ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΠΟΛΥΜΕΣΩΝ

Κίνδυνοι στο Ηλεκτρονικό Εμπόριο με Έμφαση στην Ασφάλεια Προσωπικών Δεδομένων

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Α. Τριανταφυλλόπουλος

Επιβλέπων: Εμμανουήλ Σφακιανάκης

Ηράκλειο 2007

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

1. Εισαγωγή

Με την ολοένα και ταχύτερη ανάπτυξη των τεχνολογιών και των επικοινωνιών και ιδίως την ραγδαία, τα τελευταία χρόνια, ανάπτυξη του Διαδικτύου, η φύση και η δραστηριότητα του εμπορίου έχει αλλάξει. Μια νέα μορφή εμπορίου, το ηλεκτρονικό εμπόριο (electronic commerce) έχει κάνει δυναμική εμφάνιση και διεκδικεί σημαντικό μερίδιο από το παραδοσιακό εμπόριο. Κάθε εμπορική δραστηριότητα που πριν από μερικά χρόνια ήταν δυνατή, μόνο χάρη στη φυσική παρουσία και μεσολάβηση ανθρώπων ή υλικών μέσων (π.χ. εμπορική αλληλογραφία), σήμερα μπορεί να επιτευχθεί αυτόματα, ηλεκτρονικά και εξ' αποστάσεως. Η ανάπτυξή του ηλεκτρονικού εμπορίου οφείλεται ακριβώς στο γεγονός ότι προσφέρει τη δυνατότητα να πραγματοποιούνται κάθε είδους συναλλαγές, συμπεριλαμβανομένων της πώλησης αγαθών και υπηρεσιών, μέσα από ηλεκτρονικά μέσα με μεγάλη ταχύτητα και μικρό κόστος.

Στις μέρες μας, το ηλεκτρονικό εμπόριο αποτελεί αναπόσπαστο κομμάτι του παγκοσμίου εμπορίου. Για πολλούς θεωρείται ίσως η δεύτερη μεγαλύτερη τεχνολογική εξέλιξη μετά τη βιομηχανική επανάσταση, καθώς εξοικονομεί χρόνο και χρήμα και μπορεί να μεταμορφώσει μια μικρή εταιρεία ακόμα και σε κολοσσό. Αυτή τη στιγμή περισσότεροι από 40.000.000 άνθρωποι σε όλο τον κόσμο δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και σε πολύ λίγα χρόνια ο αριθμός αυτός αναμένεται να αυξηθεί ραγδαία.

Ο όρος ηλεκτρονικό εμπόριο καλύπτει οποιαδήποτε μορφή επιχειρηματικής δραστηριότητας, εμπορικής συναλλαγής ή ανταλλαγής πληροφοριών η οποία διεξάγεται χρησιμοποιώντας κάθε μορφής Τεχνολογία Πληροφορικής ή Επικοινωνιών. Ο ορισμός αυτός ενσωματώνει όχι μόνο συναλλαγές που λαμβάνουν χώρα μέσω του Διαδικτύου, αλλά μια ευρεία γκάμα δυνατοτήτων συναλλαγής, όπως για παράδειγμα μέσω κινητών τηλεφώνων ή πρωτοκόλλων διακίνησης δεδομένων που επιτρέπουν την Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange, EDI). Η Ηλεκτρονική Ανταλλαγή Δεδομένων δημιουργήθηκε στις αρχές της δεκαετίας του '70 και είναι μια κοινή δομή αρχείων που σχεδιάστηκε ώστε να επιτρέπει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσα από μεγάλα ιδιωτικά δίκτυα.

Αν και ο παραπάνω ορισμός για το ηλεκτρονικό εμπόριο, καλύπτει ένα ευρύ φάσμα συναλλαγών, συνήθως χρησιμοποιείται για τις αγοραπωλησίες που πραγματοποιούνται διαμέσου του Διαδικτύου. Για τις υπόλοιπες δραστηριότητες χρησιμοποιείται, τα τελευταία χρόνια, ο όρος ηλεκτρονικό επιχειρείν (electronic business). Η έννοια του ηλεκτρονικού επιχειρείν καλύπτει και άλλες επιχειρηματικές δραστηριότητες όπως την ενδοεπιχειρησιακή επικοινωνία και τη συνεργασία σε επίπεδο επιχειρήσεων.

Οι επιχειρήσεις, στην προσπάθεια διατήρησης σημαντικής θέσης στην αγορά ή απόκτησης ανταγωνιστικού πλεονεκτήματος μέσω καινοτόμων διαδικασιών μείωσης κόστους και βελτίωσης της εξυπηρέτησης των πελατών, ολοένα και περισσότερο στρέφονται στο ηλεκτρονικό εμπόριο. Ήδη, πλειάδα επιχειρήσεων, τόσο στην Ευρώπη όσο και στην Αμερική, διαθέτουν τα προϊόντα τους μέσω του Διαδικτύου. Κορυφαίο παράδειγμα αυτής της εξέλιξης αποτελεί το Amazon.com, το οποίο είναι αυτή τη στιγμή το μεγαλύτερο ηλεκτρονικό βιβλιοπωλείο στον κόσμο. Στην Ελλάδα, αν και υπάρχει μια σχετική καθυστέρηση σε αυτό τον τομέα, οι εξελίξεις είναι σημαντικές και υπάρχουν ήδη αρκετές εταιρείες και επιχειρήσεις που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Επιπλέον υπάρχουν ήδη στη χώρα μας και εταιρείες που προσφέρουν λύσεις ηλεκτρονικού εμπορίου σε επιχειρήσεις που έχουν ανοίξει ή θα ήθελαν να ανοίξουν κάποιο ηλεκτρονικό κατάστημα. Σε κάθε περίπτωση, ο κύριος λόγος που μια επιχείρηση δραστηριοποιείται σε

ηλεκτρονικό επίπεδο είναι για να προσελκύσει αγοραστικό κοινό πέρα από τα στενά όρια της γεωγραφικής της έδρας, αυξάνοντας έτσι τις πωλήσεις των προϊόντων της.

Το ηλεκτρονικό εμπόριο εμφανίζεται με δύο τύπους δραστηριότητας και τρεις μορφές. Ως προς τους τύπους, το ηλεκτρονικό εμπόριο διακρίνεται ανάμεσα στο έμμεσο ηλεκτρονικό εμπόριο**,** όπου η παραγγελία των προϊόντων γίνεται μέσω Η/Υ, τα οποία στη συνέχεια παραδίδονται στον πελάτη με φυσικό τρόπο χρησιμοποιώντας μεταφορικά και ταχυδρομικά μέσα, και το άμεσο ηλεκτρονικό εμπόριο, όπου η παραγγελία, πώληση αλλά και παράδοση προϊόντων και υπηρεσιών γίνεται ηλεκτρονικά (π.χ. πώληση προγραμμάτων λογισμικού, παροχή πληροφόρησης κ.α). Από την άλλη πλευρά οι πιο συνηθισμένες μορφές ηλεκτρονικού εμπορίου ανάλογα με τα μέρη που εμπλέκονται σε μια ηλεκτρονική συναλλαγή αφορούν:

Επιχείρηση προς Καταναλωτή (Business to Consumer, B2C)

Είναι ίσως η πιο κλασσική μορφή ηλεκτρονικού εμπορίου, όχι όμως και η πιο διαδεδομένη. Αποτελεί το ηλεκτρονικό ανάλογο των καθημερινών συναλλαγών για αγορά προϊόντων ή χρήση υπηρεσιών. Η επιχείρηση-προμηθευτής διατηρεί έναν διαδικτυακό τόπο (site) στον οποίο παρουσιάζει τα προϊόντα της ή/και τις υπηρεσίες της. Ο τόπος αυτός καλείται ηλεκτρονικό κατάστημα ή και e-shop.

Το ηλεκτρονικό κατάστημα αποτελείται από ιστοσελίδες που παρουσιάζουν τα προϊόντα ή τις υπηρεσίες του καταστήματος. Ο χρήστης-επισκέπτης και πιθανός καταναλωτής μπορεί να περιηγηθεί στις ιστοσελίδες του καταστήματος, να δει τα παρουσιαζόμενα προϊόντα, να επιλέξει τις αγορές του και στο τέλος να προχωρήσει στη διαδικασία πληρωμής και τελικής προμήθειας του προϊόντος.

Η πληρωμή γίνεται συνήθως μέσω πιστωτικών καρτών, ενώ η παράδοση της παραγγελίας γίνεται είτε μέσω ταχυδρομείου είτε, σε περιπτώσεις που η παραγγελία αφορά ηλεκτρονικό υλικό, υπάρχει η δυνατότητα ηλεκτρονικής παραλαβής.

Το ηλεκτρονικό εμπόριο έχει γνωρίσει αρκετή διάδοση στον τομέα του λιανικού εμπορίου. Χαρακτηριστικά τέτοια παραδείγματα είναι η πώληση βιβλίων, CD, πακέτων λογισμικού αλλά οι κλάδοι δραστηριοτήτων των εταιρειών ηλεκτρονικού εμπορίου δεν σταματούν εδώ. Στο διαδίκτυο υπάρχουν ακόμα και super-market που δίνουν τη δυνατότητα πραγματοποίησης on-line αγορών.

Σε ότι αφορά τις υπηρεσίες εδώ εντάσσονται οι δυνατότητες home-banking, δηλαδή πραγματοποίηση τραπεζικών συναλλαγών με τη χρήση υπολογιστή (πληρωμή λογαριασμών, δάνεια), κράτηση εισιτηρίων, δωματίων κλπ. Σημειώνεται ότι σχεδόν όλες οι μεγάλες αεροπορικές εταιρείες παρέχουν τη δυνατότητα κράτησης θέσεων από τον δικτυακό τους τόπο. Συγκεκριμένα η εταιρεία EasyJet κάνει πάνω από το 75% των κρατήσεων της on-line.

Επιχείρηση προς Επιχείρηση (Business to Business, B2B)

Αυτή η μορφή ηλεκτρονικού εμπορίου περιλαμβάνει τη συνδιαλλαγή μεταξύ επιχειρήσεων. Πρόκειται για τον δυναμικότερο και ταχύτερα αναπτυσσόμενο κλάδο του ηλεκτρονικού εμπορίου. Οι συναλλαγές Επιχείρησης-προς-Επιχείρηση, περιλαμβάνουν τις καθιερωμένες συναλλαγές της επιχείρησης με τους προμηθευτές αλλά με πραγματοποίηση των προμηθειών με ηλεκτρονικό τρόπο.

Το ηλεκτρονικό εμπόριο επιτρέπει στις επιχειρήσεις να βελτιώσουν τη μεταξύ τους συνεργασία, απλοποιώντας τις διαδικασίες των προμηθειών, το κόστος, την ταχύτερη αποστολή τους και τον αποτελεσματικότερο έλεγχο του επιπέδου αποθεμάτων. Επίσης κάνει ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και την παροχή καλύτερης εξυπηρέτησης σε πελάτες. Η διαχείριση των επαφών με εταίρους (διανομείς, μεταπωλητές, μετόχους) της επιχείρησης γίνεται πολύ πιο αποτελεσματική. Κάθε αλλαγή μπορεί να ανακοινώνεται μέσα από μια ιστοσελίδα και το ηλεκτρονικό ταχυδρομείο, εκμηδενίζοντας την ανάγκη για ομαδικές επιστολές και άλλες δαπανηρές μορφές ειδοποίησης. Η δυνατότητα ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς, και η πραγματοποίηση ηλεκτρονικών πληρωμών, βελτιώνουν ακόμη περισσότερο την αποτελεσματικότητα: οι ηλεκτρονικές πληρωμές περιορίζουν το ανθρώπινο λάθος, αυξάνουν την ταχύτητα και μειώνουν το κόστος των συναλλαγών.

Δημόσιοι Φορείς προς το Κοινό

Αυτή η μορφή ηλεκτρονικού εμπορίου περιλαμβάνει τη δυνατότητα πληροφόρησης, ανταλλαγής πληροφοριών και διεκπεραίωσης λειτουργιών μεταξύ των δημόσιων φορέων και των πολιτών. Οι πολίτες (επιχειρηματίες ή μη) χρησιμοποιούν το Διαδίκτυο για να πληροφορηθούν και να φέρουν σε πέρας γραφειοκρατικές διαδικασίες.

Αυτή η μορφή ηλεκτρονικού εμπορίου περιλαμβάνει κυρίως δύο πλαίσια δραστηριοτήτων:

1. Παροχή δυνατότητας στις επιχειρήσεις για διεκπεραίωση των συναλλαγών τους με το κράτος, με ηλεκτρονικό τρόπο.
2. Παροχή δυνατότητας στους πολίτες για διεκπεραίωση των υποθέσεων τους με δημόσιες υπηρεσίες, με ηλεκτρονικό τρόπο. Αυτή η μορφή ηλεκτρονικού εμπορίου αναμένεται να γνωρίσει έκρηξη τα επόμενα χρόνια καθώς ολοένα και περισσότερες υπηρεσίες πληροφόρησης και ενημέρωσης παρέχονται από κρατικούς φορείς μέσω Διαδικτύου. Συγκεκριμένα αναμένεται να αναπτυχθούν ηλεκτρονικές συναλλαγές για τις πληρωμές κοινωνικής πρόνοιας και ιδιωτικών φόρων.

Οφέλη από το ηλεκτρονικό εμπόριο

Το ηλεκτρονικό εμπόριο αλλάζει ριζικά την παραδοσιακή θεώρηση της δοσοληψίας και γι’ αυτό το λόγο, παρουσιάζει σημαντικά οφέλη σε ότι αφορά τόσο τους καταναλωτές όσο και τις επιχειρήσεις που το υιοθετούν. Ακολουθούν κάποια βασικά πλεονεκτήματα του ηλεκτρονικού εμπορίου που αφορούν τους καταναλωτές:

- Υπάρχει απεριόριστη δυνατότητα επιλογής προϊόντων.
- Οι καταναλωτές έχουν τη δυνατότητα να κάνουν άμεση σύγκριση τιμών στα προϊόντα που αγοράζουν.
- Παρέχεται η δυνατότητα χρήσης του καταστήματος και πραγματοποίησης συναλλαγών σε οποιαδήποτε ώρα, οποιασδήποτε μέρας.
- Εξοικονομείται ο χρόνος που πιθανόν να σπαταλούταν σε πολύωρη αναμονή για εξυπηρέτηση και στην εμπλοκή με γραφειοκρατικές διαδικασίες.
- Αίρονται οι γεωγραφικοί φραγμοί στις αγορές.

- Εξατομίκευση των πληροφοριών και των περιεχομένων του καταστήματος με βάση τις προτιμήσεις και τις ιδιαιτερότητες του πελάτη.
- Το κόστος των προϊόντων που πωλούνται μέσω Διαδικτύου είναι κατά γενικό κανόνα πολύ χαμηλότερο από τις τιμές του εμπορίου, αφού ένα ηλεκτρονικό κατάστημα είναι απαλλαγμένο από μεγάλο μέρος του λειτουργικού κόστους ενός πραγματικού καταστήματος (ενοικίαση χώρου και «αέρα», ηλεκτρικό, νερό κλπ) και γενικά απαιτεί πολύ λιγότερο υπαλληλικό προσωπικό.

Το ηλεκτρονικό εμπόριο προσφέρει σημαντικά οφέλη στις επιχειρήσεις, μερικά από τα οποία παρουσιάζονται παρακάτω:

Κάθε εταιρεία που έχει ηλεκτρονική παρουσία μπορεί να διευρύνει τον κύκλο εργασιών της επεκτείνοντας τα γεωγραφικά όρια των συναλλαγών της. Αυτό σημαίνει πως κάθε επιχείρηση που διαθέτει τα προϊόντα της online μπορεί και αποκτά πελάτες σε περιοχές που βρίσκονται μακριά από την έδρα της, ακόμα και στο εξωτερικό. Με άλλα λόγια, κάθε επιχείρηση που έχει ένα ηλεκτρονικό κατάστημα, είναι σαν να έχει υποκαταστήματα σε πολλές περιοχές και μάλιστα με ελάχιστο λειτουργικό κόστος.

- Κάθε εταιρεία που χρησιμοποιεί τις νέες τεχνολογίες, όπως το Διαδίκτυο, γίνεται εξ'ορισμού πιο ανταγωνιστική, αφού μπορεί να ενημερώνεται πιο εύκολα για τις τρέχουσες εξελίξεις στο χώρο της. Με άλλα λόγια και με δεδομένο το ότι σε λίγα χρόνια όλες οι εμπορικές δραστηριότητες θα γίνονται μέσω Διαδικτύου, το ηλεκτρονικό εμπόριο είναι η νέα μεγάλη πρόκληση για κάθε εταιρεία που θέλει να είναι ανταγωνιστική.
- Οι ηλεκτρονικές συναλλαγές επιτρέπουν την αμφίδρομη σχέση μεταξύ επιχείρησης και καταναλωτή. Αυτό σημαίνει πως κάθε εταιρεία μέσω των ηλεκτρονικών συναλλαγών μπορεί να συλλέξει πολλά στοιχεία για τις συνήθειες, τις ανάγκες και τα γούστα των καταναλωτών και σύμφωνα με αυτά να αναπροσαρμόσει την πολιτική της προς το θετικότερο.

Ιστορική Αναδρομή Ηλεκτρονικού Εμπορίου

Καθ' όλη τη διάρκεια της ιστορίας, γίνεται προσπάθεια να προωθηθούν νέοι τρόποι επικοινωνίας με απλά μέσα με τα οποία να αυξηθούν οι ευκαιρίες για την ευκολία, την αποδοτικότητα και την ασφάλεια. Τα θεμέλια στα οποία το ηλεκτρονικό εμπόριο είναι βασισμένο άρχισαν 125 έτη πριν με τη χρήση της τεχνολογίας τηλέγραφων στις πληροφορίες ηλεκτρονόμων σχετικά με τη μεταφορά των κεφαλαίων, όπως το τηλέτυπο αποθεμάτων και το σύστημα μεταφοράς χρημάτων Δυτικής Ένωσης. Από τα πρώτα βήματά του, το Internet φάνηκε ιδιαίτερα χρήσιμο εργαλείο στα χέρια όλων και κυρίως των επιχειρήσεων, για τις οποίες και αρχικά κατασκευάστηκε. Η εξέλιξή του, όμως, ήταν απρόσμενη, αφού ξεπέρασε κάθε προηγούμενο. Ο Roddy J. David (1999) σημειώνει ότι ενώ το τηλέφωνο χρειάστηκε 35 χρόνια για να μπει στο 25% των νοικοκυριών της Αμερικής, το Internet χρειάστηκε 7 χρόνια. «Κατόρθωσε σε περίπου 5 χρόνια να χρησιμοποιείται από 50 εκατομμύρια χρήστες». Το ηλεκτρονικό εμπόριο, αρχικά, είχε μόνο διαφημιστική διάσταση. Δηλαδή, οι επιχειρήσεις χρησιμοποιούσαν το Διαδίκτυο και την τεχνολογία, γενικότερα, σαν μέσο προβολής των ίδιων και των προϊόντων/ υπηρεσιών τους. Μέχρι και σήμερα, αυτή είναι η πιο αναπτυγμένη διάσταση, του ηλεκτρονικού εμπορίου και

το Internet παραμένει ένα από τα δημοφιλέστερα μέσα προβολής των επιχειρήσεων. Οι ειδικοί, υποστηρίζουν, ότι κάτι τέτοιο, δε λέγεται ηλεκτρονικό εμπόριο.

Η εμφάνιση των πιστωτικών καρτών το 1914, ξεσήκωσε το εμπόριο για τους καταναλωτές, ως ανάγκες για την αποδοτικότητα και την ευκολία των συναλλαγών συναντήθηκε. Οι τράπεζες ήταν τα πρώτα όργανα για να αυτοματοποιήσουν τις λειτουργίες εμπορίου. Το ηλεκτρονικό εμπόριο συνεχίστηκε στη δεκαετία του '80 με την εμφάνιση των αυτόματων αφηγητών, ή του ATM, το 1986. Η ίδια τεχνολογία - πληροφορίες που ταξιδεύουν ηλεκτρονικά πέρα από τα καλώδια - ήταν η βάση για το Διαδίκτυο.

Η σύλληψη της ιδέας του Διαδικτύου έγινε το 1969, όταν μια προηγμένη αντιπροσωπεία ερευνητικών προγραμμάτων χρηματοδότησε την έρευνα της δικτύωσης υπολογιστών. Η έρευνα εστίασε στη δημιουργία ενός packet-switched network - σύστημα στο οποίο οι πληροφορίες που πρόκειται να διαβιβαστούν είναι σπασμένες σε μικρά πακέτα που κινούνται ανεξάρτητα, στις ενδεχομένως διαφορετικές πορείες, μέσω των διάφορων δικτύων και των διακοπτών έως ότου φθάνουν στους προορισμούς τους και συγκεντρώνονται εκ νέου.

Το διαδίκτυο ως μέσον για το εμπόριο δε πραγματοποιήθηκε μέχρι τη δεκαετία του '90, όταν και έγινε ένα δημοφιλές και επικρατών μέσο για διασπορά των πληροφοριών. Λόγω της χαμηλής τιμής και της ταχύτητάς του, οι μεγάλης απόστασης συναλλαγές εμπορίου όλων των ειδών ήταν δυνατές. Η αύξηση στην ταχύτητα προβλέπει σε έναν πολύ μεγάλο όγκο ηλεκτρονικών συναλλαγών, αλλά και στην καλύτερη εξυπηρέτηση πελατών, που παρέχουν στα οικονομικά όργανα ένα καθορισμένο ανταγωνιστικό πλεονέκτημα πέρα από τις επιχειρήσεις που δεν χρησιμοποιούν το Διαδίκτυο.

Ως αποτέλεσμα των αυξήσεων στην τεχνολογία, όλο και περισσότερες επιχειρήσεις έχουν επιλέξει να στηριχθούν στο διαδίκτυο ως μέσο επέκτασης και σταθεροποίησης της βάσης πελατών τους.

Σιγά-σιγά άρχισε η επικοινωνία μεταξύ των επιχειρήσεων, για την ανταλλαγή εγγράφων, πληροφοριών κτλ. Και αργότερα, τα δεδομένα της αγοράς ενέπνευσαν τους επιχειρηματίες, να προσφέρουν τα προϊόντα τους, ηλεκτρονικά. Επειδή, μια επιχείρηση δε μπορεί να έχει το «know-how» και στην κατασκευή ηλεκτρονικού καταστήματος, συχνά καταφεύγει στη λύση της ανάθεσης έργου. Για ευνόητους λόγους «από τα μέσα του ’90 οι επιχειρήσεις διατηρούσαν προμηθευτές λογισμικού, εξοφλώντας τους σε μηνιαία βάση». Σήμερα, στόχος είναι η «προσωποποίηση» των πωλήσεων (κατά άτομο πωλήσεις) μέσα από το ΗΕ. Ουσιαστικά, το επιθυμητό αποτέλεσμα είναι η ηλεκτρονική συναλλαγή, να προσομοιώνει, όσο το δυνατό περισσότερο, τη «φυσική» συναλλαγή. Για το λόγο αυτό, οι Ιστοσελίδες σήμερα, έχουν δυναμικό χαρακτήρα, υποστηρίζονται από Βάση δεδομένων και η επόμενη γενιά Ιστοσελίδων, θα αποτελεί μέρος ενός ενοποιημένου, ολοκληρωμένου συστήματος, που θα διαχειρίζεται τις επιχειρηματικές διαδικασίες κάθε επιχείρησης. Επειδή, όπως έχει τονιστεί επανειλημμένως, προμηνύονται θετικές εξελίξεις, παρατηρήθηκε ότι «οι συναλλαγές ηλεκτρονικού εμπορίου διπλασιάζονται ετησίως».

Σημαντικές Ημερομηνίες

- 1960: Εισαγωγή των Η/Υ στις εσωτερικές Λειτουργίες των Τραπεζών
- 1970: Πιστωτικές κάρτες και Ηλεκτρονική Μεταφορά χρήματος
- 1980: Αυτοματοποίηση Συναλλαγών (ATM)

- 1984: Το EDI, ή η ηλεκτρονική ανταλλαγή δεδομένων, τυποποιήθηκε μέσω του ASC X12.(American Standards Committee - **X12**, electronic. Data Interchange) Αυτό εγγυήθηκε ότι οι επιχειρήσεις θα ήταν σε θέση να ολοκληρώσουν τις συναλλαγές τους, η μια με την άλλη, σοβαρά.
- 1992: Το Compuserve προσφέρει τα λιανικά προϊόντα σε απευθείας σύνδεση στους πελάτες του. Αυτό δίνει στους ανθρώπους την πρώτη ευκαιρία να αγοράσουν τα πράγματα από τον υπολογιστή τους.
- 1994: Ο Netscape έφθασε. Παρέχοντας στους χρήστες έναν απλό browser για να κάνει σερφ στο Διαδίκτυο και μια ασφαλή τεχνολογία συναλλαγής, σε απευθείας σύνδεση, αποκαλούμενο ασφαλές στρώμα υποδοχών.
- 1995: Δύο από τα μεγαλύτερα ονόματα στο ηλεκτρονικό εμπόριο ξεκινούν: Amazon.com και eBay.com.
- 1996: Νέες Υπηρεσίες - Διεκπεραίωση Συναλλαγών από το σπίτι
- 1998: Το DSL, ή η ψηφιακή γραμμή συνδρομητών, παρέχει γρήγορες, πάντα συνδεδεμένες υπηρεσίες Διαδικτύου στους συνδρομητές κατά μήκος της Καλιφόρνια. Αυτό προτρέπει τους ανθρώπους να ξοδέψουν περισσότερο χρόνο, και χρήματα, on-line.
- 1999: Τα λιανικά έξοδα μέσω του Διαδικτύου φθάνουν σε $20 δισεκατομμύρια, σύμφωνα με το Business.com.
- 2000: Η κυβέρνηση των Η.Π.Α επέκτεινε την παύση των φόρων Διαδικτύου μέχρι τουλάχιστον το 2005.

Μορφές Ηλεκτρονικού Εμπορίου

- E-Commerce (Ηλεκτρονικό Εμπόριο)
- E-Business (Ηλεκτρονικό Επιχειρείν)
- E-Enterprise (Ηλεκτρονική Επιχείρηση)
- M-Commerce (Κινητό Ηλεκτρονικό Εμπόριο)
- E-Marketplace (Ηλεκτρονική Αγορά, B2B)
- E-Malls (Ηλεκτρονικά Εμπορικά Κέντρα)
- E-Procurement (Σύστημα Ηλεκτρονικών Προμηθειών)
- E-Auctions (Σύστημα Ηλεκτρονικών Δημοπρασιών)
- E-Infobrokers (Μεσίτες πληροφοριών)

E-Commerce

Μία τυπική συναλλαγή Ηλεκτρονικού Εμπορίου 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

Κατηγοριοποίηση Όρων:

- Business-to-Business (B2B)
- Business-to-Government (B2Government)

- Business-to-Consumer (B2C)
- Individual-to-Government (C2G)

(π.χ. Amazon.com)

E-Business
Ηλεκτρονικό Επιχειρείν : οι συναλλαγές και η αλληλεπίδραση ανάμεσα στην εταιρία και τους εταιρικούς πελάτες της αλλά και τους συνεταίρους της
Χαρακτηριστικά της κατηγορίας αυτής είναι:

- η εστίαση της επιχειρηματικότητας στις βασικές ικανότητες του οργανισμού
- ο προσανατολισμός στη συσσώρευση διαδικασιών

(π.χ. MetalSite.com)

E-Enterprise
Συνδυασμός των κατηγοριών B2B & B2C :
συνδυασμός των παραδοσιακών ενεργητικών της εταιρίας
και της αποτελεσματικής διαμεσολάβησης με τους
καταναλωτές, πελάτες, διανομείς, συνεργάτες και
Ανταγωνιστές.
Οι συν-ανταγωνιστικοί (co-opetitive) οργανισμοί.
(π.χ.http://www.Dell.Com)

M-Commerce

- Ενώ η κινητή τηλεφωνία στην Ελλάδα έχει φτάσει το70%, δεν έχει γίνει διύσδειση του M-Commerce ακόμη
- Βασικοί Φορείς ανάπτυξης του M-Commerce:
  - Παροχείς Δικτυακών Υπηρεσιών
  - Έμπιστα Τρίτα Πρόσωπα
  - Ρυθμιστικά Όργανα (π.χ. ΕΕΤΤ)
  - Κατασκευαστές Τηλεφώνων και Συσκευών
  - Δίκτυα Λιανικού Εμπορίου
  - Εταιρικοί Πελάτες
  - Δημόσιος Τομέας
  - Καταναλωτές

E-marketplace

- Υιοθετείται από : μια επιχείρηση-ενδιάμεσο που εμπλέκεται μεταξύ αγοραστών και πωλητών προκειμένου να δημιουργήσει μια ηλεκτρονική αγορά (π.χ Yeses.com).
- Επιτρέπεται συνήθως η είσοδος συγκεκριμένων αγοραστών και προμηθευτών
- Το επιχειρηματικό μοντέλο ανήκει στις εφαρμογές ηλεκτρονικού εμπορίου B2B

Οι βασικότερες υπηρεσίες είναι :

- Δημιουργία ηλεκτρονικών καταλόγων με τα προϊόντα των προμηθευτών
- Τήρηση αρχείου πελατών
- Εξελιγμένος μηχανισμός αναζήτησης ώστε οι αγοραστές να βρίσκουν με ευκολία τα προϊόντα που τους ενδιαφέρουν
- Ολοκλήρωση της διαδικασίας της παραγγελίας και των πληρωμών

- Παροχή μηχανισμών ασφάλειας για την αυθεντικοποίηση του χρήστη και την ασφαλή μετάδοση των δεδομένων στο Internet

E-malls
Οι παρεχόμενες υπηρεσίες του συγκεκριμένου επιχειρηματικού μοντέλου :

- Παρουσίαση Προϊόντων (π.χ. ηλεκτρονικοί κατάλογοι)
- Εξελιγμένος μηχανισμός αναζήτησης προϊόντων και καταστημάτων
- Δυναμική ενημέρωση του καλαθιού αγορών
- Ολοκληρωμένος μηχανισμός πληρωμών
- Παρακολούθηση Παραγγελιών
- Μηχανισμοί Διαφημίσεων

(π.χ. http://emallsofamerica.com/, http://www.premier-net.com/vvtc/DepartmentStores/emalls/)

E-procurement

- Μεγάλες εταιρίες ή δημόσιοι οργανισμοί υλοποιούν εφαρμογές ηλεκτρονικών προμηθειών στο διαδίκτυο
- Επιτυγχάνεται η αυτοματοποίηση της διαδικασίας των προμηθειών

(π.χ. http://www.ciol.com/content/e_ent/procurement/)

Οι λειτουργίες αυτού του επιχειρηματικού μοντέλου είναι :

- Παρουσίαση καταλόγων προϊόντων
- Διαχείριση παραγγελιών
- Διαχείριση πληρωμών
- Μηχανισμός αξιολόγησης προσφορών

E-auctions
Οι εμπλεκόμενες οντότητες σε ένα σύστημα ηλεκτρονικών δημοπρασιών είναι:

- Ο «πλειστηριαστής»: καθορίζει τους όρους με βάση τους οποίους θα πραγματοποιηθεί η δημοπρασία
- Ο «προμηθευτής»: προσφέρει τα προϊόντα του προς πώληση
- Ο «πελάτης»: προσφέρει τιμή για τα προϊόντα που επιθυμεί να αγοράσει

(π.χ. http://www.0aaa.com/auction/)

E-Infobrokers
Μεσίτες Πληροφορίας με ασφαλή και γρήγορο τρόπο
Λειτουργίες:

- Εντοπισμός Πληροφορίας
- Συγκέντρωση Πληροφορίας
- Αποθήκευση Πληροφορίας
- Λειτουργία ως TTP

(π.χ. http://www.es.stelnet.com/contatti.html)

2. Νομικό και Κανονιστικό Πλαίσιο

Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να εναρμονίζονται με τη νομοθεσία των χωρών στις οποίες λειτουργούν. Με την εμφάνιση του διαδικτύου και την πραγματοποίηση εμπορικών συναλλαγών μέσω αυτού ανέκυψε μια σειρά από νομικά ζητήματα που απασχόλησαν τόσο την Ευρωπαϊκή Ένωση όσο και τα επιμέρους κράτη μέλη. Το βασικό πρόβλημα σε επίπεδο νομοθεσίας που αντιμετώπισαν οι περισσότερες εφαρμογές ηλεκτρονικού εμπορίου, που αναπτύχθηκαν με την εμφάνιση του διαδικτύου, ήταν η έλλειψη ξεκάθαρων νομοθετικών ρυθμίσεων που διέπουν το ηλεκτρονικό εμπόριο. Η απότομη τεχνολογική ανάπτυξη και η ραγδαία εξάπλωση του ηλεκτρονικού εμπορίου βρήκαν απροετοίμαστη τη νομοθεσία σε παγκόσμιο επίπεδο, η οποία αποδείχθηκε ελλιπείς και αδύναμη να προσαρμοστεί τόσο γρήγορα στα νέα δεδομένα.

Παρά την παγκόσμια φύση των ηλεκτρονικών επικοινωνιών, είναι αναγκαίος ο συντονισμός των εθνικών κανονιστικών μέτρων σε επίπεδο Ευρωπαϊκής Ένωσης για να αποφευχθεί η κατάτμηση της εσωτερικής αγοράς και για να εγκαθιδρυθεί ένα κατάλληλο ευρωπαϊκό κανονιστικό πλαίσιο. Για να επιτραπεί η απρόσκοπτη ανάπτυξη του ηλεκτρονικού εμπορίου, το νομικό πλαίσιο πρέπει να είναι σαφές, απλό και συμβατό με τους κανόνες που ισχύουν σε διεθνές επίπεδο. Για τους λόγους αυτούς, η Ευρωπαϊκή Ένωση έχει εκδώσει δέσμη Οδηγιών που σχετίζονται άμεσα ή έμμεσα με το ηλεκτρονικό εμπόριο. Συμπεριλαμβάνονται η Οδηγία 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, η οποία καθορίζει κανόνες σχετικά με τη νομική αναγνώριση των ηλεκτρονικών υπογραφών και τις διαδικασίες πιστοποίησης, και η Οδηγία 2000/31/ΕΚ για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.

Κάθε κράτος μέλος της Ευρωπαϊκής Ένωσης πρέπει να ενσωματώσει τις διάφορες νομοθετικές ρυθμίσεις της Ευρωπαϊκής Ένωσης στον τοπικό του νόμο. Η Ελλάδα έχει ενσωματώσει ήδη αρκετές από τις Οδηγίες στο εθνικό της δίκαιο. Ενδεικτικά, έχει ενσωματώσει την Οδηγία για το ηλεκτρονικό εμπόριο στο Προεδρικό Διάταγμα 131/2003 και την Οδηγία σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές στο Προεδρικό Διάταγμα 150/2001. Στα πλαίσια της δημιουργίας του εθνικού μας κανονιστικού πλαισίου καθορίστηκε η Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής (ΠΥΠ), καθώς και για τη λειτουργία μηχανισμών εθελοντικής διαπίστευσης των ΠΥΠ και διαπίστωσης της συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής.

Πολύ σημαντικό ρόλο στο ελληνικό νομοθετικό πλαίσιο για το ηλεκτρονικό εμπόριο παίζει ένας ανεξάρτητος διοικητικός φορέας, η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) που δραστηριοποιείται τα τελευταία χρόνια. Βασική αρμοδιότητα της είναι η προστασία του απορρήτου των επικοινωνιών. Για το σκοπό αυτό η ΑΔΑΕ έχει εκδώσει κάποιους κανονισμούς για τη διασφάλιση του απορρήτου των επικοινωνιών και κάθε εγκατεστημένος στην Ελλάδα οργανισμός που έχει ως γενικό αντικείμενο την επικοινωνία, συνεπώς και κάθε οργανισμός ηλεκτρονικού εμπορίου, θα πρέπει να τους τηρεί. Επίσης, ευθύνη της ΑΔΑΕ είναι και ο έλεγχος τήρησης των κανονισμών, που εκδίδει, από τους εν λόγω οργανισμούς.

2.1 Σχετική Νομοθεσία

Η συνεχώς αυξανόμενη χρήση του διαδικτύου για τη σύναψη εμπορικών συμβάσεων, το ηλεκτρονικό εμπόριο και οι ανυπολόγιστες επιδράσεις του στην οικονομία, δραστηριοποίησαν διεθνείς οργανισμούς, την Επιτροπή Ευρωπαϊκών Κοινοτήτων καθώς και κυβερνήσεις διαφόρων χωρών, προκειμένου να ορίσουν το νομικό πλαίσιο του ηλεκτρονικού εμπορίου.

Σε διεθνές επίπεδο, η Επιτροπή Διεθνούς Εμπορικού Δικαίου των Ηνωμένων Εθνών (UNCITRAL) συνέταξε το 1996 τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο, ρυθμίζοντας ζητήματα όπως η εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης, η νομική ισχύς της ηλεκτρονικής υπογραφής, η αποδεικτική δύναμη των ηλεκτρονικών κειμένων, ο τόπος, ο χρόνος και απόδειξη παραλαβής του ηλεκτρονικού μηνύματος.

Μέσα στο πλαίσιο αυτό, η Ευρωπαϊκή Ένωση πραγματοποιεί σταδιακά μια συντονισμένη προσπάθεια να θέσει σταθερές νομικές βάσεις που να δημιουργούν ένα δίχτυ ασφάλειας για το ηλεκτρονικό εμπόριο. Βασικός γνώμονας είναι η ανάπτυξη του ηλεκτρονικού εμπορίου με την απαραίτητη, όμως, υποδομή που να αποδίδει την κατάλληλη νομική ισχύ στις ηλεκτρονικές συναλλαγές. Τα τελευταία χρόνια η Ευρωπαϊκή Ένωση έχει κάνει αρκετά για την ενίσχυση του ηλεκτρονικού εμπορίου. Έχει εκδώσει Οδηγίες, προτάσεις, συστάσεις για τη δημιουργία νομικού πλαισίου για το ηλεκτρονικό εμπόριο. Κάθε χώρα μέλος πρέπει να ενσωματώσει τις διάφορες νομοθετικές ρυθμίσεις της Ευρωπαϊκής Ένωσης στον τοπικό της νόμο. Κατά μέσον όρο, τα κράτη μέλη έχουν μια διετή περίοδο μετάβασης να μεταφράσουν μια Οδηγία σε εθνικό νόμο.

Η ελληνική έννομη τάξη προσπαθεί να προσαρμοστεί στις προσταγές της νέας εμπορικής πραγματικότητας κυρίως με την προσαρμογή των ευρωπαϊκών νομοθετημάτων στο εσωτερικό δίκαιο. Παρόλο που παρουσιάζεται γενικά μια καθυστέρηση στην υιοθέτηση κάποιων επιμέρους Οδηγιών, αρχίζει και παίρνει μορφή το νομοθετικό καθεστώς που αρμόζει στο ηλεκτρονικό εμπόριο.

2.1.1 Ευρωπαϊκή Νομοθεσία

Στο επίκεντρο των προσπαθειών της Ευρωπαϊκής Ένωσης για τη νομοθετική ρύθμιση του ηλεκτρονικού εμπορίου βρίσκεται η Οδηγία για το Ηλεκτρονικό Εμπόριο (2000/31/ΕΚ) που θέτει τις βάσεις για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία αυτή καθιερώθηκε η αρχή της ελευθερίας σύναψης ηλεκτρονικών συμβάσεων, η αρχή της χώρας προέλευσης, που σημαίνει ότι το Δίκαιο που διέπει τις συναλλαγές με ηλεκτρονικά μέσα είναι το Δίκαιο της χώρας μόνιμης εγκατάστασης του φορέα παροχής υπηρεσιών, και ο εξωδικαστικός διακανονισμός των διαφορών που θα προκύψουν.

Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου συμπληρώνουν μια σειρά από Οδηγίες, συστάσεις και κανονισμοί που είτε συστάθηκαν προκειμένου να ρυθμίσουν ηλεκτρονικές μορφές εμπορίου είτε είναι σχετικές χωρίς βέβαια να αναφέρονται ρητά στο ηλεκτρονικό εμπόριο. Κάθε χώρα μέλος της Ευρωπαϊκής Ένωσης έχει προσαρμόσει το νομικό αυτό πλαίσιο στο δικό της εσωτερικό δίκαιο, δημιουργώντας τους δικούς της Κανόνες. Στη συνέχεια παρουσιάζεται η Ευρωπαϊκή Νομοθεσία σχετικά με το ηλεκτρονικό εμπόριο.

Δικαιώματα Πνευματικής Ιδιοκτησίας

Οδηγία 2004/48/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την επιβολή του δικαιώματος πνευματικής ιδιοκτησίας.

Οδηγία 2001/29/ΕC της 22ας Μαΐου 2001 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας.

Οδηγία 96/9/ΕC της 11ης Μαρτίου 1996 σχετικά με τη νομική προστασία των βάσεων δεδομένων.

Οδηγία 92/100/ΕΕC σχετικά με το δικαίωμα εκμίσθωσης το δικαίωμα δανεισμού και ορισμένα δικαιώματα συγγενικά προς την πνευματική ιδιοκτησία στον τομέα των προϊόντων της διανοίας.

Ηλεκτρονικό Εμπόριο

- Οδηγία 2000/31/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (Οδηγία για το ηλεκτρονικό εμπόριο: περιγράφεται αναλυτικά στην παράγραφο 2.2).

Προστασία Δεδομένων

- Οδηγία 95/46/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η Οδηγία αυτή περιγράφεται αναλυτικά στην παράγραφο 2.4.1.
- Κανονισμός (ΕC) 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της κοινότητας και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Προστασία Δεδομένων στον Τηλεπικοινωνιακό Τομέα

- Οδηγία 97/66/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.
- Οδηγία 2002/58/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα (Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες: περιγράφεται αναλυτικά στην παράγραφο 2.4.2).

Προστασία των Ηλεκτρονικών Συνδρομητικών Υπηρεσιών

- Οδηγία 98/84/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη νομική προστασία των υπηρεσιών που βασίζονται ή συνίστανται στην παροχή πρόσβασης υπό όρους (συνδρομητικές υπηρεσίες).

Ηλεκτρονικές Υπογραφές

- Οδηγία 1999/93/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.

Εξ αποστάσεως Πωλήσεις

- Οδηγία 97/7/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

Παραπλάνηση και Συγκριτική Διαφήμιση

- Οδηγία 97/55/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Οκτωβρίου 1997, για την τροποποίηση της Οδηγίας 84/450/EEC, σχετικά με την παραπλανητική διαφήμιση προκειμένου να συμπεριληφθεί η συγκριτική διαφήμιση.

Μια ιδιαίτερα σημαντική εξέλιξη των τελευταίων χρόνων είναι η δημιουργία του προγράμματος eEurope. Το πρόγραμμα αυτό, στο οποίο η Ελλάδα έχει ενεργό μέρος, ιδρύθηκε από την Ευρωπαϊκή Ένωση σε μια προσπάθεια διερεύνησης των δυνατοτήτων χρήσης του διαδικτύου στον ευρωπαϊκό χώρο και των προκλήσεων που αυτό δημιουργεί για εταιρείες και ιδιώτες. Μια από τις σημαντικότερες προτεραιότητες του προγράμματος είναι η βελτίωση της ασφάλειας των ηλεκτρονικών συναλλαγών, προκειμένου να αναπτυχθεί η εμπιστοσύνη των χρηστών στο διαδίκτυο και να αυξηθούν οι ηλεκτρονικές συναλλαγές. Παράλληλα, το πρόγραμμα eEurope προσπαθεί να συμβάλει στην ενίσχυση του νομοθετικού πλαισίου της Ευρωπαϊκής Ένωσης.

2.1.2 Ελληνική Νομοθεσία

Όπως σε κάθε χώρα της Ευρωπαϊκής Ένωσης, έτσι και στην Ελλάδα οι αρμόδιες αρχές προσπαθούν να συμμορφώσουν το εθνικό δίκαιο προς τα ευρωπαϊκά νομοθετήματα που ήδη υπάρχουν. Η σταδιακή δημιουργία του νομοθετικού πλαισίου αποτελεί τη βάση για τη ρύθμιση του ηλεκτρονικού εμπορίου.

Στη συνέχεια παρουσιάζεται η Ελληνική Νομοθεσία σχετικά με το ηλεκτρονικό εμπόριο.

Δικαιώματα Πνευματικής Ιδιοκτησίας

- Νόμος 2121/1993 για την πνευματική ιδιοκτησία, τα συγγενικά δικαιώματα και τα πολιτιστικά θέματα.

Ηλεκτρονικό Εμπόριο

- Προεδρικό Διάταγμα 131/2003, το οποίο αποτελεί προσαρμογή στην Οδηγία για το ηλεκτρονικό εμπόριο (2000/31/EC).

Προστασία Δεδομένων

- Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ.
- Νόμος 2225/1994 για την προστασία του απορρήτου των επικοινωνιών, ο οποίος όμως καθορίζει και τις περιπτώσεις άρσης του απορρήτου αυτού.

Προστασία Δεδομένων στον Τηλεπικοινωνιακό Τομέα

- Νόμος 2774/1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Ο Νόμος αυτός αποτελεί προσαρμογή στην Οδηγία 97/66/ΕC.

Προστασία των Ηλεκτρονικών Συνδρομητικών Υπηρεσιών

- Προεδρικό Διάταγμα 343/2002 για τη νομική προστασία των υπηρεσιών που βασίζονται ή συνίστανται στην παροχή πρόσβασης υπό όρους (συνδρομητικές υπηρεσίες). Το Διάταγμα αυτό αποτελεί προσαρμογή στην Οδηγία 98/84/ΕC.

Ηλεκτρονικές Υπογραφές

- Προεδρικό Διάταγμα 150/2001 αποτελεί προσαρμογή στην Οδηγία 1999/93/ΕC σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.
- Κανονισμός ΕΕΤΤ για την Παροχή Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (ΦΕΚ 603/Β'/16-5-2002).
- Προεδρικό Διάταγμα 342/2002 για τη διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημόσιων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων.
- Κανονισμός ΕΕΤΤ για την Εθελοντική Διαπίστευση των Παρόχων Υπηρεσιών Πιστοποίησης (295/65).
- Κανονισμός ΕΕΤΤ για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων (295/64).
- Κανονισμός ΕΕΤΤ για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης (295/63).

Εξ αποστάσεως Πωλήσεις

- Νόμος 2251/1994 για την προστασία των καταναλωτών (ΦΕΚ 191 Α'/16 Νοεμβρίου 1994).

Παραπλάνηση και Συγκριτική Διαφήμιση

- Νόμος 2251/1994 για την προστασία των καταναλωτών (ΦΕΚ 191 Α'/16 Νοεμβρίου 1994).

3. Εφαρμογές και Προοπτικές του World Wide Web

3.1 Εμπορικές εφαρμογές του World Wide Web

Μέσα στο Web διαμορφώνεται ταχύτατα μία νέα παγκόσμια αγορά, συναρπαστική και εύκολα προσπελάσιμη από κάθε χρήστη του δικτύου Internet. Σε αυτήν, μπορεί κάποιος να συναντήσει καταστήματα κάθε μεγέθους, όπως ακριβώς και στον πραγματικό κόσμο. Τα μικρότερα από αυτά φιλοξενούν τα προϊόντα ή τις υπηρεσίες μίας μόνο επιχείρησης, ενώ τα μεγαλύτερα αποτελούν κολοσσιαία εμπορικά κέντρα τα οποία συστεγάζουν εκατοντάδες εταιρείες.

3.2 Ηλεκτρονικά εμπορικά κέντρα

Μία νέα τάση που εδραιώνεται ταχύτατα στο εξωτερικό και αναμένεται να επικρατήσει σταδιακά και στην Ελλάδα είναι τα ηλεκτρονικά εμπορικά κέντρα ή Cybermalls, όπως καλούνται συνήθως. Αυτά είναι ειδικοί χώροι στους Web servers, συνήθως κάποιων εταιρειών παροχής on-line υπηρεσιών, όπου βρίσκονται ταξινομημένες σελίδες εμπορικών καταστημάτων. Στις περισσότερες περιπτώσεις υπάρχει μία ομοιομορφία στο σχεδιασμό και την παρουσίαση για όλους τους συμμετέχοντες, ενώ και οι εισαγωγικές σελίδες έχουν μία καθορισμένη εμφάνιση που είναι κοινή σε όλους. Αυτό, βέβαια, μπορεί να είναι περιοριστικό σε πολλές περιπτώσεις όπου οι διαφημιζόμενες εταιρείες θα επιθυμούσαν πλουσιότερο περιεχόμενο, είναι όμως ιδανικό για μικρά καταστήματα που θέλουν να έχουν μία ηλεκτρονική παρουσία στο Internet, αφού όπως είναι προφανές το κόστος είναι μικρό. Το φάσμα των καταστημάτων που συμμετέχουν σε αυτά τα οργανωμένα εμπορικά κέντρα του Web είναι αξιοθαύμαστο. Δισκοπωλεία, βιβλιοπωλεία, καταστήματα ηλεκτρικών ειδών και οτιδήποτε μπορεί ο καθένας να φανταστεί είναι μερικά παραδείγματα. Επιπλέον, γιατροί, δικηγόροι και άλλοι επαγγελματίες έχουν καταχωρίσεις σε ειδικούς χώρους που προσφέρονται από τις εταιρείες παροχής υπηρεσιών στο δίκτυο Internet και σε κατάλληλα διαμορφωμένες ενότητες σελίδων ενός ηλεκτρονικού εμπορικού κέντρου. Όλοι αυτοί, φυσικά, δεν είναι απαραίτητο να έχουν κάποιες ειδικές γνώσεις σχετικά με την πληροφορική. Απλά ετοιμάζουν το υλικό που θέλουν και το παραδίδουν στην εταιρεία που παρέχει πρόσβαση στο Internet, η οποία με τη σειρά της το εισάγει στον Web server στον προβλεπόμενο για το σκοπό αυτό χώρο, αφού προηγουμένως μορφοποιήσει τις σελίδες σύμφωνα με το ανάλογο μοτίβο. Η όλη προσπάθεια βέβαια έχει καθαρά διαφημιστικό χαρακτήρα για τον ενδιαφερόμενο.

Ένα μικρό κατάστημα, για παράδειγμα, θέλει να πληροφορήσει τους χρήστες που επισκέπτονται τον συγκεκριμένο κόμβο για τις υπηρεσίες που προσφέρει ή τα προϊόντα που διαθέτει, μαζί ίσως με κάποια συνοδευτική φωτογραφία, τη διεύθυνση και το τηλέφωνο, καθώς και κάποιον μικρό τιμοκατάλογο. Στην ουσία, έχουμε την περίπτωση μίας ηλεκτρονικής διαφήμισης, μίας διαφημιστικής καταχώρησης στον χώρο του Web, για την οποία περισσότερα αναφέρονται παρακάτω. Στην περίπτωση τώρα του ελεύθερου επαγγελματία, το περιεχόμενο της σελίδας θα περιλαμβάνει ένα είδος "βιογραφικού σημειώματος" για τις μέχρι τώρα δραστηριότητές του, διεύθυνση και τηλέφωνο του γραφείου ή της κατοικίας του, περιγραφή των παρεχόμενων υπηρεσιών, μία φωτογραφία ενδεχομένως και ό,τι άλλο κρίνει ο ίδιος κατάλληλο για την προσωπική του προβολή.

3.3 Ηλεκτρονικές διαφημίσεις

Με την ονομασία ηλεκτρονικές διαφημίσεις, ή ισοδύναμα με τον αγγλικό όρο Cyberads, καλούνται συνήθως οι διαφημιστικές καταχωρίσεις στο World Wide Web. Ένας

άλλος όρος που χρησιμοποιείται επίσης είναι on-line advertisements. Τις περισσότερες φορές, η ίδια η σελίδα στο Web αποτελεί παράλληλα και μία διαφήμιση. Υπάρχουν όμως και κάποιες ειδικότερες περιπτώσεις. Η πιο σημαντική από αυτές είναι η ενοικίαση χώρου στην εισαγωγική σελίδα ενός πολυσύχναστου Web site και η παράθεση σε κάποιο ευδιάκριτο σημείο της σελίδας μίας εμβόλιμης καταχώρησης με τη μορφή κάποιας εικόνας. Φυσικά η γραφική αυτή εικόνα είναι ένας υπέρ-σύνδεσμος που οδηγεί σε αναλυτικές σελίδες της διαφημιζόμενης εταιρείας. Για να κατανοήσουμε καλύτερα πως λειτουργεί το όλο σύστημα, ας σκεφτούμε τι συμβαίνει σήμερα στα περιοδικά. Ο ενδιαφερόμενος καταβάλλει κάποιο χρηματικό ποσό ανάλογα με την κυκλοφορία του περιοδικού και την έκταση που καταλαμβάνει η διαφήμισή του μέσα σε αυτό. Μάλιστα, όπως στον πραγματικό κόσμο, έτσι και στον ηλεκτρονικό, υπάρχει και η έννοια της χορηγίας, ή sponsoring, αν και προς το παρόν εφαρμόζεται κυρίως από εταιρείες πληροφορικής.

Ως παράδειγμα μπορούμε να αναφέρουμε τους κόμβους στο Web κάποιων πανεπιστημίων, των οποίων ο εξοπλισμός έχει παρασχεθεί ως έναν βαθμό από μεγάλες εταιρείες κατασκευής υπολογιστικών συστημάτων (π.χ. IBM, Silicon Graphics, Sun Microsystems κ.ά.) με τη μορφή δωρεάς. Το πανεπιστήμιο στη συνέχεια αναλαμβάνει τη δέσμευση να προσθέσει στην κεντρική του σελίδα μία ένδειξη προέλευσης του εξοπλισμού του, συνήθως μαζί με κάποιο λογότυπο και ίσως έναν σύνδεσμο προς την εταιρεία-χορηγό. Οι ηλεκτρονικές αυτές διαφημίσεις αποτελούν ένα δυναμικά αναπτυσσόμενο κομμάτι, διότι προσφέρουν μερικά πλεονεκτήματα που δεν είναι δυνατόν να περάσουν απαρατήρητα:

1. Οι ηλεκτρονικές διαφημίσεις είναι οικονομικές. Μία τέτοια καταχώρηση, ακόμα και όταν τοποθετείται στην κεντρική σελίδα ενός πολυσύχναστου κόμβου που δέχεται εκατομμύρια επισκέψεις το μήνα, είναι συμφέρουσα εάν συγκριθεί με τα υπόλοιπα παραδοσιακά διαφημιστικά μέσα (τηλεόραση, ραδιόφωνο, εφημερίδες, περιοδικά).

2. Η ηλεκτρονική διαφήμιση είναι ενεργός 24 ώρες το 24ωρο. Ενώ κάποιο διαφημιστικό spot στην τηλεόραση διαρκεί λίγα δευτερόλεπτα, ένα γραφικό μήνυμα σε κάποια σελίδα του Web είναι συνεχώς ενεργό, για το χρονικό διάστημα συνήθως που έχει συμφωνηθεί με την εταιρεία παροχής πρόσβασης στο Internet.

3. Ο διαφημιζόμενος γνωρίζει κάθε στιγμή την αποτελεσματικότητα της διαφήμισής του. Όλοι οι σύγχρονοι servers παρέχουν τη δυνατότητα ακριβούς καταγραφής πολλών στατιστικών στοιχείων. Για παράδειγμα, πόσοι χρήστες επισκέφθηκαν μία σελίδα, σε ποια χρονικά διαστήματα, από ποιους servers, με ποια προγράμματα κ.λ.π. Όλα αυτά τα δεδομένα αποθηκεύονται σε αρχεία και μπορούν να αποσταλούν μέσω ηλεκτρονικού ταχυδρομείου στους ενδιαφερόμενους. Βάσει αυτών των στατιστικών στοιχείων μπορούν οι managers και οι άνθρωποι του marketing διάφορων εταιρειών να λάβουν αποφάσεις για την προώθηση των προϊόντων τους.

4. Η δημιουργία μίας ηλεκτρονικής διαφήμισης δεν απαιτεί κάποια ιδιαίτερη προεργασία και είναι μία διαδικασία απλή. Αρκεί να υπάρχει το κατάλληλο προσωπικό που θα κωδικοποιήσει τις σελίδες.

Η έννοια του on-line shopping

Η έννοια του on-line shopping αναφέρεται εδώ με τη μεγαλύτερη δυνατή ευρύτητα του όρου. Ως έννοια, περιλαμβάνει την αγορά καταναλωτικών αγαθών (π.χ. σπίτια, αυτοκίνητα, είδη ρουχισμού κ.ά.), αναλώσιμων καταναλωτικών ειδών (π.χ. είδη διατροφής ή γραφική ύλη), την κράτηση θέσεων (booking) σε εστιατόρια, ξενοδοχεία, αεροπλάνα κ.λ.π. και τις συμφωνίες για παροχή χρηματοοικονομικών υπηρεσιών (π.χ. deals, δημιουργία χαρτοφυλακίων, αγοραπωλησίες μετοχών και αμοιβαίων κεφαλαίων). Αυτό που

πρέπει να διευκρινιστεί είναι ότι το on-line shopping δεν ανακαλύφθηκε με την εισαγωγή του World Wide Web ως υπηρεσίας του δικτύου Internet, αν και σαφώς αυτό αποτελεί σήμερα το πιο "καυτό" σημείο αγορών.

Η ιστορία του on-line shopping ξεκινά πολύ νωρίτερα, στις αρχές της δεκαετίας του 1980, όταν η αμερικανική εταιρεία παροχής on-line υπηρεσιών Compuserve έδωσε τη δυνατότητα στους Αμερικανούς συνδρομητές, μέσα από το text περιβάλλον της, να παραγγέλνουν κάποια προϊόντα. Την εποχή εκείνη, βέβαια, οι παρεχόμενες υπηρεσίες ήταν στοιχειώδεις και τα συστήματα αποτελούσαν φυσική συνέχεια του τηλεφωνικού teleshopping (σε συνδυασμό με το τηλεοπτικό marketing). Φυσικά, ένα τόσο απλό σύστημα μίας on-line υπηρεσίας, που βασιζόταν σε κείμενο και σε κάποια απλοϊκά μενού, δεν ήταν δυνατό να γνωρίσει αξιόλογη επιτυχία, παρά μόνο μεταξύ των επαγγελματιών της Πληροφορικής που αποτελούσαν και τη συντριπτική πλειοψηφία των δικτυωμένων χρηστών εκείνη την εποχή. Με ένα τόσο περιορισμένο αγοραστικό κοινό και χωρίς ακόμα τις επαναστατικές υπηρεσίες που προσφέρει σήμερα το World Wide Web, ήταν επόμενο να οδηγηθούμε σε μία στάσιμη κατάσταση, η οποία ελάχιστα ενδιέφερε τους μεγάλους προμηθευτές και απέτρεπε τις όποιες επενδύσεις τους.

Η κατάσταση αυτή άλλαξε ριζικά κατά τη διάρκεια της δεκαετίας του 1990 και αυτό δεν συνέβη τυχαία. Καταλυτικό ρόλο έπαιξε η σαρωτική επικράτηση διάφορων γραφικών και εύχρηστων λειτουργικών συστημάτων και προγραμμάτων, τα οποία κατέστησαν τον προσωπικό υπολογιστή προσιτό σε ένα μεγάλο μέρος του καταναλωτικού κοινού. Έτσι, σε συνδυασμό με τη συνεχή πτώση στις τιμές των μηχανημάτων και των περιφερειακών συσκευών ενός Η/Υ, άνθρωποι, οι οποίοι είχαν μικρή ή ανύπαρκτη εξοικείωση με τους υπολογιστές, έδωσαν μεγάλη ώθηση στην πληροφορική επανάσταση που διανύουμε. Την κατάσταση αυτή εκμεταλλεύτηκαν άμεσα μεγάλες εταιρείες παροχής on-line υπηρεσιών σε όλον τον κόσμο. Το περιβάλλον επικοινωνίας μέσα από τα δίκτυα βελτιώθηκε και έγινε προσιτό και πιο εύχρηστο σε όλους, με αποτέλεσμα πολλές εταιρείες να προσφέρουν τώρα πλέον τα προϊόντα τους μέσα από τις οθόνες. Ο συνεχώς αυξανόμενος αριθμός των χρηστών έκανε ελκυστική την προοπτική συμμετοχής διάφορων προμηθευτών, ενώ το οργανωμένο και ασφαλές περιβάλλον που προσφέρει μία on-line υπηρεσία λειτούργησε καταλυτικά.

3.4 Ηλεκτρονικό χρήμα

Προς το παρόν, οι αγορές μέσω του δικτύου Internet έχουν περιορισμένο εύρος. Το σύστημα αγορών βασίζεται στις πιστωτικές κάρτες. Για παράδειγμα, ένας χρήστης συνδέεται σε κάποιον κόμβο και μέσω ενός υπέρ-συνδέσμου μπορεί να επισκεφθεί έναν εκδοτικό οίκο. Εκεί, υπάρχουν σελίδες του Web με τα περιεχόμενα των βιβλίων και άλλες χρήσιμες πληροφορίες. Αν κάποιος τίτλος κινεί το ενδιαφέρον του χρήστη, αυτός μπορεί στη συνέχεια να συμπληρώσει on-line μία ηλεκτρονική φόρμα παραγγελίας και να καταχωρίσει τα στοιχεία του, μαζί με τον αριθμό της πιστωτικής του κάρτας. Η αίτηση θα καταχωρηθεί στον server και το βιβλίο θα αποσταλεί στον ενδιαφερόμενο αγοραστή ταχυδρομικά. Ουσιαστικά εδώ δηλαδή, δεν υπάρχει κάτι το πρωτότυπο ή διαφορετικό. Αντί ο χρήστης να δώσει τον αριθμό της κάρτας του μέσω τηλεφώνου, τον πληκτρολογεί στον υπολογιστή και η πληρωμή πραγματοποιείται με την κλασσική μέθοδο. Αυτό όμως σύντομα πρόκειται να αλλάξει.

Ας πάρουμε για παράδειγμα την έννοια του E-Cash, η οποία χρησιμοποιείται αρκετά συχνά τελευταία και αποτελεί σύντμηση του αγγλικού όρου Electronic Cash (ηλεκτρονικό χρήμα). Ο όρος αυτός συναντάται και με άλλα ονόματα, όπως Net Cash, Virtual Cash, Digital Cash κ.λ.π. Όλα είναι στην ουσία παραλλαγές του ίδιου θέματος. Η κεντρική ιδέα έχει ως εξής: πρόκειται για ηλεκτρονικές χρηματικές μονάδες που παρέχει σε έναν χρήστη

κάποια ηλεκτρονική τράπεζα, με αντίτιμο βέβαια "πραγματικά" χρήματα. Με απλά λόγια, ο χρήστης καταβάλλει κάποιο χρηματικό ποσό και ο ηλεκτρονικός του λογαριασμός τροφοδοτείται με το αντίστοιχο "ηλεκτρονικό". Στη συνέχεια, αυτός έχει τη δυνατότητα να επισκεφθεί ένα οποιοδήποτε ηλεκτρονικό εμπορικό κέντρο (cybermall) και να πραγματοποιήσει τις αγορές του. Στη διάρκεια των δοσοληψιών το ηλεκτρονικό του απόθεμα ενημερώνεται διαρκώς, καθώς τα αποτελέσματα των εμπορικών του συναλλαγών καταχωρούνται σε μία ηλεκτρονική τράπεζα. Συνεπώς, τα "ψηφιακά" χρήματα του χρήστη μειώνονται, ενώ αντίστοιχα αυξάνονται εκείνα του πωλητή μέσω ενός αυτόματου μηχανισμού συναλλαγών.

Όπως στον πραγματικό κόσμο, έτσι και στον αντίστοιχο ηλεκτρονικό, οι μέθοδοι πληρωμών υπάγονται σε δύο ευρείες κατηγορίες: χρέωση και πίστωση. Στην πρώτη περίπτωση, συγκεντρώνουμε πρώτα τα χρήματα και έπειτα πληρώνουμε κάποιον λογαριασμό. Στη δεύτερη, πραγματοποιούμε κάποιες αγορές και καταβάλλουμε το ανάλογο χρηματικό ποσό αργότερα. Όπως οι έννοιες, λοιπόν, cash και credit συνυπάρχουν στον σημερινό πραγματικό επιχειρησιακό κόσμο, το ίδιο συμβαίνει και στον αντίστοιχο ψηφιακό. Με τον όρο electronic ή digital cash εννοείται το ηλεκτρονικό ισοδύναμο ενός π.χ. χαρτονομίσματος, με ονομασία έναν μοναδικό αναγνωριστικό αριθμό και το ποσό που αναπαριστά.

Ο όρος digital credit υποδηλώνει το ίδιο πιστωτικό σύστημα που ισχύει και στις κανονικές συναλλαγές. Η μόνη διαφορά έγκειται στην ενσωμάτωση ψηφιακών χρονομετρών και υπογραφών για λόγους καταχώρησης των συναλλαγών. Κατά την αγορά, δημιουργείται μία περιγραφή της συναλλαγής με τα ονόματα του λήπτη και αυτού που καταβάλλει το χρηματικό ποσό, την ημερομηνία και ώρα της συναλλαγής και το ποσό της πληρωμής. Ο αγοραστής υπογράφει με το ιδιωτικό του κλειδί (κωδικό) το "έγγραφο" της δοσοληψίας και ο πωλητής στη συνέχεια, χρησιμοποιώντας ένα δημόσιο κλειδί, επιβεβαιώνει την πράξη της συναλλαγής και ενημερώνει το σύστημα εκκαθαρίσεων κάποιας ηλεκτρονικής τράπεζας.

Μία on-line πληρωμή περιλαμβάνει γενικά τρία μέρη. Ο πελάτης πληρώνει, ο έμπορος λαμβάνει το αντίτιμο και η τράπεζα λογίζει τη δοσοληψία, φροντίζοντας τα χρήματα να καταλήξουν από τον πελάτη στο λογαριασμό του εμπόρου. Σε ένα ομότιμο (peer-to-peer) σύστημα οι χρήστες μπορούν να δρουν ως πελάτες και πωλητές μαζί, ανάλογα με την περίσταση. Ο πελάτης χρησιμοποιεί ειδικό λογισμικό, συνήθως κάποιον WWW browser με πρωτόκολλο ασφαλείας, όπως είναι το SSL (Security Sockets Layer) ή το S-HTTP (Secure HyperText Transfer Protocol). Κάποιο αντίστοιχο πρόγραμμα server υπάρχει και από τη μεριά του πωλητή. Τέλος, ένας payment server χρησιμοποιείται από την τράπεζα στο δίκτυο για να επιβεβαιώσει τη συναλλαγή και να προβεί στις απαραίτητες ενημερώσεις λογαριασμών. Προς το παρόν, η ασφάλεια του συστήματος επιτυγχάνεται μέσω κρυπτογράφησης των κωδικών, οπότε διατηρούνται και αντίγραφα σε χαρτί για κάθε περίπτωση. Αργότερα, όταν η τεχνολογία αυτή θα έχει "ωριμάσει" αρκετά, το όλο σύστημα θα είναι εξαιρετικά σταθερό και ασφαλές. Η επιθυμία μας, βέβαια, να μεταβούμε σε ένα ηλεκτρονικό σύστημα συναλλαγών μέσω του Internet και του World Wide Web δεν είναι αναίτια, αλλά έχει τη βάση της στα οφέλη που αποκομίζουμε: μειωμένο κόστος διεκπεραίωσης, ταχύτητα και ευελιξία, και λιγότερη γραφειοκρατία.

Τέτοια ηλεκτρονικά εμπορικά κέντρα είναι το Amazon, το e-bay.com, open24.gr, shops.gr.

ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΔΙΚΑΙΟ

Η νομική έννοια του διαδικτύου και του κυβερνοχώρου

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

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

Συνήθη εγκλήματα του κυβερνοχώρου

Τα πλέον συνηθισμένα εγκλήματα που παρουσιάζονται αυτή την στιγμή στον κυβερνοχώρο είναι : Οι απάτες (με πιστωτικές κάρτες ή μη), η διακίνηση παιδικής πορνογραφίας, εγκλήματα κατά της Εθνικής Ασφάλειας (οδηγίες για κατασκευή Βομβών, εισβολή σε συστήματα ασφαλείας, που έχουν σχέση με την εθνική υποδομή) , οδηγίες για παρασκευή ναρκωτικών . Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν: σε εγκλήματα κατά των προσωπικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον περιουσιακών αγαθών .

4 Η ασφάλεια στο διαδίκτυο

4.1 Γενικές παρατηρήσεις

Στην καθομιλουμένη γλώσσα ασφάλεια είναι η κατάσταση εκείνη, στην οποία δεν υπάρχει κίνδυνος, όπου αισθάνεται κάποιος ότι, δεν απειλείται. Είναι επίσης η αποτροπή κινδύνου ή απειλής, ή εξασφάλιση σιγουριάς και βεβαιότητας . Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του. Ετσι π.χ. για τον στρατιωτικό η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο απ΄ ότι για τον αστυνομικό, ο οποίος επίσης αντιλαμβάνεται την ίδια έννοια εντελώς διαφορετικά απ΄ ότι ο εργαζόμενος σε οικοδομικές εργασίες κλπ. Αλλά και στον ίδιο ευρύτερο επαγγελματικό κλάδο η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο, ανάλογα με την επιμέρους ενασχόληση του κάθε προσώπου. Ετσι π.χ. για τον στρατιωτικό που ασχολείται με τα όπλα η έννοια της ασφάλειας, δεν ταυτίζεται με αυτή που αντιλαμβάνεται ο ασχολούμενος με τους ηλεκτρονικούς υπολογιστές του ίδιου κλάδου. Ακόμα όμως και στον ίδιο στενώτερο - επιμέρους κλάδο, η οπτική γωνία θεωρήσεως του όρου ασφάλεια είναι εντελώς διαφορετική. Ετσι, π.χ. διαφορετικά αντιλαμβάνεται τον όρο "ασφάλεια" ο τεχνικός ασφαλείας δικτύων υπολογιστικών συστημάτων και διαφορετικά ο τεχνικός ασφάλειας τραπεζικών πληροφοριακών συστημάτων.

Σε κάθε περίπτωση όμως όλοι, όσοι ασχολούνται με θέματα ασφαλείας "συναντώνται" στην κατάσταση εκείνη, όπου δεν υπάρχει κίνδυνος, όπου αισθάνονται ασφαλείς, όπου δεν απειλούνται, όπου πρέπει να αποτρέψουν τον κίνδυνο ή την απειλή και όπου πρέπει να εξασφαλίσουν την σιγουριά και την βεβαιότητα κατά την ενάσκηση του έργου των. Είναι ευνόητον βέβαια ότι, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα, τις επιχειρήσεις, αλλά ακόμα και αυτές τις οργανωμένες πολιτείες .

4.2 Η νομική έννοια της ασφάλειας στον κυβερνοχώρο

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

Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό. Θα έλεγα, χωρίς επιφύλαξη ότι, ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικώς ότι, ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό .

Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Ετσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επόμενα, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την

απάτη την σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέρος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).

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

4.3 Βασικές Αρχές του όρου "ασφάλεια" στο Διαδίκτυο

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

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής, όσο και από νομικής απόψεως. Από τεχνική άποψη διότι, κάθε τεχνικός τρόπος που αποβλέπει στην ασφάλεια του διαδικτύου, μπορεί να εξουδετερωθεί και συνήθως εξουδετερώνεται) από ένα άλλο τρόπο "αντιασφάλειας". Από νομική άποψη διότι, ο νομοθέτης δεν "προφταίνει" να παρακολουθεί τις τεχνολογκές εξελήξεις και τις κοινωνικές επιπτώσεις και συνέπειες των, ώστε να μπορέσει να τις ρυθμίσει. Με άλλα λόγια οι αλλαγές στην τεχνική δομή του κυβερνοχώρου και κατά συνέπεια στη νομική αντιμετώπισή του, είναι τόσο ραγδαίες, που, εάν το θέμα δεν "σταθεροποιηθεί" κάπου από τεχνολογικής απόψεως, ο νομοθέτης δεν θα καταφέρει να λάβει οποιοδήποτε μέτρο , σε ουσιαστικό ή δικονομικό επίπεδο.

4.4 Η τεχνική διάσταση του όρου ασφάλεια στο διαδίκτυο

Από τεχνική άποψη, ασφάλεια (security) είναι η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημιά. Αυτή επιτυγχάνεται με την πρόληψη της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα . Κλασσικό παράδειγμα ασφαλείας αποτελεί η συναλλαγή (αγοραπωλησία) που γίνεται στο διαδίκτυο με την χρήση πιστωτικής κάρτας. Σ΄ αυτήν την περίπτωση πρέπει να εξασφαλιστεί ότι, δεν είναι δυνατόν να ``συλλάβει`` (υποκλέψει) κάποιος τον αριθμό της πιστωτικής κάρτας ή να τον αντιγράψει από τον διακομιστή, που είναι αποθηκευμένος. Επίσης πρέπει να επαληθευτεί ότι, ο αριθμός της πιστωτικής κάρτας αποστέλλεται πράγματι, από το πρόσωπο, που ισχυρίζεται ότι τον στέλνει.

Η ασφάλεια δηλαδή των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να ικανοποιεί την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων.

Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος .

Ακεραιότητα (integrity) των δεδομένων είναι η ιδιότητά των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή των να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας .

Διαθεσιμότητα (availability) των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος .

4.5 Σχέση ασφάλειας και μυστικότητας στο διαδίκτυο.

Μυστικότητα είναι το δικαίωμα που έχει κάποιος να μην μοιράζεται τις πληροφορίες (π.χ. ηλικία, θρήσκευμα, αριθμούς πιστωτικής κάρτας κλπ) που αφορούν το άτομό του με άλλους. Οι πληροφορίες αυτές είναι καταγεγραμμένες στο διαδίκτυο. Η ασφάλεια και η μυστικότητα στο χώρο του διαδικτύου είναι (ουσιαστικώς) θεωρητικές έννοιες. Στην πράξη, ότι κινείται στον χώρο του διαδικτύου μπορεί να γίνει γνωστό, ουσιαστικώς δηλαδή να υποκλαπεί. Εχει χαρακτηριστικά λεχθεί ότι, ``κανένα κινούμενο ηλεκτρόνιο του πλανήτη δεν μπορεί να τρέφει σοβαρές ελπίδες ότι θα ξεφύγει από τον ιστό της παρακολούθησης ``. Κατά συνέπεια η ασφάλεια και η μυστικότητα του διαδικτύου δεν είναι μόνο νομικές, αλλά και τεχνικές έννοιες . Μπορεί όμως να λεχθεί ότι, η ασφάλεια είναι πρωτίστως τεχνική και δευτερευόντως νομική έννοια, ενώ αντίθετα η μυστικότητα είναι πρωτίστως νομική και δευτερευόντως τεχνική έννοια. Σε κάθε περίπτωση όμως, με την χρήση της τεχνολογίας και ιδιαίτερα του διαδικτύου, η προσωπική ζωή του ατόμου έχει γίνει "διαφανής" .

Συμπερασματικώς, μυστικότητα και η ασφάλεια είναι εντελώς διαφορετικά πράγματα, δεν είναι όμως υπερβολικό να λεχθεί ότι, ασφάλεια και μυστικότητα στο διαδίκτυο αποτελούν τις δυο διαφορετικές όψεις, ενός και του ίδιου νομίσματος.

4.6 Σχέση ασφάλειας και κρυπτογραφίας στο διαδίκτυο

Κρυπτογραφία (cryptography) είναι η χρήση κωδίκων για την μετατροπή δεδομένων, κατά τέτοιο τρόπο, ώστε να μπορούν να διαβαστούν μόνο από συγκεκριμένο παραλήπτη με τη χρήση ενός κλειδιού . Σκοπός της κρυπτογραφίας είναι να αποτραπεί η πρόσβαση στα δεδομένα, σε μη εξουσιοδοτημένα άτομα ιδιαίτερα κατά την διάρκεια μετάδοσής των. Σχετικοί είναι οι όροι " διαχείριση κινδύνων " (risk management) και ανάλυση κινδύνων (risk analysis). Είναι χαρακτηριστικό ότι οι μεγάλες εταιρείες προσλαμβάνουν ειδικώς εκπαιδευμένο προσωπικό (security administration), που καταστρώνει ειδικά σχέδια προστασίας του δικτύου της εταιρείας (system administration).

Μέχρι προσφάτως ο όρος ``κρυπτογραφία`` περιοριζόταν μόνο στον στρατιωτικό και τον διπλωματικό χώρο. Σήμερα όμως που η επικοινωνία με το ηλεκτρονικό ταχυδρομείο (e-mail) έχει αυξηθεί αλματωδώς, η κρυπτογραφία αποτελεί σημαντικό παράγοντα του κυβερνοχώρου. Με την χρήση της κρυπτογραφίας δεν διακινούνται βέβαια μόνον νόμιμα, αλλά και παράνομα δεδομένα στον κυβερνοχώρο, όπως π.χ. ανταλλαγή

πορνογραφικού υλικού, ανταλλαγή παρανόμων μηνυμάτων από οργανωμένους ή μη εγκληματίες κλπ.

Η διαδικασία της κωδικοποίησης των δεδομένων λέγεται κρυπτογράφηση (enscryption). Η κρυπτογράφηση στηρίζεται σε κλειδί (key) που πρέπει να κατέχει τόσο αυτός που στέλνει τα δεδομένα, όσο και αυτός που τα παραλαμβάνει. Αν ο παραλήπτης δεν κατέχει το κλειδί, υπάρχει κίνδυνος να γίνει υποκλοπή του κατά την μεταβίβαση (διαδρομή). Γενικώς η κρυπτογράφηση - αποκρυπτογράφηση γίνεται με την βοήθεια μιας μαθηματικής διαδικασίας.

Η διαδικασία της αποκατάστασης των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή λέγεται αποκρυπτογράφηση.

Είναι ευνόητο ότι, με την χρήση της κρυπτογραφίας αποκρύπτεται, όχι μόνον το περιεχόμενο του παράνομου υλικού που διακινείται, αλλά αποφεύγεται επιπλέον και ο εντοπισμός του δράστη. Βέβαια ο εντοπισμός του δράστη μπορεί να αποφευχθεί και με την λεγομένη ``ανωνυμία στον κυβερνοχώρο``.

Από νομικής απόψεως ενδιαφέρον παρουσιάζει το ερώτημα, εάν είναι σύμφωνα με τις βασικές Αρχές του Δικαίου, η απαγόρευση χρήσεως της κρυπτογραφίας ή ο περιορισμός αυτής σε άτομα ή φορείς (π.χ. κρατικούς), που έχουν ειδική προς τούτο άδεια.

4.7 Σχέση ασφάλειας και δικαιώματος ανωνυμίας στο διαδίκτυο.

Είναι γνωστό ότι κάθε χρήστης του διαδικτύου (Internet) αφήνει στον χώρο την (ηλεκτρονική) ταυτότητά του. Με κατάλληλες όμως τεχνικές παρεμβάσεις μπορεί να έχει κάποιος πρόσβαση στο διαδίκτυο ως ανώνυμος ή ακόμα και με ψευδή στοιχεία που αναφέρονται σε άλλο άτομο. Η παρουσίαση βέβαια με ψευδή στοιχεία μπορεί να γίνει και στο "κοινό" εγκληματικό περιβάλλον. Εκεί όμως ο εντοπισμός του δράστη είναι ευκολότερος. Μπορεί ακόμα ο χρήστης του διαδικτύου να έχει ως στοιχείο ταυτότητος το όνομα "ανώνυμος", οπότε τυπικά φαίνεται ότι έχει όνομα. Η δυνατότητα αυτής της ανωνυμίας στο διαδίκτυο (Internet) διευκολύνει την διάπραξη παρανομιών και κάνει δύσκολο, αν όχι και αδύνατο τον εντοπισμό του δράστη. Επιπλέον η ανωνυμία, σε συνδυασμό με την ανυπαρξία ή την δυσκολία εφαρμογής των νομικών κανόνων, κάνει τους ``ηλεκτρονικούς δράστες`` να αισθάνονται ασφαλείς κατά την διάπραξη των εγκλημάτων των.

Το ερώτημα που προκύπτει στο σημείο αυτό είναι, μήπως σε περίπτωση ψήφισης σχετικού νόμου για το διαδίκτυο, πρέπει να ποινικοποιηθεί η ανώνυμη χρήση του, ή ακόμα και η παρουσία με ψευδή στοιχεία. Κάτι τέτοιο βέβαια επαφίεται στην βούληση του νομοθέτη. Αξίζει όμως να σημειωθεί, σχετικός νόμος που ψηφίστηκε στις Η.Π.Α και τιμωρούσε ποινικά την ανώνυμη χρήση ή την χρήση με ψεύτικο όνομα στο διαδίκτυο , κηρύχθηκε αντισυνταγματικός από τα Δικαστήρια των ΗΠΑ . Και αυτό γιατί, η ανωνυμία δεν χρησιμοποιείται στο διαδίκτυο μόνον από τους παράνομους, αλλά και από όσους θέλουν να αποκρύψουν αυστηρώς προσωπικά των (νόμιμα) στοιχεία .

5 Κίνδυνοι και μέτρα προφύλαξης στο διαδίκτυο

5.2 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:

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.

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).

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.

5.2 Μέτρα ασφάλειας από πλευράς χρηστών

Εκτός από τα μέτρα ασφάλειας που τίθενται σε ισχύ από την ΕΕ, πρέπει και οι ίδιοι οι χρηστές να διαδραματίζουν ένα σημαντικό ρόλο έτσι ώστε οι προσωπικές τους πληροφορίες να μένουν μυστικές.

Προτείνουμε έντονα να παρατηρείτε πάντα τις ακόλουθες άψογες τεχνικές ασφαλείας κάθε φορά που κρίνεται απαραίτητο.

Σβήστε την online σύνοδός σας

Αναβαθμίστε τους browsers σας ώστε να υποστηρίζουν την 128-bit SSL κρυπτογράφηση

Μην αποθηκεύσετε τον CPF αριθμό λογαριασμού σας ή τον προσωπικό SingPass χρησιμοποιώντας τον browser σας

Καθαρίστε την browser cache

Προστατέψτε τον υπολογιστή σας από τους ιούς και τα κακόβουλα προγράμματα

Χρησιμοποιήστε μόνο PCs ή τις συσκευές που εμπιστεύεστε

Εξασφαλίστε αυθεντικότητα του Website

Διατηρήστε την ασφάλεια ηλεκτρονικού ταχυδρομείου

Κρατήστε τον προσωπικό SingPass σας εμπιστευτικό πάντα

Αφαιρέστε τα προσωρινά αρχεία μετά από κάθε συναλλαγή

Μην εκτελείτε τα αρχεία από τις untrusted δισκέτες

Ελέγξτε το ιστορικό της συναλλαγής σας τακτικά

Σβήστε την online σύνοδός σας

Σβήστε την online σύνοδό σας μόλις ολοκληρώσετε την συναλλαγή ή ακόμα και αν πρέπει να αφήσετε το PC σας για λίγο. Μπορείτε επίσης να ενεργοποιήσετε τον κωδικό πρόσβασης-προστατευμένο screen saver σας για να αποτρέψετε την αναρμόδια πρόσβαση στο PC σας εάν πρέπει να φύγετε έστω και για λίγο.

Αναβαθμίστε τους browsers σας ώστε να υποστηρίζουν την 128-bit SSL κρυπτογράφηση

Για να απολαύσετε το πιο υψηλό διαθέσιμο επίπεδο ασφάλειας, πρέπει να αναβαθμίσετε τα προγράμματά σας, browsers και εφαρμογών για να υποστηρίζουν την 128-bit SSL κρυπτογράφηση ή τα υψηλότερα πρότυπα κρυπτογράφησης.

Μην αποθηκεύσετε τον CPF αριθμό λογαριασμού σας ή τον προσωπικό SingPass χρησιμοποιώντας τον browser σας

Αποφύγετε να αποθηκεύσετε τον CPF αριθμό λογαριασμού σας ή τον προσωπικό SingPass χρησιμοποιώντας την λειτουργία "Autocomplete" του browser σας. Αυτό είναι επειδή μερικοί browsers αποθηκεύουν και δείχνουν τις πιθανές αντιστοιχίες από τις προηγούμενες καταχωρήσεις σας.

Καθαρίστε την browser cache

Τα αρχεία cache είναι προσωρινά αρχεία που αποθηκεύονται στον υπολογιστή σας. Θυμηθείτε να καθαρίσετε την κρύπτη του browser μετά από κάθε χρησιμοποίηση του Internet, με την ακολουθία αυτών των απλών οδηγιών:

Πλοηγός 4.X Netscape

Επιλέξτε "Edit" από το μενού επιλογών

Επιλέξτε "Preferences”

Κάντε click στην επιλογή "Advanced" και στη συνέχεια επιλέξτε "Cache"

Επιλέξτε την "CLEAR DISK CACHE" που ακολουθείται από "OK"

Επιλέξτε "OK" για να βγείτε από το μενού

Internet Explorer 4.X / 5.X

Επιλέξτε "View" από το μενού επιλογών(για IE. 4.X)

Επιλέξτε "Tools" από το μενού επιλογών (για IE 5.X)

Επιλέξτε τις "Internet Options "

Επιλέξτε τη "General" ετικέττα

Επιλέξτε την "Delete files" στο πλαίσιο των προσωρινών αρχείων Internet και κάντε click στο "OK"

Επιλέξτε "OK" για να βγείτε από μενού

Προστατέψτε τον υπολογιστή σας από τους ιούς και τα κακόβουλα προγράμματα

Πρέπει να πάρετε την απαραίτητη προφύλαξη για να προστατεύσετε τον υπολογιστή σας από τους ιούς/τα κακόβουλα προγράμματα (π.χ. τρωικά άλογα) που μπορούν να καταστρέψουν τα κρίσιμα στοιχεία. Αυτά τα προγράμματα μπορούν επίσης να κλέψουν τους κωδικούς πρόσβασης και τις προσωπικές πληροφορίες σας χωρίς την άδεια σας.

Για να αποφευχθεί η μόλυνση από ιούς, σας συμβουλεύουμε:

Να εξοπλίσετε τον υπολογιστή σας με το πιο πρόσφατο λογισμικό ανίχνευσης ιών και το προσωπικό σας firewall,τα οποία προστατεύουν από τις επιθέσεις ιών, τους χάκερ και τα κακόβουλα προγράμματα. Αυτά πρέπει να αναβαθμίζονται τακτικά.

Αποφύγετε την χρήση λογισμικών από μη αξιόπιστα websites

Διαγράψτε τα άχρηστα e-mails

Αποφύγετε τα προγράμματα που επιτρέπουν την αυτόματη πρόσβαση σε αρχεία

Χρησιμοποιήστε μόνο PCs ή τις συσκευές που εμπιστεύεστε

Αποφύγετε την εκτέλεση των online συναλλαγών σας σε κοινό/δημόσιο PC ή συσκευές. Και αυτό γιατί μπορεί κάποιος να έχει keystokes εφαρμογή που μπορεί να καταγράψει τον κωδικό χρήστη και τους κωδικούς πρόσβασης. Εάν πρέπει πραγματικά να κάνετε αυτό, εξασφαλίστε ότι το PC είναι απαλλαγμένο από τους ιούς και ότι η κρύπτη του browser έχει καθαριστεί πριν από τη χρήση.

Εξασφαλίστε την αυθεντικότητα του Website

Ελέγξτε το URL και το όνομα της επιτροπής στο ψηφιακό πιστοποιητικό πριν εισάγετε τον CPF αριθμό λογαριασμού και το προσωπικό SingPass. Αυτό πρόκειται να εξασφαλίσει ότι ο Website που επισκέπτεστε ανήκει στην επιτροπή.

Διατηρήστε την ασφάλεια ηλεκτρονικού ταχυδρομείου

Διαγράψτε τα άχρηστα e-mails. Αποφύγετε μια σύνδεση εάν προέρχεται από μια άγνωστη/ύποπτη πηγή. Διαγράψτε τα αρχεία πριν καν τα διαβάσετε.

Κρατήστε τον προσωπικό SingPass σας εμπιστευτικό πάντα

Το προσωπικό SingPass σας χρησιμεύει ως ένα σημαντικό κλειδί για να καθιερώσει την ταυτότητά σας στο online περιβάλλον. Είναι επομένως απαραίτητο να προστατεύετε και να ασφαλίζετε τον κωδικό πρόσβασής σας χρησιμοποιώντας τις ακόλουθες συμβουλές:

Εξασφαλίστε ότι κανένας μπορεί να δει τον λογαριασμό σας ή το SingPass σας όταν είναι συνδεδεμένος στο σύστημα

Κρατήστε το SingPass σας εμπιστευτικό πάντα. Μην τον αποκαλύψετε σε κανέναν

Μην επιλέξτε έναν κωδικό πρόσβασης που είναι εύκολο να ανακαλυφθεί, όπως το τηλέφωνό σας, τα αρχικά σας ,τον αριθμό ταυτότητας, την ημερομηνία γέννησης κλπ. Πρέπει να επιλέγει ένα ισχυρό και μοναδικό SingPass. (Σημείωση:Το SingPass αποτελείται από ένα ελάχιστο 8 και ένα μέγιστο 24 χαρακτήρων. Μπορεί να είναι όλα άλφα, όλοι αριθμητικοί ή ένας συνδυασμός αλφαριθμητικών.)

Αποφύγετε τον ίδιους χαρακτήρες / ψηφία δύο φορές (π.χ. 12234567), διαδοχικοί αριθμοί (π.χ. 12345678) ή την επαναχρησιμοποίηση ενός κωδικού πρόσβασης

Αλλάζετε το SingPass σας τακτικά. (π.χ. κάθε 90 ημέρες)

Θυμηθείτε το SingPass σας. Μην τον αποθηκεύστε στο σκληρό δίσκο PC, σε δισκέτα, σε κομμάτια χαρτί ή οποιαδήποτε άλλα επισφαλή μέσα.

Εξασφαλίστε ότι το URL προηγείται από "τα https" κατά την εκτέλεση των online συναλλαγών σας.
Netscape: Μια εικόνα που μοιάζει με κλειδαριά / κλειδί μπορεί να βρεθεί στον browser.
Internet Explorer: Κάντε click στην σελίδα και επιλέξτε “Properties" για να ελέγξετε ότι η σύνοδός σας είναι ασφαλής.

Αφαιρέστε τα προσωρινά αρχεία μετά από κάθε συναλλαγή

Αυτό θα βοηθούσε να αποτρέψει τον λογαριασμό σας από την ξένη εισβολή ειδικά εάν έχετε πρόσβαση από κοινό / δημόσιο PC. Τα προσωρινά αρχεία Internet σώζονται συνήθως στο C:\WINDOWS\Temporary Internet Files.

Μην εκτελείτε τα αρχεία από τις untrusted δισκέτες

Πάντα ανιχνεύστε τις δισκέτες πριν εκτελέσετε τα αρχεία. Μπορούν να περιέχουν τους κακόβουλους κώδικες ή τους ιούς.

Ελέγξτε το ιστορικό συναλλαγής σας τακτικά

Αυτό πρόκειται να εξασφαλίσει ότι δεν υπάρχει καμία αναρμόδια συναλλαγή

6 Ασφάλεια Εφαρμογών Ηλεκτρονικού Εμπορίου

Οι εφαρμογές ηλεκτρονικού εμπορίου αποτελούν αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων και της πλαστοπροσωπίας. Τα προβλήματα αυτά αντιμετωπίζονται με τη χρήση κρυπτογραφίας, η οποία επιτρέπει τη μετάδοση εμπιστευτικών πληροφοριών μέσα από ένα δίκτυο χωρίς να υπάρχει κίνδυνος υποκλοπής ή ανεπιθύμητων παρεμβάσεων. Παράλληλα επιτρέπει στις δύο πλευρές που επικοινωνούν, δηλαδή στον έμπορα και στον πελάτη, να προβαίνουν σε αμοιβαία πιστοποίηση ταυτότητας.

Στην πράξη, οι κρυπτογραφικές αρχές πρέπει να ενσωματωθούν σε εργάσιμα πρωτόκολλα επικοινωνίας και λογισμικό. Υπάρχει μια ποικιλία κρυπτογραφικών πρωτοκόλλων στο διαδίκτυο, καθένα από τα οποία είναι ειδικευμένο για διαφορετική λειτουργία. Το πρωτόκολλο SSL (Secure Sockets Layer), το οποίο παρέχει κρυπτογραφημένη επικοινωνία μεταξύ ενός προγράμματος πλοήγησης (web browser) και ενός εξυπηρετητή web (web server), αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο. Το πρωτόκολλο SSL παρέχει απόρρητη επικοινωνία μεταξύ πελατών και εμπόρων, υποστηρίζοντας πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών, προσφέροντας έτσι ένα ικανοποιητικό επίπεδο ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου.

Για να υπάρχει όμως ασφάλεια στις εφαρμογές ηλεκτρονικού εμπορίου απαιτείται η ύπαρξη ενός ασφαλούς εξυπηρετητή διαδικτύου (web server). Ο εξυπηρετητής διαδικτύου πρέπει να προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης του πελάτη στον εξυπηρετητή του καταστήματος. Οι εξυπηρετητές διαδικτύου διαχειρίζονται και διανέμουν τις πληροφορίες στο διαδίκτυο.

6.1 Πρωτόκολλο Ασφάλειας SSL

Το SSL (Secure Socket Layer) είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκόσμιου Ιστού, το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server). Δηλαδή το πρωτόκολλο αυτό μπορεί να παρέχει απόρρητη επικοινωνία μεταξύ εμπόρου και πελάτη σε μια συναλλαγή πληρωμής και για το λόγο αυτό το SSL αποτελεί το κύριο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο. Συγκεκριμένα, το πρωτόκολλο SSL παρέχει κρυπτογράφηση της μεταδιδόμενης πληροφορίας (data encryption), υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρετητή (server authentication) και προαιρετική πιστοποίηση της ταυτότητας του πελάτη (client authentication) μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Επιπλέον εξασφαλίζει την ακεραιότητα των δεδομένων (data integrity), εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Για κάθε κρυπτογραφημένη συναλλαγή δημιουργείται ένα κλειδί συνόδου (session key) το μήκος του

οποίου μπορεί να είναι 40 bits ή 128 bits. Είναι γνωστό ότι όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο ασφαλής είναι η κρυπτογραφημένη επικοινωνία.

Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Έχουν υπάρξει τρεις εκδόσεις του SSL. Η ιστορία της εξέλιξης του SSL έχει ως εξής:

Ιούλιος 1994: Κυκλοφόρησε η πρώτη έκδοση v.1.0 του πρωτοκόλλου SSL από τη Netscape, η οποία χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της εταιρείας.

Δεκέμβριος 1994: Κυκλοφόρησε η δεύτερη έκδοση v.2.0 του πρωτοκόλλου, η οποία ενσωματώθηκε στο web browser της Netscape, τον Netscape Navigator.

Ιούλιος 1995: Εκδόθηκε ο αντίστοιχος web browser της Microsoft, ο Internet Explorer, ο οποίος υποστηρίζει και αυτός την έκδοση v.2.0 του SSL, με κάποιες όμως επεκτάσεις της Microsoft.

Το SSL πρωτόκολλο, στην έκδοση v.2.0, καθιερώθηκε ως de facto πρότυπο για κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων. Το HTTP (Hyper Text Transfer Protocol) είναι ένα πρωτόκολλο που φροντίζει τη μεταφορά και τον τρόπο μετάδοσης δεδομένων στο διαδίκτυο. Ωστόσο το SSL v.2.0 είχε αρκετούς περιορισμούς τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητα του. Για το λόγο αυτό υπήρχε η ανάγκη για βελτίωση της έκδοσης v.2.0. Έτσι το πρωτόκολλο αναβαθμίστηκε σε SSL v.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία.

Νοέμβριος 1995: Κυκλοφόρησε επισήμως η έκδοση v.3.0 του SSL, ενώ λίγους μήνες πιο πριν εφαρμοζόταν σε προϊόντα της εταιρείας, όπως τον Netscape Navigator.

Μάιος 1996: Το SSL περνά στη δικαιοδοσία του Internet Engineering Task Force - IETF, ο οποίος δημιουργεί την ειδική ομάδα εργασίας TLS group και μετονομάζει την νέα έκδοση του SSL, σε TLS (Transport Layer Security).

Η ομάδα εργασίας TLS group καθιερώθηκε το 1996 για να τυποποιήσει το πρωτόκολλο Transport Layer Security. Η TLS group εργάστηκε πάνω SSL v.3.0 πρωτόκολλο. Η ομάδα αυτή έχει ολοκληρώσει μια σειρά από προδιαγραφές που περιγράφουν τις εκδόσεις 1.0 και 1.1 του TLS πρωτοκόλλου, και ετοιμάζει την έκδοση 1.2.

Ιανουάριος 1999: Εκδίδεται η πρώτη έκδοση του πρωτοκόλλου TLS, η οποία μπορεί να θεωρείται και ως η έκδοση v.3.1 του SSL.

Δεκέμβριος 2005: Δημοσιεύεται η έκδοση 1.1 του TLS πρωτοκόλλου από την TLS group.

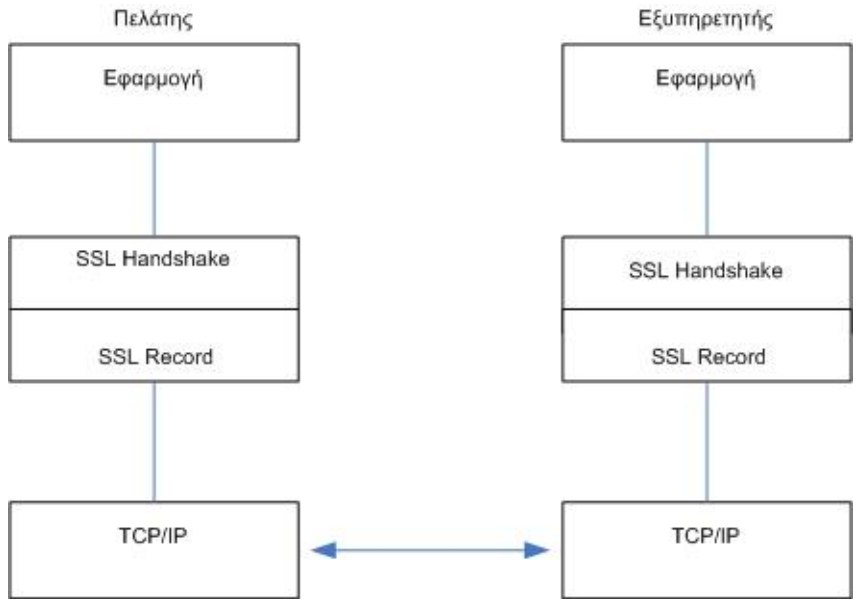
Η τρίτη έκδοση του πρωτοκόλλου SSL κάλυψε πολλές αδυναμίες της δεύτερης έκδοσης. Οι σημαντικότερες αλλαγές αφορούν: α) στη μείωση των απαραίτητων μηνυμάτων κατά το στάδιο εγκαθίδρυσης της σύνδεσης («χειραψία», «handshake»), β) στην επιλογή των αλγορίθμων συμπίεσης και κρυπτογράφησης από τον εξυπηρετητή και γ) στην εκ νέου διαπραγμάτευση του κυρίως κλειδιού (master-key) και του «αναγνωριστικού» συνόδου (session-id). Ακόμη αυξάνονται οι διαθέσιμοι αλγόριθμοι κρυπτογράφησης και προστίθενται νέες τεχνικές για τη διαχείριση των κλειδιών. Γενικά, η τρίτη έκδοση του SSL (v.3.0) είναι πιο ολοκληρωμένη σχεδιαστικά από τη δεύτερη, με μεγαλύτερο εύρος υποστήριξης και λιγότερες ατέλειες.

Επειδή η Netscape επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου SSL, γεγονός που ερχόταν σε σύγκρουση με την τότε νομοθεσία των Η.Π.Α περί εξαγωγής

κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει τη χρήση αλγορίθμων κρυπτογράφησης με κλειδί των 40 bits στις προς εξαγωγή εφαρμογές SSL, τη στιγμή που η κανονική έκδοση χρησιμοποιεί κλειδί των 128 bits. Γενικές πληροφορίες για την κρυπτογραφία και τους αλγόριθμους κρυπτογράφησης υπάρχουν στο Παράρτημα.

6.1.1 Αρχιτεκτονική του SSL

Η αρχιτεκτονική τοποθέτηση του SSL απεικονίζεται στο Σχήμα.



Σχήμα 6-1 : Αρχιτεκτονική Τοποθέτηση του SSL

Το SSL μπορεί να λειτουργήσει πάνω από οποιοδήποτε πρωτόκολλο μεταφοράς. Δεν εξαρτάται από την ύπαρξη του TCP/IP και υποστηρίζει πρωτόκολλα εφαρμογών όπως τα HTTP, FTP και TELNET. Το TCP/IP (Transmission Control Protocol/Internet Protocol) είναι το πρωτόκολλο επικοινωνίας (communication protocol) για την επικοινωνία ανάμεσα σε υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο. Τα αρχικά TCP/IP αναφέρονται σε δύο από τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο, δηλ. στο TCP και στο IP. Το FTP (File Transfer Protocol) είναι ένα πρωτόκολλο μεταφοράς αρχείων, το οποίο φροντίζει για τη διακίνηση αρχείων μέσα στο διαδίκτυο, και το TELNET είναι ουσιαστικά μια υπηρεσία του διαδικτύου με την οποία οι χρήστες αποκτούν απευθείας πρόσβαση σε άλλους υπολογιστές στο διαδίκτυο.

Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο διασύνδεσης ανοικτών συστημάτων (Open System Interconnection, OSI), έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του OSI και όχι ως πρωτόκολλο αντικατάστασης. Επιπλέον η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το SSL. Το S/HTTP (Secure HTTP) πρωτόκολλο φροντίζει για την ασφαλή μεταφορά δεδομένων στο διαδίκτυο.

Ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς σε οποιαδήποτε TCP/IP εφαρμογή στρωματοποιείτε στην κορυφή του.

Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:

Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.

Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.

Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs.

Για τη γενική λειτουργία του πρωτοκόλλου SSL υπάρχουν δύο βασικές οντότητες: σύνοδος SSL και σύνδεση SSL.

Η σύνοδος SSL αποτελεί τη δημιουργία μιας σχέσης μεταξύ ενός πελάτη και ενός εξυπηρετητή. Οι σύνοδοι δημιουργούνται από το SSL Handshake protocol και είναι ομάδες παραμέτρων ασφάλειας, οι οποίες μπορούν να διαμοιραστούν ταυτόχρονα σε πολλές συνδέσεις. Ο κύριος λόγος για αυτό είναι η αποφυγή χρονοβόρων διαπραγματεύσεων νέων παραμέτρων ασφάλειας για κάθε νέα σύνδεση.

Οι παράμετροι που περιέχονται και μοιράζονται σε μια σύνοδο είναι οι ακόλουθοι:

Αναγνωριστικό συνόδου: επιλέγεται από τον εξυπηρετητή για αναγνώριση μιας ενεργούς ή επαναληπτικής κατάστασης συνόδου.

Ψηφιακό πιστοποιητικό (μεταξύ ομότιμων οντοτήτων).

Μέθοδος συμπίεσης των δεδομένων: Αλγόριθμος που χρησιμοποιείται για συμπίεση δεδομένων πριν την κρυπτογράφηση.

Αλγόριθμος κρυπτογράφησης των δεδομένων.

Κύριο μυστικό (master secret): Μοναδικός αριθμός μήκους 48-byte, κοινό μυστικό μεταξύ εξυπηρετητή και πελάτη.

Δυνατότητα επανεκκίνησης της συνόδου.

Σύνδεση SSL είναι η μεταφορά των πληροφοριών μεταξύ δύο οντοτήτων. Στο SSL οι συνδέσεις αυτές είναι σχέσεις μεταξύ ομότιμων οντοτήτων και είναι παροδικές.

Οι παράμετροι που περιέχονται σε μια σύνδεση είναι οι ακόλουθοι:

Τυχαίοι αριθμοί μεταξύ πελάτη και εξυπηρετητή, οι οποίοι είναι διαφορετικοί για κάθε σύνδεση.

Μυστικό MAC εξυπηρετητή: Μυστικό που χρησιμοποιείται για MAC λειτουργίες σε δεδομένα εγγεγραμμένα από τον εξυπηρετητή.

Μυστικό MAC πελάτη: Μυστικό που χρησιμοποιείται για MAC λειτουργίες σε δεδομένα εγγεγραμμένα από τον πελάτη.

Κλειδί που χρησιμοποιείται για κρυπτογράφηση δεδομένων στον εξυπηρετητή και αποκρυπτογράφηση από τον πελάτη.

Κλειδί που χρησιμοποιείται για κρυπτογράφηση δεδομένων στον πελάτη και αποκρυπτογράφηση από τον εξυπηρετητή.

Διανύσματα αρχικοποίησης της σύνδεσης

Αριθμοί ακολουθίας: Κάθε μέλος (εξυπηρετητής, πελάτης) διατηρεί ξεχωριστούς αριθμούς ακολουθίας για αποστολή και λήψη μηνυμάτων σε κάθε σύνδεση.

Όπως απεικονίζεται στο Σχήμα 6-1, το πρωτόκολλο SSL αποτελείται από δύο επιμέρους πρωτόκολλα, το SSL record protocol και το SSL handshake protocol. Το SSL record protocol παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Συγκεκριμένα το πρωτόκολλο αυτό τοποθετεί τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει. Επίσης εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Το SSL handshake protocol είναι ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών το οποίο επίσης διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφάλειας. Συγκεκριμένα το πρωτόκολλο αυτό διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του εξυπηρετητή και του πελάτη αν αυτό ζητηθεί. Μετά την ολοκλήρωση του SSL handshake protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας.

6.1.2 Το SSL στο Ηλεκτρονικό Εμπόριο

Το πρωτόκολλο SSL μπορεί να χρησιμοποιείται για την εγκαθίδρυση ασφαλών συνδέσεων μεταξύ εξυπηρετουμένων (πελάτης) και εξυπηρετητών (έμπορας). Συγκεκριμένα μπορεί να χρησιμοποιείται για να αυθεντικοποιεί έναν εξυπηρετητή και προαιρετικά τον εξυπηρετούμενο, να εκτελεί ανταλλαγή κλειδιών και να παρέχει αυθεντικοποίηση και ακεραιότητα μηνυμάτων σε εφαρμογές ηλεκτρονικού εμπορίου και γενικά σε εφαρμογές διαδικτύου. Για τους λόγους αυτούς το πρωτόκολλο SSL αποτελεί σήμερα το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο.

Η μη διασφάλιση αυθεντικοποίησης εξυπηρετούμενου βοήθησε το πρωτόκολλο SSL να διαδοθεί σε περιβάλλοντα ηλεκτρονικού εμπορίου. Η υποστήριξη της αυθεντικοποίησης εξυπηρετούμενου απαιτεί ξεχωριστά δημόσια κλειδιά και πιστοποιητικά για κάθε εξυπηρετούμενο. Είναι λοιπόν φανερό ότι η αυθεντικοποίηση κάθε πελάτη στο ηλεκτρονικό εμπόριο είναι πρακτικά αδύνατη. Επίσης είναι πιο σημαντικό οι τελικοί καταναλωτές να μπορούν να ενημερώνονται σχετικά με την ταυτότητα των εμπόρων με τους οποίους συναλλάσσονται, παρά να απαιτείται ίδιος βαθμός ασφάλειας και από τους εμπόρους για τους καταναλωτές. Επιπλέον αφού ο αριθμός των εμπόρων-εξυπηρετητών διαδικτύου είναι πολύ μικρότερος από τον αριθμό των καταναλωτών-χρηστών, είναι ευκολότερο και πιο πρακτικό να εφοδιάζονται οι εξυπηρετητές με τα απαραίτητα δημόσια κλειδιά και πιστοποιητικά.

Σήμερα το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας για Διαδίκτυο γενικά και το ηλεκτρονικό εμπόριο συγκεκριμένα. Αξίζει να σημειωθεί ότι αν όχι όλες, οι περισσότερες τράπεζες που προσφέρουν τις υπηρεσίες τους διαμέσου του

διαδικτύου έχουν αναπτύξει την ασφάλεια των εφαρμογών ηλεκτρονικής τραπεζικής με βάση το πρωτόκολλο SSL.

Το πρωτόκολλο SSL χρησιμοποιείται συνήθως σε HTTP προϊόντα εξυπηρετητών και εξυπηρετούμενων. Για παράδειγμα, υπάρχουν αρκετοί HTTP εξυπηρετητές διαθέσιμοι οι οποίοι υποστηρίζουν το SSL. Από την πλευρά του εξυπηρετούμενου, σήμερα, οι περισσότεροι browsers ιστού υποστηρίζουν το SSL. Τα περισσότερα από αυτά τα προϊόντα υποστηρίζουν τον αλγόριθμο RC4 για κρυπτογράφηση και τα MD2 και MD5 για σύνοψη.

Μειονέκτημα της χρήσης του SSL αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του browser του εξυπηρετούμενου με τον HTTPS εξυπηρετητή. Η καθυστέρηση οφείλεται στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίηση της SSL συνόδου. Πρακτικά οι χρήστες αντιλαμβάνονται λίγα δευτερόλεπτα καθυστέρηση μεταξύ της έναρξης σύνδεσης με τον HTTPS εξυπηρετητή και της ανάκτησης της πρώτης HTML σελίδας από αυτόν.

7 Το Πρότυπο ISO 17799

Η ασφάλεια των πληροφοριών και των δεδομένων είναι ένα από τα σημαντικότερα ζητήματα που αντιμετωπίζει το ηλεκτρονικό εμπόριο. Κάθε επιχείρηση που δραστηριοποιείται στο ηλεκτρονικό εμπόριο καλό είναι να πιστοποιείται κατά πρότυπο ISO 17799 καταδεικνύοντας έτσι, τόσο στους πελάτες, όσο και στους συνεργάτες της, το υψηλό επίπεδο ασφάλειας των πληροφοριών της.

Το πρότυπο 17799 ISO/IEC (the International Organizational for Standardization / the International Electrotechnical Commission), προετοιμάστηκε από το British Standards Institution (BS 7799) και υιοθετήθηκε από την Joint Technical Committee JTC 1 "Information Technology".

Το πρότυπο αυτό (ISO 17799) παρέχει γενικές κατευθύνσεις για τη διαχείριση της ασφάλειας πληροφοριών (information security management) και απευθύνεται στους υπεύθυνους της ασφάλειας σε έναν οργανισμό. Περιγράφει την αποτελεσματική διαχείριση της ασφάλειας πληροφοριών και τη δημιουργία εμπιστοσύνης κατά τις συναλλαγές ανάμεσα σε οργανισμούς. Οι προτάσεις του προτύπου αυτού πρέπει να επιλεγούν και να χρησιμοποιηθούν σύμφωνα με τη σχετική νομοθεσία.

Το ISO 17799 δημοσιεύθηκε αρχικά το Δεκέμβριο του 2000, και έκτοτε εφαρμόζεται από εταιρείες που αποσκοπούν στην εγκατάσταση ή βελτίωση κανόνων ασφάλειας δεδομένων και πληροφοριών. Το ISO 17799 εξελίσσεται ταχύτατα στο de facto πρότυπο ασφάλειας πληροφοριών σε όλο τον κόσμο. Μεγάλες πολυεθνικές, όπως η Citibank, η KPMG, η Sony και η Unisys, έχουν πιστοποιηθεί κατά το πρότυπο αυτό. Αλλά και στην Ελλάδα δεν είναι λίγοι εκείνοι που έχουν ήδη πιστοποιηθεί με το ISO 17799. Εταιρείες όπως ο ΟΠΑΠ ΑΕ, και η INTRAKOM είναι μερικές από αυτές.

Το ISO 17799 έχει εφαρμογή σε όλους τους τομείς της βιομηχανίας, του εμπορίου και των υπηρεσιών. Έχει ιδιαίτερη σημασία στις επιχειρήσεις που δραστηριοποιούνται στο χώρο του ηλεκτρονικού εμπορίου. Η ασφάλεια των δεδομένων σε μια τέτοια επιχείρηση είναι ζωτικής σημασίας, αφού πιθανή απώλεια κάποιων δεδομένων μπορεί να επιφέρει ανυπολόγιστη ζημιά στην φήμη της επιχείρησης. Οπότε, αν μια επιχείρηση στο χώρο του ηλεκτρονικού εμπορίου θέλει να προστατεύει τα δεδομένα, τόσο τα δικά της όσο και των πελατών της, και επιπλέον να είναι ανταγωνιστική, θα πρέπει να πιστοποιείται από το εν λόγω πρότυπο. Η πιστοποίηση μιας τέτοιας εταιρείας από το πρότυπο αυτό, της προσφέρει τα εξής πλεονεκτήματα:

Με την προστασία των πληροφοριών από μια ευρεία σειρά απειλών εξασφαλίζεται η επιχειρησιακή συνέχεια και ελαχιστοποιούνται οι επιχειρησιακές απώλειες.

Εκτός από την προστασία των ζωτικής σημασίας πληροφοριών της, καταδεικνύει και τη συμμόρφωση της με τα διεθνή πρότυπα ασφάλειας.

Ενδυναμώνει την εμπιστοσύνη των πελατών που εμπιστεύονται σημαντικές πληροφορίες σε αυτήν (π.χ. προσωπικά στοιχεία, αριθμούς πιστωτικών καρτών, κλπ.).

Ενισχύει το ανταγωνιστικό πλεονέκτημα της επιχείρησης με τη δημιουργία εμπιστοσύνης, τόσο εξωτερικά (αγορά) όσο και εσωτερικά (προσωπικό).

7.1 Ασφάλεια Πληροφοριών

Η πληροφορία είναι ένα αγαθό, το οποίο, όπως όλα τα υπόλοιπα σημαντικά αγαθά έχει αξία για έναν οργανισμό και επομένως πρέπει να προστατεύεται κατάλληλα.

Η πληροφορία μπορεί να εμφανιστεί υπό διάφορες μορφές. Μπορεί να γραφεί σε χαρτί, να αποθηκευτεί ηλεκτρονικά, να μεταδοθεί με φυσικά (π.χ. ταχυδρομείο) ή ηλεκτρονικά μέσα, ή να αναφερθεί σε κάποια συζήτηση. Ανεξάρτητα από τη μορφή της, η πληροφορία πρέπει πάντοτε να προστατεύεται. Η ασφάλεια των πληροφοριών χαρακτηρίζεται ως η διαφύλαξη των ακόλουθων ιδιοτήτων:

Εμπιστευτικότητα (confidentiality): Εξασφάλιση ότι η πληροφορία είναι προσβάσιμη μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι.

Ακεραιότητα (integrity): Προστασία της ακρίβειας και πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας της.

Διαθεσιμότητα (availability): Εξασφάλιση ότι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στην πληροφορία όποτε απαιτείται.

Η ασφάλεια πληροφοριών επιτυγχάνεται με την υλοποίηση των κατάλληλων μηχανισμών ελέγχου, οι οποίοι μπορεί να είναι πολιτικές, πρακτικές, διαδικασίες, οργανωτικές δομές και λειτουργίες λογισμικού.

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών είναι ιδιαίτερα σημαντικά για τη διατήρηση ανταγωνιστικού πλεονεκτήματος, τη συμμόρφωση με τους νόμους, την εταιρική εικόνα και τα κέρδη μιας επιχείρησης που δραστηριοποιείται στο χώρου του ηλεκτρονικού εμπορίου.

Οι οργανισμοί και τα πληροφοριακά τους συστήματα και δίκτυα συνεχώς αντιμετωπίζουν απειλές στην ασφάλεια τους από ένα μεγάλο εύρος διαφορετικών πηγών, όπως ηλεκτρονική απάτη, βιομηχανική κατασκοπεία, βανδαλισμός, φυσικά φαινόμενα. Επιπλέον επιθέσεις με ιούς (computer viruses), hacking και επιθέσεις τύπου άρνησης παροχής υπηρεσιών έχουν γίνει πλέον συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπιση τους. Καθώς οι επιχειρήσεις εξαρτώνται από τα πληροφοριακά τους συστήματα, οι απειλές προς αυτά επηρεάζουν σημαντικά τις λειτουργίες των ίδιων των επιχειρήσεων.

Στην αρχική σχεδίαση πολλών πληροφοριακών συστημάτων δεν έχουν συμπεριληφθεί χαρακτηριστικά ασφάλειας. Η ασφάλεια που προσφέρουν είναι περιορισμένη και πρέπει να συμπληρωθεί από κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών. Η επιλογή των κατάλληλων μηχανισμών ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό.

7.1.1 Απαιτήσεις Ασφάλειας

Είναι σημαντικό ένας οργανισμός να προσδιορίσει τις πραγματικές απαιτήσεις του σε θέματα ασφάλειας. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτό:

Η αποτίμηση των κινδύνων που αντιμετωπίζει ο οργανισμός. Έτσι αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του συστήματος, εκτιμάται η ευπάθεια του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησης τους και το κόστος που θα έχουν για τον οργανισμό.

Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

Το σύνολο των αρχών, των απαιτήσεων και των στόχων για την επεξεργασία των πληροφοριών, που ορίζει ο ίδιος ο οργανισμός.

7.1.2 Κίνδυνοι Ασφάλειας

Οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν ύστερα από μεθοδική καταγραφή των κινδύνων που αντιμετωπίζει ο οργανισμός. Το κόστος των μηχανισμών ασφάλειας θα πρέπει να δικαιολογείται από την πιθανή ζημιά στον οργανισμό σε περίπτωση που παραβιαστεί η ασφάλεια του.

Η αποτίμηση των κινδύνων ασφάλειας είναι μια συστηματική εξέταση των ακόλουθων παραγόντων:

Της πιθανής ζημιάς που θα υποστεί ο οργανισμός σε περίπτωση που προκύψει κάποιος κίνδυνος ασφάλειας, συμπεριλαμβανομένων των συνεπειών από την απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των πληροφοριών.

Της ρεαλιστικής εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφάλειας σε σχέση με τους υπάρχοντες μηχανισμούς ελέγχου.

Τα αποτελέσματα αυτής της αποτίμησης καθορίζουν τις κατάλληλες ενέργειες και προτεραιότητες του οργανισμού, καθώς και τους τρόπους υλοποίησης των μηχανισμών ελέγχου της ασφάλειας απέναντι σε αυτούς τους κινδύνους. Η διαδικασία αποτίμησης των κινδύνων και η επιλογή των κατάλληλων μηχανισμών ελέγχου μπορεί να επαναληφθεί πολλές φορές προκειμένου να καλύψει διαφορετικά τμήματα του οργανισμού.

Είναι σημαντικό να γίνεται περιοδικός έλεγχος των κινδύνων ασφάλειας όπως και των μηχανισμών προστασίας προκειμένου να επιτυγχάνεται προσαρμογή στις ανάγκες και τις προτεραιότητες του οργανισμού, επέκταση στην προστασία από νέους κινδύνους, καθώς και επιβεβαίωση της ορθής και αποτελεσματικής λειτουργίας των υπαρχόντων μηχανισμών προστασίας.

7.1.3 Μηχανισμοί Ασφάλειας

Αφού καθοριστούν οι απαιτήσεις ασφάλειας, μπορεί να γίνει η επιλογή των κατάλληλων μηχανισμών ελέγχου και προστασίας, οι οποίοι θα μειώσουν τον κίνδυνο σε αποδεκτά επίπεδα. Οι μηχανισμοί αυτοί μπορούν να επιλεγούν από οποιοδήποτε σύνολο είναι κατάλληλο για τον οργανισμό.

Οι μηχανισμοί θα πρέπει να επιλεγούν με βάση το κόστος υλοποίησης τους σε σχέση με τους κινδύνους που θα αντιμετωπίζουν καθώς και το κόστος των πιθανών επιπτώσεων των κινδύνων αυτών στον οργανισμό. Ποιοτικοί παράγοντες, όπως απώλεια φήμης του οργανισμού θα πρέπει να λαμβάνονται υπόψη.

Ένας αριθμός μηχανισμών ελέγχου και προστασίας θεωρούνται θεμελιώδεις και αποτελούν τη βάση για την ασφάλεια πληροφοριών. Οι μηχανισμοί αυτοί βασίζονται είτε σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική στην ασφάλεια.

Μηχανισμοί βασισμένοι στη νομοθεσία:

Προστασία προσωπικών δεδομένων.

Προστασία δεδομένων του οργανισμού.

Δικαιώματα πνευματικής ιδιοκτησίας.

Μηχανισμοί που έχουν καθιερωθεί ως κοινή πρακτική:

Πολιτική ασφάλειας πληροφοριών.

Καταμερισμός καθηκόντων που σχετίζονται με την ασφάλεια.

Εκπαίδευση και κατάρτιση σε θέματα ασφάλειας.

Αναφορά συμβάντων ασφάλειας.

Διαχείριση επιχειρησιακής συνέχειας.

Οι πιο πάνω μηχανισμοί αποτελούν βασικά βήματα στην ασφάλεια και μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε οργανισμό.

7.1.4 Βασικοί Παράγοντες Επιτυχίας

Υπάρχουν κάποιοι βασικοί παράγοντες οι οποίοι έχουν ιδιαίτερη σημασία στην υλοποίηση της ασφάλειας πληροφοριών μέσα σε ένα οργανισμό:

Πολιτική ασφάλειας, στόχοι και δραστηριότητες που αντικατοπτρίζουν τους στόχους του οργανισμού.

Εφαρμογή διαδικασιών ασφάλειας σύμφωνα με την κουλτούρα του οργανισμού.

Ενεργή υποστήριξη από τη διοίκηση του οργανισμού.

Κατανόηση των απαιτήσεων ασφάλειας, της αποτίμησης κινδύνων και της διαχείρισης τους.

Γνώση της πολιτικής ασφάλειας από όλο το προσωπικό του οργανισμού.

Εκπαίδευση και κατάρτιση του προσωπικού.

Ένα ισορροπημένο σύστημα μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος ασφάλειας των πληροφοριών και να προτείνει πιθανές βελτιώσεις.

8 Ασφάλεια Περιμέτρου

Πολλοί οργανισμοί ηλεκτρονικού εμπορίου έχουν συνδέσει τα εσωτερικά τους δίκτυα με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών, αλλά και για τη λήψη χρήσιμων πληροφοριών από τον παγκόσμιο ιστό. Η σύνδεση όμως ενός συστήματος στο διαδίκτυο (δημόσιο δίκτυο) δίνει τη δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Δηλαδή οι χρήστες του ιδιόκτητου δικτύου μπορούν να έχουν πρόσβαση στο διαδίκτυο. Ταυτόχρονα και οι χρήστες του διαδικτύου μπορούν να επικοινωνήσουν με το ιδιόκτητο δίκτυο, κάτι το οποίο δεν είναι πάντα επιθυμητό αφού εμπιστευτικές πληροφορίες που βρίσκονται στα συστήματα ενός οργανισμού μπορούν να διαρρεύσουν.

Ειδικά για το ηλεκτρονικό εμπόριο, όπου στα δίκτυα των οργανισμών φυλάσσονται έμπιστα δεδομένα, απαιτείται ένα υψηλό επίπεδο ασφάλειας δικτύου. Πρέπει δηλαδή να εμποδίζονται οι εξωτερικοί χρήστες από το να προσεγγίσουν τις ιδιωτικές πληροφορίες του οργανισμού έτσι ώστε τα προσωπικά δεδομένα των πελατών του οργανισμού ηλεκτρονικού εμπορίου να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Συνεπώς είναι απαραίτητη η ασφάλεια περιμέτρου του ιδιόκτητου δικτύου.

Ως Περίμετρος Δικτύου ορίζονται, σύμφωνα με την ΑΔΑΕ, «όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα (π.χ. διαδίκτυο)». Σύμφωνα πάντα με την ΑΔΑΕ, κάθε οργανισμός που συνδέει το εσωτερικό του δίκτυο με κάποιο δημόσιο δίκτυο, π.χ. το διαδίκτυο, θα πρέπει να εφαρμόζει μια πολιτική ασφάλειας περιμέτρου. Ο πρωταρχικός σκοπός της πολιτικής αυτής είναι να προστατεύσει τους διάφορους πόρους του οργανισμού από εισβολείς, δηλαδή να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του οργανισμού. Η ΑΔΑΕ υποχρεώνει κάθε πάροχο διαδικτύου, οπότε έμμεσα και κάθε οργανισμό ηλεκτρονικού εμπορίου, να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου του με το διαδίκτυο και επιπλέον τον υποχρεώνει να χρησιμοποιεί συστήματα ανίχνευσης εισβολών για την ενίσχυση της προστασίας του δικτύου του.

Ένα σύστημα firewall καλείται να λειτουργήσει ως ένας μηχανισμός «περιμετρικής άμυνας», ο οποίος δρα συμπληρωματικά με τους υπόλοιπους μηχανισμούς ασφάλειας. Σκοπός του είναι ο έλεγχος και η καταγραφή όλων των προσπαθειών προσπέλασης οι οποίες κατευθύνονται προς το προστατευόμενο σύστημα, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του.

Τα συστήματα ανίχνευσης εισβολών (IDS) προσπαθούν να ανιχνεύσουν οποιαδήποτε παράνομη δραστηριότητα στοχεύει σε δικτυακούς και υπολογιστικούς πόρους. Τα συστήματα αυτά συλλέγουν πληροφορίες από μια πληθώρα δικτυακών πηγών και συστημάτων και στη συνέχεια αναλύουν τις πληροφορίες για ενδείξεις εισβολής, προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης.

Τα firewalls και τα IDS αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο. Στη συνέχεια του κεφαλαίου αυτού γίνεται μια αναλυτική περιγραφή των δυνατοτήτων και των περιορισμών των δύο αυτών σημαντικών τεχνολογιών για την ασφάλεια περιμέτρου, των firewalls και των IDS.

8.1 Firewalls

Τα δίκτυα των οργανισμών ηλεκτρονικού εμπορίου συνδέονται με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών. Όπως αναφέρθηκε παραπάνω, αυτό εγκυμονεί κινδύνους, αφού οι χρήστες του διαδικτύου μπορούν να προσεγγίσουν τις ιδιωτικές πληροφορίες του οργανισμού.

Για έναν οργανισμό ηλεκτρονικού εμπορίου είναι πολύ σημαντικό να μπορεί να διαφυλάξει τα προσωπικά δεδομένα των πελατών του από μη εξουσιοδοτημένη πρόσβαση. Είναι επιθυμητό να υπάρχει ένα είδος διαχωρισμού ανάμεσα στο δίκτυο του οργανισμού και το διαδίκτυο. Η παρεμβολή ενός ενδιάμεσου συστήματος ανάμεσα στα δύο δίκτυα θα μπορούσε να τα διαχωρίσει. Ένα τέτοιο ενδιάμεσο σύστημα θα προστατεύει το ιδιόκτητο δίκτυο από επιθέσεις που προέρχονται από τον έξω κόσμο και θα παρέχει ένα μοναδικό σημείο ελέγχου, όπου θα ελέγχεται η κίνηση από και προς το δίκτυο. Επιπλέον το ενδιάμεσο αυτό σύστημα θα μπορούσε να χρησιμοποιηθεί και για συλλογή πληροφοριών διαχείρισης για χρήση του δικτύου, αφού μπορεί να καταγράφει οτιδήποτε διακινείται από ή προς το δίκτυο. Αυτά τα ενδιάμεσα συστήματα ονομάζονται φράγματα ασφαλείας (firewalls).

Firewall είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το ιδιόκτητο δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Λειτουργεί σαν μια πύλη από την οποία περνάει όλη η κίνηση δεδομένων από και προς το εξωτερικό δίκτυο. Στην πύλη εξετάζεται και αποφασίζεται αν θα επιτραπεί ή όχι η διέλευση των δεδομένων, σύμφωνα με την πολιτική ασφάλειας που εφαρμόζει ο οργανισμός του συστήματος. Το firewall δεν είναι απλώς ένα σύνολο συνιστωσών λογισμικού ή υλικού, αλλά η τεχνική έκφραση μιας συγκεκριμένης στρατηγικής προστασίας των πόρων ενός οργανισμού.

Ένα firewall είναι ουσιαστικά ένα «τείχος» ασφάλειας μεταξύ του μη ασφαλούς δημόσιου δικτύου και του ιδιόκτητου δικτύου που θεωρείται ασφαλές και αξιόπιστο. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποία πακέτα επιτρέπεται και ποια όχι να περάσουν στο «απέναντι» δίκτυο.

Ένα firewall δεν μπορεί να λειτουργήσει σωστά, ανεξαρτήτως του πως έχει σχεδιαστεί ή υλοποιηθεί, εάν δεν έχει καθοριστεί μια σαφής πολιτική ασφάλειας. Το firewall που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφάλειας που βρίσκεται κάθε φορά σε ισχύ και πρέπει να είναι συγκεκριμένη και σαφής. Το firewall αποτελεί την πρώτη γραμμή άμυνας του οργανισμού απέναντι στους επίδοξους εισβολείς, αλλά ποτέ τη μοναδική.

Η χρήση ενός φράγματος ασφάλειας δεν αποτελεί πανάκεια για την ασφάλεια του δικτύου. Όπως όλα τα συστήματα ασφάλειας μπορεί να παραβιαστεί από κάποιον ικανό εισβολέα. Επιπλέον το firewall αλληλεπιδρά με το διαδίκτυο και χρειάζεται ιδιαίτερη προσοχή στην εγκατάσταση του και την σωστή διαμόρφωσή του.

8.1.1 Η Αναγκαιότητα Χρήσης των Firewalls

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

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

8.1.2 Δυνατότητες των Firewalls

Η λειτουργικότητα των firewalls εκτείνεται στα ακόλουθα:

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

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

Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο: Εφόσον όλη η κίνηση διέρχεται από το firewall, μπορεί αυτό να καταγράφει όλες τις επιτρεπόμενες και μη δραστηριότητες σε ένα αρχείο συμβάντων, το οποίο είναι διαθέσιμο στο διαχειριστή του δικτύου.

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

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

8.1.3 Αδυναμίες των Firewalls

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

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

Το firewall δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού: Οι εσωτερικοί χρήστες είναι σε θέση να υποκλέψουν δεδομένα, να καταστρέψουν υλικό και λογισμικό, να τροποποιήσουν προγράμματα και γενικότερα να παραβιάσουν την πολιτική ασφάλειας του οργανισμού χωρίς καν να έρθουν σε επαφή με το firewall. Οι εσωτερικές απειλές απαιτούν εσωτερικά μέτρα ασφάλειας, όπως ασφάλεια σε επίπεδο ξενιστή υπολογιστή (host security).

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

Το firewall δεν μπορεί να προστατέψει τον οργανισμό από απειλές άγνωστου τύπου: Το firewall μπορεί να προστατέψει το δίκτυο μόνο από γνωστές απειλές που έχουν αντιμετωπιστεί στο παρελθόν, εφόσον διαθέτει την απαιτούμενη τεχνολογία.

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

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

8.1.4 Ζητήματα Σχεδίασης των Firewalls

Η υλοποίηση ενός firewall δεν αποτελεί τετριμμένο θέμα και δεν παρέχεται ενσωματωμένη σε κανένα λειτουργικό σύστημα. Ο λόγος είναι ότι ένα firewall αποτελεί περισσότερο φιλοσοφία προστασίας και λιγότερο υλικό και λογισμικό που παρέχει πλήρη προστασία από κάθε εξωτερική απειλή. Υπάρχει μια αντίληψη ότι το firewall εξασφαλίζει την πλήρη προστασία ενός δικτύου απέναντι σε κάθε είδους απειλή. Η αντίληψη αυτή είναι τελείως λανθασμένη και μπορεί να οδηγήσει το διαχειριστή ασφάλειας ενός οργανισμού ηλεκτρονικού εμπορίου στην καταστροφική άποψη ότι με την εγκατάσταση ενός firewall είναι εγγυημένη η ασφάλεια του εσωτερικού δικτύου του οργανισμού την οποία διαχειρίζεται.

Η εγκατάσταση ενός firewall αποτελεί σημαντική σχεδιαστική απόφαση για τους παρακάτω λόγους:

Η εγκατάσταση ενός firewall επιφέρει καθυστέρηση στο χρόνο απόκρισης των προγραμμάτων που υλοποιούν τις υπηρεσίες που παρέχει η ιστοθέση.

Η εγκατάσταση ενός firewall θα επιφέρει αναστάτωση, για κάποιο χρονικό διάστημα, στο προσωπικό του οργανισμού μέχρι αυτό να εξοικειωθεί με τις ήδη υπάρχουσες υπηρεσίες, που όμως τώρα θα υλοποιούνται με διαφορετικό τρόπο. Αυτό συμβαίνει επειδή δεν υλοποιούνται όλες ανεξαιρέτως οι υπηρεσίες διαμέσου του firewall με διαφανή τρόπο ως προς το χρήστη.

Κατά την εγκατάσταση ενός firewall, οι υπηρεσίες δε θα μπορούν να παρέχονται στους χρήστες για περιορισμένο διάστημα κάτι το οποίο μπορεί επίσης να προκαλέσει προβλήματα.

Απαιτείται συνεχής συντήρηση και ενημέρωση ενός firewall, καθώς προστίθενται νέες υπηρεσίες και απαξιώνονται παλαιότερες.

Εφόσον ληφθούν υπόψη τα παραπάνω και παρθεί η απόφαση για την εγκατάσταση ενός firewall, υπάρχουν ορισμένα σχεδιαστικά ζητήματα τα οποία θα πρέπει να αντιμετωπιστούν. Τα ζητήματα αυτά περιλαμβάνουν τα εξής:

Χρηστικότητα (usability) του firewall: Τα firewalls χρησιμοποιούνται για να παρέχουν ασφάλεια στα δίκτυα. Το πιο ασφαλές δίκτυο είναι αυτό που δεν συνδέεται με κανένα άλλο δίκτυο, κάτι το οποίο προφανώς δεν είναι καθόλου αποδοτικό, αφού οι χρήστες του δικτύου δε θα μπορούν να έχουν πρόσβαση σε εξωτερικούς πόρους και ούτε οι κλασσικές εφαρμογές ηλεκτρονικού εμπορίου θα μπορούν να πραγματοποιούνται. Πρέπει συνεπώς να γίνουν συμβιβασμοί μεταξύ ασφάλειας και χρηστικότητας.

Εκτίμηση του κινδύνου: Η διασύνδεση με εξωτερικό δίκτυο περιέχει κινδύνους. Επομένως απαιτείται η εκτίμηση της επίδρασης που θα έχει η εισβολή μιας εξωτερικής οντότητας που αποκτά πρόσβαση στο δίκτυο. Οπότε πρέπει η σχεδίαση του firewall να γίνει με τέτοιο τρόπο ώστε ζώνες διαφορετικού κινδύνου να προστατεύονται διαφορετικά.

Εκτίμηση των απειλών: Κατά τη διασύνδεση του δικτύου ενός οργανισμού με άλλα δίκτυα, απαιτείται η εκτίμηση των απειλών από τις οποίες κινδυνεύει το δίκτυο. Αν πρόκειται για διασύνδεση με το εξωτερικό τμήμα του ίδιου οργανισμού, τότε το επίπεδο των απειλών είναι χαμηλό αφού πρόκειται για έμπιστους συνεργάτες. Εάν όμως πρόκειται για διασύνδεση με το διαδίκτυο, υπάρχουν σοβαρές απειλές.

Εκτίμηση του κόστους: Προκειμένου ένας οργανισμός να αποκτήσει firewall, έχει δύο επιλογές: είτε να αγοράσει ένα εμπορικό προϊόν, είτε να το κατασκευάσει ο ίδιος ο οργανισμός. Για να πάρει όμως τη σωστή απόφαση ο οργανισμός πρέπει να υπολογίσει ακριβώς το κόστος υλοποίησης του firewall.

Τύπος firewall: Υπάρχουν διάφοροι τύποι firewalls. Είναι προφανές ότι πρέπει να επιλεγεί ο κατάλληλος τύπος firewall, ο οποίος ικανοποιεί τις ανάγκες του οργανισμού.

8.1.4.1 Πολιτική Σχεδίασης των Firewalls

Όπως προαναφέρθηκε, το firewall αποτελεί μια φιλοσοφία ασφάλειας και βοηθά στην υλοποίηση μιας ευρύτερης πολιτικής ασφάλειας που καθορίζει τις υπηρεσίες και την πολιτική προσπέλασης σε ένα δίκτυο.

Υπάρχουν γενικά δύο επίπεδα πολιτικής ασφάλειας που επηρεάζουν άμεσα το σχεδιασμό, την εγκατάσταση και τη χρήση ενός firewall:

Η υψηλού επιπέδου πολιτική ή αλλιώς πολιτική πρόσβασης σε υπηρεσίες. Αυτή καθορίζει τα πρωτόκολλα της στοίβας TCP/IP και τις υπηρεσίες που θα πρέπει να επιτρέπονται ή να απαγορεύονται από το προστατευόμενο δίκτυο.

Η χαμηλού επιπέδου πολιτική ή αλλιώς πολιτική σχεδίασης του φράγματος ασφάλειας. Αυτή περιγράφει το πώς λειτουργεί το φράγμα ασφαλείας και υλοποιεί τους περιορισμούς στα πρωτόκολλα TCP/IP και στις υπηρεσίες, όπως αυτοί υπαγορεύονται από την πολιτική πρόσβασης υψηλού επιπέδου.

Η πολιτική ασφάλειας του firewall πρέπει να είναι όσο το δυνατό πιο ευέλικτη, λόγω του ότι το διαδίκτυο συνεχώς αλλάζει, προσφέρει καινούργιες υπηρεσίες, μεθόδους και επιχειρηματικές δυνατότητες και συνεπώς οι ανάγκες του οργανισμού μπορεί να αλλάζουν με το χρόνο. Οι καινούργιες υπηρεσίες όμως, εγείρουν και καινούργια θέματα ασφάλειας τα οποία πρέπει να αντιμετωπίσει η πολιτική ασφάλειας των firewalls.

Πολιτική Πρόσβασης σε Υπηρεσίες

Η πολιτική πρόσβασης σε υπηρεσίες ενός οργανισμού αποτελεί επέκταση της γενικότερης πολιτικής του οργανισμού για την προστασία των πληροφοριακών του πόρων. Για να είναι ρεαλιστική η πολιτική πρόσβασης σε υπηρεσίες πρέπει να διασφαλίζει την προστασία του δικτύου από υπαρκτούς κινδύνους ασφάλειας, ενώ ταυτόχρονα να παρέχει στους χρήστες ικανοποιητική πρόσβαση στους πόρους του δικτύου.

Μια τυπική πολιτική είναι να επιτρέπεται μερική πρόσβαση των έξω προς το δίκτυο και επιπλέον αυτή η πρόσβαση να δίνεται μόνο όταν είναι απαραίτητο και μόνο σε συγκεκριμένους εξουσιοδοτημένους χρήστες των οποίων η ταυτότητα πιστοποιείται.

Για να είναι το firewall που θα υλοποιήσει την πολιτική πρόσβασης επιτυχημένο, πρέπει αυτή να είναι ρεαλιστική και να αντικατοπτρίζει το επίπεδο ασφάλειας που απαιτείται για το δίκτυο του οργανισμού. Ένας δικτυακός τόπος υψίστης ασφάλειας και απόρρητων δεδομένων δεν χρειάζεται καθόλου την ύπαρξη firewall γιατί απλούστατα δεν θα πρέπει καν να είναι συνδεδεμένος στο διαδίκτυο. Μια ρεαλιστική πολιτική πρόσβασης σε υπηρεσίες είναι εκείνη που παρέχει μια ισορροπία ανάμεσα στην προστασία του ιδιόκτητου δικτύου από γνωστούς κινδύνους ασφάλειας και τη διατήρηση της πρόσβασης των χρηστών του δικτύου σε εξωτερικούς πόρους όπως το διαδίκτυο. Γενικά υπάρχει συμβιβασμός μεταξύ της προσβασιμότητας και της ασφάλειας των πόρων του συστήματος.

Πολιτική Σχεδιασμού του Firewall

Η πολιτική σχεδιασμού του firewall ορίζει του κανόνες που χρησιμοποιούνται από το firewall για την υλοποίηση της πολιτικής πρόσβασης σε υπηρεσίες. Υπάρχουν δύο γενικές στρατηγικές που μπορεί να υλοποιεί ένα φράγμα ασφάλειας:

Να επιτρέπει τη διέλευση πακέτων που αντιστοιχούν σε κάθε υπηρεσία εκτός και αν μια υπηρεσία απαγορεύεται ρητά.

Να απαγορεύει τη διέλευση πακέτων κάθε είδους υπηρεσίας εκτός και αν αυτή επιτρέπεται ρητά.

Ένα firewall που ακολουθεί την πρώτη στρατηγική επιτρέπει να περάσει κάθε είδος κίνησης υπηρεσιών και πρωτοκόλλων του TCP/IP, με εξαίρεση εκείνες τις υπηρεσίες και τα πρωτόκολλα που χαρακτηρίζονται ως απαγορευμένα από την πολιτική πρόσβασης. Από τη σκοπιά της ασφάλειας αυτή η στρατηγική είναι λιγότερο επιθυμητή αφού προσφέρει πολλές οδούς παράκαμψης του firewall από επίδοξους εισβολείς.

Ένα firewall που ακολουθεί τη δεύτερη στρατηγική αρνείται να εξυπηρετήσει την κίνηση όλων των υπηρεσιών και πρωτοκόλλων του TCP/IP εκτός και αν αυτές χαρακτηρίζονται ρητά ως επιτρεπόμενες από την πολιτική πρόσβασης. Από τη σκοπιά της ασφάλειας αυτή η στρατηγική προτιμάται, αν και είναι δυσκολότερο να υλοποιηθεί.

Για να οδηγηθεί μια επιχείρηση σε μια πολιτική σχεδίασης του firewall και τελικά σε ένα ολοκληρωμένο σύστημα που υλοποιεί την πολιτική αυτή, καλό θα ήταν να ξεκινήσει ακολουθώντας τη δεύτερη στρατηγική. Στη συνέχεια ο σχεδιαστής ασφάλειας πρέπει να λάβει υπόψη του τα εξής:

Ποιες υπηρεσίες του Internet σχεδιάζει η επιχείρηση να χρησιμοποιήσει (π.χ. Telnet, ftp).

Πώς θα γίνεται η χρήση των υπηρεσιών (π.χ. σε τοπική βάση, διαμέσου του Internet, με χρήση dial-up υπηρεσίας από το σπίτι).

Τι επιπρόσθετες ανάγκες και υπηρεσίες (π.χ. κρυπτογραφία) μπορούν να υποστηριχθούν.

Πώς προσδιορίζεται η σχέση που συνδέει την ασφάλεια με τη λειτουργικότητα. Σε περίπτωση σύγκρουσης σε ποια από τις δύο έννοιες δίνεται προτεραιότητα.

8.1.5 Αρχιτεκτονική των Firewalls

Ένα από τα βασικά ζητήματα σχεδίασης είναι η επιλογή κατάλληλου τύπου firewall, ο οποίος ανταποκρίνεται στις ανάγκες του οργανισμού που επιθυμεί την εγκατάσταση του. Τα firewalls ανάλογα με το επίπεδο στο οποίο λειτουργούν και ανάλογα με το βαθμό λειτουργικότητας τους διακρίνονται σε φίλτρα πακέτων και πύλες εφαρμογών.

8.1.5.1 Φίλτρα Πακέτων

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

Τον αριθμό πρωτοκόλλου που δείχνει το είδος του πρωτοκόλλου που χρησιμοποιείται.

Τη διεύθυνση IP του αποστολέα.

Τη διεύθυνση IP του αποδέκτη.

Το TCP ή UDP port προέλευσης.

Το TCPή UDP port προορισμού.

Άλλες πληροφορίες.

Γενικά τα φίλτρα πακέτων δεν έχουν μνήμη κατάστασης. Κάθε πακέτο IP εξετάζεται ξεχωριστά και ανεξάρτητα του τι συνέβη στο παρελθόν. Υπάρχουν όμως και μερικά πιο εξελιγμένα φίλτρα πακέτων που διατηρούν μια λίστα με τα δεδομένα κατάστασης των πακέτων που φτάνουν στο φίλτρο. Οι πληροφορίες των πακέτων που προηγήθηκαν, επιτρέπουν στα μελλοντικά πακέτα που αντιστοιχούν στην ίδια σύνοδο να περάσουν ή να απορριφθούν χωρίς πολλούς ελέγχους. Δηλαδή τα συγκεκριμένα φίλτρα πακέτων ελέγχουν συνόδους δικτύου και όχι μεμονωμένα πακέτα. Μια σύνοδος δικτύου αποτελείται από πακέτα τα οποία κινούνται και προς τι δύο κατευθύνσεις. Τα απλά φίλτρα πακέτων απαιτούν δύο κανόνες για κάθε σύνοδο: Έλεγχος πακέτων τα οποία κατευθύνονται από υπολογιστή προέλευσης προς υπολογιστή προορισμού, και έλεγχος πακέτων τα οποία

επιστρέφουν από υπολογιστή προορισμού προς υπολογιστή προέλευσης. Τα εξελιγμένα φίλτρα πακέτων δεν απαιτούν την ύπαρξη του δεύτερου κανόνα.

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

Σχήμα 8-1: Τοποθέτηση ενός φίλτρου πακέτων μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου

Τα περισσότερα φίλτρα πακέτων συμπεριφέρονται και σαν δρομολογητές και ονομάζονται «δρομολογητές διαλογής». Ένας απλός δρομολογητής όταν δεχθεί ένα πακέτο, κοιτάζει την επικεφαλίδα του και εξετάζει τη διεύθυνση προορισμού. Αν ο δρομολογητής γνωρίζει πώς να στείλει το πακέτο τότε το δρομολογεί. Αν όμως δε γνωρίζει επιστρέφει το πακέτο στον αποστολέα. Ένας δρομολογητής διαλογής εξετάζει το πακέτο διεξοδικότερα. Έτσι δεν καθορίζει μόνο εάν το πακέτο μπορεί να δρομολογηθεί προς τον προορισμό του, αλλά και το αν πρέπει να δρομολογηθεί, εφαρμόζοντας την πολιτική ασφάλειας που έχει καθορίσει ο οργανισμός. Συνεπώς κάθε δρομολογητής διαλογής φιλτράρει τα πακέτα και επιπλέον τα δρομολογεί.

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

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

8.1.5.1.1 Πλεονεκτήματα και Μειονεκτήματα Φίλτρων Πακέτων (και Δρομολογητών Διαλογής)

Τα σημαντικότερα πλεονεκτήματα των φίλτρων πακέτων και των δρομολογητών διαλογής είναι τα εξής:

Το φιλτράρισμα πακέτων είναι φθηνή τεχνολογία.

Το φιλτράρισμα πακέτων είναι μια διαφανής διεργασία για τους χρήστες: Επειδή τα firewalls αυτής της κατηγορίας δεν ασχολούνται καθόλου με το τμήμα δεδομένων του

πακέτου, δεν είναι απαραίτητο οι χρήστες να μάθουν κάποιες ιδιαίτερες εντολές για να τα χειρίζονται.

Τα firewalls αυτής της κατηγορίας εγκαθίστανται και διαμορφώνονται πολύ εύκολα.

Η τεχνολογία των φίλτρων πακέτων και των δρομολογητών διαλογής δεν στηρίζεται στην κρυπτογραφία και έτσι μπορεί να εξαχθεί από τις ΗΠΑ ελεύθερα. Αυτό επιτρέπει την πώληση προϊόντων που χρησιμοποιούν τεχνολογία φιλτραρίσματος πακέτων σε όλο τον κόσμο.

Τα φίλτρα πακέτων και οι δρομολογητές διαλογής έχουν ορισμένες αδυναμίες και μειονεκτήματα. Η κυριότερη αδυναμία τους έγκειται στην πολυπλοκότητα της ορθής ρύθμισης και διαχείρισης των κανόνων φιλτραρίσματος. Ειδικότερα:

Το να οριστούν σωστά οι κατάλληλοι κανόνες φιλτραρίσματος είναι μια δύσκολη και επιρρεπής σε λάθη διαδικασία.

Η σειρά με την οποία πρέπει να εισαχθούν οι κανόνες φιλτραρίσματος παίζει σπουδαίο ρόλο και καθιστά ακόμη πιο δύσκολη την εύρεση ενός κατάλληλου συνόλου κανόνων.

Πρέπει μερικές φορές να υπάρχουν εξαιρέσεις στους κανόνες φιλτραρίσματος, ώστε να επιτρέπονται μερικά είδη υπηρεσιών που κανονικά θα έπρεπε να παρεμποδιστούν. Οι εξαιρέσεις αυτές καθιστούν το σύνολο των κανόνων πολύπλοκο.

Κάθε firewall επιπέδου δικτύου αποφασίζει για κάθε πακέτο αν θα το προωθήσει ή θα το απορρίψει βασιζόμενο σε μη πιστοποιημένη πληροφορία. Οποιοσδήποτε σταθμός θα μπορούσε να προσποιηθεί ότι είναι κάποιος άλλος, αλλάζοντας την IP διεύθυνση προέλευσης στα πακέτα του. Το πρωτόκολλο IPSP (IP Security Policy) προστατεύει από τέτοιου είδους επιθέσεις. Έτσι ένας δρομολογητής διαλογής χρησιμοποιώντας το πρωτόκολλο IPSP μπορεί να ρυθμιστεί ώστε να απορρίπτει κάθε πακέτο IP που δεν είναι κατάλληλα πιστοποιημένο από μια έγκυρη επικεφαλίδα πιστοποίησης.

8.1.5.2 Πύλες Εφαρμογών (Application Gateways)

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

Αν η πύλη λειτουργεί στο επίπεδο εφαρμογής ονομάζεται πύλη επιπέδου εφαρμογής (application-level gateway) ή απλά πύλη εφαρμογών. Αντίστοιχα αν η πύλη λειτουργεί στο επίπεδο μεταφοράς ονομάζεται πύλη επιπέδου κυκλώματος (circuit-level gateway).

Οι περισσότερες πύλες που χρησιμοποιούνται σε διατάξεις firewalls λειτουργούν στο επίπεδο εφαρμογής, είναι δηλαδή πληρεξούσιοι εξυπηρετητές (proxy servers).

Όταν ένας χρήστης που βρίσκεται στο εσωτερικό δίκτυο θέλει να επικοινωνήσει με μια υπηρεσία του εξωτερικού δικτύου, η πύλη εφαρμογών παρεμβάλλεται. Δηλαδή αντί ο

χρήστης να επικοινωνήσει άμεσα με την υπηρεσία, επικοινωνεί με την πύλη εφαρμογών η οποία διαχειρίζεται παρασκηνιακά όλη τη μεταξύ τους επικοινωνία. Συγκεκριμένα όταν ένας πελάτης συνδέεται με την πύλη εφαρμογών χρησιμοποιώντας ένα από τα πρωτόκολλα εφαρμογής του TCP/IP, όπως το Telnet ή το FTP, η πύλη του ζητά πληροφορίες όπως ένα όνομα εισόδου (login) και ένα κωδικό πρόσβασης (password) για την πιστοποίηση της ταυτότητας του. Αν η πύλη αναγνωρίσει και δεχτεί το χρήστη, ο χρήστης της δίνει το όνομα του απομακρυσμένου συστήματος (υπηρεσία) που επιθυμεί να προσπελάσει, η πύλη εφαρμογών συνδέεται για λογαριασμό του χρήστη με αυτό το απομακρυσμένο σύστημα και εγκαθιστά μια δευτερεύουσα σύνδεση. Στη συνέχεια μετάγει τα δεδομένα της εφαρμογής μεταξύ των δύο συνδέσεων.

Στην περίπτωση μιας πύλης εφαρμογών μπορεί η κίνηση δεδομένων να παρακολουθείται και επιπλέον να επιβληθούν εξειδικευμένοι περιορισμοί σχετικά με την κίνηση αυτών από και προς το ιδιωτικό δίκτυο με σκοπό να αποτραπεί η υποκλοπή πολύτιμων προγραμμάτων ή δεδομένων.

Σχήμα 8-2: Τοποθέτηση μιας πύλης εφαρμογών μεταξύ ενός ιδιωτικού δικτύου και του διαδικτύου

Η πύλη εφαρμογών φιλοξενείται σε ένα υπολογιστή γενικού σκοπού, ο οποίος ονομάζεται Bastion host (ή υπολογιστής-οχυρό). Ο υπολογιστής-οχυρό απαιτείται να παρέχει μεγάλη ασφάλεια διότι αποτελεί το κύριο σημείο επικοινωνίας για τους χρήστες του εσωτερικού δικτύου. Επιπλέον επειδή ο υπολογιστής-οχυρό εκτίθεται σε άμεσες επιθέσεις από το διαδίκτυο θα πρέπει να είναι ρυθμισμένος με τέτοιο τρόπο ώστε να είναι ιδιαίτερα ασφαλής. Συνήθως το λειτουργικό σύστημα του bastion host είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητες του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται. Έτσι μειώνεται η πιθανότητα ύπαρξης τυχόν «οπών ασφαλείας» και συνεπώς ενισχύεται η ασφάλεια του bastion host.

8.1.5.2.1 Πληρεξούσιοι Εξυπηρετητές (Proxy Servers)

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

εφαρμογή στον υπολογιστή-οχυρό. Ο proxy server με τη σειρά του πρέπει να πιστοποιήσει την αυθεντικότητα του χρήστη και να τον εξουσιοδοτήσει για πρόσβαση.

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

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

8.1.5.2.2 Πλεονεκτήματα και Μειονεκτήματα Πυλών Εφαρμογών (και Proxy Servers)

Υπάρχουν αρκετά πλεονεκτήματα σχετικά με τη χρήση πυλών επιπέδου εφαρμογής γενικότερα και proxy servers ειδικότερα, μερικά από τα οποία είναι τα εξής:

Παρέχουν μεγαλύτερη ασφάλεια: Τα firewalls αυτού του τύπου έχουν τη δυνατότητα προσθήκης μιας λίστας ελέγχου προσπέλασης για τις διάφορες υπηρεσίες, απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης προτού τους επιτραπεί πρόσβαση σε κάποια από τις υπηρεσίες.

Επιπλέον τα συστήματα αυτού του τύπου παρέχουν μεγαλύτερη ασφάλεια αφού «τρέχουν» μειωμένο σετ εφαρμογών και ένα ασφαλές λειτουργικό σύστημα. Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο από τον proxy server εμποδίζοντας έτσι την απευθείας σύνδεση.

Υπάρχουν κάποιοι «έξυπνοι» proxy servers που λέγονται Application Layer Gateways (ALGs), οι οποίοι μπορούν να μπλοκάρουν συγκεκριμένα τμήματα ενός πρωτοκόλλου. Για παράδειγμα ένας (ALGs) για FTP μπορεί να διαχωρίζει την εντολή “put” από την εντολή “get”. Έτσι ένας οργανισμός μπορεί να επιτρέπει στους χρήστες του να «κατεβάζουν» αρχεία αλλά να μην αφήνει τους έξω να παίρνουν τα αρχεία των δικών του συστημάτων.

Παρέχουν καλύτερη καταγραφή συμβάντων: Ένα βασικό χαρακτηριστικό των firewalls αυτής της κατηγορίας είναι ο on-line έλεγχος, ο οποίος επιτρέπει την παρακολούθηση της δραστηριότητας και την καταγραφή συγκεκριμένων γεγονότων.

Τα firewalls επιπέδου εφαρμογής έχουν ορισμένα μειονεκτήματα:

Ένα firewall επιπέδου εφαρμογής απαιτεί ένα ξεχωριστό proxy server για κάθε υπηρεσία δικτύου: Οι πύλες επιπέδου εφαρμογής επιτρέπουν μόνο εκείνα τα πρωτόκολλα

και υπηρεσίες TCP/IP για τα οποία υπάρχει proxy server. Για παράδειγμα αν ένα firewall φιλοξενεί proxy servers για Telnet και FTP, τότε μόνο η κυκλοφορία Telnet και FTP επιτρέπεται, ενώ όλες οι άλλες υπηρεσίες παρεμποδίζονται. Εάν απαιτείται η υποστήριξη κάποιας άλλης υπηρεσίας από το firewall, είναι αναγκαίο να προστεθεί ένας νέος proxy server. Συνεπώς αν παρουσιαστεί μια νέα υπηρεσία στο Internet και το firewall δεν έχει τον αντίστοιχο proxy server, οι χρήστες του δικτύου δεν θα έχουν τη δυνατότητα πρόσβασης σε αυτή την υπηρεσία.

Δεν είναι πάντοτε διαφανή προς το χρήστη

Είναι δυσκολότερα στην υλοποίηση

Η ταχύτητα και η απόδοση των firewalls επιπέδου εφαρμογής δεν είναι τόσο ικανοποιητική όσο των firewalls επιπέδου δικτύου.

8.1.5.3 Υβριδικά Συστήματα Ασφάλειας

Συνήθως η κατασκευή ενός firewall δε στηρίζεται μόνο σε μια από τις αρχιτεκτονικές που αναφέρθηκαν πιο πάνω. Για την κατασκευή ενός firewall συνδυάζονται τα firewalls επιπέδου δικτύου (φίλτρα πακέτων, δρομολογητές διαλογής) και τα firewalls επιπέδου εφαρμογής (πύλες εφαρμογών, proxy servers). Τα συνδυασμένα firewalls που προκύπτουν ονομάζονται υβριδικά συστήματα ασφάλειας και οδηγούν στην επίλυση συνδυασμένων προβλημάτων. Τα προς επίλυση προβλήματα εξαρτώνται από τις υπηρεσίες τις οποίες θέλει να προσφέρει ένας οργανισμός στους χρήστες, καθώς και από το επίπεδο του κινδύνου που είναι διατεθειμένος να δεχτεί.

Σε ένα υβριδικό σύστημα ασφάλειας, τα λαμβανόμενα πακέτα υπόκεινται πρώτα στον έλεγχο τον οποίο διενεργεί το firewall επιπέδου δικτύου. Ακολούθως τα πακέτα είτε απορρίπτονται, είτε διέρχονται και κατευθύνονται προς τον προορισμό τους, είτε προωθούνται σε κάποιο proxy server για περαιτέρω επεξεργασία. Όταν το εσωτερικό δίκτυο ενός οργανισμού απαιτεί την ασφάλεια την οποία παρέχει ένα firewall επιπέδου εφαρμογής για ορισμένες υπηρεσίες και την ταχύτητα και ευελιξία ενός firewall επιπέδου δικτύου για ορισμένες άλλες υπηρεσίες, τότε βέλτιστη λύση αποτελεί ένα υβριδικό σύστημα ασφάλειας.

Ένα υβριδικό σύστημα ασφάλειας είναι σαφώς ακριβότερο, καθώς παρέχει μεγαλύτερη λειτουργικότητα και περισσότερα χαρακτηριστικά από ένα απλό firewall επιπέδου δικτύου.

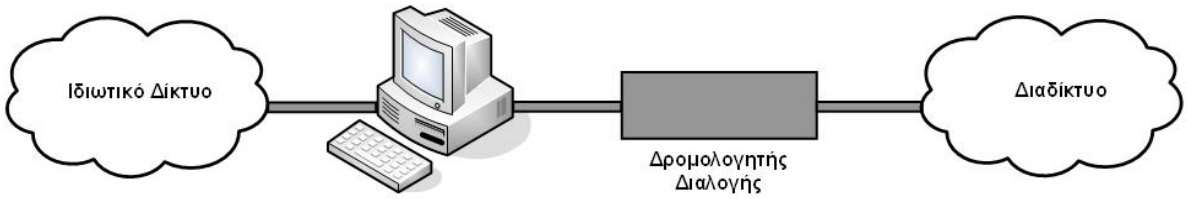
Τα εξής υβριδικά συστήματα ασφάλειας εφαρμόζονται σήμερα ευρέως στο διαδίκτυο: Διπλοσυνδεδεμένα Φράγματα Ασφάλειας (Dual-Homed Firewalls), Φράγματα Ασφάλειας Υπολογιστή Διαλογής (Screened Host Firewalls), και Φράγματα Ασφάλειας Υποδικτύου Διαλογής (Screened Subnet Firewalls).

8.1.5.3.1 Διπλοσυνδεδεμένα Φράγματα Ασφαλείας (Dual-Homed Firewalls)

Τα διπλοσυνδεδεμένα firewalls αποτελούν καλύτερη εναλλακτική λύση σε σχέση με τα firewalls επιπέδου δικτύου, καθώς η πρόσβαση στο προστατευόμενο δίκτυο μπορεί να γίνει μόνο μέσω των proxy servers που τρέχουν στον υπολογιστή-οχυρό. Τα διπλοσυνδεδεμένα firewalls συνδυάζουν τόσο τα firewalls επιπέδου δικτύου, όσο και τα firewalls επιπέδου εφαρμογής, όπως κάθε υβριδικό σύστημα.

Ένα διπλοσυνδεδεμένο firewall αποτελείται από ένα υπολογιστή-οχυρό που είναι συνδεδεμένος και με τα δύο δίκτυα (ιδιωτικό δίκτυο και διαδίκτυο) και έχει απενεργοποιημένες τις δυνατότητες για προώθηση και δρομολόγηση IP. Αυτό σημαίνει ότι τα πακέτα IP από το ένα δίκτυο, το Internet, δε μπορούν να δρομολογηθούν άμεσα προς το εσωτερικό προστατευόμενο δίκτυο. Η IP κίνηση είναι πλήρως ελεγχόμενη, αφού τα συστήματα του εσωτερικού δικτύου και τα συστήματα του διαδικτύου δεν επιτρέπεται να επικοινωνήσουν άμεσα μεταξύ τους. Επιπλέον τοποθετείται και ένας δρομολογητής διαλογής μεταξύ του υπολογιστή-οχυρό και του διαδικτύου. Σκοπός του είναι να διασφαλίσει ότι κάθε πακέτο IP που φθάνει από το διαδίκτυο απευθύνεται με σωστό τρόπο στον υπολογιστή-οχυρό. Αν κάποιο πακέτο φθάνει με κάποια άλλη IP διεύθυνση προορισμού πρέπει να απορριφθεί. Στο

Σχήμα 8-3 φαίνεται η βασική δομή ενός διπλοσυνδεδεμένου firewall.



Σχήμα 8-3: Ένα διπλοσυνδεδεμένο firewall.

Για λόγους απόδοσης μπορούν να χρησιμοποιηθούν περισσότεροι του ενός υπολογιστές-οχυρά, όπου όλοι θα είναι συνδεδεμένοι και στο εσωτερικό και στο εξωτερικό δικτυακό τμήμα.

Το διπλοσυνδεδεμένο firewall είναι ένας απλός αλλά ασφαλής σχηματισμός. Η πρόσβαση στο ενδοεπιχειρησιακό δίκτυο μπορεί να περάσει μόνο από proxy servers που τρέχουν στον υπολογιστή-οχυρό. Έτσι καμιά υπηρεσία δεν περνά εκτός από αυτές για τις οποίες υπάρχουν proxy servers. Με τον τρόπο αυτό υλοποιείται η πολιτική σχεδιασμού όπου κάθε υπηρεσία απαγορεύεται εκτός και αν αυτή ρητά επιτρέπεται.

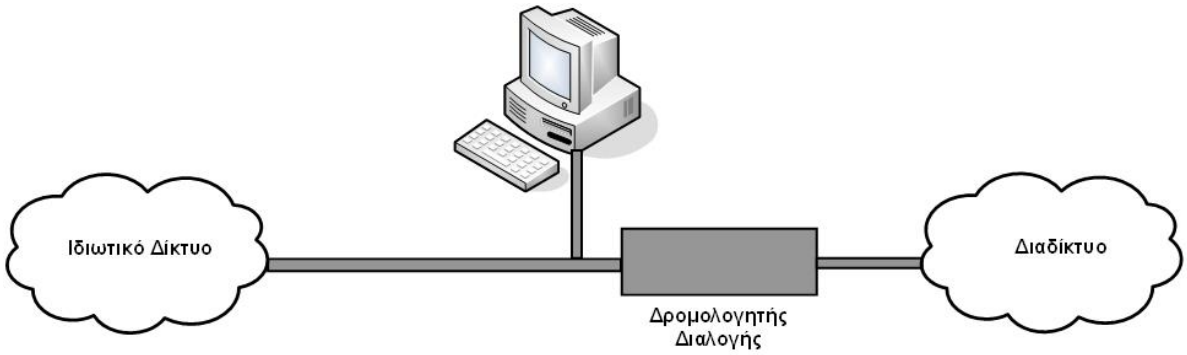
Το διπλοσυνδεδεμένο firewall έχει το μικρότερο κόστος από τις τρεις υβριδικές αρχιτεκτονικές που εξετάζονται, αλλά παρουσιάζει ένα σοβαρότατο μειονέκτημα: Αποτελεί μοναδικό σημείο δυνητικής αποτυχίας στο δίκτυο, συνεπώς αν ένας κακόβουλος επιτιθέμενος εισβάλει σε αυτό, τότε όλο το δίκτυο εκτίθεται σε κίνδυνο. Επιπλέον υπάρχουν και κάποια πρακτικά προβλήματα στη χρήση αυτού του μηχανισμού που σχετίζονται με το ότι δεν υπάρχουν proxy servers για ιδιόκτητα εταιρικά TCP/IP πρωτόκολλα εφαρμογής, όπως τα Lotus Notes, SQLnet και SAP.

8.1.5.3.2 Φράγματα Ασφάλειας Υπολογιστή Διαλογής (Screened Host Firewalls)

Ένα firewall υπολογιστή διαλογής παρέχει υπηρεσίες μέσω ενός υπολογιστή που είναι προσαρτημένος μόνο στο εσωτερικό δίκτυο. Στο σχηματισμό αυτό υπάρχει και ένας δρομολογητής διαλογής που συνδέει το εσωτερικό δίκτυο με το διαδίκτυο και πρέπει να είναι ρυθμισμένος έτσι ώστε να στέλνει όλη την κυκλοφορία IP που προέρχεται από το

διαδίκτυο στην πύλη εφαρμογών που τρέχει στον υπολογιστή-οχυρό. Πριν όμως προωθήσει την κυκλοφορία IP σε αυτόν τον υπολογιστή, ο δρομολογητής διαλογής πρέπει να εφαρμόσει τους κανόνες φίλτρου πακέτων του. Μόνο η πληροφορία που είναι συμβατή με τους κανόνες διοχετεύεται στον υπολογιστή-οχυρό, ενώ όλη η άλλη πληροφορία απορρίπτεται. Συνεπώς οι πίνακες δρομολόγησης του δρομολογητή διαλογής πρέπει να προστατεύονται ισχυρά από εισβολή, διότι αν μια καταχώρηση στον πίνακα αλλάξει έτσι ώστε η κυκλοφορία να μην προωθείται στον υπολογιστή-οχυρό αλλά να στέλνεται απευθείας στο εσωτερικό δίκτυο, το firewall «αστοχεί».

Στο
Σχήμα 8-4 παρουσιάζεται ο σχηματισμός ενός firewall υπολογιστή διαλογής.



Σχήμα 8-4: Ένας σχηματισμός firewall υπολογιστή διαλογής.

Ο μηχανισμός firewall υπολογιστή διαλογής είναι πιο ευέλικτος. Επιτρέπει στο δρομολογητή διαλογής να «περνάει» ορισμένες αξιόπιστες υπηρεσίες κατευθείαν στο εσωτερικό δίκτυο. Οπότε έχει τη δυνατότητα να επιτρέπει και στις υπηρεσίες για τις οποίες δεν υπάρχουν proxy servers, να περνάνε στο εσωτερικό δίκτυο, κάτι το οποίο δεν μπορούσε να πραγματοποιήσει αρχιτεκτονική διπλοσυνδεδεμένων firewalls.

Επειδή η αρχιτεκτονική αυτή επιτρέπει και τη μεταφορά πακέτων από το Internet κατευθείαν στο εσωτερικό δίκτυο, ίσως φαίνεται πιο επικίνδυνη από την αρχιτεκτονική διπλοσυνδεδεμένων firewalls, η οποία δεν επιτρέπει σε κανένα πακέτο να περάσει απευθείας από το Internet στο εσωτερικό δίκτυο. Πρακτικά όμως η αρχιτεκτονική διπλοσυνδεδεμένων firewalls είναι επιρρεπής σε ενδεχόμενες αποτυχίες οι οποίες θα έχουν ως αποτέλεσμα τη μεταφορά πακέτων από το εξωτερικό προς το εσωτερικό δίκτυο. Από την άλλη πλευρά είναι ευκολότερο να αμυνθεί κανείς με τη χρήση ενός δρομολογητή ο οποίος παρέχει ένα περιορισμένο σύνολο υπηρεσιών, παρά με τη χρήση ενός υπολογιστή. Στις περισσότερες περιπτώσεις πάντως, η αρχιτεκτονική υπολογιστή διαλογής παρέχει μεγαλύτερη ασφάλεια και χρησιμότητα.

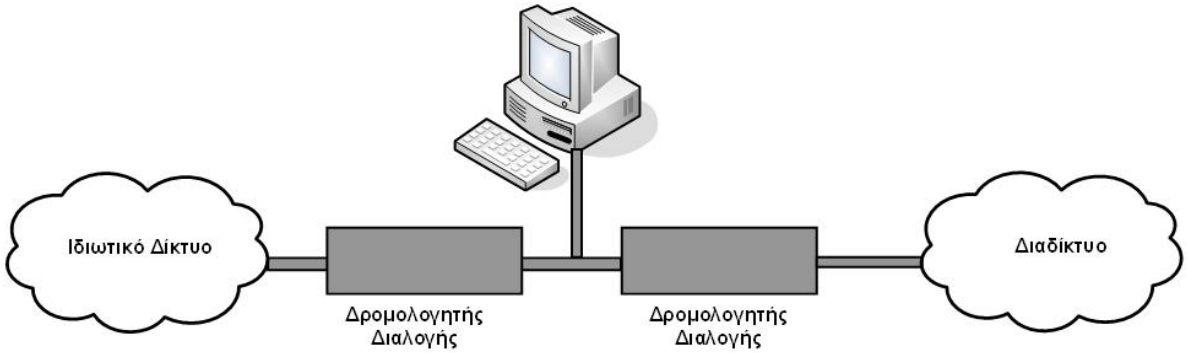
Η αρχιτεκτονική αυτή παρουσιάζει ένα σοβαρότατο μειονέκτημα: Βασίζεται σε δύο ξεχωριστές συσκευές ασφάλειας, το δρομολογητή διαλογής και τον υπολογιστή-οχυρό. Εάν κάποια από τις δύο αυτές συσκευές αποτύχει, τότε το δίκτυο εκτίθεται σε κίνδυνο. Αν για παράδειγμα ένας εισβολέας καταφέρει να παραβιάσει τον υπολογιστή-οχυρό, τότε θα έχει ελεύθερη πρόσβαση στο εσωτερικό δίκτυο. Ομοίως αν ο δρομολογητής εκτεθεί σε κίνδυνο, όλο το δίκτυο είναι πλέον ανασφαλές. Για αυτούς τους λόγους η πιο διαδεδομένη αρχιτεκτονική είναι η επόμενη.

8.1.5.3.3 Φράγματα Ασφάλειας Υποδικτύου Διαλογής (Screened Subnet Firewalls)

Ένα firewall υποδικτύου διαλογής αποτελείται από δύο δρομολογητές διαλογής με τον υπολογιστή-οχυρό να βρίσκεται ενδιάμεσα. Έτσι δημιουργείτε ένα εσωτερικό (περιμετρικό) υποδίκτυο διαλογής, ανάμεσα στο εσωτερικό και εξωτερικό δίκτυο. Στο
Σχήμα 8-5 απεικονίζεται ο σχηματισμός firewall υποδικτύου διαλογής.

Αυτή η αρχιτεκτονική εισάγει ένα επιπλέον επίπεδο ασφάλειας σε σχέση με την αρχιτεκτονική υπολογιστή διαλογής, προσθέτοντας το περιμετρικό υποδίκτυο το οποίο απομονώνει περισσότερο το εσωτερικό δίκτυο από το Internet.

Αυτό το περιμετρικό υποδίκτυο αναφέρεται και ως «αποστρατιωτικοποιημένη ζώνη» (DMZ-demilitarized zone). Είναι δυνατό να υπάρχουν περισσότεροι του ενός υπολογιστές-οχυρά στο απομονωμένο αυτό δίκτυο για λόγους απόδοσης.



Σχήμα 8-5 : Ένας σχηματισμός firewall υποδικτύου διαλογής.

Ο λόγος για τον οποίο προστίθεται ένα επιπλέον δίκτυο είναι ότι οι υπολογιστές-οχυρά αποτελούν τις πλέον ευπαθείς συσκευές του δικτύου, καθώς είναι τα συστήματα τα οποία κατεξοχήν μπορούν να δεχτούν επιθέσεις. Στην αρχιτεκτονική υπολογιστή διαλογής, ανάμεσα στον υπολογιστή-οχυρό και στο εσωτερικό δίκτυο δεν υπάρχει κανένας άλλος μηχανισμός άμυνας. Παραβιάζοντας κάποιος τον υπολογιστή-οχυρό μπορεί να έχει πλήρη πρόσβαση στο εσωτερικό δίκτυο. Η αρχιτεκτονική υποδικτύου διαλογής προσφέρει περισσότερη ασφάλεια, απομονώνοντας τον υπολογιστή-οχυρό στο περιμετρικό υποδίκτυο. Έτσι ακόμη και αν κάποιος εισβολέας αποκτήσει κάποια πρόσβαση στον υπολογιστή-οχυρό, θα έχει να αντιμετωπίσει ακόμη ένα δρομολογητή για μπορέσει να εισβάλει στο εσωτερικό δίκτυο.

Όπως έχει αναφερθεί, στο περιμετρικό υποδίκτυο περιλαμβάνονται δύο δρομολογητές διαλογής. Ο εσωτερικός δρομολογητής βρίσκεται μεταξύ του εσωτερικού δικτύου και του περιμετρικού υποδικτύου, ενώ ο εξωτερικός δρομολογητής βρίσκεται μεταξύ του περιμετρικού υποδικτύου και του εξωτερικού δικτύου, συνήθως του Internet.

Ο εσωτερικός δρομολογητής προστατεύει το εσωτερικό δίκτυο, τόσο από το Internet, όσο και από το περιμετρικό υποδίκτυο. Ο δρομολογητής αυτός αναλαμβάνει το μεγαλύτερο βάρος υλοποίησης του μηχανισμού φιλτραρίσματος πακέτων του firewall. Έτσι επιτρέπει να περάσουν μόνο επιλεγμένες υπηρεσίες από το εσωτερικό δίκτυο προς το

Internet. Τέτοιες υπηρεσίες αφορούν εξερχόμενες συνόδους Telnet, FTP, WAIS, Copher και άλλες συνόδους.

Ο εξωτερικός δρομολογητής προστατεύει τόσο το περιμετρικό υποδίκτυο όσο και το εσωτερικό δίκτυο από το Internet. Ο εξωτερικός δρομολογητής τείνει να επιτρέπει οτιδήποτε κατευθύνεται από το περιμετρικό υποδίκτυο προς τον εξωτερικό κόσμο. Σε γενικές γραμμές είναι απαραίτητο οι κανόνες οι οποίοι τίθενται για την προστασία των εσωτερικών μηχανών να συμφωνούν τόσο στον εσωτερικό όσο και στον εξωτερικό δρομολογητή. Οι μοναδικοί κανόνες φιλτραρίσματος πακέτων που εφαρμόζονται αποκλειστικά σε έναν εξωτερικό δρομολογητή, είναι αυτοί οι οποίοι προστατεύουν τον υπολογιστή-οχυρό και το εσωτερικό δίκτυο από το Internet.

Με αυτή την αρχιτεκτονική υποδικτύου διαλογής, το ιδιωτικό δίκτυο προστατεύεται ακόμη περισσότερο, αφού ένας επιτιθέμενος θα πρέπει να υπονομεύσει, όχι μόνο τον υπολογιστή-οχυρό αλλά και τους δρομολογητές για να φτάσει στο εσωτερικό δίκτυο. Έτσι δεν υπάρχει πλέον ένα και μοναδικό σημείο ευπάθειας το οποίο να θέτει σε κίνδυνο όλο το εσωτερικό δίκτυο.

8.1.6 Εγκατάσταση Firewall

Η εγκατάσταση ενός firewall περιλαμβάνει μια σειρά διαδοχικά εκτελούμενων φάσεων. Αυτές είναι:

Σχεδιασμός Πολιτικής

Ο σχεδιασμός ενός firewall προϋποθέτει τον ακριβή προσδιορισμό των ορίων των διακριτών περιοχών ασφάλειας του δικτύου, καθεμιά από τις οποίες λειτουργεί με βάση συγκεκριμένη πολιτική ασφάλειας. Στη συνέχεια επιλέγονται:

Η βασική αρχιτεκτονική (αριθμός υπολογιστών, μέθοδοι συνδέσεων, λειτουργίες που εκτελούνται).

Οι λειτουργίες που θα υλοποιηθούν (επίπεδο δικτύου, επίπεδο εφαρμογής, υβριδικός συνδυασμός).

Το αρχιτεκτονικό σχέδιο του firewall (διπλοσυνδεδεμένο, με υπολογιστή διαλογής, με υποδίκτυο διαλογής).

Απόκτηση υλικού και λογισμικού για firewalls

Στη φάση αυτή εξασφαλίζεται η ύπαρξη του κατάλληλου εξοπλισμού (υλικό και λογισμικό), για να είναι δυνατή η εγκατάσταση, ο δοκιμαστικός έλεγχος, η λειτουργία και η επίβλεψη του firewall. Συγκεκριμένα εκτελείται:

Προσδιορισμός των απαραίτητων τμημάτων υλικού (υπολογιστές, δρομολογητές, επεξεργαστές, μνήμη, δίσκος, κάρτες, καλώδια κλπ).

Προσδιορισμός των απαραίτητων τμημάτων λογισμικού (λειτουργικά συστήματα, patches, device drivers, λογισμικό firewall, λογισμικό παρακολούθησης δικτύου).

Απόκτηση τεκμηρίωσης, εκπαίδευσης και υποστήριξης

Ανάλογα με τον επιλεγέντα αρχιτεκτονικό σχεδιασμό, πιθανότατα απαιτείται επιπρόσθετη εκπαίδευση και υποστήριξη από την προμηθεύτρια εταιρεία. Εάν ο

οργανισμός δε διαθέτει εμπειρία στις τεχνολογίες που πρόκειται να υλοποιήσει, υπάρχει σοβαρό ενδεχόμενο να οδηγηθεί σε σφάλματα που θα μπορούσαν να προκαλέσουν καθυστέρηση στην εγκατάσταση, στη ρύθμιση και στη λειτουργία του firewall. Επιπλέον η συντήρηση του υλικού και του λογισμικού μπορεί να είναι τόσο περίπλοκη ώστε να απαιτείται εκπαίδευση και συνεχής υποστήριξη. Όλα αυτά πρέπει να μελετηθούν λεπτομερώς στη φάση αυτή.

Εγκατάσταση υλικού και λογισμικού

Στη φάση αυτή εγκαθίσταται και ρυθμίζεται το λειτουργικό σύστημα που θα υποστηρίξει το λογισμικό του firewall. Το λειτουργικό σύστημα περιλαμβάνει μόνο τις υπηρεσίες που είναι απαραίτητες για τη λειτουργία του firewall, ενώ όλες οι υπόλοιπες υπηρεσίες πρέπει να είναι απενεργοποιημένες. Στη συνέχεια το λογισμικό του firewall εγκαθίσταται στο επιλεγμένο υλικό για δοκιμαστικό έλεγχο.

Ρύθμιση της δρομολόγησης

Όταν ένα πακέτο φτάνει σε ένα δρομολογητή, ο δρομολογητής πρέπει να αποφασίσει για τη διάθεση του. Στόχοι του μηχανισμού δρομολόγησης είναι η απόδοση και η αξιοπιστία, όχι η υλοποίηση πολιτικής ασφάλειας.

Ρύθμιση των κανόνων φιλτραρίσματος πακέτων

Ο μηχανισμός φιλτραρίσματος ελέγχει το περιεχόμενο του πακέτου και με βάση ορισμένα κριτήρια και κανόνες υλοποιεί την πολιτική ασφάλειας αποφασίζοντας για την προώθηση ή απόρριψη του πακέτου. Εάν στην αρχιτεκτονική σχεδίαση περιλαμβάνονται και proxy servers, τότε πρέπει στη φάση αυτή να εγκατασταθεί το λογισμικό για κάθε υποστηριζόμενη υπηρεσία.

Ρύθμιση μηχανισμών καταγραφής και έγκυρης προειδοποίησης

Στη φάση αυτή πρέπει να γίνει επιλογή των περιπτώσεων φιλτραρίσματος πακέτων που θα καταγράφονται. Επιπλέον θα πρέπει να οριστούν εκείνα τα συμβάντα για τα οποία πρέπει να σημάνει συναγερμός.

Έλεγχος στο σύστημα firewall

Το σύστημα ελέγχεται στο περιβάλλον δοκιμών για τυχόν λάθη και ελλείψεις με χρήση συστημάτων ανίχνευσης εισβολής, σαρωτών θυρών (ports scanners), εργαλείων ανίχνευσης αδυναμιών, εργαλείων παραγωγής κίνησης στο δίκτυο και εργαλείων παρακολούθησης δικτύων. Επιπλέον εκτελούνται πιθανά σενάρια για επιβεβαίωση της ορθής λειτουργίας του firewall.

Εγκατάσταση του firewall

Αν το firewall πρόκειται να συνδέσει δύο ασύνδετα δίκτυα, τότε εγκαθίσταται σταδιακά. Αν το firewall πρόκειται να αντικαταστήσει ένα υπάρχον σύστημα, τότε το

firewall εγκαθίσταται παράλληλα με τη λειτουργία του υπάρχοντος συστήματος, προσέχοντας πάντοτε να μην επηρεαστεί το παραγωγικό περιβάλλον λειτουργίας.

8.1.7 Συμπεράσματα

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

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

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

Κάθε οργανισμός ηλεκτρονικού εμπορίου οφείλει να διαφυλάσσει τα προσωπικά δεδομένα των πελατών του και να λαμβάνει μέτρα ώστε αυτά να μην εκτίθονται σε μη εξουσιοδοτημένη πρόσβαση. Τα firewalls μπορούν να προσφέρουν αποτελεσματικές υπηρεσίες ελέγχου πρόσβασης για τα εσωτερικά δίκτυα των οργανισμών ηλεκτρονικού εμπορίου καθώς αποτελούν την πρώτη γραμμή άμυνας απέναντι σε εξωτερικές επιθέσεις. Συνεπώς τα firewalls αποτελούν αναμφισβήτητα ένα πανίσχυρο εργαλείο υλοποίησης σημαντικού μέρους της πολιτικής ασφάλειας των οργανισμών ηλεκτρονικού εμπορίου που εκθέτουν τους πόρους τους στο διαδίκτυο.

9. Το θεσμικό πλαίσιο του e-commerce

9.1 Ασφάλεια στο Internet σε θέματα πνευματικής ιδιοκτησίας

Το Internet είναι ένα κατεξοχήν περιβάλλον πολλαπλής δικαιοδοσίας. Οι χρήστες μπορούν να έχουν πρόσβαση στο Internet σχεδόν από κάθε γωνιά της Γης. Χάρη στην τεχνολογία packet-switching και τη σύνθετη δομή των ψηφιακών δικτύων και της τηλεπικοινωνιακής υποδομής, η ψηφιοποιημένη πληροφορία, για να φτάσει στον προορισμό της, ενδέχεται να διασχίσει διάφορες χώρες, καθεμία από τις οποίες έχει το δικό της νομικό σύστημα.

Λόγω της σημαντικής επίδρασης αυτού του διεθνούς μέσου σ' έναν κόσμο φτιαγμένο από ανεξάρτητες χώρες, τα θέματα που αφορούν στη δικαιοδοσία, φαντάζουν δυσεπίλυτα. Ξεπερνούν τα όρια της πνευματικής ιδιοκτησίας, που έχει αναδειχθεί σε μείζον θέμα, και πέρα από τα συμβόλαια που προαναφέρθηκαν αφορούν και σε άλλους τομείς, όπως το Ποινικό Δίκαιο, για να αντιμετωπίζονται οι απάτες και κάθε είδους αδικοπραξίες, η προστασία του καταναλωτή, η φορολογία, καθώς και οι κανόνες για το on-line περιεχόμενο, για την προστασία κυρίως της ηθικής τάξης.

Στο ηλεκτρονικό εμπόριο αυτά τα θέματα γίνονται πολύπλοκα λόγω του ότι ένα ή περισσότερα από τα μέλη που εμπλέκονται σε τέτοιου είδους εμπορικές δραστηριότητες – οι χρήστες του Internet, οι παροχείς υπηρεσιών και περιεχομένου, οι αγοραστές, οι πωλητές, οι επιχειρήσεις και τα περιουσιακά στοιχεία τους, τα τεχνολογικά συστήματα και οι servers – πολύ συχνά βρίσκονται σε διαφορετικές χώρες. Έτσι, δεν δημιουργείτε απλώς αβεβαιότητα όσον αφορά στο πού πραγματοποιούνται οι σχετικές δραστηριότητες, αλλά και οι ίδιες οι δραστηριότητες ενδέχεται να έχουν σκόπιμες ή αθέλητες συνέπειες σε ολόκληρη την υφήλιο, με αποτέλεσμα μία ακόμα μεγαλύτερη αβεβαιότητα όταν έρχεται η στιγμή να προσδιοριστεί το αρμόδιο δικαστήριο και ο εφαρμόσιμος νόμος ή να εκτελεστεί κάποια απόφαση δικαστηρίου.

Στο γενικότερο διεθνές πλαίσιο, τα θέματα της δικαιοδοσίας, του εφαρμόσιμου νόμου, της αναγνώρισης και της επιβολής των αποφάσεων ξένων χωρών μέχρι στιγμής αντιμετωπίζονται με παραπομπή στο ιδιωτικό διεθνές δίκαιο. Κατά κανόνα, κάθε χώρα ψηφίζει τους δικούς της κανόνες ιδιωτικού διεθνούς δικαίου. Παρ' όλο που σε κάποιες περιοχές του κόσμου ορισμένοι από αυτούς τους κανόνες έχουν εναρμονιστεί βάσει συνθηκών, η γενική εικόνα εξακολουθεί να παρουσιάζει μια ανομοιογενή συρραφή πολύπλοκων διατάξεων.

Στο γενικότερο πλαίσιο του ηλεκτρονικού εμπορίου, ο στόχος της αποτελεσματικής επίλυσης των διαφορών δεν εξυπηρετείται από ένα τέτοιο περιβάλλον.

Τον Ιούνιο του 1997, στη Συνδιάσκεψη της Χάγης για το Ιδιωτικό Διεθνές Δίκαιο, συστήθηκε ειδική επιτροπή για να μελετήσει τη διεθνή δικαιοδοσία και την ισχύ των δικαστικών αποφάσεων ξένων χωρών σε ό,τι αφορά το Αστικό και Εμπορικό Δίκαιο. Έπειτα από μία σειρά συναντήσεων, η ειδική επιτροπή ανέπτυξε ένα 'Προκαταρκτικό Σχέδιο Συνθήκης για τη Δικαιοδοσία και τις Αποφάσεις Ξένων Χωρών σε θέματα Αστικού και Εμπορικού Δικαίου'. Ο στόχος της σχεδιαζόμενης συνθήκης είναι διττός: Πρώτον, να εναρμονιστούν οι νόμοι περί δικαιοδοσίας και να περιοριστούν τα δικαστήρια στα οποία είναι δυνατόν να εγείρονται οι σχετικές αγωγές, ώστε να αποφεύγονται άσκοπες πολλαπλές διώξεις αλλά και η πιθανότητα αλληλοσυγκρουόμενων αποφάσεων. Δεύτερον, να απλοποιηθούν τόσο η αναγνώριση όσο και η επιβολή των αποφάσεων που είναι σύμφωνες με όσα προβλέπει η συνθήκη.

Η ειδική επιτροπή, ωστόσο, ανέβαλε για αργότερα την πρόταση μέτρων για το ηλεκτρονικό εμπόριο. Μία συνάντηση ειδικών, που διοργάνωσε η καναδική κυβέρνηση, συνήλθε τον Φεβρουάριο του 2000 στην Οτάβα, για να συζητηθούν τα θέματα του ηλεκτρονικού εμπορίου και της διεθνούς δικαιοδοσίας, τα αποτελέσματα της οποίας λήφθηκαν υπόψη κατά τη Συνδιάσκεψη της Χάγης τον Μάιο του 2000. Και ενώ τα σχέδια προέβλεπαν ότι τα μέλη της συνδιάσκεψης θα έφερναν για επικύρωση το σχέδιο της συνθήκης σε μία διπλωματική διάσκεψη που αρχικά είχε οριστεί για το φθινόπωρο του 2000, η διάσκεψη αυτή αναβλήθηκε, προκειμένου να εκτιμηθούν πληρέστερα οι νέες εμπορικές πρακτικές του ηλεκτρονικού εμπορίου, καθώς και τα θέματα της πνευματικής ιδιοκτησίας και της δικαιοδοσίας.

Αλλά και η Ευρωπαϊκή Επιτροπή έκανε πρόσφατα μια προσπάθεια εκσυγχρονισμού και εναρμόνισης της νομοθεσίας του ιδιωτικού διεθνούς δικαίου όσον αφορά στη δικαιοδοσία, την αναγνώριση και στην επιβολή των αποφάσεων. Τον Ιούλιο του 1999 εξέδωσε μία 'Πρόταση για τη ρύθμιση θεμάτων δικαιοδοσίας και επιβολής των αποφάσεων του Αστικού και Εμπορικού Δικαίου'. Στόχος ήταν η ρύθμιση αυτή να αντικαταστήσει το Πρωτόκολλο της Συνδιάσκεψης των Βρυξελλών του 1968, προκειμένου να βελτιωθεί και να επισπευσθεί η ελεύθερη διακίνηση των αποφάσεων Αστικού και Εμπορικού Δικαίου στο εσωτερικό της ευρωπαϊκής αγοράς.

Τα συμβόλαια του ηλεκτρονικού εμπορίου θα πρέπει να συνεχίσουν να υπόκεινται στις παραδοσιακές αρχές που είναι απαραίτητες για την εγκυρότητά τους.

9.2 Copyright και συναφή δικαιώματα

Η προστασία του copyright καλύπτει μία ευρεία γκάμα της ανθρώπινης δημιουργικότητας. Μεγάλο μέρος του δημιουργικού περιεχομένου που τροφοδοτεί το ηλεκτρονικό εμπόριο υπόκειται σε τέτοιου είδους προστασία. Σύμφωνα με τη σημαντικότερη διεθνή συνθήκη για το copyright, τη Συνθήκη της Βέρνης, η προστασία του καλύπτει όλα τα 'λογοτεχνικά και καλλιτεχνικά έργα' . Αυτός ο ορισμός περικλείει διάφορες μορφές δημιουργικότητας:

Τα συγγραφικά έργα, είτε είναι φανταστικά είτε όχι. Σ' αυτά περιλαμβάνονται και τα επιστημονικά και τεχνικά κείμενα, καθώς και τα προγράμματα των υπολογιστών.

Οι βάσεις δεδομένων που θεωρούνται πρωτότυπες, λόγω του τρόπου συλλογής ή της ταξινόμησης των δεδομένων τους.

Τα μουσικά έργα.

Τα έργα ήχου και εικόνας.

Τα καλλιτεχνικά έργα, στα οποία περιλαμβάνονται τα σχέδια και οι πίνακες ζωγραφικής.

Οι φωτογραφίες.

Ως 'συναφή' χαρακτηρίζονται τα δικαιώματα των τρίτων που δημιουργούν προστιθέμενη αξία κατά την παρουσίαση των συγγραφικών και των καλλιτεχνικών έργων στο κοινό. Σ' αυτούς περιλαμβάνονται:

Οι ηθοποιοί, οι χορευτές, οι τραγουδιστές και οι μουσικοί.

Οι παραγωγοί των φωνογραφημάτων, συμπεριλαμβανομένων και των CDs .

Οι τηλεοπτικοί και ραδιοφωνικοί σταθμοί.

Η ψηφιακή τεχνολογία επιτρέπει τη μετάδοση και τη χρήση όλων αυτών των προστατευμένων υλικών σε ψηφιακή μορφή μέσω δικτύων. Μολονότι η μετάδοση κειμένου, ήχου, εικόνων και προγραμμάτων πληροφορικής μέσω του Internet είναι πλέον κοινός τόπος, σύντομα το ίδιο θα ισχύει και για τις κινηματογραφικές ταινίες, καθώς ο τεχνικός περιορισμός της ανεπάρκειας του εύρους συχνοτήτων αρχίζει να εκλείπει.

Όλα αυτά τα θέματα εξετάζονται εδώ και πολλά χρόνια, τόσο στο πλαίσιο του WIPO (World International Property Organization), που υπάγεται στα Ηνωμένα Έθνη, όσο και από άλλους διεθνείς οργανισμούς, αλλά και σε εθνικό και περιφερειακό επίπεδο. Η πρόοδος που έχει σημειωθεί είναι σημαντική και ήδη για αρκετά θέματα έχει επιτευχθεί κοινή συμφωνία μεταξύ των περισσότερων κρατών. Το 1996 υπογράφτηκαν δύο Συνθήκες στο πλαίσιο του WIPO: η WIPO Copyright Treaty (WCT) και η WIPO Performances and Phonograms Treaty (WPPT), οι οποίες αναφέρονται συνήθως ως 'Συνθήκες του Internet'. Οι συνθήκες αυτές, μολονότι δεν έχουν τεθεί ακόμα σε ισχύ, καλύπτουν θέματα όπως είναι ο ορισμός και η έκταση των δικαιωμάτων στο ψηφιακό περιβάλλον, καθώς και μία πρώτη προσέγγιση για τους τρόπους κατοχύρωσής τους.

Πολλά από τα μεγάλα προβλήματα του χώρου, ωστόσο, παραμένουν ανεπίλυτα. Ενδεικτικά αναφέρουμε τα δικαιώματα των καλλιτεχνών που λαμβάνουν μέρος σε παραστάσεις, την εξασφάλιση της αξιοπιστίας των επιχειρήσεων που παρέχουν υπηρεσίες, καθώς και θέματα του ιδιωτικού διεθνούς δικαίου, σημαντικότερο από τα οποία είναι η δικαιοδοσία των δικαστηρίων

.

9.3 Προστασία του Εμπορικού σήματος – Trade Marks

Το εμπορικό σήμα αποτελεί σημαντικό εργαλείο στο εμπόριο. Παρέχει τη δυνατότητα στους καταναλωτές να αναγνωρίζουν την πηγή ενός προϊόντος και να το συνδέουν με τον κατασκευαστή του στις διεθνείς αγορές. Το αποκλειστικό δικαίωμα χρήσης του σήματος, που μπορεί να είναι αόριστης διάρκειας, παρέχει στον κάτοχο την δυνατότητα να 'χτίσει' το όνομα και τη φήμη της, ενώ παράλληλα εμποδίζει τους τρίτους να παραπλανούν τους καταναλωτές, ώστε να συνδέουν κάποια προϊόντα με μια επιχείρηση από την οποία δεν προέρχονται στην πραγματικότητα.

Τα εμπορικά σήματα είναι ουσιαστικής σημασίας στο ηλεκτρονικό εμπόριο. Είναι πια κοινή διαπίστωση ότι στο Internet θα αποκτήσουν τουλάχιστόν όση σπουδαιότητα έχουν στον off-line κόσμο. Και στον κυβερνοχώρο οι επιχειρήσεις είναι υποχρεωμένες να χτίσουν την αναγνωρισιμότητά τους και τη φήμη τους και να εμπνεύσουν εμπιστοσύνη στο καταναλωτικό κοινό, τόσο για τις ίδιες όσο και για τα προϊόντα τους. Ιδιαίτερα όταν πρόκειται για μία εικονική αγορά, όπου οι επαφές πρόσωπο με πρόσωπο είναι σπάνιες και υπάρχουν λίγες ή και καθόλου δυνατότητες εξέτασης των προϊόντων ή υπηρεσιών πριν από την αγορά τους, οι καταναλωτές είναι πρόθυμοι να ανταμείβουν τις πηγές που εμπνέουν εμπιστοσύνη και προσφέρουν ανταγωνιστικά προϊόντα. Κάτω από αυτές τις συνθήκες, το εμπορικό σήμα μιας επιχείρησης γίνεται ζωτικής σημασίας μέσο αναγνώρισης και διάκρισης.

Όλοι συμφωνούν ότι η προστασία του εμπορικού σήματος θα πρέπει να επεκταθεί και στο Internet, καθώς και ότι δεν θα πρέπει να είναι ούτε πιο περιορισμένη ούτε εκτενέστερη αυτής που ισχύει στον φυσικό κόσμο. Τα υπάρχοντα εθνικά ή περιφερειακά νομικά συστήματα θα πρέπει να ισχύσουν κι εδώ, σε συνδυασμό με τις σχετικές διεθνείς συνθήκες. Ωστόσο οι διατάξεις αυτές είναι γενικής φύσεως, που εφαρμόζονται σε ‘εδαφική’ βάση και δεν είναι σχεδιασμένες για τον χωρίς σύνορα κόσμο του ηλεκτρονικού εμπορίου. Εξάλλου οι προκλήσεις δεν περιορίζονται στα εμπορικά σήματα, αλλά σημειώνονται σε κάθε είδους διακριτικά σήματα που χρησιμοποιούνται στο ηλεκτρονικό εμπόριο, συμπεριλαμβανομένων των εμπορικών επωνυμιών και των γεωγραφικών ενδείξεων.

Καθώς το θέμα είναι ευρύτατο και η προσέγγιση της κατοχύρωσης, της μεταβίβασής τους κ.λπ. διαφέρει από χώρα σε χώρα, η εναρμόνιση των νομοθεσιών κρίνεται μη ρεαλιστική.

Ο WIPO προσπαθεί να αντιμετωπίσει και αυτό το θέμα. Η Μόνιμη Επιτροπή (SCT), που είναι αρμόδια για θέματα της νομοθεσίας των εμπορικών σημάτων, του βιομηχανικού σχεδιασμού και των γεωγραφικών ενδείξεων, μελέτησε τη σκοπιμότητα και το κατά πόσο θα είναι επιθυμητή η εναρμόνιση των εθνικών ή περιφερειακών νόμων που αφορούν στη χρήση των εμπορικών σημάτων και άλλων διακριτικών σε ό,τι αφορά το Internet. Στη συνέχεια , το Διεθνές Γραφείο ετοίμασε και έστειλε σε όλες τις χώρες ένα ερωτηματολόγιο με υποθετικές καταστάσεις σε σχέση με τη χρήση των εμπορικών σημάτων στο Internet και τη νομική αντιμετώπισή τους. Τα αποτελέσματα αποτελούν ήδη αντικείμενο μελέτης της SCT. Παράλληλα, στο πρόγραμμα και στον προϋπολογισμό για την περίοδο 2000-2001 του WIPO περιλαμβάνεται μια μελέτη για τους τρόπους καταπολέμησης των ενεργειών αθέμιτου ανταγωνισμού στο Internet.

Όλοι συμφωνούν ότι η προστασία του εμπορικού σήματος θα πρέπει να επεκταθεί και στο Internet, καθώς και ότι δεν θα πρέπει να είναι ούτε πιο περιορισμένη ούτε εκτενέστερη αυτής που ισχύει στον φυσικό κόσμο.

Οι συνέπειες του ηλεκτρονικού εμπορίου σε ό,τι έχει σχέση με copyright , συναφή δικαιώματα, ευρεσιτεχνίες, εμπορικά σήματα και άλλα διακριτικά είναι τρομοκρατικές, ενώ όλα αυτά, με τη σειρά τους, θα επηρεάσουν την ανάπτυξη του ηλεκτρονικού εμπορίου. Αν οι σχετικές νομοθεσίες δεν αναπροσαρμοστούν και δεν παράγουν τα επιθυμητά αποτελέσματα, η ψηφιακή τεχνολογία έχει τη δυνατότητα να ενδυναμώσει τις θεμελιώδεις δομές του εμπορίου.

Αναφορές

[1] http://www.dpa.gr/
[2] http://www.euro2day.gr/articles/
[3] http://www.go-online.gr/
[4] http://www.netmode.ntua.gr/mambo/
[5] http://www.ebusinessforum.gr/
[6] http://newmedia.medill.northwestern.edu/courses/nmpspring01/brown/Revstream/ecommerceindex.htm
[7] http://ezinearticles.com/
[8] http://europa.eu/index_el.htm
[9] http://wiki.media-culture.org.au/index.php/Electronic_Commerce
[10] http://www.lawnet.gr/default.asp
[11] http://www.bambooweb.com/articles/e/l/Electronic_Commerce.html
[12] http://www.webopedia.com/
[13] http://www.cisco.com/en/US/netsol/ns340/ns394/ns50/ns140/networking_solutions_white_paper09186a0080136858.shtml
[14] http://www.iso-17799.com/
[15] http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html
[16] http://en.wikipedia.org/wiki/Main_Page
[17] David W Chadwick, "Network Firewall Technologies", IS Institute, University of Salford, England
[18] Marcus J. Ranum, "Thinking About Firewalls", Trusted Information Systems, Inc. Glenwood, Maryland.
[19] S. Hadjiefthymiades - D. Martakos, "WWW Proxies, Internet Firewalls", 1998.
[20] http://homoecumenicus.com/copyright_law24.htm