διοίκηση

Καλύπτει όλες τις συναλλαγές μεταξύ επιχειρήσεων και δημόσιων οργανισμών. Για παράδειγμα, στις ΗΠΑ οι λεπτομέρειες για τις προμήθειες των προσεχών κυβερνήσεων, εκδίδονται στο Internet και οι ενδιαφερόμενες επιχειρήσεις, ανταποκρίνονται ηλεκτρονικά. Προς το παρόν, αυτή η κατηγορία είναι σε νηπιακό στάδιο, αλλά μπορεί να αναπτυχθεί ραγδαία όσο οι κυβερνήσεις χρησιμοποιούν τις δικές τους λειτουργίες για να προωθήσουν την αντίληψη τους για το Ηλεκτρονικό Εμπόριο. Επιπροσθέτως, οι διοικήσεις πρέπει να παρέχουν την ευκαιρία ηλεκτρονικών συναλλαγών για καταστάσεις όπως επιστροφές ΦΠΑ και δασμών.

πελάτης - δημόσια διοίκηση

Δεν έχει ακόμα ενεργοποιηθεί. Στον βωμό της ανάπτυξης των 2 προηγούμενων κατηγοριών, οι επιχειρήσεις πρέπει να αναπτύξουν τις ηλεκτρονικές συναλλαγές σε περιοχές όπως πληρωμές κοινωνικής πρόνοιας και ιδιωτικών φόρων.

9.1.2 Φάσεις Ηλεκτρονικού Εμπορίου

Για να αντιληφθεί πλήρως τη σημασία του ηλεκτρονικού εμπορίου, μια επιχείρηση πρέπει να εκπληρώσει τις παρακάτω φάσεις :

Φάση 1:Ανάπτυξη Web Σελίδας & Προώθηση προϊόντος

- Δημιουργία Web site , ανάπτυξη, και φιλοξενία (hosting) .
- Διαφήμιση και πρώτη εικόνα προϊόντων ή υπηρεσιών.
- Ζήτηση και διακίνηση πληροφοριών μέσω του Internet.

Φάση 2:Software Κατασκευή & Διαχείριση Βάσεων Δεδομένων

- Παραγγελία προϊόντων ή υπηρεσιών μέσω του Internet.
- Database λύσεις που απαιτούν οι σύγχρονες πολύπλοκες υψηλές τεχνολογίες

Φάση 3:Πληρωμή & Επεξεργασία Συναλλαγών

- Αναγνώριση πιστότητας πιστωτικής κάρτας και παραγγελία μέσω Internet.
- Ηλεκτρονική μεταφορά χρημάτων.

Φάση 4:Εκπλήρωση & EDI Διανομή αποθεμάτων :

- Αποστολή προϊόντος και αποθήκευση.
- Καταχώρηση παραγγελίας και καταστάσεων.
- Ηλεκτρονική παραγγελία διαμέσου EDI και εξειδικευμένη παρουσία πελατών στο Internet.

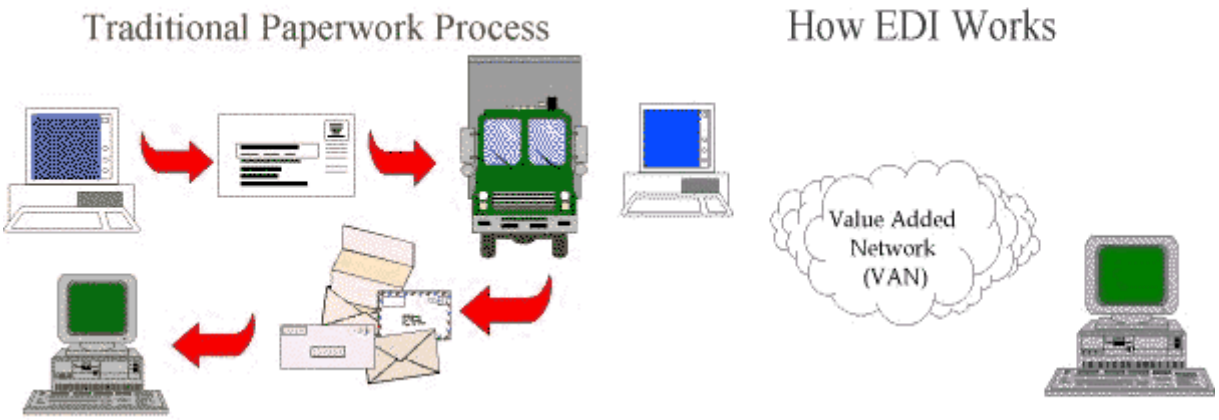
Φάση 5:Υπηρεσίες Τηλεφωνικού κέντρου

- Υποστήριξη προϊόντων και ειδικά εκπαιδευμένοι αντιπρόσωποι για την εκπλήρωση ειδικών αναγκών των πελατών.
- Εξερχόμενο και εισερχόμενο direct marketing.

9.1.3 Τι είναι το EDI;

Τα πλεονεκτήματα της ηλεκτρονικής ανταλλαγής δεδομένων (EDI) είναι γνωστά, στενότερες εμπορικές σχέσεις, αναπτύσσει την αποτελεσματικότητα της επιχείρησης και το μειωμένο κόστος, αλλά το τί πραγματικά είναι, ποιοί συντελεστές παίρνουν μέρος σε μια EDI και πώς αυτοί συνεργάζονται. Ένας καλός ορισμός της EDI είναι: "Η ηλεκτρονική ανταλλαγή δεδομένων διευκολύνει την ανταλλαγή της πληροφορίας σε μια οργανωμένη μορφή, μεταξύ των παραγόντων που αποφάσισαν να συναλλαχθούν με αυτόν τον τρόπο". Οι 2 εικόνες δείχνουν την αντίθεση ανάμεσα στην συνηθισμένη ανταλλαγή πληροφορίας και στην ηλεκτρονική ανταλλαγή δεδομένων - EDI.

Ένα τυπικό σενάριο EDI περιλαμβάνει ένα κατάστημα λιανικών πωλήσεων που δέχεται πληροφορίες για τις πωλήσεις και παραγγελίες από τα υποκαταστήματα του. Αυτή η πληροφορία προβάλλεται και οι παραγγελίες ετοιμάζονται και στέλνονται μέσω EDI. Με απλά λόγια, η πληροφορία διακινείται από τον ένα υπολογιστή μέσω του δικτύου στον άλλον - έτσι εξοικονομείται πολύτιμος χρόνος, ενώ παράλληλα η ασφαλή και έγκαιρη μεταφορά της πληροφορίας είναι βέβαιη.



Ποιός χρησιμοποιεί EDI ;

Περίπου πενήντα χιλιάδες ιδιωτικού τομέα εταιρίες στις ΗΠΑ, όπως για παράδειγμα η Federal Express, η Kodak, η American Airlines, η Nike και άλλες σημαντικές εταιρίες χρησιμοποιούν EDI. Η EDI χρησιμοποιείται πολύ διαδεδομένα στη βιομηχανία, στον τραπεζικό τομέα, στις ασφάλειες και σε άλλου είδους εργοστάσια. Σύμφωνα με μια πρόσφατη μελέτη ο αριθμός των εταιριών αυτών αναμένεται να τετραπλασιαστεί μέσα στα επόμενα έξι χρόνια.

9.2 ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΕΠΙΔΡΑ ΣΕ ΕΝΑ ΜΕΓΑΛΟ ΑΡΙΘΜΟ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

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

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

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

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

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

9.2.1 ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΠΟ ΟΡΙΣΜΕΝΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΑ ΟΦΕΛΗ ΜΕ ΤΗ ΧΡΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

- Μειωμένα έξοδα διαφήμισης
- Μειωμένα έξοδα μεταφοράς, ιδιαίτερα για αγαθά που μπορούν να μεταφερθούν ηλεκτρονικά
- Μειωμένα έξοδα στο σχεδιασμό και στην παραγωγή
- Ανεπτυγμένος στρατηγικός σχεδιασμός
- Περισσότερες ευκαιρίες για niche marketing
- Ιση πρόσβαση στις αγορές από όλους
- Πρόσβαση σε νέες αγορές
- Ανάμειξη του πελάτη στο προϊόν και καινοτομία υπηρεσιών

Πληροφορίες για οποιαδήποτε αγορά και χώρα μπορούν πλέον να προωθηθούν ηλεκτρονικά και να αναπτυχθούν στο εμπορικό περιβάλλον, δημιουργώντας όμως έτσι και έναν αριθμό από προβλήματα όπως η μυστικότητα (privacy) που είναι ανάγκη να διευθετηθεί .

Επαφές μεταξύ εταιριών μπορούν να διευκολυνθούν με on-line επιχειρησιακούς καταλόγους και να βελτιωθούν με εθνικά ή τοπικά πληροφοριακά κέντρα. Επαφές μεταξύ εταιριών και καταναλωτών μπορούν να υποστηριχθούν με σημαντικά μέσα, συμπεριλαμβανομένων on-line διαφημίσεων και κλειστών αγορών. Εταιρίες μπορούν να προωθήσουν αναλυτικές πληροφορίες για τα προϊόντα τους και τις υπηρεσίες τους καθώς επίσης και να απαντήσουν σε ερωτήσεις που υποστηρίζονται από κατανοητές ευκολίες πλοήγησης και αναζήτησης.

Τα τελευταία χρόνια έγιναν προσπάθειες για να βελτιωθεί η επιχειρησιακή αποδοτικότητα και αυτό το γεγονός επέδρασε καταλυτικά και ξεπέρασε έτσι τα "σύνορα" εταιριών και πελατών. Ένα τέτοιο παράδειγμα συμβαίνει με την λεγόμενη "virtual enterprise", εκεί όπου κάθε τέτοιου είδους εταιρία παίζει τον δικό της ρόλο σε ένα πολύ κοντινό δίκτυο εταιριών απευθύνοντας μια πολύ συγκεκριμένη ευκαιρία αγοράς.

9.2.2 ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΠΟ ΣΤΡΑΤΗΓΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΒΑΣΙΣΜΕΝΕΣ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

- Ηλεκτρονική παρουσία στο χώρο αγοράς: προώθηση πωλήσεων
- Interactive TV / Internet αγορές
- Διοίκηση αποτελεσματικής ανταπόκρισης πελατών
- Διοίκηση αλυσίδας προσφοράς
- Καταγραφή πωλήσεων σε επίπεδο πωλητών

Το ηλεκτρονικό εμπόριο επιτρέπει επίσης ικανοποιητική υποστήριξη για μοιραζόμενες επιχειρηματικές εργασίες άσχετα με τη φύση τους και δίχως να λαμβάνεται υπόψη η γεωγραφική τους θέση ή η χρονολογική τους τοποθέτηση.

Η αιτιολόγηση και τα παραδείγματα που δώσαμε παραπάνω, ενδυναμώνουν το επιχείρημα ότι το ηλεκτρονικό εμπόριο είναι ένα φαινόμενο το οποίο θα πρέπει να ληφθεί σοβαρά υπόψη από όλους μας κάτω από το πρίσμα των διαφορετικών πολιτικών που ακολουθούνται και των δεκάδων υπαρχόντων τομέων αγοράς.

9.3 Στρατηγική Πώλησης

Το αποτελεσματικό μάρκετινγκ παίζει αποφασιστικό ρόλο για την επιτυχία οποιασδήποτε επιχείρησης. Η απλή κατανόηση όμως της αγοράς δεν αρκεί. Πρέπει να κάνετε πράξη τα σχέδια μάρκετινγκ, μετατρέποντας τη θεωρία σε κέρδη. Μια καλή στρατηγική πωλήσεων θα σας βοηθήσει να εντοπίσετε και να εκμεταλλευτείτε τις καλύτερες ευκαιρίες.
Παρακάτω θα αναλύσουμε τα εξής:

- Τη διευκρίνηση των στόχων πωλήσεών σας
- Την απόφαση πώς θα προσεγγίσετε τους πελάτες στόχους
- Το σχεδιασμό και την υποστήριξη της προσπάθειάς σας για πωλήσεις
- Την παρακολούθηση και βελτίωση της αποτελεσματικότητας

9.3.1 Η σωστή προσέγγιση

Α. Βασίστε τη στρατηγική πωλήσεών σας στα επιχειρηματικά σας σχέδια και τα σχέδια μάρκετινγκ.
- Καθορίστε λεπτομερώς τον τρόπο κατά τον οποίο θα επιτύχετε τους στόχους του μάρκετινγκ, θα προσεγγίσετε διάφορα τμήματα της αγοράς στόχου και θα υποστηρίξετε τις σημαντικές δραστηριότητες μάρκετινγκ, όπως τις προωθητικές ενέργειες.
- Εντοπίστε τους κύριους στόχους της στρατηγικής σας. Για παράδειγμα, σε ποιες αγορές στοχεύετε, καθώς και τους συνεπαγόμενους χρονικούς ορίζοντες.
- Κάντε ρεαλιστικά και ακριβή σχέδια, εξασφαλίζοντας τη συμμετοχή των πωλητών στο στάδιο κατάρτισής τους.

Β. Κατανοήστε την αγορά σας.
- Μάθετε περισσότερα για τους πελάτες σας. Για παράδειγμα, τι προϊόντα προτιμούν και τι επίπεδο εξυπηρέτησης απαιτούν.
- Εξακριβώστε πότε, που και πώς αγοράζουν οι υπάρχοντες πελάτες.
Αν πουλάτε σε άλλες επιχειρήσεις, εντοπίστε ποιος επηρεάζει τις αποφάσεις αγοράς, ποιος τις λαμβάνει στην πραγματικότητα και ποιος είναι υπεύθυνος για τις παραγγελίες.
- Παρακολουθήστε τις βασικές τάσεις στην αγορά σας, όπως τις μεταβολές στην αγορά και τις δραστηριότητες των ανταγωνιστών.
Λάβετε υπόψη σας τα μεταβαλλόμενα γούστα των πελατών και τις εξελίξεις στην τεχνολογία ή τη νομοθεσία.
Εντοπίστε τις κύριες κινητήριες δυνάμεις της επιχείρησής σας.

Γ. Εστιάστε στη δημιουργία κερδοφόρων δραστηριοτήτων.

- Ταξινομήστε τους πελάτες κατά σειρά κερδοφορίας, εντοπίζοντας τους υπάρχοντες και τους πιθανούς βασικούς πελάτες. Λάβετε υπόψη σας το συνολικό κόστος των πωλήσεων σε καθέναν από αυτούς.
Για παράδειγμα, οι απαιτητικοί πελάτες μπορεί να είναι ακριβοί όσον αφορά την εξυπηρέτησή τους.
- Εντοπίστε τους τομείς στους οποίους είστε καλός, αναλύοντας τις δραστηριότητες που σας οδήγησαν στις πιο κερδοφόρες πωλήσεις σας κατά το προηγούμενο έτος.
- Καθορίστε τα οφέλη για την επιχείρησή σας και της εξυπηρέτησης κάθε είδους πελάτη.
Σταθμίστε όλα τα οφέλη και εστιάστε τις ενέργειες πώλησης στους πελάτες εκείνους για τους οποίους τα αμοιβαία οφέλη είναι σημαντικότερα.
- Να πουλάτε σε μη κερδοφόρους πελάτες μόνο εάν έχετε ένα καλό λόγο.
Για παράδειγμα, ένας μεγάλος, εδραιωμένος πελάτης μπορεί να επιφέρει αξιοπιστία για την επιχείρησή σας και τη δυνατότητα για μια πιο κερδοφόρα πελατεία αλλού.
- Προσπαθήστε να βελτιώσετε τα μικτά περιθώρια κέρδους σας με λιγότερο δαπανηρές πωλήσεις. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε ένα οικονομικότερο κανάλι πωλήσεων.

9.3.2 Οι πελάτες- στόχος

Η ανάπτυξη της επιχείρησης εξαρτάται από τη δημιουργία νέων, κερδοφόρων επιχειρηματικών δραστηριοτήτων με διαφορετικά είδη πελατών.

Α. Καθιερώστε επιχειρηματικές δραστηριότητες με νέες προοπτικές.
Αναλύστε τους δέκα καλύτερους υπάρχοντες πελάτες σας και εντοπίστε πελάτες με παρόμοιο προφίλ.
- Σχεδιάστε τον τρόπο κατά τον οποίο θα προσεγγίσετε κάθε νέο πελάτη. Για παράδειγμα, για να κερδίσετε την πελατεία ενός βασικού πελάτη, μπορείτε να μειώσετε τις τιμές σας – δημιουργώντας ένα προϊόν προσέλκυσης - ή να προσφέρετε δοκιμαστικά το προϊόν σας δωρεάν.

Β. Αναπτύξτε περισσότερες συναλλαγές με υπάρχοντες πελάτες.
- Καθορίστε τι θα κάνετε για να ωθήσετε τους υπάρχοντες πελάτες να κάνουν αγορές μεγαλύτερης αξίας και να αγοράσουν διαφορετικά προϊόντα (τεχνικές πρόσθετης πώλησης up-selling και cross-selling).
- Σχεδιάστε πώς θα διατηρήσετε τους υπάρχοντες πελάτες ικανοποιημένους και θα οικοδομήσετε σταθερές σχέσεις.

Γ. Βρείτε ένα μίγμα πελατών που θα σας βοηθήσουν να διαφυλάξετε το εισόδημα από τις πωλήσεις σας.
Μη βασίζεστε υπερβολικά σε ένα πελάτη, ιδιαίτερα σε ραγδαία μεταβαλλόμενες αγορές, όπως το ηλεκτρονικό εμπόριο.
- Βρείτε μια λογική ισορροπία μεταξύ του χρόνου που ξοδεύετε για την ανάπτυξη νέας πελατείας και του χρόνου που ξοδεύετε για να διατηρείτε τους υπάρχοντες πελάτες ικανοποιημένους.
- Να συνειδητοποιείτε και να διαχειρίζεστε σωστά τις εποχιακές πωλήσεις.

Πολλές επιχειρήσεις ανακαλύπτουν ότι μόνο δέκα στους δώδεκα μήνες έχουν εισόδημα.

9.3.3 Προσέγγιση του πελάτη

Αφού αποφασίστε ποιους πελάτες θα στοχεύσετε, πρέπει να αποφασίσετε ποια κανάλια πωλήσεων θα είναι πιο αποτελεσματικά.
Μπορείτε είτε να πουλάτε απευθείας, είτε μέσω ενός μεσάζοντα. Θυμηθείτε να σταθμίσετε το κόστος του κάθε καναλιού σε σύγκριση με τα οφέλη που θα αποφέρει.

Α. Οι περισσότερες επιχειρήσεις πωλούν στους πελάτες απευθείας.
Οι απευθείας μέθοδοι πώλησης συμπεριλαμβάνουν την πώληση πρόσωπο με πρόσωπο, τις υπηρεσίες direct mail, τις τηλεπωλήσεις και το ηλεκτρονικό εμπόριο.
- Η πώληση πρόσωπο με πρόσωπο είναι η πιο δαπανηρή μέθοδος πώλησης, αλλά και η πλέον ενδεδειγμένη για πωλήσεις υψηλής αξίας.
Τα περίπλοκα προϊόντα (π.χ. λογιστικό λογισμικό στα μέτρα του πελάτη) πρέπει να περιγράφονται και να πωλούνται από ένα έμπειρο πωλητή.
- Οι υπηρεσίες direct mail και οι τηλεπωλήσεις είναι πιο αποδοτικές επιλογές για προϊόντα χαμηλότερης αξίας.
Για παράδειγμα, μπορείτε να στοχεύσετε να ολοκληρώσετε όλες τις πωλήσεις κάτω των 100 Ευρώ από το τηλέφωνο.
- Η πώληση μέσω του δικτυακού σας τόπου μπορεί να είναι η οικονομικότερη μέθοδος από όλες.
Εξασφαλίστε τη συμμετοχή των πωλητών και των υπαλλήλων στο τμήμα μάρκετινγκ κατά το σχεδιασμό και το στήσιμο του δικτυακού τόπου.

Β. Αν δε μπορείτε προσεγγίσετε τους πελάτες σας απευθείας, χρησιμοποιήστε ένα μεσάζοντα.
- Αν οι πελάτες στόχος σας είναι μεμονωμένοι καταναλωτές, μπορείτε να επιλέξετε τις πωλήσεις μέσω ενός δικτύου λιανικής.
- Αν εισέρχεστε σε αγορές στο εξωτερικό, σκεφτείτε το ενδεχόμενο να χρησιμοποιήσετε έναν αντιπρόσωπο.
Μπορεί να χρειαστεί να εστιάσετε στην πώληση στους μεσάζοντες. Για παράδειγμα, να πείσετε τους λιανικούς πωλητές να παρουσιάσουν το προϊόν σας σε εμφανή θέση.

Γ. Μπορεί να έχετε τη δυνατότητα να συνενώσετε τις δυνάμεις σας με άλλες επιχειρήσεις ώστε να δώσετε ώθηση στην προσπάθεια πωλήσεών σας.
- Για παράδειγμα, οι συναφείς αλλά μη ανταγωνιστικές εταιρείες μπορεί να μοιράζονται στοιχεία πελατών.

Δ. Προωθήστε και στηρίξτε τα κανάλια πωλήσεών σας επικοινωνώντας με τους πελάτες σας.
- Διαφημιστείτε για να επιτύχετε αναγνώριση για το προϊόν σας.
- Παρέχετε προωθητικό υλικό σε ενδιάμεσους που πωλούν το προϊόν ή την υπηρεσία σας.
Για παράδειγμα, μπροσούρες και διαφημιστικά φυλλάδια.
Σκεφτείτε προσεκτικά πώς θα προτιμούσαν οι πελάτες να ακούσουν για το προϊόν ή τις υπηρεσίες σας και να τα αγοράσουν.

9.3.4 Προγραμματισμός πωλήσεων

Α. Σε συνεργασία με τους πωλητές σας, προετοιμάστε την πρόβλεψη πωλήσεών σας.
Η πρόβλεψη αυτή είναι μια λεπτομερής ανάλυση των πωλήσεων που σχεδιάζετε να επιτύχετε ανά μήνα, ανά πελάτη και ανά προϊόν.
- Βασίστε τις προβλέψεις στις πωλήσεις που πραγματοποιήσατε το προηγούμενο έτος. Λάβετε υπόψη σας στοιχεία σχετικά με σημαντικές νέες παραγγελίες, μεταβολές στις αγοραστικές συνήθειες των πελατών, καθώς και άλλους παράγοντες, όπως ενέργειες τιμολόγησης και μάρκετινγκ.
- Δηλώστε την πιθανότητα επίτευξης των πωλήσεων εκφρασμένη ως ποσοστό, και καθορίστε πότε αναμένετε να τις οριστικοποιήσετε.
- Συμφωνήστε πόσες νέες επαφές χρειάζονται για την επίτευξη της προβλεπόμενης ανάπτυξης. Καθορίστε πόσες από τις νέες αυτές επαφές θα πρέπει να προέρχονται από νέους και πόσες από υπάρχοντες πελάτες.
- Να αναγνωρίζετε τους πελάτες από το όνομά τους ή από το μέγεθος πωλήσεων που αναμένετε να πραγματοποιήσετε σε αυτούς.
- Καθορίστε τα μεγέθη πωλήσεων που αναμένεται από έναν αριθμό επισκέψεων, κλήσεων ή άλλων μορφών επικοινωνίας.
- Καθορίστε τη συχνότητα και τα επίπεδα των ενεργειών πώλησης που απαιτούνται για την επίτευξη των στόχων.
Για παράδειγμα, κατανείμετε το χρόνο που δαπανάται για κάθε λογαριασμό. Μην ξεχάσετε να συμπεριλάβετε όλο το φάσμα των ενεργειών που απαιτούνται για την ολοκλήρωση μιας πώλησης.
- Αποφασίστε πόσους πωλητές χρειάζεστε για να επιτύχετε τους στόχους πωλήσεών σας και κατανείμετε τις περιοχές ευθύνης ή τους λογαριασμούς .
- Λάβετε υπόψη σας τις δαπάνες πώλησης, καθώς και τα προωθητικά υλικά, τους μισθούς και τον εξοπλισμό.

Σχεδιάστε τις δαπάνες πώλησης κατά αναλογία με τα κέρδη που αναμένετε να επιτύχετε.

Β. Προετοιμάστε τον ετήσιο προϋπολογισμό πωλήσεών σας.
Ο προϋπολογισμός αυτός είναι μια περίληψη της πρόβλεψης πωλήσεων. Δεν αλλάζει και λειτουργεί ως μέτρο σύγκρισης με το οποίο μπορείτε να συγκρίνετε τις ενημερωμένες προβλέψεις σας.
- Προετοιμάστε απαισιόδοξες, ρεαλιστικές και αισιόδοξες εκδοχές του προϋπολογισμού σας και σχεδιάστε τι θα κάνετε σε κάθε περίπτωση.

Γ. Αναθεωρείτε τις προβλέψεις πωλήσεών σας ανά τρίμηνο, ή ετησίως έχοντας τις προηγούμενες επιδόσεις ως μέτρο σύγκρισης.
- Συγκρίνετε τις πραγματοποιηθείσες πωλήσεις με τον προϋπολογισμό πωλήσεών σας.
- Υπάρχει σημαντική διαφορά μεταξύ των δυο μεγεθών; μάθετε το λόγο.
Ίσως να χρειαστεί να σχεδιάσετε νέες πρωτοβουλίες πώλησης ή να προσαρμόσετε τα έξοδα των πωλήσεών σας.

Δ. Να έχετε επίγνωση των κύκλων πωλήσεων. Ο συνολικός χρόνος που μπορεί να απαιτηθεί για την ολοκλήρωση μιας πώλησης μπορεί να έχει ισχυρές επιπτώσεις στην ταμειακή ροή σας.
- Αν διαθέτετε ένα νέο, μη δοκιμασμένο προϊόν ή υπηρεσία, μπορεί να χρειαστείτε περισσότερο χρόνο για την πώλησή του.
- Προσαρμοστείτε στις συνήθειες λήψης αποφάσεων των πελατών. Για παράδειγμα, οι μεγαλύτεροι οργανισμοί μπορεί να είναι βραδύτεροι στη λήψη αποφάσεων.
- Βρείτε τη σωστή χρονική στιγμή για τις προωθητικές ενέργειες πωλήσεων και τις παρουσιάσεις νέων προϊόντων. Για παράδειγμα, ο κλάδος λιανικής δίνει έμφαση στην πραγματοποίηση πωλήσεων σε εκθέσεις στην αρχή κάθε έτους.

Ε. Συντονίστε τις πωλήσεις με τις υπόλοιπες επιχειρηματικές σας δραστηριότητες.
Για παράδειγμα, μη σχεδιάζετε πωλήσεις τις οποίες δεν μπορούν να ικανοποιήσουν οι διαδικασίες παραγωγής σας.
- Σχεδιάστε τις διαφημιστικές εκστρατείες ώστε να υποστηρίζουν τις προσπάθειες προώθησης (π.χ. παρουσιάσεις νέων προϊόντων).
- Αφού καθορίσετε τη στρατηγική πωλήσεών σας, ίσως να χρειαστεί να προσαρμόσετε το σχέδιο μάρκετινγκ σας ανάλογα.
Για παράδειγμα, οι πωλητές σας μπορεί να εντοπίσουν μια νέα ομάδα πελατών στην οποία θα στοχεύσετε.

9.3.5 Εργαλεία πώλησης

Α. Χρησιμοποιήστε εργαλεία πώλησης για να αυξήσετε την αποδοτικότητα.
- Μια καλή βάση δεδομένων ή ένα σύστημα ταξινόμησης πληροφοριών είναι απαραίτητο για τη διαχείριση των στοιχείων πελατών. Όπου είναι δυνατό, συνδέστε τα στοιχεία που τηρούνται σε διαφορετικές βάσεις δεδομένων.
- Σκεφτείτε τι είδους εξοπλισμός θα έκανε τους πωλητές σας πιο παραγωγικούς (π.χ. κινητά τηλέφωνα ή φορητοί υπολογιστές).
Παρέχετε επίσης την κατάλληλη διοικητική υποστήριξη ώστε να δώσετε τη δυνατότητα στους πωλητές να εστιάσουν στην πώληση.

Β. Παρέχετε στο προσωπικό πωλήσεων τα οποιαδήποτε πρότυπα έγγραφα που χρειάζονται.
- Εδώ περιλαμβάνονται δελτία προς συμπλήρωση, πρότυπες συμβάσεις, έντυπα προτάσεων, και προωθητικό υλικό.
- Χρησιμοποιήστε τα έγγραφα αναφοράς πωλήσεων για να καταγράψετε σχετικές πληροφορίες για κάθε πελάτη.
Για παράδειγμα, το όνομα του πελάτη, το λόγο επικοινωνίας, τα ζητήματα που καλύπτονται και την απαιτούμενη παρακολούθηση.
- Συμβουλευτείτε ένα δικηγόρο για τη σύνταξη σημαντικών νομικών εγγράφων, όπως μακροχρόνιων συμβάσεων ή αποκλειστικές συμφωνίες διανομής.

Γ. Οργανώστε την ομάδα πωλήσεών σας.
- Βεβαιωθείτε ότι οι πωλητές σας κατανοούν αυτό που διαφοροποιεί το προϊόν ή την υπηρεσία σας από τα προϊόντα και τις υπηρεσίες των ανταγωνιστών και πείστε τους να το μεταφέρουν στους πελάτες.

- Παρέχετε στους πωλητές βασικές πληροφορίες, όπως για παράδειγμα, σχετικά με τιμολόγηση, περιθώρια πωλήσεων και διαπραγματεύσιμους τομείς.
- Απαιτείστε από τους πωλητές να καταγράφουν τις δραστηριότητές τους και να παράγουν εβδομαδιαίες αναφορές.
- Εκπαιδεύστε τους πωλητές σας ώστε να βελτιωθεί η γνώση του προϊόντος και της αγοράς, καθώς οι δεξιότητες πώλησής τους.
- Να στηρίζετε, να μετράτε και να αναπτύσσετε τις δραστηριότητες κατά τη διάρκεια προσωπικών εβδομαδιαίων συναντήσεων.

9.3.6 Μέτρηση των επιδόσεων

Α. Διεξάγετε ετήσια ή τριμηνιαία ανάλυση κερδοφορίας.
- Εξετάστε και δικαιολογήστε το χρόνο και τα χρήματα που δαπανώνται για διαφορετικούς πελάτες. Εστιάστε περισσότερο στην κερδοφορία παρά στο μέγεθος πωλήσεων, και στην ποιότητα παρά στην ποσότητα των επαφών.
- Μάθετε αν ο κύκλος εργασιών ήταν χαμηλότερος ή υψηλότερος από τον προβλεπόμενο, καθώς και το λόγο για τον οποίο συνέβη αυτό.
- Παρακολουθήστε τα αποτελέσματα βάσει του κόστους πώλησης. Διαχωρίστε το κόστος των αντιπροσώπων πώλησης από το κόστος της υποστήριξης των πωλήσεων.
- Συγκρίνετε τις πωλήσεις του τρέχοντος έτους με τις πωλήσεις του προηγούμενου έτους και με τις πωλήσεις αντίστοιχων εταιρειών στην αγορά σας.

Β. Αναλύστε τους μηνιαίους ρυθμούς μετατροπής των επαφών σε πωλήσεις, με τη βοήθεια των εβδομαδιαίων αναφορών δραστηριότητας των πωλητών.
- Εξακριβώστε πόσες πωλήσεις πραγματοποιήθηκαν και υπολογίστε τη μέση αξία τους.
- Παρακολουθήστε την κίνηση τόσο με νέους όσο και με υπάρχοντες πελάτες.
- Εξετάστε κάθε στάδιο της διαδικασίας πώλησης για να διαπιστώσετε που αποτυγχάνουν οι επαφές πωλήσεων. Για παράδειγμα, μπορεί να διαπιστώσετε ότι οι τεχνικές κλεισίματος χρειάζονται βελτίωση.

Γ. Εντοπίστε τα προβλήματα και εξακριβώστε την αιτία τους.
Για παράδειγμα, μπορεί να παρατηρείτε μειώσεις κατά τις πωλήσεις σε βασικούς πελάτες, οι οποίες έχουν προκληθεί από μια αναξιόπιστη εταιρεία μεταφορών.

- Εντοπίστε τους αδρανείς λογαριασμούς και προσπαθήστε να υποκινήσετε το ενδιαφέρον των πελατών.

- Μάθετε τι ποσοστό της πελατειακής σας βάσης δεν αγοράζει πια από εσάς και γιατί.

9.4 Ηλεκτρονικό κατάστημα: Από ποιά στοιχεία αποτελείται ένα καλό και επιτυχημένο e-shop;

- **Διεύθυνση (domain name)**: Η διεύθυνση ενός web site έχει τη μορφή www.onoma.gr ή www.onoma.com . Μια σωστή διεύθυνση μπορεί να συμβάλλει σε αυξημένο αριθμό επισκέψεων στο site, και την καλλιέργεια ενός ευκολομνημόνευτης εμπορικής ταυτότητας. Λέγοντας "σωστή" αναφερόμαστε σε κάποια συγκεκριμένα κριτήρια που κάνουν μια διεύθυνση περισσότερο η λιγότερο κατάλληλη για επισκέπτες και μηχανές αναζήτησης.

- **Όμορφο αισθητικά ηλεκτρονικό κατάστημα - web site**: Το ηλεκτρονικό κατάστημα - web site είναι σαν ένα κανονικό κατάστημα. Αν είναι όμορφο αισθητικά και άρτια τεχνικά κατασκευασμένο, θα προκαλέσει την καλή διάθεση του επισκέπτη και το αίσθημα εμπιστοσύνης. Αν ο επισκέπτης-πιθανός πελάτης πιστεί ότι πίσω από αυτό υπάρχει μια εταιρεία με σοβαρότητα και επαγγελματισμόα θα προχωρήσει σε συναλλαγές και αγορές από αυτή.

- **Μέτρα ασφάλειας στις συναλλαγές**: Ο μεγαλύτερος φόβος των χρηστών του Internet που τους εμποδίζει να πραγματοποιήσουν συναλλαγές, είναι τα θέματα ασφαλείας των διαφόρων ηλεκτρονικών καταστημάτων - web site. Αν και κανείς δε μπορεί να εγγυηθεί 100% ασφάλεια από κακόβουλους χάκερ (hacker), σήμερα, η τεχνολογία μας παρέχει τα καλύτερα μέτρα ασφαλείας που υπήρξαν ποτέ. Από τις προτεραιότητες ενός ηλεκτρονικού καταστήματος, είναι η χρήση των πιο σύγχρονων τεχνικών και προδιαγραφών ασφαλείας (κρυπτογράφηση, αυθεντικοποίηση, σαφείς όροι χρήσης site, πολιτικές προστασίας δεδομένων κτλ) ώστε ο επισκέπτης του, να αισθάνεται ασφάλεια κατά την περιήγηση του στις ιστοσελίδες του και την παραγγελία προϊόντων από αυτό.

- **Ευκολία στους τρόπους πληρωμής**: Έχει αποδειχθεί με έρευνες και στατιστικές ανάμεσα σε δημοφιλή ηλεκτρονικά καταστήματα και χρήστες τους, ότι όσο πιο απλή και εύκολη είναι η παραγγελία ενός προϊόντος μέσω Internet, τόσο πιο πολλές είναι οι πωλήσεις του καταστήματος και οι ικανοποιημένοι πελάτες του. Το ηλεκτρονικό κατάστημα πρέπει να παρέχει στους επισκέπτες εναλλακτικούς τρόπους πληρωμής.

- **Σωστή διαφήμισή του στο χώρο του Internet**: Ένα άρτιο ηλεκτρονικό κατάστημα, με καλαίσθητες ιστοσελίδες και σύγχρονες τεχνικές ασφαλείας, είναι καταδικασμένο σε αποτυχία αν οι χρήστες του Internet δε γνωρίζουν γι' αυτό. Η αποτελεσματική διαφημιστική προώθησή του σε sites, μηχανές αναζήτησης και banners θα φέρει τους νέους επισκέπτες-πιθανούς πελάτες. Πέρα από μια απλή καταγραφή του στις μηχανές αναζήτησης, καλό θα ήταν να μπορούσε να εμφανίζεται στις υψηλότερες θέσεις αποτελεσμάτων σε αναζητήσεις με τις λέξεις κλειδιά (keywords) που είναι σχετικά με αυτό.

9.5 Γιατί να φτιάξω ένα web site ή ένα ηλεκτρονικό κατάστημα για την επιχείρησή μου;

- Γιατί ήδη **συνεργάτες και ανταγωνιστές** σου είναι εκεί.
- Για να παρουσιάσεις τον **κατάλογο με τα προϊόντα ή τις υπηρεσίες** σου σε ένα ευρύ κοινό.
- Για να **πουλήσεις προϊόντα σου μέσω internet σε ολόκληρη την Ελλάδα και τον Κόσμο.**
- Περισσότερη **επικοινωνία** με τους πελάτες και προμηθευτές: Ευκολότερη, Γρηγορότερη, Οικονομικότερη, Αποτελεσματικότερη.
- Βρίσκεις **νέους πελάτες** και μαθαίνεις για αγορές που δεν ήξερες ότι υπήρχαν.
- **Ανοίγεις δρόμο σε νέες αγορές**, αυξάνεις τη διείσδυση στις υπάρχουσες, εξυπηρετείς τους πελάτες σου πιο αποτελεσματικά.
- Τονίζεις το **σύγχρονο επαγγελματικό προφίλ**, προφίλ μιάς εταιρείας που παρακολουθεί τις εμπορικές και τεχνολογικές εξελίξεις και δε θέλει να μείνει πίσω.
- Μπορείς να **μειώνεις το κόστος** σου μέσω ηλεκτρονικών συναλλαγών, χτίζοντας στενότερες, πιο εύκαμπτες εμπορικές σχέσεις με τους πελάτες σου και τους προμηθευτές σου.
- **Βελτιώνεις τον τρόπο διανομής** των προϊόντων και υπηρεσιών καθώς και εξυπηρέτησης των πελατών.
- Ανακαλύπτεις **νέες ευκαιρίες** για να πραγματοποιήσεις νέες επιχειρηματικές ιδέες.
- Καλύτερο και φτηνότερο **One-To-One Marketing.**
- Βρίσκεις **άμεση και εύκολη πληροφόρηση** για νόμους, υπηρεσίες του δημοσίου τομέα και της κυβέρνησης, φορολογικά θέματα.
- Το Internet επιτρέπει στις **Μικρές και Μεσαίες Επιχειρήσεις** να ευδοκιμήσουν καθώς το μέγεθος της επιχείρησης δεν παίζει πια κανένα ρόλο. **Αυτό που έχει σημασία είναι να είσαι... δικτυωμένος**! Να συμμετέχεις σε κοινότητες επιχειρήσεων για να μπορείς να προγραμματίσεις την ανάπτυξη σου και να μειώσεις το κόστος των προμηθειών, να μαθαίνεις από τους άλλους, τεχνολογία και μεθόδους παραγωγής και προσέγγισης της αγοράς.

9.6 Internet και διαφήμιση

Η διαφήμιση στο internet διαφέρει με όλα τα άλλα παραδοσιακά μέσα, ο στόχος εδώ είναι πιο συγκεκριμένος και άμεσος. Η διαφήμιση στο internet προσδοκά από τον χρήστη να επισκεφθεί την σελίδα με την οποία είναι συνδεδεμένη η διαφήμιση, προσπαθώντας να του δώσει το κίνητρο να μάθει περισσότερα για το προιόν που

προωθεί πριν το πουλήσει. Και θα πρέπει να ανταποκριθεί μόνος του ο χρήστης, ανταποκρινόμενος στο μήνυμα του banner.

Στο **internet** η παρουσία μιας εταιρείας πρέπει να είναι συνολική και όχι περιστασιακή, δηλαδή περιορισμένη σε ένα μήνυμα ή διαφήμιση.

Πρέπει να προβάλλουμε το σύνολο της εταιρείας. Δεν μπορούμε να μεταφέρουμε τα marketing plans άλλων μέσων στο internet χωρίς τις απαραίτητες αλλαγές και προσαρμογές για το νέο μέσο. **Συμπέρασμα:** η προώθηση προιόντων και υπηρεσιών στο internet συνδυάζει γνώσεις marketing αλλά και γνώσεις του νέου μέσου.

Το Internet θα αποτελέσει:

- Πηγή πληροφοριών για τους καταναλωτές
- Πηγή αγορών
- Πηγή για έρευνες αγοράς
- Τάσεις on-line διαφήμισης
- Υποστήριξη
- Ενημέρωση επενδυτών

Customer support ή υποστήριξη πελατών σε 24ωρη βάση με ελάχιστο κόστος

1. Παροχή έτοιμων πληροφοριών
2. Απαντήσεις σε ερωτήματα

...η χρήση του Internet για την υποστήριξη και παροχή τεχνικών χαρακτηριστικών των προιόντων ή υπηρεσιών, εξασφαλίζει οφέλη για την επιχείρηση καθώς επιτρέπει την ταυτόχρονη ενημέρωση και πρόσβαση μεγάλου αριθμού χρηστών με ελάχιστο κόστος.

Αναλυτικότερα :
- μείωση του κόστους διανομής πληροφοριακού υλικού.
- αύξηση της διαθεσιμότητας της τεχνικής υποστήριξης ακόμη και εκτός ωρών εργασίας της επιχείρησης.
- παροχή πληροφορίας και υποστήριξης με e-mail.
- μειωμένο κόστος εξοπλισμού.
- βελτιωμένη εικόνα της επιχείρησης.
- υποστήριξη, όταν την χρεάζεται ο πελάτης ανεξάρτητα των ωρών εργασίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. NETWORK SECURITY ESSENTIALS (APPLICATIONS AND STANDARDS)-WILLIAM STALLINGS-PRENTICE HALL

2. ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ-ΙΑΚΩΒΟΣ ΣΤ. ΒΕΝΙΕΡΗΣ ΕΥΓΕΝΙΑ ΝΙΚΟΛΟΥΖΟΥ- ΕΚΔΟΣΕΙΣ ΤΖΙΟΛΑ

3. ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ(2η έκδοση) – ΑΡΣΕΝΗΣ ΠΑΣΧΟΠΟΥΛΟΣ & ΠΑΝΑΓΙΩΤΗΣ ΣΚΑΛΤΣΑΣ-ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

4. http://www.fv.com

5. http://www.protocols.com

6. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΟ ΧΩΡΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΠΙΧΕΙΡΕΙΝ

http://forum.ebusiness.uoc.gr/

7. ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ- ΘΡΗΣΚΟΥ ΧΡΥΣΑΝΘΗ & ΜΗΛΙΟΥ ΑΙΚΑΤΕΡΙΝΗ

http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/2002/Thriskou/MBAecom.pdf

8. Ε-ΕΠΙΧΕΙΡΕΙΝ ΠΛΗΡΗΣ ΟΔΗΓΟΣ ΑΝΑΛΥΣΗΣ ΤΕΧΝΙΚΩΝ ΚΑΙ ΕΜΠΟΡΙΚΩΝ ΘΕΜΑΤΩΝ- Μ.ΓΚΙΟΥΡΔΑΣ 2001

9. RAM ΤΕΥΧΟΣ 144- ΦΕΒΡΟΥΑΡΙΟΣ 2001

10. ΚΙΝΔΥΝΟΙ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ – ΝΙΚΟΣ ΚΥΡΛΟΓΛΟΥ

11. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ – ΣΤΕΦΑΝΟΥ ΓΚΡΙΤΖΑΛΗ , ΣΩΚΡΑΤΗ Κ.ΚΑΤΣΙΚΑ , ΔΗΜΗΤΡΗ ΓΚΡΙΤΖΑΛΗ – ΕΚΔΟΣΕΙΣ ΠΑΠΑΣΩΤΗΡΙΟΥ

12. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ – ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΓΕΩΡΓΙΟΣ , ΠΟΜΠΟΡΤΣΗΣ ΑΝΔΡΕΑΣ – ΕΚΔΟΣΕΙΣ ΤΖΙΟΛΑ