

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (Πάτρα)

*Τίτλος Εργασίας:*

## ***Ε-ΕΠΙΧΕΙΡΕΙΝ ΚΑΙ ΑΣΦΑΛΕΙΑ***

*Πτυχιακή Εργασία της Μαρίας – Χαράς Αλεξίου*

*Επιβλέπων: Δημήτριος Παπαδόπουλος*

**ΠΑΤΡΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2015**

## **Περίληψη**

Σκοπός της παρούσας εργασίας αποτελεί η ενασχόληση με το ζήτημα του ηλεκτρονικού επιχειρείν αναφορικά με το θέμα της ασφάλειας και παρουσιάζεται σε έξι κεφάλαια ως εξής: Στο πρώτο κεφάλαιο καταγράφονται τα εισαγωγικά στοιχεία της μελέτης, στο δεύτερο αναλύονται οι συνθήκες του ηλεκτρονικού εμπορίου σε σχέση με διάφορα επιστημονικά πεδία, στο τρίτο παρουσιάζονται επιχειρηματικά μοντέλα του διαδικτύου, ενώ στο τέταρτο γίνεται λόγος για την ασφάλεια συναλλαγών μέσω του διαδικτύου στον κλάδο του ηλεκτρονικού εμπορίου. Στο πέμπτο κεφάλαιο γίνεται αναφορά στους μηχανισμούς ασφαλείας και στο πρωτόκολλο SET και στο έκτο παρουσιάζεται η μελέτη περιπτώσεων δύο ηλεκτρονικών καταστημάτων και μιας τράπεζας που λειτουργούν διαδικτυακά και διαθέτουν συγκεκριμένους κανόνες ασφάλειας δεδομένων.

## **Abstract**

The present is a research that aims to explore the issue of e-business in terms of safety and has been analyzed in six chapters as follows: the first chapter presents the introductory elements of the study; the second discusses the conditions of e-commerce in relation to various scientific fields, the third chapter presents the e-business models, while the fourth describes the issue of secure online transactions in the e-commerce industry. The fifth chapter refers to the security mechanisms and the SET protocol and the sixth discusses the case study of two e-shops and a bank, that operate online and have specific data security standards.

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1 <sup>ο</sup> Εισαγωγή στη Μελέτη	7
1.1 Εισαγωγή	7
1.2 Σκοπός και στόχοι της μελέτης	7
1.3 Δομή Ανάπτυξης του Θέματος	7
Κεφάλαιο 2 <sup>ο</sup> Ηλεκτρονικό Εμπόριο	9
2.1 Ορισμός	9
2.2 Ιστορία του Ηλεκτρονικού Εμπορίου	10
2.3 Φύση των συναλλαγών στο Ηλεκτρονικό Εμπόριο	11
2.4 Αλληλεπίδραση με διάφορα επιστημονικά πεδία	14
2.5 Πλεονεκτήματα και οφέλη του Ηλεκτρονικού Εμπορίου	16
2.6 Περιορισμοί του Ηλεκτρονικού Εμπορίου	21
Κεφάλαιο 3 <sup>ο</sup> Επιχειρηματικά Μοντέλα Διαδικτύου	24
3.1 Παρουσίαση των Μοντέλων	24
3.1.1 Ηλεκτρονικό Κατάστημα (e-Shop)	24
3.1.2 Κινητό Ηλεκτρονικό Εμπόριο (m-Commerce)	25
3.1.3 Ηλεκτρονικό Επιχειρείν (e-Business)	26
3.1.4 Ηλεκτρονική Επιχείρηση (e-Enterprise)	26
3.1.5 Μεσίτες Πληροφοριών (e-Infobrokers)	27
3.1.6 Ηλεκτρονική Αγορά (e-Marketplace)	27
3.1.7 Ηλεκτρονικές Δημοπρασίες (e-Auction)	28
3.1.8 Ηλεκτρονικές Προμήθειες (e-Procurement)	28
3.1.9 Ηλεκτρονικό Εμπορικό Κέντρο (e-Mail)	29
3.2 Πλεονεκτήματα Ηλεκτρονικού Εμπορίου	29

3.2.1 Πλεονεκτήματα ως προς τον Καταναλωτή _____	29
3.2.2 Πλεονεκτήματα ως προς την Εταιρεία _____	30
3.3 Μειονεκτήματα Ηλεκτρονικού Εμπορίου _____	31
3.4 Τεχνολογία και Εφαρμογές _____	32
<b>Κεφάλαιο 4<sup>ο</sup> Ηλεκτρονικό εμπόριο και Ασφάλεια Συναλλαγών _____</b>	<b>35</b>
4.1 Ασφάλεια στο Ηλεκτρονικό Εμπόριο _____	35
4.2 Η σημασία της Ασφάλειας _____	35
4.3 Απαιτήσεις Ασφάλειας _____	36
4.4 Κίνδυνοι Ασφάλειας _____	38
4.4.1 Ιοί _____	38
4.4.2 Χάκερ _____	41
<b>Κεφάλαιο 5<sup>ο</sup> Ασφάλεια στο Διαδίκτυο- Μηχανισμοί Ασφαλείας _____</b>	<b>43</b>
5.1 Ασφάλεια Διαχείρισης Δικτύων Υπολογιστών _____	43
5.1.1 Η πιστοποίηση και αυθεντικοποίηση _____	46
5.1.2 Η διασφάλιση της εμπιστευτικότητας _____	47
5.1.3 Η διασφάλιση της ακεραιότητας _____	47
5.1.4 Η μη αποποίηση ευθύνης _____	48
5.2 Συμμετρική Κρυπτογραφία _____	48
5.2.1 Κρυπτογράφηση _____	48
5.3 Ασύμμετρη Κρυπτογραφία _____	49
5.3.1 Αλγόριθμοι κρυπτογράφησης _____	50
5.4 Ψηφιακές Υπογραφές _____	50
5.5 Διαχείριση Δημοσίων Κλειδιών _____	51
5.6 Smart Cards _____	51

5.7 Antivirus	51
5.8 Πρωτόκολλο Secure Sockets Layer	52
5.9 Κρυπτογράφηση	53
5.10 Ψηφιακοί φάκελοι	56
5.11 Αρχές πιστοποίησης και ψηφιακά πιστοποιητικά	56
5.12. Το πρωτόκολλο SET	57
Κεφάλαιο 6 <sup>ο</sup>	59
6.1.Μελέτη περίπτωσης ηλεκτρονικού καταστήματος	59
6.2.Ηλεκτρονικό κατάστημα nail tips	59
6.2.1.Ασφάλεια δεδομένων εταιρίας	59
6.3.Ασφαλιστική εταιρία ANY TIME	62
6.3.1.Ασφάλεια Προσωπικών Δεδομένων	62
6.3.1.1 Προσωπικά Δεδομένα	62
6.3.2.Cookies	64
6.4 Μελέτη περίπτωσης τράπεζας ALPHA BANK	65
6.4.1 Πλαίσιο εφαρμογής e-banking από την ALPHA BANK	69
Κεφάλαιο 7 <sup>ο</sup> Συμπεράσματα	77
Βιβλιογραφία	78

# **Κεφάλαιο 1<sup>ο</sup> Εισαγωγή στη Μελέτη**

## **1.1 Εισαγωγή**

Στη σημερινή εποχή οι περισσότερες επιχειρήσεις χρησιμοποιούν το ηλεκτρονικό εμπόριο, διότι παρέχει τη δυνατότητα για αύξηση των κερδών (μέσω των υψηλότερων πωλήσεων ή του χαμηλότερου κόστους) και ως εκ τούτου συμβάλλει στην αύξηση της βιωσιμότητας της επιχείρησης. Τέλος, το ηλεκτρονικό εμπόριο έχει τη δυνατότητα να βελτιώσει σημαντικά την αποδοτικότητα των διαδικασιών σε όλες τις φάσεις της επιχειρησιακής αλυσίδας εφοδιασμού, ενώ μπορεί να ωφελήσει μια επιχείρηση στο σχεδιασμό του προϊόντος, την προμήθεια και διαχείριση των αποθεμάτων, την παραγωγή, το μάρκετινγκ, τις πωλήσεις και τη διανομή των πελατών και των υπηρεσιών. Η παρούσα μελέτη συγκεκριμένα θα εστιάσει στο ηλεκτρονικό επιχειρείν σε σχέση με την ασφάλεια.

## **1.2 Σκοπός και στόχοι της μελέτης**

Σκοπός της μελέτης είναι να αναλύσει τις διαδικτυακές τεχνολογίες που έχουν αναπτύξει οι επιχειρήσεις με στόχο να εστιάσει στο πόσο ασφαλείς μπορούν να είναι οι επιχειρήσεις μέσα από τη χρήση της τεχνολογίας. Επιμέρους στόχος είναι η διερεύνηση του κλάδου του ηλεκτρονικού εμπορίου αλλά και η προβολή των συστημάτων ασφαλείας.

## **1.3 Δομή Ανάπτυξης του Θέματος**

Η παρούσα μελέτη πρόκειται να ολοκληρωθεί μέσα από έξι κεφάλαια, όπου πιο αναλυτικά, αρχικά θα παρουσιαστούν εισαγωγικά στοιχεία αναφορικά με το τι θα επακολουθήσει στην εργασία, στη συνέχεια θα εντοπιστούν τα δεδομένα αναφορικά με το ηλεκτρονικό εμπόριο αλλά και τα ηλεκτρονικά επιχειρηματικά μοντέλα. Αργότερα θα ακολουθήσει η ανάπτυξη για στοιχεία που αναφέρονται στην ασφάλεια

αναφορικά με ηλεκτρονικές συναλλαγές στο τομέα του ηλεκτρονικού εμπορίου. Έπειτα θα καταγραφούν οι μηχανισμοί ασφαλείας και τέλος θα ακολουθήσει η μελέτη περίπτωσης ηλεκτρονικών καταστημάτων με διαδικτυακή λειτουργία. Η εργασία θα ολοκληρωθεί με τα συμπεράσματα που θα προκύψουν.



## Κεφάλαιο 2<sup>ο</sup> Ηλεκτρονικό Εμπόριο

### 2.1 Ορισμός

Το ηλεκτρονικό εμπόριο είναι μια δραστηριότητα που ασχολείται άμεσα με το εμπόριο αγαθών και υπηρεσιών και με άλλες σχετικές επιχειρηματικές δραστηριότητες, στις οποίες το μέσο ηλεκτρονικής επικοινωνίας διαδραματίζει κεντρικό ρόλο. Οι δραστηριότητες αυτές περιλαμβάνουν την επικοινωνία των πληροφοριών, τη διαχείριση των πληρωμών, τη διαπραγμάτευση και την εμπορία των χρηματοπιστωτικών μέσων, καθώς και τη διαχείριση των μεταφορών. Ως οικονομική δραστηριότητα, το ηλεκτρονικό εμπόριο αποτελεί μια ενδοεπικοινωνία των φυσικών, ανθρώπινων και κοινωνικών πόρων.

Το ηλεκτρονικό εμπόριο συνδέεται συνήθως με την αγορά και την πώληση μέσω του Διαδικτύου, ή τη διεύθυνση οποιασδήποτε συναλλαγής που περιλαμβάνει τη μεταφορά της ιδιοκτησίας ή των δικαιωμάτων στα αγαθά χρήσης ή τις υπηρεσίες και πραγματοποιείται εξ αποστάσεως μέσω ενός υπολογιστή και της χρήσης του Διαδικτύου. Αν και δημοφιλής, αυτός ο ορισμός δεν είναι αρκετά περιεκτικός για να συλλάβει τις πρόσφατες εξελίξεις σε αυτό το νέο και επαναστατικό επιχειρησιακό φαινόμενο. Ένας πληρέστερος ορισμός είναι ο εξής:

Το ηλεκτρονικό εμπόριο είναι η χρήση των ηλεκτρονικών επικοινωνιών και της ψηφιακής τεχνολογίας επεξεργασίας πληροφοριών στις επιχειρησιακές συναλλαγές που δημιουργούν, που μετασχηματίζουν και που επαναπροσδιορίζουν τις σχέσεις για τη δημιουργία αξίας μεταξύ των οργανώσεων και μεταξύ των οργανώσεων και των ατόμων.

## 2.2 Ιστορία του Ηλεκτρονικού Εμπορίου

Στη δεκαετία του '70 μια πρώτη μορφή ηλεκτρονικού εμπορίου αναφέρεται στην μεταφορά ηλεκτρονικών στοιχείων προκειμένου να σταλούν επιχειρησιακά έγγραφα όπως π.χ. οι εντολές αγοράς καθώς και για τη μεταφορά κεφαλαίων. Ωστόσο, οι αιτήσεις περιορίζονταν στις μεγάλες εταιρίες και σε λίγες τολμηρές μικρές επιχειρήσεις. Κατόπιν ήρθε η ηλεκτρονική ανταλλαγή δεδομένων (EDI), μια τεχνολογία που χρησιμοποιήθηκε στα ηλεκτρονικά στερεότυπα έγγραφα μεταφοράς, τα οποία επέκτειναν τις ηλεκτρονικές μεταφορές από τις οικονομικές συναλλαγές σε άλλους τύπους επεξεργασιών κατά την δεσοληψία.

Το EDI διεύρυνε την ομάδα των συμμετεχουσών επιχειρήσεων από τα οικονομικά όργανα στους κατασκευαστές, τους λιανοπωλητές, τις υπηρεσίες καθώς και πολλούς άλλους τύπους επιχειρήσεων. Τέτοια συστήματα αποτέλεσαν οι εφαρμογές συστημάτων (IOS) και η στρατηγική αξία τους στις επιχειρήσεις έχει αναγνωριστεί ευρέως. Περισσότερες νέες εφαρμογές ηλεκτρονικού εμπορίου ακολούθησαν, κυμαινόμενος από τα συστήματα κρατήσεων ταξιδιού ως τις εμπορικές συναλλαγές αποθεμάτων.

Το Διαδίκτυο άρχισε τη ζωή σαν ένα πείραμα από την κυβέρνηση των ΗΠΑ το 1969 και οι αρχικοί χρήστες του ήταν κατά ένα μεγάλο μέρος ένα τεχνικό ακροατήριο των κυβερνητικών αντιπροσωπειών και των ακαδημαϊκών ερευνητών και επιστημόνων. Όταν το Διαδίκτυο εμπορευματοποιήθηκε και οι χρήστες άρχισαν να συμμετέχουν στο World Wide Web στις αρχές του 1990, αναπτύχθηκε ο όρος ηλεκτρονικό εμπόριο. Ένας μεγάλος αριθμός αποκαλούμενος dot-coms, ή Internet start-ups (που αποτέλεσαν τα ξεκινήματα του Διαδικτύου) εμφανίστηκαν επίσης.

Ένας λόγος για αυτήν την γρήγορη επέκταση ήταν η ανάπτυξη των νέων δικτύων, των πρωτοκόλλων και του λογισμικού ηλεκτρονικού εμπορίου. Ο άλλος λόγος ήταν η αύξηση του ανταγωνισμού και άλλων επιχειρησιακών πιέσεων.

Από το 1995 και μετά οι χρήστες του Διαδικτύου έχουν αξιοποιήσει την ανάπτυξη πολλών καινοτόμων εφαρμογών, που κυμαίνονται από τις σε απευθείας σύνδεση άμεσες πωλήσεις ως την εξ αποστάσεως εμπειρία. Σχεδόν κάθε μέση και μεγάλου μεγέθους οργάνωση στον κόσμο έχει τώρα έναν ιστοχώρο σε όλο τον κόσμο

και ιδιαίτερα στις ΗΠΑ. Οι εταιρίες έχουν τις περιεκτικές πύλες μέσω των οποίων οι υπάλληλοι, οι επιχειρησιακοί συνεργάτες και το κοινό μπορούν να έχουν πρόσβαση στις εταιρικές πληροφορίες. Πολλές από αυτές τις περιοχές περιέχουν δεκάδες χιλιάδες από τις σελίδες και τις συνδέσεις. Το 1999, η έμφαση του ηλεκτρονικού εμπορίου μετατοπίστηκε από το B2C στο B2B, και το 2001 από το B2B στο B2E, το συνεργατικό εμπόριο, την e-κυβέρνηση και το κινητό εμπόριο.

Το 2005, τα κοινωνικά δίκτυα άρχισαν να καταλαμβάνουν ένα αρκετό κομμάτι της προσοχής, όπως λόγω χάρη οι ασύρματες εφαρμογές. Λαμβάνοντας υπόψη τη φύση της τεχνολογίας και του Διαδικτύου, το ηλεκτρονικό εμπόριο θα συνεχίσει αναμφισβήτητα να μετατοπίζεται και να αλλάζει και οι δυνατότητές του να εξελίσσονται (Athitakis, 2003, Mullaney, 2004).

## 2.3 Φύση των συναλλαγών στο Ηλεκτρονικό Εμπόριο

Υπάρχουν διάφοροι τύποι του ηλεκτρονικού εμπορίου και πολλές διαφορετικές μέθοδοι για να χαρακτηρίσει αυτά τα συμπλέγματα. Οι Ακαδημαϊκοί έχουν καθορίσει έναν αριθμό πλαισίων για την ταξινόμηση του ηλεκτρονικού εμπορίου, αλλά το καθένα θέλει να τονίσει ότι αποτελούν μια μοναδική προοπτική. Αυτοί είναι οι εξής :

- **Επιχείρηση προς Επιχείρηση (Business to Business – B2B):** Θεωρείται σήμερα ως το πιο σημαντικό τμήμα του ηλεκτρονικού εμπορίου, που αντιπροσωπεύει συναλλαγές (παροχή) αγαθών και υπηρεσιών μεταξύ επιχειρήσεων (Κατασκευαστές, προμηθευτές, διανομείς, εμπόρους λιανικής πώλησης, κλπ). Τα κύρια συστατικά αυτής της προσέγγισης είναι ηλεκτρονικές υποδομές (που εξασφαλίζει τις ελάχιστες απαιτήσεις σχετικά με την υλικοτεχνική υποστήριξη και το λειτουργικό λογισμικό) και τις ηλεκτρονικές αγορές, ή ιστοσελίδες που λειτουργούν ως εικονικοί χώροι συνάντησης, όπου οι καταναλωτές αλληλεπιδρούν με τους πλειοδότες. Ο σκοπός του B2B βρίσκει χρησιμότητα στις συναλλαγές που είναι προσανατολισμένες προς τον καταναλωτή.

- **Επιχείρηση προς Καταναλωτή (Business to Consumer – B2C):** Είναι το δεύτερο στοιχείο του ηλεκτρονικού εμπορίου, που επικεντρώνεται γύρω από το μηχανισμό που είναι σε θέση να ικανοποιήσει τα συμφέροντα και τις επιθυμίες των καταναλωτών (πώληση / αγορά αγαθών και υπηρεσιών, πληροφοριών, κλπ) μέσω του εμπορίου μεταξύ των παραγωγών και των αγοραστών. Οι κύριες αγορές είναι τα ηλεκτρονικά σε απευθείας σύνδεση χρηματοπιστωτικά μέσα λιανικής πώλησης (e-banking) σχεδιασμένο για την προσωπική χρηματοδότηση διαχείρισης και οι πλατφόρμες.
- **Καταναλωτής προς Καταναλωτή (Consumer to Consumer – C2C):** Είναι ο τύπος του εμπορίου μεταξύ των αγοραστών και των ατόμων. Ένα από τα καλύτερα παραδείγματα είναι το eBay με το σύστημα ηλεκτρονικής δημοπράτησης του.
- **Καταναλωτής προς επιχείρηση (Consumer to Business – C2B):** Σε αυτήν την περίπτωση οι καταναλωτές γνωστοποιούν μια ιδιαίτερη ανάγκη για ένα προϊόν ή μια υπηρεσία, και οι οργανώσεις ανταγωνίζονται για να παρέχουν το προϊόν ή την υπηρεσία στους καταναλωτές (ένα παράδειγμα είναι και το Priceline.com, όπου ο πελάτης ονομάζει την τιμή και οι προμηθευτές προσπαθούν να την εκπληρώσουν).
- **Ενδοεπιχειρησιακό Ηλεκτρονικό Εμπόριο (Intra – Business E-Commerce):** Σε αυτή την κατηγορία εντάσσονται όλες οι εσωτερικές οργανωτικές δραστηριότητες οι οποίες συνήθως πραγματοποιούνται σε intranets και αφορούν σε: ανταλλαγή αγαθών, υπηρεσίες ή πληροφορίες κλπ., ενώ οι δραστηριότητες αυτές μπορεί να κυμαίνονται από την πώληση, τα εταιρικά προϊόντα σε μισθωτούς μέχρι την online εκπαίδευση.
- **Μη επιχειρησιακό Ηλεκτρονικό Εμπόριο (Non Business E-Commerce):** Κοινωνικές και άλλες οργανώσεις (όχι για το κέρδος) καθώς και εκπαιδευτικά ιδρύματα χρησιμοποιούν επίσης τις εφαρμογές ηλεκτρονικού εμπορίου για τις διάφορες δραστηριότητες, όπως ο έρανος και τα πολιτικά φόρουμ. Αυτές οι οργανώσεις χρησιμοποιούν επίσης το ηλεκτρονικό εμπόριο για την εξυπηρέτηση

πελατών και για την αγορά προκειμένου να μειώσουν το κόστος και να εξασφαλίσουν την καλύτερη ταχύτητα.

- **Συνεργατικό Εμπόριο (Collaborative Commerce – CC):** Σε αυτόν τον τύπο οι επιχειρησιακοί συνεργάτες συνεργάζονται ηλεκτρονικά. Τέτοια συνεργασία εμφανίζεται συχνά μεταξύ των επιχειρησιακών συνεργατών κατά μήκος της αλυσίδας ανεφοδιασμού.
- **Κυβέρνηση προς Πολίτες (Government to Citizens – G2C):** Σε αυτήν την περίπτωση η κυβέρνηση παρέχει τις υπηρεσίες στους πολίτες της μέσω των τεχνολογιών ηλεκτρονικού εμπορίου. Οι κυβερνήσεις μπορούν να κάνουν επιχειρήσεις με άλλες κυβερνήσεις (G2G) καθώς επίσης και με τις επιχειρήσεις (G2B).
- **Κινητό Εμπόριο (Mobile Commerce – MC):** Όταν το ηλεκτρονικό εμπόριο γίνεται σε ένα ασύρματο περιβάλλον, όπως η χρησιμοποίηση των κινητών τηλεφώνων και των i-phone για να έχει πρόσβαση στο Διαδίκτυο ονομάζεται κινητό εμπόριο.

## 2.4 Αλληλεπίδραση με διάφορα επιστημονικά πεδία

Το ηλεκτρονικό εμπόριο καθώς αποτελεί ένας σχετικά καινούργιος τομέας έχει αναπτύξει θεωρητικά και επιστημονικά πεδία τα οποία βασίζονται σε διάφορες αρχές. Οι σημαντικότερες αρχές του ηλεκτρονικού εμπορίου μαζί με μερικά δείγματα των ζητημάτων αυτών είναι και τα εξής (Athitakis, 2003, Mullaney, 2004):

- Ø **Μάρκετινγκ:** Υπάρχουν διάφορα θέματα που σχετίζονται με την απευθείας σύνδεση με το ηλεκτρονικό εμπόριο όπως: τα κόστη, τα κέρδη, οι διαφημίσεις, η προώθηση προϊόντων, στρατηγικές διαφήμισης, η εμπορική διαφήμιση και τα διαλογικά περίπτερα.
- Ø **Επιστήμη Υπολογιστών:** Πολλά από τα ζητήματα στην υποδομή του ηλεκτρονικού εμπορίου όπως οι γλώσσες προγραμματισμού, πολυμέσα και δίκτυα Ηλεκτρονικών Υπολογιστών εντάσσονται στις αρχές της επιστήμης των υπολογιστών. Οι ευφυείς πράκτορες επίσης παίζουν έναν κύριο ρόλο στο ηλεκτρονικό εμπόριο.
- Ø **Συμπεριφορά Καταναλωτή και Ψυχολογία :** Η συμπεριφορά των καταναλωτών είναι το κλειδί για την επιτυχία των επιχειρήσεων απέναντι στον πελάτη καθώς και των πωλητών των επιχειρήσεων. Η σχέση μεταξύ του πολιτισμού και της καταναλωτικής τοποθέτησης στην ηλεκτρονική αγορά είναι ένα παράδειγμα του ερευνητικού ζητήματος σε αυτόν τον τομέα.
- Ø **Χρηματοδότηση:** Οι χρηματοοικονομικές αγορές και οι τράπεζες είναι ένας από τους σημαντικότερους συμμετέχοντες στο ηλεκτρονικό εμπόριο. Επίσης, οι ρυθμίσεις χρηματοδότησης είναι μέρος πολλών σε απευθείας σύνδεση συναλλαγών. Ζητήματα όπως η αξιοποίηση του Διαδικτύου ως υποκατάστατο ενός χρηματιστηρίου, διάφορες διεργασίες όπως οι αγορές μέσω πιστωτικής κάρτας, αλλά και καταπολέμηση της απάτης στις σε απευθείας σύνδεση συναλλαγές αποθεμάτων είναι ένα δείγμα των πολλών θεμάτων αυτού του πεδίου.
- Ø **Οικονομικά:** Το ηλεκτρονικό εμπόριο επηρεάζεται από τις οικονομικές δυνάμεις και ασκεί σημαντική επίδραση στις οικονομίες όλων των χωρών. Επίσης, οι θεωρίες του μικροϋπολογιστή και οι μακροοικονομίες πρέπει να εξεταστούν στον

προγραμματισμό του ηλεκτρονικού εμπορίου, καθώς επίσης και τις οικονομικές επιδράσεις του ηλεκτρονικού εμπορίου στις εταιρίες.

- Ø **Πληροφοριακά Συστήματα:** Το τμήμα συστημάτων πληροφοριών είναι συνήθως αρμόδιο για την επέκταση του ηλεκτρονικού εμπορίου. Αυτή η αρχή καλύπτει μια μεγάλη έκταση ζητημάτων: από την ανάλυση συστημάτων και την ολοκλήρωση των συστημάτων, για να μην αναφέρουμε τον προγραμματισμό, την εφαρμογή, την ασφάλεια των συναλλαγών καθώς και τα συστήματα πληρωμής, μεταξύ άλλων.
- Ø **Λογιστική και έλεγχος:** Οι διαδικασίες της υπηρεσίας διεκπεραίωσης συναλλαγών των ηλεκτρονικών συναλλαγών είναι παρόμοιος με άλλες συναλλαγές σύμφωνα με διάφορες απόψεις, αλλά διαφορετικές σε άλλες. Για παράδειγμα, οι ηλεκτρονικές συναλλαγές ελέγχου παρουσιάζουν μια πρόκληση για το επάγγελμα της λογιστικής, έτσι με αυτόν τον τρόπο διευρύνει την ανάπτυξη της μεθοδολογίας όσον αφορά τη σχέση κόστους- οφέλους.
- Ø **Διοίκηση:** Οι διεργασίες του ηλεκτρονικού εμπορίου πρέπει να διευθετούνται κατάλληλα από τις επιχειρήσεις τόσο λόγω της διεπιστημονικής φύσης του ηλεκτρονικού εμπορίου όσο επειδή η σωστή διαχείρισή τους ενδέχεται να απαιτήσει νέες προσεγγίσεις και θεωρίες για την καλύτερη λειτουργία της επιχείρησης.
- Ø **Επιχειρησιακοί Νόμοι και Ηθική:** Τα νομικά και ηθικά ζητήματα είναι εξαιρετικά σημαντικά στο ηλεκτρονικό εμπόριο, ειδικά στη σφαίρα της αγοράς. Ένας μεγάλος αριθμός νομοθετικών ζητημάτων είναι εκκρεμή και σχετίζονται με κανονισμούς που αφορούν στη διασφάλιση του απορρήτου και την πνευματική ιδιοκτησία.
- Ø **Άλλα πεδία και αρχές:** Διάφορες άλλες αρχές εμπλέκονται στις διάφορες πτυχές του ηλεκτρονικού εμπορίου σε μικρότερο βαθμό, παραδείγματος χάριν, η γλωσσολογία (μετάφραση στο διεθνές εμπόριο), η ρομποτική και η επιχειρησιακή έρευνα, η δημόσια και πολιτική διοίκηση, η στατιστική κλπ. Επίσης, το ηλεκτρονικό εμπόριο επικεντρώνεται και σε άλλους τομείς όπως: η υγειονομική

περίθαλψη, η εφαρμοσμένη μηχανική, οι επικοινωνίες, οι εκδόσεις και η ψυχαγωγία (Athitakis, 2003, Mullaney, 2004).

## 2.5 Πλεονεκτήματα και οφέλη του Ηλεκτρονικού Εμπορίου

Λίγες καινοτομίες που έχουν εφαρμοστεί περιλαμβάνουν τόσα πολλά οφέλη όπως είναι για παράδειγμα το ηλεκτρονικό εμπόριο. Ο παγκόσμιος χαρακτήρας του, η τεχνολογία, η ευκαιρία να φτάσουμε σε εκατοντάδες εκατομμύρια ανθρώπους, η διαδραστική φύση του, η ποικιλία δυνατοτήτων για τη χρήση του, η επινοητικότητα και η ταχεία ανάπτυξη της υποστήριξης των υποδομών, ιδιαίτερα του Διαδικτύου έχει οδηγήσει σε πολλά δυνητικά οφέλη για τις **επιχειρήσεις**, τους **καταναλωτές** και την **κοινωνία**. Τα οφέλη αυτά μόλις τώρα αρχίζουν να υλοποιούνται, αλλά θα αυξηθούν σημαντικά με τον τρόπο που επεκτείνεται το ηλεκτρονικό εμπόριο (Athitakis, 2003, Mullaney, 2004).

### A. Οφέλη για τις επιχειρήσεις

Πολλές επιχειρήσεις υιοθετούν ένα μοντέλο ηλεκτρονικού εμπορίου επειδή παρέχει στον ιδιοκτήτη μεγαλύτερη ευκολία από την άποψη της λειτουργίας τόσο της θέσης όσο και του χρόνου (ωράριο). Το ηλεκτρονικό εμπόριο δηλαδή μπορεί να δώσει την ευκαιρία σε έναν επιχειρηματία να αλλάξει τον τρόπο ζωής του, ο οποίος δεν θα επικεντρώνεται πια μόνο στο χώρο εργασίας. Πιο αναλυτικά, αυτή η ενισχυμένη ευελιξία επιτρέπει στους επιχειρηματίες να παραμένουν σε ισχύ και ταυτόχρονα να επωφεληθούν από την εγγύτητα με την οικογένεια, τους φίλους καθώς και την ευκαιρία για απόλαυση άλλων σημαντικών πλεονεκτημάτων.

Στις επόμενες παραγράφους θα παρουσιάσουμε εν συντομία ορισμένα ακόμη οφέλη που έχει η χρήση του ηλεκτρονικού εμπορίου, τα οποία είναι τα εξής:

**§ Παγκόσμια παρουσία:** Τα όρια του ηλεκτρονικού εμπορίου δεν εξαρτώνται από τα γεωγραφικά ή εθνικά σύνορα, αλλά από την κάλυψη των δικτύων υπολογιστών. Καθώς τα πιο σημαντικά δίκτυα έχουν παγκόσμια εμβέλεια, το ηλεκτρονικό



εμπόριο επιτρέπει ακόμη και στους μικρότερες προμηθευτές να επιτύχουν μια παγκόσμια παρουσία και να επεκτείνουν τις επιχειρήσεις σε όλο τον κόσμο. Το όφελος για τον πελάτη είναι μεγάλο καθώς είναι σε θέση να κάνει την επιλογή του σε ένα ευρύτερο πλαίσιο, δηλαδή την προσφορά όπου μπορεί να επιλέξει ανάμεσα σε όλους τους δυνητικούς προμηθευτές ενός συγκεκριμένου προϊόντος ή υπηρεσίας ανεξάρτητα από τη γεωγραφική τους θέση.

**§ Η αύξηση της ανταγωνιστικότητας / Ποιότητα υπηρεσιών:** Το ηλεκτρονικό εμπόριο επιτρέπει στους προμηθευτές να αυξήσουν την ανταγωνιστικότητα, ενώ με αυτόν τον τρόπο έρχονται πιο κοντά στους πελάτες της. Για παράδειγμα, πολλές εταιρείες χρησιμοποιούν την τεχνολογία του ηλεκτρονικού εμπορίου προκειμένου να παρέχουν την καλύτερη -πριν και μετά- πώληση, υποστήριξη, αυξάνοντας τα επίπεδα των πληροφοριών για το προϊόν π.χ. μέσω ειδικών ηλεκτρονικών καταλόγων πετυχαίνοντας έτσι μια γρήγορη ανταπόκριση στις απαιτήσεις των πελατών. Το αντίστοιχο όφελος για τον πελάτη είναι η βελτίωση της ποιότητας των αγαθών-προϊόντων.

**§ Βελτιωμένη ποιότητα των παρεχόμενων υπηρεσιών :** Η ποιότητα της υπηρεσίας καθίσταται απαραίτητη για το στοιχείο της απόκτησης και διατήρησης του πελάτη. Αυτή η ενότητα CRM (Customer Relationship Management) είναι μια εκ των ων ουκ άνευ για τη σωστή παρακολούθηση του εργαλείου εξυπηρέτησης πελατών. Τέτοιες εφαρμογές μπορεί με τη σειρά τους να αναλύσουν τη συμπεριφορά και τις ανάγκες των χρηστών, ενθαρρύνοντας έτσι **τις επιχειρήσεις να ταιριάζουν καλύτερα τους πελάτες τους** και να προσδιοριστούν οι αγορές θέσεων με βάση τη ζήτηση.

**§ Γενικά / εξατομικευμένα προϊόντα και υπηρεσίες επάρκειας:** Οι προμηθευτές μπορούν να έχουν λεπτομερή στοιχεία σχετικά με τις ανάγκες του κάθε πελάτη και να ρυθμίσουν αυτόματα τα προϊόντα και τις υπηρεσίες τους. Αυτό έχει ως αποτέλεσμα τα προϊόντα να είναι εύκολα συγκρίσιμα με εκείνα που προσφέρονται από ειδικούς, καθώς και οι τιμές στη μαζική αγορά. Ένα απλό παράδειγμα είναι ένα online κατάστημα που έχει σχεδιαστεί για μεμονωμένους αναγνώστες όπου με κάθε πρόσβασή τους μπορούν να επισημαίνουν τα στοιχεία που παρουσιάζουν

ενδιαφέρον και να αποκλείουν αυτά που ήδη έχουν διαβάσει.

- § Μικρότερες αλυσίδες διανομής / ταχύτερη απόκριση:** Το ηλεκτρονικό εμπόριο συχνά μειώνει δραστικά τις αλυσίδες διανομής. Υπάρχουν πολλά κοινά παραδείγματα εμπορευμάτων που πωλούνται απευθείας από τους παραγωγούς στους καταναλωτές, αποφεύγοντας τις ταχυδρομικές καθυστερήσεις, τις διάφορες ρυθμίσεις και τις καθυστερήσεις της διανομής. Παρά το γεγονός ότι το ηλεκτρονικό εμπόριο εδώ δεν είναι δυνατόν να καταστήσει μια άμεση διανομή πιθανή (η οποία μπορεί να ληφθεί μόνο με τη χρήση καταλόγων χειρόγραφα και παραγγελιών από το τηλέφωνο ή μέσω e-mail) ωστόσο είναι πρακτικό από άποψη τιμής και χρόνου.
- § Μείωση κόστους / τιμών:** Μια από τις σημαντικότερες συνεισφορές του ηλεκτρονικού εμπορίου είναι η μείωση του κόστους των συναλλαγών. Ενώ το κόστος μιας εμπορικής συναλλαγής που αφορά την ανθρώπινη αλληλεπίδραση μπορεί να μετρηθεί σε δολάρια, το κόστος της διεξαγωγής μιας παρόμοιας συναλλαγής ηλεκτρονικά μπορεί να είναι μερικά ευρώ. Ως εκ τούτου, ορισμένες εμπορικές διεργασίες που περιλαμβάνουν συνήθεις αλληλεπιδράσεις μπορεί να μειώσουν σημαντικά το κόστος, το οποίο μπορεί να οδηγήσει σε ουσιαστικές μειώσεις των τιμών για τους πελάτες.
- § Νέα επιχείρηση / Νέα προϊόντα και υπηρεσίες:** Εκτός από τον επαναπροσδιορισμό των αγορών για τα υπάρχοντα προϊόντα και υπηρεσίες, το ηλεκτρονικό εμπόριο προβλέπει επίσης εντελώς νέα προϊόντα και υπηρεσίες. Τέτοια παραδείγματα περιλαμβάνουν υπηρεσίες δικτύωσης, υπηρεσίες καταλόγου ή υπηρεσίες επαφών, δηλαδή την ανάπτυξη πρώτων επαφών μεταξύ των δυνητικών προμηθευτών και των πελατών καθώς και πολλούς ακόμη τύπους υπηρεσιών πληροφοριών στο διαδίκτυο. Παρά το γεγονός ότι οι ευκαιρίες και τα οφέλη είναι διαφορετικά, υπάρχουν ισχυρές αλληλεξαρτήσεις μεταξύ τους. Για παράδειγμα, η αύξηση της ανταγωνιστικότητας και της ποιότητας των υπηρεσιών μπορεί να οδηγήσει σε ένα τμήμα της μαζικής εξατομίκευσης, ενώ η μείωση αλυσίδων διανομής μπορούν να συμβάλουν στη μείωση του κόστους και των τιμών.

**§ Ενίσχυση των σχέσεων με τους πελάτες:** Πολλές επιχειρήσεις που δραστηριοποιούνται στην τουριστική βιομηχανία εξαρτώνται από το ηλεκτρονικό εμπόριο, καθώς παρέχει τρόπους για τη διατήρηση και την ενίσχυση των πελατειακών σχέσεων. Μέσα από στοχευμένες δράσεις και στρατηγικές μάρκετινγκ οι επιχειρήσεις μπορούν να προσεγγίσουν τους πελάτες, ακόμη και όταν δεν βρίσκονται στην ίδια περιοχή. Ένα τέτοιο παράδειγμα αποτελεί η Sivertson Gallery όπου στέλνει ειδοποιήσεις μέσω e-mail στους πελάτες που έχουν αγοράσει έργα τέχνης από καλλιτέχνες, ιδίως όταν προκύπτουν νέες εργασίες από αυτές που εμφανίζονται στην γκαλερί. Έτσι η σύνδεση γίνεται με το χαρακτηριστικό καλάθι αγορών του τόπου. Αυτή η άμεση επαφή μάρκετινγκ επιτρέπει στους πελάτες να αγοράσουν τα προϊόντα μετά την τουριστική περίοδο και εκτός της περιοχής. Ιδιαίτερα στην τουριστική βιομηχανία είναι πολύ ευέλικτο εργαλείο καθώς οι πελάτες μπορούν να προγραμματίσουν κάθε πτυχή του ταξιδιού τους στο διαδίκτυο, από διαδρομές στα μενού, και πριν και μετά το ταξίδι, ενώ τα e-mails παρέχουν στους πελάτες τις πληροφορίες σχετικά με το ταξίδι τους και τους ιδιοκτήτες των επιχειρήσεων με χρήσιμες πληροφορίες σχετικά για τις ανάγκες-προτιμήσεις και τις εμπειρίες των πελατών.

**§ Νέες ροές του χρήματος:** Το ηλεκτρονικό εμπόριο απαιτεί ειδικά συστήματα πληρωμών για την πραγματοποίηση των συναλλαγών. Η ηλεκτρονική τραπεζική (virtual POS) στα συστήματα πληρωμών όπως το PayPal έχει γίνει ένα σημαντικό μέρος της διαδικασίας μάρκετινγκ, ενθαρρύνοντας την κίνηση του εικονικού χρήματος και αφήνοντας στο παρασκήνιο τη χρήση των φυσικών χρημάτων.

## **B. Οφέλη για τους καταναλωτές**

Το ηλεκτρονικό εμπόριο επιτρέπει στους πελάτες να ψωνίσουν ή να κάνουν άλλες συναλλαγές 24 ώρες τη μέρα, όλη την εβδομάδα, όλο το χρόνο, από σχεδόν οποιαδήποτε γεωγραφική τοποθεσία.

**ü** Το ηλεκτρονικό εμπόριο παρέχει σε κάθε πελάτη περισσότερες επιλογές ώστε να μπορεί να επιλέξει ανάμεσα σε πολλούς πωλητές και σε πολλά άλλα

προϊόντα.

- Û Το ηλεκτρονικό εμπόριο προσφέρει συχνά στους πελάτες λιγότερο ακριβά προϊόντα και υπηρεσίες, επιτρέποντάς τους να ψωνίζουν σε πολλά μέρη, ενώ μπορούν μέσω μιας διεξαγωγής μπορούν να κάνουν γρήγορα συγκρίσεις με πολλά άλλα προϊόντα και διαφορετικές τιμές.
- Û Σε ορισμένες περιπτώσεις, ειδικά με τα ψηφιακά προϊόντα το ηλεκτρονικό εμπόριο επιτρέπει τη γρήγορα αποστολή-παράδοση των προϊόντων.
- Û Οι πελάτες μπορούν να λάβουν σχετικές και λεπτομερείς πληροφορίες σε δευτερόλεπτα, αντί ημέρες ή εβδομάδες, όπως γινόταν παλαιότερα.
- Û Το ηλεκτρονικό εμπόριο καθιστά εύκολη τη συμμετοχή σε εικονικές δημοπρασίες.
- Û Το ηλεκτρονικό εμπόριο επιτρέπει στους πελάτες να αλληλεπιδράσουν με άλλους πελάτες σε ηλεκτρονικές κοινότητες και να ανταλλάξουν ιδέες, καθώς και να συγκρίνουν τις εμπειρίες τους.
- Û Το ηλεκτρονικό εμπόριο διευκολύνει τον ανταγωνισμό, ο οποίος οδηγεί σε σημαντικές εκπτώσεις.

### **Γ. Οφέλη για την κοινωνία**

- Û Το ηλεκτρονικό εμπόριο επιτρέπει σε περισσότερα άτομα να εργάζονται στο σπίτι και να κάνουν λιγότερα ταξίδια για ψώνια, με συνέπεια τη λιγότερη κίνηση στους δρόμους και λιγότερη έκθεση σε ατμοσφαιρική ρύπανση.
- Û Το ηλεκτρονικό εμπόριο επιτρέπει σε ορισμένα εμπορεύματα να πωληθούν σε χαμηλότερες τιμές, έτσι οι λιγότεροι εύποροι άνθρωποι μπορούν να αγοράσουν περισσότεροι και να αυξήσουν το βιοτικό επίπεδό τους.
- Û Το ηλεκτρονικό εμπόριο επιτρέπει στους ανθρώπους στις χώρες του τρίτου κόσμου και τις αγροτικές περιοχές να απολαύσουν τα προϊόντα και τις υπηρεσίες που διαφορετικά δεν θα μπορούσαν να είναι διαθέσιμα σε αυτούς.

- Το ηλεκτρονικό εμπόριο διευκολύνει την παροχή δημόσιων υπηρεσιών, όπως η υγειονομική περίθαλψη, η εκπαίδευση, και η διανομή των κυβερνητικών κοινωνικών υπηρεσιών με μειωμένο κόστος ή/και βελτιωμένη ποιότητα. Οι υπηρεσίες υγειονομικής περίθαλψης, π.χ., μπορούν να φθάσουν στους ασθενείς στις αγροτικές περιοχές.

## 2.6 Περιορισμοί του Ηλεκτρονικού Εμπορίου

Οι περιορισμοί του ηλεκτρονικού εμπορίου μπορούν να ομαδοποιηθούν σε δύο κατηγορίες οι οποίες είναι οι ακόλουθες (Athitakis, 2003, Mullaney, 2004):

- A) Οι τεχνικοί περιορισμοί
- B) Οι μη τεχνικοί τεχνικοί περιορισμοί

### A) Οι τεχνικοί περιορισμοί:

- Υπάρχει έλλειψη παγκόσμιων προτύπων για την ποιότητα, την ασφάλεια και την αξιοπιστία.
- Δεν υπάρχει επαρκές εύρος ζώνης τηλεπικοινωνιών, ιδιαίτερα για το κινητό εμπόριο (m-commerce)
- Τα εργαλεία ανάπτυξης λογισμικού συνεχίζουν να εξελίσσονται και να αλλάζουν πολύ γρήγορα.
- Είναι δύσκολο να ενσωματωθούν το Internet στο λογισμικό του ηλεκτρονικού εμπορίου με τις υπάρχουσες εφαρμογές και βάσεις δεδομένων.
- Οι πωλητές ενδέχεται να χρειάζονται ειδικούς διακομιστές Web και άλλες υποδομές εκτός από εξυπηρετητές δικτύου.
- Ορισμένα λογισμικά του ηλεκτρονικού εμπορίου δεν μπορούν να ταιριάζουν με κάποιο υλικό ή μπορεί να είναι ασύμβατα με ορισμένα λειτουργικά συστήματα
- Η προσβασιμότητα στο Διαδίκτυο εξακολουθεί να κοστίζει ακριβά ή να μην

είναι εξυπηρετική για ορισμένους δυνητικούς καταναλωτές

- Ø Καθώς ο χρόνος θα περνά προβλέπεται ότι αυτοί οι περιορισμοί θα μειωθούν ή θα ξεπεραστούν στο μέλλον, ωστόσο χρειάζεται από σήμερα ένας κατάλληλος σχεδιασμός ούτως ώστε να ελαχιστοποιηθούν οι επιπτώσεις τους.

## **B) Οι μη τεχνικοί περιορισμοί:**

Με βάση έρευνα που έχει πραγματοποιηθεί από το Internetweek, οι βασικότεροι μη τεχνικοί περιορισμοί που επιβραδύνουν την εξάπλωση του ηλεκτρονικού εμπορίου είναι οι εξής:

- Ø Ένα σημαντικό μειονέκτημα του ηλεκτρονικού εμπορίου είναι ότι το Διαδίκτυο δεν έχει ακόμη αγγίξει τις ζωές πολλών ανθρώπων, τόσο λόγω της έλλειψης γνώσης ή εμπιστοσύνης.
- Ø Η έλλειψη ασφάλειας και ο κίνδυνος παραβίασης του ιδιωτικού απορρήτου προκαλεί μεγάλη ανησυχία στους πελάτες.
- Ø Η έλλειψη εμπιστοσύνης στη χρήση του ηλεκτρονικού εμπορίου και στους άγνωστους πωλητές εμποδίζει την διεύρυνση της αγοράς.
- Ø Οι άνθρωποι δεν εμπιστεύονται ακόμη επαρκώς την εικονική, απρόσωπη διαδικασία συναλλαγής.
- Ø Σε κάποιες περιπτώσεις η online παραγγελία δεν επιτρέπει τη δυνατότητα στον καταναλωτή να αγγίξει και να δει από κοντά το προϊόν, έτσι σε περίπτωση που αυτό είναι ελαττωματικό καθώς έχει καταβάλλει εκ των προτέρων το χρηματικό ποσό δεν μπορεί να το πάρει πίσω και να επιστρέψει την παραγγελία.
- Ø Ένας μεγάλος αριθμός των ατόμων δεν χρησιμοποιούν το Διαδίκτυο σε οποιοδήποτε τύπο των χρηματοπιστωτικών συναλλαγών.
- Ø Πολλοί άνθρωποι έχουν επιφυλάξεις σχετικά με την απαίτηση να αποκαλύπτουν προσωπικές πληροφορίες που ζητούνται (όνομα, αριθμός

ταυτότητας, αριθμός λογαριασμού κλπ).

- Ø Πολλές φορές η νομιμότητα και η αυθεντικότητα των διάφορων sites με λογισμικό ηλεκτρονικού εμπορίου έχουν αμφισβητηθεί.
- Ø Ένας άλλος περιορισμός του ηλεκτρονικού εμπορίου είναι ότι δεν είναι κατάλληλο για ευπαθή προϊόντα, όπως είναι τα τρόφιμα.
- Ø Οι άνθρωποι προτιμούν να ψωνίζουν με τον συμβατικό τρόπο παρά με τη χρήση του ηλεκτρονικού εμπορίου για την αγορά τροφίμων. Έτσι, το ηλεκτρονικό εμπόριο δεν είναι κατάλληλο για τους τομείς δραστηριότητας, όπως αυτό.
- Ø Η χρονική περίοδος που απαιτείται για τη μεταφορά των υλικών προϊόντων μπορεί επίσης να είναι πολύ σημαντική (μερικές φορές) στην περίπτωση του ηλεκτρονικού εμπορίου.
- Ø Πολλά τηλεφωνήματα και e-mail μπορεί να απαιτείται προκειμένου να ληφθούν τα επιθυμητά προϊόντα (Whitman & Mattord, 2011).

## Κεφάλαιο 3<sup>ο</sup> Επιχειρηματικά Μοντέλα Διαδικτύου

### 3.1 Παρουσίαση των Μοντέλων

Τα επιχειρηματικά μοντέλα είναι ένα κομμάτι του διαδικτύου το οποίο έχει μελετηθεί σε ευρεία βάση και έχει τραβήξει το ενδιαφέρον πολλών μελετητών. Σήμερα υπάρχει τόσο πολλή συζήτηση για το πώς το διαδίκτυο αλλάζει τα παραδοσιακά επιχειρηματικά μοντέλα, αλλά υπάρχει μικρή ξεκάθαρη απόδειξη για το τι ακριβώς σημαίνει αυτό.

Στην πιο βασική έννοια του όρου, ένα επιχειρηματικό μοντέλο είναι η μέθοδος της επιχειρηματικής δραστηριότητας με την οποία μια εταιρεία μπορεί να διατηρηθεί η ίδια - δηλαδή, τη δημιουργία εσόδων. Το επιχειρηματικό μοντέλο εξηγεί πώς μια εταιρεία παράγει χρήματα με τον καθορισμό όπου τοποθετείται στην αλυσίδα αξίας.

Το Διαδικτυακό εμπόριο θα οδηγήσει σε νέα είδη επιχειρηματικών μοντέλων, αυτό είναι βέβαιο. Οι δημοπρασίες είναι ένα τέλειο παράδειγμα. Μία από τις παλαιότερες μορφές της διαμεσολάβησης, οι πλειστηριασμοί έχουν χρησιμοποιηθεί ευρέως σε όλο τον κόσμο για τη ρύθμιση των τιμών για τα εν λόγω στοιχεία ως γεωργικά προϊόντα, τα χρηματοπιστωτικά μέσα και μοναδικά αντικείμενα, όπως η λεπτή τέχνη και οι αρχαιότητες. Το internet διέδωσε το χρήσιμο εργαλείο της δημοπρασίας και διεύρυνε τις εφαρμογές του σε ένα ευρύ φάσμα προϊόντων και υπηρεσιών. Οι βασικές κατηγορίες των επιχειρηματικών μοντέλων που θα αναλυθούν στις επόμενες παραγράφους περιλαμβάνουν τα εξής (Athitakis, 2003, Mullaney, 2004):

#### 3.1.1 Ηλεκτρονικό Κατάστημα (e-Shop)

Ένα ηλεκτρονικό κατάστημα είναι μια online επιχείρηση που πωλεί μια ποικιλία προϊόντων και υπηρεσιών. Τα ηλεκτρονικά καταστήματα έχουν τον προσανατολισμό της λογικής της συναλλαγής των επιχειρήσεων προς τους καταναλωτές.



Είναι ακριβώς όπως ένα κατάστημα λιανικής πώλησης, αλλά αντί να έχει μια φυσική θέση η θέση του είναι εικονική (δηλ. το διαδίκτυο). Ο τρόπος με τον οποίο λειτουργεί ένα ηλεκτρονικό κατάστημα όταν το επισκέπτονται οι πελάτες για πρώτη φορά είναι να περιηγηθούν στον κατάλογο του καταστήματος και στην αναζήτηση για τα αγαθά που ψάχνουν όπου μετά προσθέτουν τα προϊόντα στο καλάθι αγορών τους. Με αυτόν τον τρόπο μπορούν να διαχειρίζονται το καλάθι αγορών τους με την προσθήκη ή αφαίρεση προϊόντων οποιαδήποτε στιγμή πριν ολοκληρώσουν την αγορά.

Τα οφέλη ενός ηλεκτρονικού καταστήματος είναι ότι οι πελάτες μπορούν να ψωνίσουν όποια στιγμή θέλουν χωρίς να χρειάζεται να πάνε απευθείας στο κάθε κατάστημα (από το σπίτι τους), ενώ μετατρέπει την εμπειρία αγορών για τον πελάτη σε μια τόσο εύκολη και ελκυστική διαδικασία, όπως θα ήταν αν ψώνιζε σε ένα κανονικό κατάστημα λιανικής πώλησης (Athitakis, 2003, Mullaney, 2004).

### **3.1.2 Κινητό Ηλεκτρονικό Εμπόριο (m-Commerce)**

Το κινητό ηλεκτρονικό εμπόριο δύναται να χαρακτηριστεί κατά κάποιον τρόπο υποκατηγορία του e-commerce. Το όνομα «κινητό εμπόριο» προκύπτει από την κινητή φύση του ασύρματου περιβάλλοντος που υποστηρίζει τις κινητές ηλεκτρονικές επιχειρησιακές συναλλαγές. Συσκευές, συμπεριλαμβανομένων της ψηφιακών κινητών τηλεφώνων, τους προσωπικούς ψηφιακούς βοηθούς (PDA), τα λάπτοπ, ακόμη και τάμπλετ μπορούν να έχουν πρόσβαση στο Internet ασύρματα και να αξιοποιήσουν διάφορες δυνατότητές του, όπως το e-mail και την περιήγηση στο Web, Το κινητό ηλεκτρονικό εμπόριο συμμερίζεται τις θεμελιώδεις αρχές των επιχειρήσεων, αλλά λειτουργεί ως ένα άλλο κανάλι μέσω του οποίου η τιμή μπορεί να προστεθεί στο ηλεκτρονικό επιχειρείν. Επίσης προβλέπει νέους τρόπους μέσω των οποίων εξελίσσονται οι ανάγκες των πελατών όπου θα μπορούσαν ενδεχομένως να ικανοποιηθούν (Athitakis, 2003, Mullaney, 2004).

### **3.1.3 Ηλεκτρονικό Επιχειρείν (e-Business)**

Το ηλεκτρονικό επιχειρείν είναι η διεξαγωγή των επιχειρήσεων στο Διαδίκτυο τόσο για την αγορά και την πώληση όσο και για την εξυπηρέτηση των πελατών και τη συνεργασία με άλλες επιχειρήσεις. Οι επιχειρήσεις σήμερα έχουν συνειδητοποιήσει ότι η παρουσίαση απλά ιστοσελίδων για τους πελάτες, τους εργαζόμενους και τους εταίρους δεν αποτελεί ένα ηλεκτρονικό επιχειρείν. Με αυτό το μοντέλο πρέπει να δημιουργηθεί μια φήμη, όπως έχει κάνει η Amazon στον τομέα των βιβλιοπωλείων. Το ηλεκτρονικό επιχειρείν και η ηλεκτρονική παρουσία (Web Sites κλπ) πρέπει να είναι καινοτόμες, να προσθέτουν αξία και να παρέχουν χρήσιμες πληροφορίες. Με λίγα λόγια, η περιοχή πρέπει να οικοδομήσει μια αίσθηση της κοινότητας και της συνεργασίας όπου τελικά να γίνει το «λιμάνι» της εισόδου για τις επιχειρήσεις. Η κατανόηση για το ηλεκτρονικό επιχειρείν αρχίζει με την κατανόηση των εξής όρων:

- Αποδιοργανωτική τεχνολογία
- Εξέλιξη του Διαδικτύου
- Πρόσβαση σε πληροφορίες στο Διαδίκτυο.
- Παροχή πληροφοριών στο Διαδίκτυο

### **3.1.4 Ηλεκτρονική Επιχείρηση (e-Enterprise)**

Με βάση τη σημασία δυο κατηγοριών ηλεκτρονικού εμπορίου (Ηλεκτρονικό εμπόριο Επιχείρησης προς Καταναλωτή και Ηλεκτρονικό εμπόριο Επιχείρησης προς Επιχείρηση) και την ένταξή τους στο γενικό επιχειρηματικό πλαίσιο ορισμένων εταιρειών, μπορούμε να δούμε ότι υπάρχει μια κοινή κατεύθυνση μεταξύ των εταιρειών. Έτσι, αυτές οι εταιρείες χρησιμοποιούν την τεχνολογία για δραστηριοποιηθούν καλύτερα.

Σήμερα, μια νέα γενιά μηχανικής διαδικασίας έχει αρχίσει. Με την εμφάνιση του World Wide Web και διαφόρων προτύπων όπως η ανοικτή αγορά στο διαδίκτυο, η ασφάλεια των ηλεκτρονικών συναλλαγών κλπ, οι διαχειριστές αρχίζουν να

στρέφουν την προσοχή τους στη μηχανική και τον ανασχεδιασμό προς τα έξω επιχειρηματικών διαδικασιών για να ενώσουν τους αγοραστές, τους προμηθευτές και τους εμπορικούς εταίρους σε μια δυναμική συνεργασία και ανταλλαγή πληροφοριών σε πραγματικό χρόνο. Το αποτέλεσμα είναι μια θεμελιώδης αλλαγή στο επίκεντρο των επιχειρήσεων από τη βελτίωση των εσωτερικών διαδικασιών και στρατηγικών για τον επαναπροσανατολισμό του πυρήνα της επιχείρησης προς τα έξω με τους επιχειρηματικούς εταίρους (Whitman & Mattord, 2011).

### **3.1.5 Μεσίτες Πληροφοριών (e-Infobrokers)**

Ένας μεσίτης πληροφοριών για τις εφαρμογές του ηλεκτρονικού εμπορίου γίνεται κατανοητός ως ένας μεσάζων (ένα ηλεκτρονικό σύστημα) που συλλέγει τις πληροφορίες για προϊόντα από διάφορες πηγές και στη συνέχεια αυτός τις παρουσιάζει στους πελάτες σύμφωνα με τα μεμονωμένα σχεδιαγράμματά τους. Μια επιχείρηση που διαθέτει το σύστημα e-Infobrokers επιδιώκει να παρέχει στους πελάτες της όχι μόνο ένα προϊόν ή μια υπηρεσία που εκπληρώνει μια εκφρασμένη ανάγκη των πελατών, αλλά ένα σύνολο προϊόντων και υπηρεσιών που καλύπτουν ολόκληρη τη σειρά των προβλημάτων σχετικά το συγκεκριμένο ζήτημα που υποβάλλεται από τον πελάτη. Οι υπηρεσίες των Infobrokers είναι πολύ δημοφιλείς στο εξωτερικό τόσο από μικρές όσο και από μεσαίες και μεγάλες επιχειρήσεις οι οποίες επιδιώκουν να δραστηριοποιηθούν στο διεθνές εμπορικό και επιχειρηματικό περιβάλλον μέσω αυτού του μοντέλου και τις πολλαπλές δυνατότητες που προσφέρει σήμερα το διαδίκτυο σε ιδιώτες και επιχειρήσεις.

### **3.1.6 Ηλεκτρονική Αγορά (e-Marketplace)**

Μια ηλεκτρονική αγορά μπορεί να περιγραφεί ως μια διαδικτυακή πλατφόρμα B2B που παρέχει μια διαδικτυακή λύση που στοχεύει στη διευκόλυνση της ανάπτυξης νέων εμπορικών σχέσεων μεταξύ πελατών -προμηθευτών. Οι ηλεκτρονικές αγορές μπορεί να αντιπροσωπεύουν έναν πιο αποτελεσματικό και λιγότερο δαπανηρό τρόπο για την πώληση προϊόντων ή την παροχή υπηρεσιών σε

παγκόσμιο επίπεδο, χωρίς γεωγραφικούς φραγμούς. Αυτό το ηλεκτρονικό μοντέλο συμβάλλει στην αναμόρφωση των σχέσεων μεταξύ αγοραστή-πωλητή, βελτιώνει της επιχειρηματικές διαδικασίες και επιπλέον βοηθά στην πρόσβαση σε νέες αγορές ή τμήματα μέσω του διαδικτύου (Athitakis, 2003, Mullaney, 2004).

### **3.1.7 Ηλεκτρονικές Δημοπρασίες (e-Auction)**

Οι ηλεκτρονικές δημοπρασίες αποτελεί μια υπηρεσία στην οποία οι χρήστες και οι συμμετέχοντες δύνανται να πουλήσουν και να προσφέρουν τα προϊόντα τους και τις υπηρεσίες τους μέσω του Internet. Στην ουσία τα e-auction αντανακλούν τις παραδοσιακές δημοπρασίες. Οι εικονικές δημοπρασίες διευκολύνουν τις σε απευθείας σύνδεση δραστηριότητες μεταξύ των αγοραστών και των πωλητών σε διαφορετικές θέσεις ή γεωγραφικές περιοχές. Οι διάφορες περιοχές δημοπρασίας παρέχουν στους χρήστες τις πλατφόρμες που τροφοδοτούνται από τους διαφορετικούς τύπους λογισμικών δημοπρασίας.

Αυτή η εφαρμογή παρέχει την ευκαιρία στον υποψήφιο αγοραστή να μπορεί να αναζητήσει προϊόντα μέσα από μια μεγάλη ποικιλία κατηγοριών (να δει αλλά και να παρουσιάσει τα δικά του), να καταθέσει τη δική του προσφορά, να έχει άμεση πρόσβαση και ενημέρωση για τις προσφορές άλλων χρηστών κλπ. Ηλεκτρονικές δημοπρασίες είναι ένα ευρέως αποδεκτό επιχειρηματικό μοντέλο, ενώ χαρακτηριστικά παραδείγματα αποτελούν το eBay, το WebStore, το eBazar κλπ.

### **3.1.8 Ηλεκτρονικές Προμήθειες (e-Procurement)**

Αυτό το μοντέλο παρέχει μια ηλεκτρονική υποβολή προσφορών για την προμήθεια αγαθών και υπηρεσιών. Οι μεγάλες εταιρείες ή δημόσιες αρχές εφαρμόζουν κάποια μορφή των ηλεκτρονικών δημόσιων συμβάσεων στο Web. Τα οφέλη είναι να υπάρχει μια ευρύτερη επιλογή των προμηθευτών που σκοπό έχει να οδηγήσει σε χαμηλότερο κόστος, καλύτερη ποιότητα, βελτίωση της παροχής υπηρεσιών και μείωση του κόστους των προμηθειών. Ο στόχος πολλών εφαρμογών ηλεκτρονικών προμηθειών είναι να συνδέσει άμεσα τους φορείς με τους καταλόγους

των προμηθευτών ώστε να μπορούν να επεξεργαστούν ολόκληρη τη συναλλαγή αγοράς σε απευθείας σύνδεση. Ένας ηλεκτρονικός κατάλογος παρουσιάζει στους πελάτες τις πληροφορίες σχετικά με τα αγαθά και τις υπηρεσίες που προσφέρονται προς πώληση αλλά και την προσφορά ή δημοπρασία στο Διαδίκτυο. Μέσω αυτού του τρόπου μπορεί ο πελάτης να διαχειριστεί μεγάλο αριθμό ατομικών στοιχείων με δυνατότητες εύκολης αναζήτησης σε ότι χρειάζεται και έτσι μπορεί γρήγορα και απλά να αγοράσει αυτό που επιθυμεί (Whitman & Mattord, 2011).

### **3.1.9 Ηλεκτρονικό Εμπορικό Κέντρο (e-Mail)**

Ένα ηλεκτρονικό εμπορικό κέντρο αποτελείται από έναν μεγάλο αριθμό ηλεκτρονικών καταστημάτων που χρησιμεύει ως πύλη μέσω της οποίας ο επισκέπτης μπορεί να έχει πρόσβαση σε αυτά τα εμπορικά καταστήματα. Ένα ηλεκτρονικό εμπορικό κέντρο μπορεί να γενικευτεί ή να ειδικευτεί ανάλογα με τα προϊόντα που προσφέρονται από τα e-shops που φιλοξενεί. Ένα τέτοιο παράδειγμα αποτελεί το ηλεκτρονικό εμπορικό κέντρο Bodensee, το οποίο προσφέρει ελεύθερη πρόσβαση σε πολλά ανεξάρτητα ηλεκτρονικά καταστήματα (Whitman & Mattord, 2011).

## **3.2 Πλεονεκτήματα Ηλεκτρονικού Εμπορίου**

### **3.2.1 Πλεονεκτήματα ως προς τον Καταναλωτή**

**§ Αγορές 24 ώρες το 24ωρο:** οι πελάτες μπορούν να έχουν πρόσβαση στα προϊόντα των καταστημάτων 24 ώρες το 24ωρο, κάθε μέρα παρέχοντας τη δυνατότητα στον κάθε καταναλωτή να κάνει συναλλαγές οποιαδήποτε ώρα επιθυμεί.

**§ Αυξημένη ευκολία:** οι πελάτες μπορούν να βρουν αυτό που ψάχνουν χωρίς να χρειάζεται να βγουν από το σπίτι τους.

**§ Μεγαλύτερη επιλογή:** οι πελάτες δεν περιορίζονται πλέον στα καταστήματα γύρω από τη γειτονιά τους (ή να διανύσουν αποστάσεις), ενώ μπορούν να κάνουν παραγγελίες ακόμη και από το εξωτερικό.

**§ Κόστος αποτελεσματικό:** ο ανταγωνισμός για μια συχνά διεθνή κλίμακα

σημαίνει ότι οι τιμές είναι φθηνότερες / πιο ανταγωνιστικές.

**§ Λεπτομέρειες προϊόντος:** μεγαλύτερο πλούτο πληροφοριών που διατίθενται στο διαδίκτυο από ό, τι μπορεί να προσφέρει ένας υπάλληλος στον πελάτη μέσα στο κατάστημα.

**§ Κριτικές πελατών:** πολλές περιοχές επιτρέπουν στους πελάτες να επανεξετάσουν τα προϊόντα ή τις υπηρεσίες που έχουν αγοράσει, αυξάνοντας την εμπιστοσύνη του αγοραστή (Whitman & Mattord, 2011).

### 3.2.2 Πλεονεκτήματα ως προς την Εταιρεία

**§ Αύξηση πωλήσεων και κερδών:** επειδή το ηλεκτρονικό εμπόριο επιτρέπει στις επιχειρήσεις να λειτουργούν 24ώρες το 24ωρο, 7ημέρες την εβδομάδα σε παγκόσμια κλίμακα, αυτό με τη σειρά του επιτρέπει στην κάθε επιχείρηση να αυξήσει τις πωλήσεις της, και με τη σειρά της τα κέρδη της.

**§ Βελτιωμένη πληροφόρηση των πελατών:** το ηλεκτρονικό εμπόριο επιτρέπει στις επιχειρήσεις να συγκεντρώνουν πληροφορίες σχετικά με τους πελάτες τους, οι οποίες μπορεί να χρησιμοποιούνται για σκοπούς μάρκετινγκ.

**§ Η μείωση του κόστους λειτουργίας:** αυτές οι δαπάνες μπορούν να μειωθούν δραστικά μέσω της αυτόματης διαδικασίας παραγγελιών. Υπάρχει επίσης η δυνατότητα της συνολικής αυτοματοποίησης μέσω της ενσωμάτωσης με το σύστημα διαχείρισης οδηγώντας έτσι στην αύξηση της γενικής παραγωγικότητας της εταιρείας.

**§ Η δυνατότητα των μικρών επιχειρήσεων να ανταγωνιστούν τις μεγάλες εταιρείες:** λόγω των λιγότερων δαπανών από τη χρήση ενός εικονικού καταστήματος οι μικρές επιχειρήσεις αντιμετωπίζουν λιγότερα εμπόδια στη διεξόδου στις αγορές που ήδη κυριαρχούνται από τις μεγάλες εταιρείες, ενώ παρέχει μεγάλη ευελιξία στην μικρή εταιρεία να αποκτήσει ένα σημαντικό πλεονέκτημα απέναντι σε άλλες επιχειρήσεις.

**§ Διεξόδου των διεθνών αγορών στις εγκαταστάσεις:** το παγκόσμιο δίκτυο δεν

περιορίζεται από σύνορα, δεν ανήκει σε κανέναν ενώ τα έξοδα για την πρόσβαση και τις δημοσιεύσεις είναι εξαιρετικά χαμηλά. Η επικοινωνία με τον πελάτη που βρίσκεται στον αντίθετο πόλο του κόσμου είναι τόσο εύκολη όσο και η επικοινωνία με κάποιον στο διπλανό δωμάτιο. Κάθε επιχειρηματίας πλέον μπορεί να πωλεί τα προϊόντα του σε οποιαδήποτε χώρα από τα μέσα του δικτυακού τόπου ενώ δεν κρίνεται επιβεβλημένη η επαφή με τις τοπικές επιχειρήσεις ή τις μεγάλες επενδύσεις (Whitman & Mattord, 2011).

### **3.3 Μειονεκτήματα Ηλεκτρονικού Εμπορίου**

**§ Θύματα Διαδικτύου:** είναι αρκετά εύκολο ένας πελάτης να πέσει θύμα απάτης ή κλοπής. Το χαμηλό κόστος πρόσβασης στο Internet και δυνατότητα διατήρησης ανωνυμίας, έχει δώσει την ευκαιρία σε διάφορα άτομα να αυξηθούν με πολύ γρήγορους ρυθμούς.

**§ Ανασφάλεια σε κωδικούς (passwords):** ο πελάτης-καταναλωτής είναι αναγκαίο να διαθέτει έναν μοναδικό κωδικό τον οποίο αφενός να διαφυλάξει σε ασφαλές μέρος και αφετέρου να μην τον έχει χρησιμοποιήσει ξανά.

**§ Επιβάρυνση στα έξοδα αποστολής:** Για τη διαδικασία παραγγελίας κάθε προϊόντος ο πελάτης-καταναλωτής υποχρεούνται να πληρώσει ένα αντίτιμο για την αποστολή του.

**§ Αμεσότητα με το αντικείμενο:** ένα εξίσου βασικό μειονέκτημα που προκύπτει από τις αγορές μέσω Internet είναι πως δεν υπάρχει αμεσότητα με το αντικείμενο που επιθυμεί να αγοράσει ο πελάτης. Η αγορά είναι εικονική με αποτέλεσμα ο πελάτης να μην έχει τη δυνατότητα να προβεί στο ηλεκτρονικό κατάστημα και να δει από κοντά τα προϊόντα.

### **3.4 Τεχνολογία και Εφαρμογές**

#### **Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)**

Είναι το πιο ευρέως διαδεδομένο πρωτόκολλο ασφάλειας που χρησιμοποιείται σήμερα. Πρόκειται ουσιαστικά για ένα πρωτόκολλο που παρέχει ένα ασφαλές κανάλι ανάμεσα σε δύο μηχανές που λειτουργούν μέσω του Internet ή ενός εσωτερικού δικτύου. Το πρωτόκολλο SSL χρησιμοποιείται συνήθως όταν ένας web browser πρέπει να συνδεθεί με ασφάλεια σε έναν web server μέσω του εγγενώς ασφαλούς Διαδικτύου (Whitman & Mattord, 2011).

#### **Έξυπνες κάρτες (Smart Cards)**

Οι έξυπνες κάρτες περιέχουν έναν μικροεπεξεργαστή (τσιπ) και είναι σε θέση όχι μόνο να αποθηκεύουν δεδομένα, αλλά έχουν και επεξεργαστική ισχύ. Έχουν πολύ μεγάλη ικανότητα αποθήκευσης. Τα δεδομένα που αποθηκεύονται μπορούν να προστατευτούν από μη εξουσιοδοτημένη πρόσβαση και παραποιήσεις. Οι έξυπνες κάρτες έχουν την ιδιότητα της πολυλειτουργικότητας. Η τεχνολογία αυτή εμφανίστηκε στις αρχές της δεκαετίας του 1980. Σήμερα οι Smart Cards έχουν τεχνολογία που προσφέρει απεριόριστες δυνατότητες χρήσης στο εμπόριο και στη δημόσια διοίκηση.

#### **Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI - Electronic Data Interchange)**

Ηλεκτρονική ανταλλαγή δεδομένων είναι η ηλεκτρονική ανταλλαγή εμπορικών πληροφοριών μέσω ενός τυποποιημένου μορφοτύπου. Πρόκειται για μια διαδικασία που επιτρέπει σε μία εταιρεία να αποστέλλει πληροφορίες σε μια άλλη εταιρεία με ηλεκτρονικά μέσα και όχι με χαρτί. Οι επιχειρηματικές οντότητες που ασκούν τη δραστηριότητά τους ηλεκτρονικά καλούνται εμπορικοί εταίροι. Πολλά επιχειρησιακά έγγραφα μπορούν να ανταλλάσσονται με χρήση του EDI, αλλά οι πιο σημαντικές λειτουργίες είναι για τα τιμολόγια και οι εντολές αγοράς. Εντούτοις, η πραγματική δύναμη του EDI είναι ότι τυποποιεί τις πληροφορίες που μεταβιβάζονται στα επιχειρησιακά έγγραφα, οι οποίες καθιστούν πιθανή μια ηλεκτρονική ανταλλαγή δίχως την ανάγκη χρήσης χαρτιού. Έτσι το EDI έχει τη δυνατότητα να ελαχιστοποιήσει ή ακόμα και να αποβάλλει τα χειρωνακτικά βήματα που συνήθως



απαιτούνταν γι' αυτήν τη μεταφορά(Furst et all, 2002).

### **Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)**

Είναι ένα ολοκληρωμένο πρωτόκολλο για τις πιστωτικές κάρτες. Δεν χρησιμοποιείται πολύ λόγω του κόστους και της πολυπλοκότητας του. Ωστόσο, αυτό έχει σχεδιαστεί για να επιτρέψει στους καταναλωτές να ψωνίζουν οπουδήποτε εύκολα και με όσο το δυνατόν μεγαλύτερη ασφάλεια με την ενσωμάτωση ψηφιακών υπογραφών, την πιστοποίηση, την κρυπτογράφηση και μια συμφωνημένη πύλη πληρωμής (στις τράπεζες). Ενώ το πρωτόκολλο SSL προστατεύει μόνο την ακεραιότητα και την ασφάλεια, το πρωτόκολλο SET μπορεί να παρέχει προστασία έναντι όλων των κινδύνων ασφαλείας (Whitman & Mattord, 2011).

### **Γραμμωτός κώδικας (Barcode)**

Ένας γραμμωτός κώδικας είναι ουσιαστικά ένας τρόπος για την κωδικοποίηση πληροφοριών σε ένα οπτικό μοτίβο που μια μηχανή μπορεί να διαβάσει. Ο συνδυασμός των μαύρων και του λευκών ράβδων (στοιχεία) αντιπροσωπεύει διαφορετικούς χαρακτήρες κειμένου που ακολουθεί ένα σύνολο αλγόριθμο για αυτόν τον τύπο barcode.

Το 1949, την ιδέα για το πρώτο βήμα των γραμμωτών κωδικών την είχε ο Bernard Silver, ένας μεταπτυχιακός φοιτητής με σκοπό την αυτόματη καταγραφή πληροφοριών σχετικά με ένα προϊόν. Τρία χρόνια αργότερα, ο μεταπτυχιακός φοιτητής Ιωσήφ Woodland και ο συνεργάτης του, έλαβαν το δίπλωμα ευρεσιτεχνίας για το ξεκίνημα του γραμμωτού κώδικα. Στη δεκαετία του 1960 το σύστημα αυτό εφαρμόστηκε για τη βιομηχανία τροφίμων. Στη δεκαετία του 1970 εφαρμόστηκε και στο βιομηχανικό περιβάλλον σε μεγάλες αυτοκινητοβιομηχανίες, ενώ στη δεκαετία του 1980 και μετά απέκτησε μεγάλη φήμη καθώς αναπτύχθηκε σε μεγάλο βαθμό ο εξοπλισμός του με αποτέλεσμα τη διεύρυνση των τρόπων χρήσης της τεχνολογίας του γραμμωτού κώδικα.

Το barcode εμφανίζεται πιο συχνά στην Ευρώπη (και το μεγαλύτερο μέρος του υπόλοιπου κόσμου). Είναι ένα αριθμητικό σύστημα κωδικού που χρησιμοποιείται για την αναγνώριση των προϊόντων λιανικής. Οι μοναδικούς αριθμούς EAN κατανέμεται σε κάθε ξεχωριστό προϊόν λιανικής πώλησης, όχι μόνο

από το εμπορικό σήμα του προϊόντος, αλλά με διαφοροποίηση (βάρος, χρώμα, γεύση κλπ.).

Επίσης ξεχωριστοί αριθμοί απαιτούνται όταν προκύπτουν διάφορες αλλαγές σε ένα προϊόν (εκτός από όταν μεταβληθεί η τιμή) (Furst et all, 2002).

### **Πιστοποίηση και ασφάλεια**

Οι στρατηγικές που χρησιμοποιούνται σήμερα από τις εταιρείες για την προστασία από τους κινδύνους που παραμονεύουν στο Internet αφορούν σε δύο θέματα: την προστασία της ακεραιότητας του δικτύου και των εσωτερικών συστημάτων της επιχείρησης και της επίτευξης της ασφάλειας των συναλλαγών μεταξύ του πελάτη και της επιχείρησης. Το κύριο εργαλείο που χρησιμοποιούν οι επιχειρήσεις για να προστατεύσουν το εσωτερικό τους δίκτυο είναι το τείχος προστασίας (firewall).

Ένα τείχος προστασίας είναι ένα υλικό του λογισμικό συστήματος που επιτρέπει μόνο σε εκείνους τους εσωτερικούς χρήστες με ειδικά χαρακτηριστικά να αποκτήσουν πρόσβαση στις υπάρχουσες υπηρεσίες. Το τείχος προστασίας έχει γίνει τώρα το κύριο σημείο της άμυνας και η βασική αρχιτεκτονική ασφάλειας των επιχειρήσεων.

Η κρυπτογράφηση είναι η πιο κοινή μέθοδος διασφάλισης του απορρήτου καθώς η ακεραιότητα των συναλλαγών απαιτεί μεθόδους που εμποδίζουν τις συναλλαγές από το να τροποποιηθούν με οποιονδήποτε τρόπο, κατά τη μεταφορά προς ή από τον πελάτη (Furst et all, 2002).

## **Κεφάλαιο 4<sup>ο</sup> Ηλεκτρονικό Εμπόριο και Ασφάλεια Συναλλαγών**

### **4.1 Ασφάλεια στο Ηλεκτρονικό Εμπόριο**

Τα τελευταία χρόνια έχει αναπτυχθεί ένα νέο είδος επίθεσης, το ηλεκτρονικό. Οι επιθέσεις αυτές, πραγματοποιούνται από τους βάνδαλους (vandals). Τα κίνητρα των επιθέσεων ποικίλουν. Κυρίως, στρέφονται εναντίον κυβερνητικών οργανισμών και υπηρεσιών.

Σε μια τυπική επίθεση σ' έναν δικτυακό τόπο, το αποτέλεσμα είναι αναστρέψιμο. Ο βάνδαλος θα διαγράψει ορισμένες σελίδες ή γραφικά και θα ανεβάσει τις δικές τους σελίδες, το περιεχόμενο των οποίων, μπορεί να είναι από χιουμοριστικό έως προπαγανδιστικό. Όταν ο ιδιοκτήτης του δικτυακού τόπου αντιληφθεί ότι έχει υποστεί μια τέτοια επίθεση, θα διορθώσει τις προβληματικές σελίδες από εφεδρικά αρχεία. Το κρίσιμο ζήτημα, σ' αυτή την περίπτωση, είναι ο χρόνος που θα απαιτηθεί για την επιδιόρθωση. Αν οι ζημιές που προκλήθηκαν είναι μεγάλες, ίσως να χρειαστεί ο δικτυακός τόπος να παραμείνει εκτός δικτύου για μεγάλο χρονικό διάστημα.

Το πλήγμα, που θα δεχθεί η εταιρεία, όταν ο δικτυακός της τόπος, που ομολογουμένως αποτελεί την εικόνα της προς εξωτερικούς συνεργάτες και υποψήφιους πελάτες, πέσει θύμα μιας τέτοιας επίθεσης, είναι τεράστιο (Furst et all, 2002).

### **4.2 Η σημασία της Ασφάλειας**

Η ροή πληροφοριών, που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση Πληροφοριακών Συστημάτων και διαδικτυακών εφαρμογών. Η λειτουργικότητα των οργανισμών αυτών στηρίζεται στην λειτουργία των Πληροφοριακών Συστημάτων και η ορθή και ασφαλή λειτουργία τους κρίνεται απολύτως απαραίτητη για την επίτευξη των στόχων τους. Η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται

σε κόστος. Σε συστήματα που περιέχουν ευαίσθητα δεδομένα οι επιπτώσεις δεν είναι μόνο οικονομικές αλλά ζωτικής σημασίας (Tipton & Krause, 2012).

Ενώ η χρήση Πληροφοριακών Συστημάτων είναι δεδομένη για κάθε οργανισμό η ασφάλεια τους ταυτόχρονα απειλείται. Έρευνες Παραβίασης Δεδομένων (Data Breach Investigations Report, DBIR) που ξεκίνησαν από το 2004, έδειξαν ότι στην πραγματικότητα, το 2011 μπορεί να είναι περήφανη για τα υψηλά ποσοστά απώλειας δεδομένων.

Αποτέλεσμα των παραβιάσεων και των επιθέσεων αυτών κατά των Πληροφοριακών Συστημάτων ενός οργανισμού οδηγούν στην ρήξη χαρακτηριστικών, όπως η εμπιστευτικότητα (Spears & Barki, 2010).

Η ασφάλεια των Πληροφοριακών Συστημάτων αποτελεί κομβικό σημείο για την σύγχρονη κοινωνία, Ανάμεσα στους τομείς της ασφάλειας Πληροφοριακών Συστημάτων συμπεριλαμβάνονται η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία (Peltier, 2013).

### **4.3 Απαιτήσεις Ασφάλειας**

Η ασφάλεια των Πληροφοριακών Συστημάτων είναι πολύ σημαντική καθώς στηρίζεται σε τρεις βασικές ιδέες οι οποίες είναι σημαντικές για την ορθή λειτουργία ενός Πληροφοριακού Συστήματος και είναι οι εξής (Hamlen et al., 2010):

1. Ακεραιότητα (Integrity): Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός ΠΣ σε μια γνωστή κατάσταση δίχως τροποποιήσεις.
2. Διαθεσιμότητα (Availability): Τα δεδομένα και οι υπολογιστικοί πόροι είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.
3. Εμπιστευτικότητα (Confidentiality): σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να ανακοινώνονται σε μη εξουσιοδοτημένα άτομα.

Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές, όπως (Whitman & Mattord, 2011):

1. Οι χρήστες των Πληροφοριακών Συστημάτων.
2. Η διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των ΠΣ στις λειτουργίες του οργανισμού.
3. Οι πελάτες του οργανισμού, είναι και συνιστώσα του πληροφοριακού συστήματος.
4. Το νομικό και ρυθμιστικό πλαίσιο όπου λειτουργεί ο οργανισμός.

Η πολιτική ασφάλειας για τα Πληροφοριακά Συστήματα μιας επιχείρησης έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. Η αξιολόγηση της ασφάλειας μπορεί να πραγματοποιηθεί με ποικίλους τρόπους, όπως χρήση προτύπων διαχείρισης σχετικά με την ασφάλεια. Στη συνέχεια δίνονται οι ορισμοί που για στην ανάλυση κινδύνων (Spears & Barki, 2010):

1. **Απειλή:** Ένα μη επιθυμητό γεγονός που μπορεί να προξενήσει μη διαθεσιμότητα του συστήματος
2. **Ευπάθεια:** Μια σχεδιαστική ατέλεια σε ένα σύστημα, με δυνατότητα παραβίασης της ασφάλειας του συστήματος.
3. **Κίνδυνος:** Ενδεχόμενο κινδύνου στο να εκμεταλλευτεί μια απειλή μια ευπάθεια.
4. **Αντίμετρο:** Μέτρο που εφαρμόζεται για την προστασία του Πληροφοριακού Συστήματος και την αντιμετώπιση των απειλών.

Η πολιτική ασφαλείας αφορά κάθε τεχνική και ενέργεια που περιορίζει τις ευπάθειες του πληροφοριακού συστήματος.(Whitman & Mattord, 2013)

Πρόληψη, Διασφάλιση, Ανίχνευση σε τεχνικές, επαναφορά. Για την επιτυχή εφαρμογή της πολιτικής ασφαλείας, το σχέδιο ασφαλείας πρέπει να περιλαμβάνει και συγκεκριμένες διαδικασίες συνεχούς ενημέρωσης με επισκοπήσεις - επιθεωρήσεις της εφαρμογής του, ώστε με τις κατάλληλες αναθεωρήσεις να είναι πάντα up-to-date σε σχέση με τις τεχνολογικές εξελίξεις και τις αλλαγές στην εταιρεία.

Με την πλήρωση του σχεδίου ασφαλείας της επιχείρησης, θα καταρτισθεί αναλυτικό σχέδιο έκτακτης ανάγκης. Η εισαγωγή μηχανισμών ασφαλείας σε ένα ΠΣ αποτελεί περίπλοκο έργο. Για την Ελλάδα η πιο σημαντική δυσκολία οφείλεται στο μεγάλο κόστος της ασφάλειας (Peltier, 2013).

## 4.4 Κίνδυνοι Ασφάλειας

### 4.4.1 Ιοί

Οι συγκεκριμένοι ιοί επηρεάζουν αρνητικά τον τομέα εκκίνησης ενός αποθηκευτικού μέσου ή μιας κατάτμησης (partition). Ο τομέας εκκίνησης περιέχει ένα πρόγραμμα μικρού μεγέθους το οποίο το λογισμικό εντοπίζει και «φορτώνει» στη κύρια μνήμη. Ένας ιός boot sector μπορεί επίσης να μολύνει την περιοχή MBR (Master Boot Record) που περιέχει τον πίνακα κατατμήσεων του δίσκου.

Η διαδικασία της μόλυνσης ξεκινά από τη στιγμή που ο ηλεκτρονικός υπολογιστής επιδιώκει να πραγματοποιήσει εκκίνηση από π.χ. μία μολυσμένη δισκέτα και ο ιός μετακινείται από τη δισκέτα στο σύστημα. Αφού ενεργοποιηθεί, ο ιός μολύνει όλους τους δίσκους καθώς και τις δισκέτες που θα τοποθετηθούν στον οδηγό δισκετών.

Ένας ιός boot sector με καταστροφικές παρενέργειες μπορεί να έχει ως αποτέλεσμα την αδυναμία εκκίνησης ενός συστήματος. Ένα χαρακτηριστικό παράδειγμα αποτελεί ο ιός Michelangelo. Ο συγκεκριμένος ήταν προγραμματισμένος να απενεργοποιήσει τους μολυσμένους Ηλεκτρονικούς Υπολογιστές στις 6 Μαρτίου 1992 («λογική βόμβα»).

Σε ένα άλλο παράδειγμα, ο Ιός Brain (1986) ήταν ο πρώτος που εμφάνιζε χαρακτηριστικά stealth: Σε περίπτωση που ένα πρόγραμμα antivirus εξέταζε τον τομέα εκκίνησης, ο Brain (ο οποίος ήταν «φορτωμένος» στη μνήμη – memory resident) προωθούσε το αίτημα στον αυθεντικό τομέα εκκίνησης προκειμένου να «ξεγελάσει» το λογισμικό antivirus (Wenbo, 2003).

Οι Κλασσικοί ιοί – Υβριδικοί ή πολυμερείς Ιοί (Multi-partite, ή Hybrid), είναι ιοί που συνδυάζουν χαρακτηριστικά δύο ή περισσότερων κατηγοριών. Κατά το παρελθόν, οι ιοί αυτού του τύπου συνδύαζαν χαρακτηριστικά ιών boot sector και παρασιτικών ιών.

Ένας Ηλεκτρονικός Υπολογιστής μολύνεται αν χρησιμοποιήσει μια «μολυσμένη» δισκέτα εκκίνησης ή αν εκτελέσει ένα μολυσμένο πρόγραμμα. Ο ιός αποτελείται από κώδικα που καλύπτει και τις δύο περιπτώσεις: Ανάλογα με την περίπτωση, εκτελείται το αντίστοιχο τμήμα. Το γεγονός αυτό αυξάνει τις πιθανότητες αναπαραγωγής ή/και μόλυνσης.

Για να αφαιρεθεί ο ιός από το σύστημα, θα πρέπει να αφαιρεθούν και τα δύο μέρη του, διαφορετικά το ένα μέρος μπορεί να επανενεργοποιήσει το άλλο. Μελέτη περίπτωσης: ο ιός Melissa (1999) μπορεί να θεωρηθεί ως ιός multipartite (μακρο-ιός & worm).

Όταν το «θύμα» άνοιγε το αρχείο word που λάμβανε μέσω email, ο ιός (ρόλος: μακρο-ιός) ενεργοποιούνταν και μόλυνε το πρότυπο normal.dot της εφαρμογής Word. Αυτό είχε ως συνέπεια να μολύνονται όλα τα έγγραφα .doc που θα δημιουργούσε στο μέλλον ο χρήστης.

Στη συνέχεια ο ιός έστειλε τον εαυτό του (ρόλος: worm) μέσω e-mail στις πρώτες 50 διευθύνσεις από το βιβλίο διευθύνσεων (address book) του χρήστη. Ο ιός είχε ως στόχο μια επίθεση Άρνησης Εξυπηρέτησης (DOS) στους διακομιστές αλληλογραφίας (mail servers). Ο ιός δεν μόλυνε προγράμματα (όπως οι παρασιτικοί ιοί) αλλά μόνον έγγραφα και πρότυπα (templates) (Wenbo, 2003).

Οι κλασσικοί Ιοί – Ιοί Συστήματος Αρχείων (File System), είναι τύπου Link, γνωστοί και ως Cluster, FAT, ή ιοί «file system», δεν συμπεριφέρονται όπως οι παραδοσιακοί ιοί, δηλαδή δε μολύνουν τον κώδικα εκτελέσιμων ή άλλων αρχείων. Έχουν τη δυνατότητα να παρεμβάλλονται κατά την κλήση ενός προγράμματος και να εκτελούν τον καταστρεπτικό τους κώδικα. Για να το επιτύχουν αυτό, τροποποιούν τον πίνακα FAT του Ηλεκτρονικού Υπολογιστή. Ο πίνακας FAT είναι ένας πίνακας, στο σκληρό δίσκο του Ηλεκτρονικού Υπολογιστή, όπου είναι καταχωρημένη η ακριβής θέση (διεύθυνση) του κάθε αρχείου στο δίσκο. Το Λειτουργικό Σύστημα χρησιμοποιεί τον πίνακα FAT για να οργανώσει τα αρχεία στο δίσκο, καθώς και κάθε

φορά που γίνεται κλήση ενός αρχείου. Ο ιός αλλάζει τον πίνακα διευθύνσεων ώστε όταν ζητείται η εκτέλεση του «μολυσμένου» προγράμματος X, το Λειτουργικό Σύστημα παραπέμπει στη θέση Y όπου βρίσκεται ο κώδικας του ιού, που στη συνέχεια φορτώνεται στη μνήμη και εκτελείται.

Πέρα από τις όποιες άλλες παρενέργειες, από τη θέση αυτή ο ιός έχει τη δυνατότητα να μολύνει όλα τα προγράμματα που θα εκτελεστούν στη συνέχεια από τον χρήστη. Συνήθως οι ιοί αυτής της κατηγορίας εμφανίζουν χαρακτηριστικά ιών stealth: αφού παρεμβληθούν κατά την εκτέλεση ενός προγράμματος και απελευθερώσουν το φορτίο τους, στη συνέχεια φορτώνουν και εκτελούν το νόμιμο πρόγραμμα που είχε ζητηθεί αρχικά (Μελέτη περίπτωσης: Ο ιός DIR-II) (Wenbo, 2003).

Οι Ιοί Flash Bios, αναπτύσσονται μέσα από τη διαδικασία που ακολουθούν οι κατασκευαστές μητρικών. Οι κατασκευαστές αποθηκεύουν το πρόγραμμα BIOS σε ένα ολοκληρωμένο μνήμης flash ROM. Η μνήμη αυτή είναι επανεγγράψιμη.

Οι ιοί flash BIOS επανεγγράφουν το λογισμικό BIOS στην μητρική πλακέτα. Το αποτέλεσμα της «μόλυνσης» είναι καταστρεπτικό (π.χ. διαγραφή των περιεχομένων του σκληρού δίσκου).

Ο ιός CIH ή Chernobyl αποτελεί ένα χαρακτηριστικό παράδειγμα ιού που τροποποιούσε τον κώδικα του προγράμματος BIOS. Σε μια από (τις αρκετές) εκδόσεις του ο ιός περιείχε μια «λογική βόμβα»: στις 26 Απριλίου ενεργοποιούνταν το φορτίο και δεν μπορούσε να γίνει εκκίνηση του συστήματος. Σε ορισμένες περιπτώσεις κρίθηκε απαραίτητη η αντικατάσταση του chip ή της μητρικής πλακέτας (motherboard) του συστήματος.

Οι Κλασσικοί Ιοί - Μακρο-Ιοί προσβάλλουν αρχεία δεδομένων που περιέχουν μακροεντολές. Οι μακρο-εντολές είναι κώδικας εντολών, γραμμένος με γλώσσες συγγραφής σεναρίων π.χ. VBA (Visual Basic for Applications) και χρησιμοποιούνται κυρίως σε προγράμματα εφαρμογών γραφείου για την αυτοματοποίηση ορισμένων από τις λειτουργίες που εκτελεί ο χρήστης.

Για παράδειγμα, κάποιος μπορεί να δημιουργήσει μια μακροεντολή στο Word ώστε με το πάτημα ενός πλήκτρου, να εκτελεί ταυτόχρονα τις ακόλουθες λειτουργίες: α) Επιλογή κειμένου, β) μορφοποίηση με γραμματοσειρά Arial, γ) αλλαγή μεγέθους



γραμματοσειράς σε 14. Οι μακροεντολές αποθηκεύονται μαζί με το αρχείο δεδομένων στο δίσκο.

Οι μακρο-ιοί λοιπόν είναι μακροεντολές που αυτοματοποιούν ένα σύνολο από καταστροφικές ενέργειες: όταν π.χ. σε έναν επεξεργαστή κειμένου εκτελεστεί η μακροεντολή ενός μολυσμένου εγγράφου, ο ιός ενεργοποιείται και απελευθερώνει το καταστροφικό του φορτίο.

Η δημοτικότητα των εφαρμογών γραφείου, έχει συνεισφέρει στην εξάπλωση αυτού του είδους των ιών. Επίσης, ο κώδικας που δημιουργείται από μια γλώσσα συγγραφής σεναρίων, μπορεί να εκτελεστεί σε όλες τις πλατφόρμες: ένας μακρο-ιός μπορεί να εκτελεστεί σε ένα PC και σε ένα MAC.

Η διαδικασία της μόλυνσης γίνεται μέσα από τη λήψη και άνοιγμα εγγράφου που περιέχει μακρο-εντολές. Οι περισσότερες μακρο-εντολές ενεργοποιούνται με το άνοιγμα ενός εγγράφου (π.χ. λειτουργία Auto-open). Στις τελευταίες εκδόσεις των εφαρμογών γραφείου, ο χρήστης προειδοποιείται για την ύπαρξη τέτοιων εντολών.

Ο μακρο-ιός συνήθως είναι προγραμματισμένος να μετατρέπει τα μολυσμένα έγγραφα σε πρότυπα προκειμένου να μολυνθούν όλα τα έγγραφα που θα δημιουργήσει μελλοντικά ο χρήστης. Η μετάδοση του γίνεται με αφαιρούμενα αποθηκευτικά μέσα ή μέσω δικτύου (Matyas et al., 2000).

#### **4.4.2 Χάκερ**

Οι Hackers έχουν προκαλέσει χάος με μερικές από τις πιο αδιαπέραστες βάσεις δεδομένων ειδικά την τελευταία πενταετία. Οι hackers έχουν καταλήξει σε καινοτόμα προγράμματα όπως το δούρειο ίππο και το αυγό Cuckoo' –κούκος προκειμένου να προβούν σε διεθνή κατασκοπεία ακόμα και έγκλημα. Ένας δούρειος ίππος είναι ένα φαινομενικά αβλαβές πρόγραμμα στο οποίο αν γίνει πρόσβαση θα δημιουργήσει χάος με ολόκληρο το σύστημα. Το «Love Bug» ή το «σ' αγαπώ» του ιού που έπληξε το κυβερνοχώρο κόσμο σαν θυελλώδης δύναμη και άφησε πίσω του την καταστροφή στο πέρασμά της, είναι ένα παράδειγμα του Δούρειου Ίππου. Το αυγό κούκος είναι ένα MP3 αρχείο που μοιάζει με πνευματικά δικαιώματα τραγούδι που διανέμονται Χωρίς την άδεια του κατόχου των πνευματικών δικαιωμάτων. Η

ομοιότητα είναι τόσο ακριβής , έχει ακόμη και το ίδιο μέγεθος και χρόνο αναπαραγωγής από το πρωτότυπο. Οι Hackers αρέσκονται περισσότερο στην απόλαυση του να ξεπεράσουν κανόνες περισσότερο από περιέργεια παρά από κάποια υστεροβουλία.

## **Κεφάλαιο 5<sup>ο</sup> Ασφάλεια στο Διαδίκτυο - Μηχανισμοί Ασφαλείας**

### **5.1 Ασφάλεια Διαχείρισης Δικτύων Υπολογιστών**

Η Διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της προσβασιμότητας των πληροφοριών. Επιπλέον, άλλες ιδιότητες όπως η αυθεντικότητα, η λογοδοσία, μη άρνηση και η αξιοπιστία μπορεί να συμπεριληφθούν.

Ο όρος «διαθεσιμότητα» δεν έχει χρησιμοποιηθεί σε αυτόν τον ορισμό, γιατί είναι ένας όρος που ορίζεται σε αυτό το τμήμα του ISO / IEC 20000 το οποίο δεν θα ήταν κατάλληλο για τον ορισμό αυτό.

Το Περιστατικό ασφάλειας πληροφορίας, αποτελεί ένα μεμονωμένο ή μια σειρά από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας των πληροφοριών που έχουν σημαντική πιθανότητα να θέτουν σε κίνδυνο τις επιχειρηματικές δραστηριότητες και απειλεί την ασφάλεια των πληροφοριών. Το Ενδιαφερόμενο μέρος είναι ένα άτομο ή ομάδα που έχει ένα ιδιαίτερο ενδιαφέρον για την απόδοση ή την επιτυχία της δραστηριότητας ή των δραστηριοτήτων του φορέα παροχής υπηρεσιών. Οι πελάτες, οι ιδιοκτήτες, η διαχείριση, οι άνθρωποι στην οργάνωση, οι προμηθευτές του φορέα παροχής υπηρεσιών, οι τραπεζίτες, οι συνδικαλιστικές οργανώσεις ή οι εταίροι.

Η Εσωτερική ομάδα αποτελεί μέρος της οργάνωσης του φορέα παροχής υπηρεσιών που συνάπτει τεκμηριωμένη συμφωνία με τον πάροχο υπηρεσιών να συμβάλλει στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών. Η εσωτερική ομάδα είναι εκτός του πεδίου εφαρμογής των SMS του φορέα παροχής υπηρεσιών. Ένα άλλο σημαίνον στοιχείο αποτελεί ένα γνωστό σφάλμα, το αποτελεί ένα πρόβλημα που έχει εντοπισμένη αιτία ή μια μέθοδος μείωσης ή εξάλειψης των επιπτώσεων του σε μια υπηρεσία μέσω της εργασίας γύρω από αυτό.

Σημαίνουν στοιχείο στην ασφάλεια των πληροφοριακών συστημάτων καθίσταται η οργάνωση η οποία είναι μια ομάδα ανθρώπων και εγκαταστάσεων, με διάταξη των ευθυνών, των αρχών και των σχέσεων. Ένα άλλο σημαίνουν στοιχείο είναι η λεγόμενη Προληπτική δράση, η οποία αποτελεί μια δράση για την αποφυγή ή την εξάλειψη των αιτιών ή τη μείωση της πιθανότητας εμφάνισης μιας πιθανής μη συμμόρφωσης ή άλλων δυνητικών ανεπιθύμητων καταστάσεων. Παρακάτω παραθέτονται επίσης σημαίνοντες ορισμοί (Γιαννόπουλος 2001):

1. Πρόβλημα: Αιτία από ένα ή περισσότερα επεισόδια. Η αιτία δεν είναι συνήθως γνωστή κατά το χρόνο καταγραφής του προβλήματος και η διαδικασία διαχείρισης των προβλημάτων είναι υπεύθυνη για την περαιτέρω έρευνα.
2. Διαδικασία: Καθορισμένος τρόπος για την πραγματοποίηση μια δραστηριότητας ή διαδικασίας.
3. Διεργασία: Το σύνολο των αλληλένδετων ή αλληλεπιδρώντων δραστηριοτήτων που μετατρέπει τις εισροές σε εκροές.
4. Καταγραφή: Έγγραφο που αναφέρει αποτελέσματα που επιτεύχθηκαν ή παρέχει αποδείξεις δραστηριοτήτων που πραγματοποιήθηκαν.
5. Απελευθέρωση: Συλλογή ενός ή περισσότερων νέων ή τροποποιημένων στοιχείων διαμόρφωσης που έχουν αναπτυχθεί στο ζωντανό περιβάλλον ως αποτέλεσμα μίας ή περισσότερων αλλαγών.
6. Αίτημα για αλλαγή: Πρόταση για μια αλλαγή που πρέπει να γίνει σε μια υπηρεσία, στοιχείο υπηρεσίας ή του συστήματος διαχείρισης των υπηρεσιών. Μια αλλαγή σε μια υπηρεσία περιλαμβάνει την παροχή μιας νέας υπηρεσίας ή την αφαίρεση μιας υπηρεσίας η οποία δεν είναι πλέον απαραίτητη.
7. Κίνδυνος: Επίδραση της αβεβαιότητας για τους στόχους. Ένα αποτέλεσμα είναι μια απόκλιση από την αναμενόμενη - θετική ή / και αρνητική. Οι στόχοι μπορούν να έχουν διαφορετικές πτυχές ( όπως οικονομικούς στόχους, την υγεία και την ασφάλεια, και περιβαλλοντικούς στόχους) και μπορεί να εφαρμοστεί σε διαφορετικά επίπεδα (όπως στρατηγικά, σε ολόκληρο τον

οργανισμό, το έργο, το προϊόν και τη διαδικασία ).

8. Υπηρεσία: Μέσο για την παροχή αξίας στον πελάτη, διευκολύνοντας τα αποτελέσματα που θέλει να επιτύχει ο πελάτης. Μια υπηρεσία μπορεί επίσης να παραδοθεί με τον παροχέα υπηρεσιών από έναν προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής.
9. Συνιστώσα των υπηρεσιών: Ενιαία μονάδα μιας υπηρεσίας που όταν συνδυάζεται με άλλες μονάδες θα παραδώσει μια πλήρη υπηρεσία.
10. Συνέχεια των υπηρεσιών: Δυνατότητα διαχείρισης των κινδύνων και των γεγονότων που θα μπορούσαν να έχουν σοβαρές επιπτώσεις σε μια υπηρεσία ή υπηρεσίες, προκειμένου να παραδώσει συνεχώς τις υπηρεσίες σε αποδεκτά επίπεδα
11. Σύμβαση Παροχής Υπηρεσιών: Τεκμηριωμένη σύμβαση μεταξύ του παρόχου υπηρεσιών και του πελάτη που προσδιορίζει τις υπηρεσίες και τους στόχους των υπηρεσιών. Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί επίσης να καθοριστεί μεταξύ του παρόχου υπηρεσιών και του προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής .Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί να συμπεριληφθεί σε μια σύμβαση ή άλλου τύπου τεκμηριωμένη σύμβαση .
12. Διαχείριση υπηρεσιών: Το σύνολο των δυνατοτήτων και των διαδικασιών που κατευθύνουν και να ελέγχουν τις δραστηριότητες και τους πόρους του φορέα παροχής υπηρεσιών για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών για την κάλυψη των απαιτήσεων των υπηρεσιών
13. Σύστημα διαχείρισης υπηρεσιών: Σύστημα διαχείρισης για να κατευθύνει και να ελέγχει τις δραστηριότητες παροχής υπηρεσιών διαχείρισης του παρόχου υπηρεσιών Ένα σύστημα διαχείρισης είναι ένα σύνολο αλληλένδετων ή αλληλεπιδρώντων στοιχείων για τη δημιουργία της πολιτικής και των στόχων και την επίτευξη των στόχων αυτών .Το SMS περιλαμβάνει όλες τις πολιτικές διαχείρισης των υπηρεσιών, τους στόχους, τα σχέδια, τις διαδικασίες, την

τεκμηρίωση και τους πόρους που απαιτούνται για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών και την εκπλήρωση των απαιτήσεων σε αυτό το τμήμα του ISO / IEC 20000 .

14. Πάροχος υπηρεσιών: Οργάνωση ή μέρος μιας οργάνωσης που διαχειρίζεται και παρέχει μια υπηρεσία ή υπηρεσίες για τον πελάτη. Ένας πελάτης μπορεί να είναι εσωτερική ή εξωτερική οργάνωσης του φορέα παροχής υπηρεσιών .
15. Αίτηση υπηρεσίας: Αίτηση παροχής πληροφοριών, συμβουλών, την πρόσβαση σε μια υπηρεσία ή ένα προ-εγκεκριμένο αλλαγή
16. Απαίτηση υπηρεσίας: Ανάγκες του πελάτη και των χρηστών της υπηρεσίας, συμπεριλαμβανομένων των απαιτήσεων σε επίπεδο εξυπηρέτησης, και τις ανάγκες του παρόχου υπηρεσιών
17. Προμηθευτής: Οργάνωση ή μέρος μιας οργάνωσης που είναι εξωτερική οργάνωση του φορέα παροχής υπηρεσιών και να συνάπτει σύμβαση με τον πάροχο υπηρεσιών να συμβάλλουν στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών ή διαδικασιών.
18. Ανώτατα διοικητικά στελέχη: Πρόσωπο ή ομάδα ανθρώπων που διευθύνουν και ελέγχουν τον πάροχο υπηρεσιών στο υψηλότερο επίπεδο
19. Μετάβαση: Δραστηριότητες που εμπλέκονται στη μετακίνηση νέων ή τροποποιημένων δρομολογίων από και προς το ζωντανό περιβάλλον (Γιαννόπουλος 2001).

### **5.1.1 Η πιστοποίηση και αυθεντικοποίηση**

Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) είναι ένας φορέας που βεβαιώνει με ακρίβεια τη σχέση ενός φυσικού προσώπου με το δημόσιο κλειδί του, με την έκδοση ενός ηλεκτρονικού πιστοποιητικού, στο οποίο ο ΠΥΠ πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του. Κύριος τύπος ψηφιακών πιστοποιητικών είναι τα πιστοποιητικά δημοσίου κλειδιού (public key certificates). Το πιστοποιητικό αναφέρει το δημόσιο κλειδί και επιβεβαιώνει ότι το συγκεκριμένο

πρόσωπο είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει. Η συσχέτιση ενός δημόσιου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του ΠΥΠ, ο οποίος υπογράφει το πιστοποιητικό του δικαιούχου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο ΠΥΠ δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) (Γιαννόπουλος 2001).

Με την ηλεκτρονική υπογραφή επιτυγχάνονται οι εξής στόχοι:

- Η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει
- Η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και
- Η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, ότι δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί τη συμμετοχή του στην εν λόγω συναλλαγή

### **5.1.2 Η διασφάλιση της εμπιστευτικότητας**

Τα δεδομένα θα πρέπει να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα.

### **5.1.3 Η διασφάλιση της ακεραιότητας**

Τα δεδομένα δεν θα πρέπει σε καμία περίπτωση να διαγραφούν ή να αλλοιωθούν από μη εξουσιοδοτημένα άτομα.

### 5.1.4 Η μη αποποίηση ευθύνης

Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της

## 5.2 Συμμετρική Κρυπτογραφία

Στους Συμμετρικούς αλγόριθμους κρυπτογράφησης ή αλλιώς Αλγορίθμους Ιδιωτικού κλειδιού, η διαδικασία κρυπτογράφησης βασίζεται στη χρήση ενός και μόνο κλειδιού το οποίο χρησιμοποιείται και στην κρυπτογράφηση και στην αποκρυπτογράφηση της πληροφορίας. Το κλειδί αυτό είναι κοινό και για τον αποστολέα αλλά και για τον παραλήπτη. Ο αποστολέας χρησιμοποιεί το μυστικό αυτό κλειδί για να κρυπτογραφήσει το μήνυμα. Ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί έτσι ώστε να αποκρυπτογραφήσει το κωδικοποιημένο μήνυμα σε απλό κείμενο. Τέτοιοι αλγόριθμοι είναι ο αλγόριθμος RSA RC4 που χρησιμοποιείται στο MPPE (Microsoft Point to Point Encryption), ο αλγόριθμος DES (Data Encryption Standard), ο 3DES και ο IDEA (International Data Encryption Algorithm). Οι συμμετρικοί αλγόριθμοι χρησιμοποιήθηκαν κυρίως σε κλειστά συστήματα και εφαρμόστηκε τη δεκαετία του '80 για τη μεταφορά τραπεζικών δεδομένων. Τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών δηλ. αυτά που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT(Γιαννόπουλος 2001).

### 5.2.1 Κρυπτογράφηση

Η κρυπτογράφηση είναι η διαδικασία κωδικοποίησης της πληροφορίας σε τέτοια μορφή έτσι ώστε κατά την αποστολή της πληροφορίας να είναι δυνατή η ανάγνωσή της μόνο από τον εξουσιοδοτημένο παραλήπτη της.



### 5.3 Ασύμμετρη Κρυπτογραφία

Διαφορετικά κλειδιά χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία, για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Το σύστημα ασύμμετρης κρυπτογράφησης αρχικά δημιουργήθηκε από τρεις μαθηματικούς, τους Ellis, Cocks και Williamson το 1973. Το 1976 οι Diffie και Hellman διατύπωσαν την βασική αρχή της κρυπτογραφίας δημόσιου κλειδιού, ενώ το 1977 οι Rivest, Shamir και Adleman δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων (Γιαννόπουλος 2001).

Στους ασύμμετρους αλγόριθμους κρυπτογράφησης που ονομάζονται και Αλγόριθμοι Κρυπτογράφησης Δημόσιου Κλειδιού, χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα για κάθε χρήστη. Το ένα είναι Ιδιωτικό και ανήκει μόνο σε έναν χρήστη ενώ το δεύτερο είναι ένα δημόσιο κλειδί το οποίο είναι διαθέσιμο σε όλους. Ένας χρήστης χρησιμοποιεί το ιδιωτικό κλειδί για να κρυπτογραφήσει μια πληροφορία, ενώ ο αποδέκτης χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί για να μπορέσει να αποκωδικοποιήσει τη πληροφορία. Τα δύο κλειδιά σχετίζονται μεταξύ τους με μια μαθηματική σχέση η οποία ορίζεται από τον αλγόριθμο κρυπτογράφησης. Συνήθως οι ασύμμετροι αλγόριθμοι χρησιμοποιούν μεγαλύτερα σε μέγεθος κλειδιά σε σχέση με τους συμμετρικούς και συνεπώς απαιτούν μεγαλύτερη επεξεργαστική ισχύ για την αποκωδικοποίηση. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγόριθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Σε ένα σύστημα ασύμμετρης κρυπτογράφησης, ο αποστολέας και ο παραλήπτης πρέπει να διαθέτει ο καθένας τα δικά του κλειδιά, ένα δημόσιο και ένα

ιδιωτικό. Πρώτα, ο αποστολέας ζητάει από τον παραλήπτη να του στείλει το δημόσιο κλειδί του μέσω απλού ταχυδρομείου, ενώ το ιδιωτικό κλειδί ο παραλήπτης το κρατάει για τον εαυτό του (Γιαννόπουλος 2001).

Όταν ο αποστολέας λάβει το δημόσιο κλειδί του παραλήπτη, το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμά του και στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη. Όταν αυτός το λάβει, είναι ο μόνος που έχει το ιδιωτικό κλειδί για το μήνυμα, και άρα ο μόνος που μπορεί να το διαβάσει. Για να απαντήσει στον αποστολέα, θα πρέπει αντίστοιχα και αυτός να πάρει ένα δημόσιο κλειδί από αυτόν.

Το κρίσιμο πλεονέκτημα που προσφέρει η ασύμμετρη κρυπτογραφία είναι ότι αποστολέας και παραλήπτης δεν χρειάζεται να ανταλλάξουν κλειδιά. Αυτό αποτρέπει κάποιον τρίτο από το να υποκλέψει το κλειδί καθώς αυτό μεταφέρεται, κάτι το οποίο θα επέτρεπε σε αυτόν τον τρίτο να κατασκοπεύει όλα τα μελλοντικά μηνύματα (Γιαννόπουλος 2001).

### **5.3.1 Αλγόριθμοι κρυπτογράφηση**

Οι αλγόριθμοι κρυπτογράφησης λειτουργούν σαν κλειδαριές με συνδυασμός όπου το κλειδί είναι ένας συνδυασμός. Όσα περισσότερα ψηφία έχει ο συνδυασμός τόσο ασφαλέστερη είναι η κλειδαριά και τελικά τόσο πιο δύσκολη η αποκρυπτογράφηση των πληροφοριών. Υπάρχουν διάφοροι τύποι αλγορίθμων κρυπτογράφησης όπως: Συμμετρικοί Αλγόριθμοι και Ασύμμετροι Αλγόριθμοι που αναφέρθηκαν παραπάνω.

## **5.4 Ψηφιακές Υπογραφές**

Το πρόβλημα της πιστοποίησης της γνησιότητας μιας πληροφορίας που λαμβάνεται σε ηλεκτρονική μορφή είναι ένα από τα σημαντικότερα σήμερα, καθώς η τάση για όλο και περισσότερο απρόσωπες και απομακρυσμένες συναλλαγές επιτάσσει την αντικατάσταση των παραδοσιακών τρόπων πιστοποίησης με βάση την υπογραφή με το χέρι, τις σφραγίδες των οργανισμών και την ανάλυση γραφικού χαρακτήρα με τρόπους που μπορούν να χειριστούν τα παραπάνω στοιχεία σε ηλεκτρονική μορφή.

Στις συναλλαγές των ανθρώπων, είναι αναγκαίο να πιστοποιούνται ημερομηνίες αποστολής εγγράφων, η ταυτότητα του αποστολέα μιας πληροφορίας, η ταυτότητα του υπολογιστή από τον οποίο στάλθηκε μια πληροφορία καθώς και πλήθος στοιχείων που μέχρι τώρα βασιζόταν σε κλασικά μέσα επεξεργασίας πληροφοριών (Γιαννόπουλος 2001).

## **5.5 Διαχείριση Δημοσιών Κλειδιών**

Η ψηφιακή υπογραφή, είναι ένα μέσο με το οποίο πολλά από αυτά τα στοιχεία μπορούν να πιστοποιηθούν. Δοσμένου ενός ηλεκτρονικού εγγράφου, η ψηφιακή του υπογραφή είναι μία πληροφορία που σχηματίζεται με βάση το έγγραφο και ενός προσωπικού αριθμού (κλειδί) του αποστολέα. Είναι ο συνδυασμός ενός μηνύματος που προκύπτει από την επεξεργασία του πιστοποιητικού με κάποιον αλγόριθμο και με το private key και ενός public key για κάθε μέρος. Με απλά λόγια, είναι σαν ο Α να έχει δύο κλειδιά, να δίνει στον Β το public key του προκειμένου να κλειδώσει το κουτί μέσα στο οποίο θα του στείλει τα δεδομένα και να το επιστρέψει στον Α, που θα το ξεκλειδώσει με το private key του, και αντίστροφα (Γιαννόπουλος 2001).

## **5.6 Smart Cards**

Ονομάζουμε τις κάρτες με τσιπ-κύκλωμα. Περιλαμβάνουν επάνω τους μια κεντρική μονάδα επεξεργασίας και γίνονται ορισμένες λειτουργίες με τα δεδομένα που είναι αποθηκευμένα μέσα στην μονάδα.

## **5.7 Antivirus**

Όπως έχει αποδειχθεί από πολλές έρευνες, η διασπορά ιών είναι η πιο διαδεδομένη μορφή επιθέσεων στο Διαδίκτυο. Καθημερινά, δημιουργούνται χιλιάδες νέοι ιοί, που απειλούν, ποικιλοτρόπως, τα υπολογιστικά συστήματα. Η πιο σημαντική μέθοδος αντιμετώπισης των ιών είναι η χρήση αντιβιοτικών προγραμμάτων (antivirus software).

Το λογισμικό αντιμετώπισης ιών, είναι ένα από τα πιο πολύπλοκα εργαλεία λογισμικού. Ένα τέτοιο λογισμικό, επιτελεί τρεις βασικές λειτουργίες:

**Ανίχνευση των ιών**

**Προσδιορισμός της ταυτότητας των ιών**

**Καθαρισμός των ιών**

**Firewalls**

Στην επιστήμη των υπολογιστών όρος Firewall προσδιορίζει μια συσκευή ή εργαλείο λογισμικού (ή και συνδυασμό των ανωτέρω), που παρακολουθεί και φιλτράρει τα πακέτα που επιχειρούν είτε να εισέλθουν, είτε να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Είναι εργαλεία που ξεχωρίζουν ένα «ασφαλές» θα λέγαμε δίκτυο (π.χ. το Intranet μιας επιχείρησης), από ένα εξωτερικό μη ασφαλές δίκτυο, όπως είναι το Internet.

Τα περισσότερα Firewalls επιτελούν δυο βασικές λειτουργίες ασφαλείας:

A) Φιλτράρισμα πακέτων

B) Πύλες εφαρμογών

## **5.8 Πρωτόκολλο Secure Sockets Layer**

Οι κύριοι στόχοι της πολιτικής ασφάλειας του δικτύου θα πρέπει να είναι να διασφαλιστεί ότι η πρόσβαση στο δίκτυο της εταιρείας παρέχεται μόνο σε εξουσιοδοτημένους χρήστες, την ύπαρξη επαρκών ελέγχων για τη διαχείριση απομακρυσμένων χρηστών, ότι όλος ο εξοπλισμός μπορεί να αναγνωριστεί μοναδικά, ότι τα δίκτυα θα πρέπει να διαχωρίζονται με βάση τις ανάγκες και τα κατάλληλα πρωτόκολλα δρομολόγησης του δικτύου. Τυπικά πολιτικές δηλώσεις για την Ασφάλεια Δικτύων περιλαμβάνουν (Security updates: The upcoming revision of ISO/IEC 27001):

§ Κατάλληλοι μηχανισμοί ελέγχου ταυτότητας πρέπει να χρησιμοποιηθούν για τον έλεγχο της πρόσβασης των απομακρυσμένων χρηστών .

- § Κατανομή των δικαιωμάτων πρόσβασης στο δίκτυο πρέπει να παρέχεται σύμφωνα με τις απαιτήσεις των επιχειρήσεων και της ασφάλειας.
- § Έλεγχος ταυτότητας δύο παραγόντων πρέπει να χρησιμοποιείται για τον έλεγχο ταυτότητας των χρηστών που χρησιμοποιούν κινητά / απομακρυσμένα συστήματα

## 5.9 Κρυπτογράφηση

Η κρυπτογράφηση των προσωπικών κωδικών των χρηστών, από τη στιγμή που πληκτρολογούνται από τους ίδιους στην ιστοσελίδα μιας τράπεζας για παράδειγμα ή μιας εταιρίας είναι ζήτημα που άπτεται των τραπεζών και των επιχειρήσεων. Οι τράπεζες είναι υπεύθυνες για θέματα καθορισμού του κατάλληλου μήκους κωδικού, απενεργοποίησης των κωδικών και τερματισμού της σύνδεσης χρηστών μετά από ένα χρονικό διάστημα μη χρήσης των υπηρεσιών. Σε κάθε περίπτωση οι τράπεζες πρέπει να ενημερώνουν τους χρήστες της ηλεκτρονικής τραπεζικής για το ευαίσθητο θέμα της ασφάλειας τους. Τα τελευταία χρόνια μερικές τράπεζες έχουν υιοθετήσει για λόγους επιπρόσθετης ασφάλειας, τα λεγόμενα εικονικά πληκτρολόγια.

Η χρήση αριθμών TAN προϋποθέτει μια συγκεκριμένη διαδικασία εγκατάστασης και ταυτοποίησης. Αρχικά θα πρέπει να γίνει η εγκατάσταση Λογισμικού Token. Η εγκατάσταση, μετά την εισαγωγή του οπτικού δίσκου στο PC από όπου θα εκτελούνται οι συναλλαγές στο e-banking, γίνεται ακολουθώντας τα παρακάτω βήματα (Εργαστήριο Εκπαιδευτικής και Γλωσσικής Τεχνολογίας.,2010):

**1ο βήμα:** επιλογή γλώσσας εμφάνισης μηνυμάτων του προγράμματος

**2ο βήμα:** εγκατάσταση οδηγών συσκευής (drivers)

**3ο βήμα:** εγκατάσταση λογισμικού

Η πρόσβαση στο e-Banking της Τράπεζας θα γίνεται ως εξής:

1. Εισάγει ο χρήστης τη συσκευή token στην USB θύρα του υπολογιστή του.
2. Πληκτρολογεί τη διεύθυνση του δικτυακού τόπου της τράπεζας στον Internet Explorer.
3. Επιλέγει το ψηφιακό πιστοποιητικό ασφαλείας πατά OK και μετά πληκτρολογεί τον αριθμό token pin και Enter.
4. Μόλις φορτωθεί η αρχική σελίδα του site θα εισάγει στο πεδίο «Όνομα Χρήστη» το user name.
5. Τέλος εισάγουμε στο πεδίο «Κωδικός χρήστη» το password.

Αναλυτικά τώρα τα σημεία ελέγχου είναι τα εξής:

1. Εγγραφή: Η εγγραφή στην υπηρεσία e-banking όπως σχεδιάζεται είναι εξαιρετικά εύκολη και απλή. Με μια μόνο επίσκεψη στη τράπεζα ο χρήστης θα αποκτήσει πρόσβαση και θα πραγματοποιεί τις συναλλαγές του γρήγορα, απλά και με απόλυτη ασφάλεια. Τα βασικά δεδομένα τα οποία χρειάζεται είναι τα ακόλουθα:

1. Να έχει έναν καταθετικό λογαριασμό.
2. Να έχετε στην κατοχή του ενεργή χρεωστική κάρτα από το κατάστημα με το άνοιγμα του λογαριασμού.
3. Να συμπληρώσει μία αίτηση εγγραφής στα Εναλλακτικά δίκτυα σε οποιοδήποτε κατάστημα της
4. Να γνωρίζει τους 2 κωδικούς

Όλα τα παραπάνω αλλά και το συγκεκριμένο βήμα το συμπεριλαμβάνουμε γιατί αποτελεί τη διαδικασία πιστοποίησης του χρήστη. Στο σημείο αυτό δίνεται η μοναδικότητα ανά χρήση, όπου ο καθένας έχοντας ένα μοναδικό κωδικό εντάσσεται στο σύστημα. Η διαδικασία εγγραφής (registration) εξασφαλίζει τη μυστικότητα και το αναλλοίωτο των δεδομένων μέσω ενός πρωτοκόλλου επικοινωνίας, το οποίο βασίζεται είτε στην κρυπτογράφηση (encryption) 40bit ή 128 bit (ισχυρή κρυπτογράφηση).

Για την ασφαλή λειτουργία του Internet Banking, χρησιμοποιείται στο σύστημα η κρυπτογράφηση 128 bit των διακινουμένων στοιχείων, η οποία θεωρείται απαραβίαστη για τις εφαρμογές στο Διαδίκτυο (Γιαννόπουλος 2001).

Σε οποιαδήποτε διαταραχή ή παρεμβολή στην επικοινωνία, η συναλλαγή θα διακόπτεται. Για την ταυτοποίηση των χρηστών e-Banking, χρησιμοποιείται ένας κωδικός χρήστη (username) και ένα προσωπικό κωδικό εισόδου (password), μοναδικούς για κάθε χρήστη της υπηρεσίας (Ιγγλεζάκης 2001).

Για τη διενέργεια όμως χρηματικών συναλλαγών, οι τράπεζες δεν αρκούν σε αυτό το επίπεδο ταυτοποίησης του χρήστη αλλά απαιτούν μια επιπλέον δικλείδα ασφαλείας, την ψηφιακή πιστοποίηση (EFG.,2009), (Bayne, 2000).

2. Πιστοποίηση Χρήστη: Η πιστοποίηση χρήστη στο Internet Banking βοηθά στην αναγνώριση των χρηστών και επιτρέπει την πρόσβασή τους στο Σύστημα.

Σε αντίθεση με τους αλγόριθμους ελέγχου της υπογραφής ενός ιού, η ευρετική μέθοδος εξετάζει τον εκτελέσιμο κώδικα ενός αρχείου με σκοπό την εύρεση εντολών (ή συνόλου από εντολές) που θα μπορούσαν να αποτελούν τμήμα κακόβουλου κώδικα, με μεγάλη πιθανότητα. Παραδείγματα αποτελούν η ύπαρξη μακροεντολών σε ένα έγγραφο Office, εντολές κλήσης-τροποποίησης προγραμμάτων, ρουτίνες αποκρυπτογράφησης, εντολές διαγραφής αρχείων ή τροποποίησης του μητρώου του συστήματος, κ.λ.π. Η τεχνική αυτή είναι προενεργή, δηλαδή προσπαθεί να εντοπίσει «ύποπτο» τμήμα κώδικα πριν αυτός εκτελεστεί.

Για μεγαλύτερη ασφάλεια, μπορεί να χρησιμοποιηθεί η κρυπτογραφική τιμή hash του κώδικα του προγράμματος. Κάθε φορά που εκτελείται ένα αρχείο, το antivirus υπολογίζει το άθροισμα ελέγχου και το συγκρίνει την αποθηκευμένη τιμή.

## 5.10 Ψηφιακοί φάκελοι

Χρήστης ηλεκτρονικού ταχυδρομείου μπορεί να χρησιμοποιήσει τα ειδικά φίλτρα που προσφέρουν τα περισσότερα web mail για να διαγράψει αυτόματα τα μηνύματα spam ή να τα διοχετεύει σε έναν ειδικό φάκελο ενοχλητικής αλληλογραφίας.

Τέτοια φίλτρα επίσης υπάρχουν στο Διαδίκτυο για την καταπολέμηση των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά στον υπολογιστή του χρήστη και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη. Επιπλέον μερικές καλές πρακτικές όσον αφορά στην ενοχλητική αλληλογραφία είναι οι εξής:

- Γενικά οι χρήστες πρέπει να είναι πολύ προσεκτικοί όταν δημοσιεύουν ή υποβάλλουν κάπου την ηλεκτρονική διεύθυνση ταχυδρομείου.
- Πρέπει να χρησιμοποιούν διαφορετικούς λογαριασμούς email σε διαφορετικές περιπτώσεις, δηλαδή ξεχωριστή για την αγορά προϊόντων και άλλη για την επαγγελματική τους δραστηριότητα. Στην πρώτη περίπτωση αν λάβει πάρα πολλά μηνύματα spam στην διεύθυνσή του, μπορεί απλά να τη διαγράψει και να δημιουργήσει μια νέα ενώ στη δεύτερη περίπτωση είναι πολύ δύσκολο.
- Ο χρήστης θα πρέπει να χρησιμοποιεί ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων (anti-spam). Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους.

## 5.11. Αρχές πιστοποίησης και ψηφιακά πιστοποιητικά

Τα ψηφιακά πιστοποιητικά δίδονται από φορείς πιστοποίησης όμως η απόκτηση και η συντήρηση ενός τέτοιου πιστοποιητικού δεν είναι εύκολη για μια υπηρεσία τόσο διαδεδομένη. Στην περίπτωση του PGP αυτό παρακάμπτεται από έναν μηχανισμό που στηρίζεται στην αμοιβαία εμπιστοσύνη μεταξύ χρηστών του προτύπου αλληλογραφίας, αλλά η περιορισμένη διάδοση έχει ως αποτέλεσμα να υπάρχουν πολλοί χρήστες που αποστέλλουν μηνύματα για τους οποίους δεν είναι δυνατή η ταυτοποίηση.



Συνεπώς θα πρέπει να τονίσουμε ότι τεχνικά υπάρχει η δυνατότητα χρήσης του ηλεκτρονικού ταχυδρομείου με πολύ υψηλές προδιαγραφές ασφάλειας και η τεχνολογία έχει αναπτύξει τέτοια πρότυπα που δίνουν αυτές τις δυνατότητες. Από την άλλη απομένει πολύς δρόμος μέχρι αυτά τα πρότυπα να μπορούν να εφαρμοστούν για κάθε χρήστη του ηλεκτρονικού ταχυδρομείου και η χρήση τους να θεωρείται δεδομένη.

## **5.12. Το πρωτόκολλο SET**

Σήμερα οι περισσότερες τράπεζες εστιάζουν στο πρωτόκολλο SET. Το πρωτόκολλο αυτό υποστηρίζεται από δυο εκ των βασικότερων χρηματοπιστωτικών οργανισμών, τη MasterCard και τη Visa, καθώς και από εταιρίες όπως η IBM, η Microsoft και η Netscape (Johnson 2006).

Το πρωτόκολλο αυτό αναφέρεται στη διαδικασία της κρυπτογράφησης αναφερόμενο σε δυο κυρίες μεθόδους. Η μια ήταν η συμμετρική και η άλλη η ασύμμετρη. Η συμμετρική κρυπτογράφηση υλοποιείται με τη χρήση του ίδιου "κλειδιού", τόσο στην κωδικοποίηση όσο και στην αποκωδικοποίηση. Πράγμα το οποίο σημαίνει ότι ο αποστολέας και ο παραλήπτης του μηνύματος μοιράζονται το ίδιο κλειδί (Peterson, 2007).

Το κλειδί το οποίο χρησιμοποιείται αναφέρεται μόνο σε εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Ένας από τους γνωστότερους αλγόριθμους που κάνουν χρήση αυτής της μεθόδου είναι το DES (Data Description Standard), που χρησιμοποιείται από τραπεζικούς οργανισμούς για τη δημιουργία των αριθμών PIN.

Η ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο κλειδιά. Το ένα (κοινό κλειδί) για να κωδικοποιήσει το μήνυμα και ένα άλλο (ιδιωτικό κλειδί) για να το αποκωδικοποιήσει.

Όσον αφορά στις τραπεζικές συναλλαγές, κάθε τράπεζα ακολουθεί τη δική της λύση, όπως είναι οι αριθμοί PIN, τα ψηφιακά πιστοποιητικά και οι αριθμοί TAN, που ακολουθούν κάθε συναλλαγή (Σπύρου, 2007).

Η πιστοποίηση της ταυτότητας του χρήστη και οι συναλλαγές του εξασφαλίζονται με ένα και μόνο ψηφιακό πιστοποιητικό το οποίο αναγνωρίζει τον υπολογιστή του χρήστη και επιτρέπει τις συναλλαγές χρημάτων μόνο από το προκαθορισμένο Ηλεκτρονικό Υπολογιστή.

## **Κεφάλαιο 6<sup>ο</sup> Μελέτες περίπτωσης**

### **6.1.Μελέτη περίπτωσης ηλεκτρονικού καταστήματος**

Στη παρούσα μελέτη θα χρησιμοποιηθούν ως μελέτη περίπτωσης δύο ηλεκτρονικά καταστήματα που λειτουργούν και διαδικτυακά τα οποία έχουν συγκεκριμένες τεχνικές ασφάλειας χρήσης μεταξύ του κοινού και των ηλεκτρονικών επιχειρήσεων.

### **6.2.Ηλεκτρονικό κατάστημα nail tips**

«Το κατάστημα ειδών μανικιούρ -πεντικιούρ και τεχνητών νυχιών **Nailtips** ξεκίνησε την λειτουργία του το 2008 με έδρα τη **Θεσσαλονίκη** και με σκοπό να παρέχει στους επαγγελματίες των άκρων μια ολοκληρωμένη γκάμα προϊόντων που αφορά Gel,ακρυλικά καθώς επίσης επαγγελματικά βερνίκια,εξοπλισμό και εργαλεία,nailart , κρέμες και sra περιποίησης άκρων. Οι πελάτες γνώρισαν κάτι διαφορετικό σε σχέση με το τι είχαν μάθει και πραγματικά επικρότησαν την προσπάθεια της εταιρίας από την πρώτη κιόλας στιγμή. Η σχέση τιμής και ποιότητας στα προϊόντα και η μεγιστοποίηση των κερδών είναι η πρωταρχική φροντίδα της εταιρίας. Η κινητήριος δύναμη είναι η αναζήτηση στο καινούριο, και τις καλλίτερες δυνατές τιμές και με άψογη ποιότητα».

#### **6.2.1.Ασφάλεια δεδομένων εταιρίας**

##### **Ασφάλεια**

«Η «ΕΤΑΙΡΕΙΑ» αναγνωρίζει τη σημασία του θέματος της ασφαλείας των Προσωπικών Δεδομένων, καθώς και των ηλεκτρονικών συναλλαγών και έχει λάβει όλα τα απαραίτητα μέτρα, με τις πιο σύγχρονες και προηγμένες μεθόδους, ώστε να εξασφαλίζεται η μέγιστη δυνατή ασφάλεια. Όλες οι πληροφορίες, οι οποίες σχετίζονται με τα προσωπικά στοιχεία των χρηστών, διασφαλίζονται ως απόρρητες.

Η ασφάλεια του Ηλεκτρονικού καταστήματος της «ΕΤΑΙΡΕΙΑΣ» επιτυγχάνεται με τις ακόλουθες μεθόδους (nailtips, 2015).

- **Αναγνώριση Πελάτη**
- Οι κωδικοί που χρησιμοποιούνται για την αναγνώρισή είναι δύο: ο Κωδικός Εισόδου (Username) και ο Προσωπικός Μυστικός Κωδικός Ασφαλείας (Password), οι οποίοι κάθε φορά που καταχωρούνται υπάρχει πρόσβαση με απόλυτη ασφάλεια στα προσωπικά στοιχεία. Ο μόνος που έχει πρόσβαση στα στοιχεία είναι μόνο ο χρήστης και είναι αποκλειστικά υπεύθυνος για την διατήρηση της μυστικότητάς του από τρίτα πρόσωπα. Σε περίπτωση απώλειας του ή διαρροής του θα πρέπει να προβεί στην άμεση ειδοποίηση της εταιρίας, αλλιώς το κατάστημα της «ΕΤΑΙΡΕΙΑΣ» δεν ευθύνεται για την χρήση του μυστικού κωδικού από μη εξουσιοδοτημένο πρόσωπο. Το ηλεκτρονικό κατάστημα της «ΕΤΑΙΡΕΙΑΣ» με κανέναν τρόπο δεν αποκαλύπτει ή δημοσιοποιεί τα προσωπικά δεδομένα και τις πληροφορίες που εμπιστεύεται το κοινό. Τα προσωπικά δεδομένα χρησιμοποιούνται αποκλειστικά για την εκτέλεση των συναλλαγών. Όλες οι πληροφορίες κρυπτογραφούνται και φυλάσσονται με απόλυτη ασφάλεια.
- **Κωδικοί Εισόδου (Username) & Ασφαλείας (Password):** Για την είσοδο στο ηλεκτρονικό κατάστημα της «ΕΤΑΙΡΕΙΑΣ» γίνεται χρήση από δύο κωδικούς, τον Κωδικό Εισόδου (Username) και τον Προσωπικό Μυστικό Κωδικό Ασφαλείας (Password). Το ηλεκτρονικό κατάστημα της «ΕΤΑΙΡΕΙΑΣ» δίνει τη δυνατότητα να μεταβληθεί ο Προσωπικός Μυστικός Κωδικός Ασφαλείας (password), για λόγους ασφαλείας.
- **Προσωπικά Δεδομένα – Απόρρητο Συναλλαγών:** Τα στοιχεία των χρηστών (όνομα, επάγγελμα, ηλεκτρονική διεύθυνση, διεύθυνση κατοικίας, σταθερό τηλέφωνο, κινητό τηλέφωνο κλπ.) και των συναλλαγών των χρηστών του ηλεκτρονικού καταστήματος θεωρούνται απόρρητα, όπως και στις συνήθεις συναλλαγές σε εμπορικό κατάστημα. Οι χρήστες κατά την παροχή των στοιχείων τους στα πλαίσια των συναλλαγών τους όπως και με το παρόν, θα

ενημερώνονται από την «ΕΤΑΙΡΕΙΑ» και συναινούν και αποδέχονται την επικείμενη επεξεργασία των στοιχείων αυτών προσωπικών δεδομένων, για τις ανάγκες της ομαλής και ευχερούς μεταξύ των μερών συναλλαγής, καθώς επίσης και της διαβίβασης των στοιχείων αυτών σε αποδέκτες οι οποίοι θα προσδιορίζονται συγκεκριμένα και είναι οι υπάλληλοι και προστιθέμενοι της εταιρίας στα πλαίσια της διεκπεραίωσης της καταρτιζόμενης σύμβασης. Επίσης και με τον παρόν γνωστοποιείται η ύπαρξη του δικαιώματος πρόσβασης και του δικαιώματος εναντίωσης του άρθρου 12 και 13 του Ν. 2472/1997. Βεβαιώνεται ότι μόνο εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση στις πληροφορίες των συναλλαγών και μόνο όποτε αυτό είναι αναγκαίο, π.χ. για τη διεκπεραίωση των παραγγελιών. Κατά τα λοιπά η «ΕΤΑΙΡΕΙΑ» δεσμεύεται να μην αποκαλύψει τα στοιχεία των πελατών και των συναλλαγών τους, εκτός αν έχει έγγραφη εξουσιοδότηση από τους ίδιους, ή αυτό επιβάλλεται από δικαστική απόφαση ή απόφαση άλλης δημόσιας αρχής. Τα προσωπικά δεδομένα που δηλώνονται στο ηλεκτρονικό κατάστημα με το εμπορικό σήμα Nail Tips χρησιμοποιούνται αποκλειστικά από αυτό ή συνεργαζόμενες με αυτό επιχειρήσεις, με σκοπό την υποστήριξη, προώθηση και εκτέλεση της συναλλακτικής σχέσης. Το σύνολο των εγγράφων και ηλεκτρονικών στοιχείων που θα ανταλλαχθούν μεταξύ των μερών στα πλαίσια της πώλησης θα τηρούνται από την «ΕΤΑΙΡΕΙΑ». Ο πελάτης μπορεί να έχει πρόσβαση σε αυτά εφόσον το επιθυμεί (nailtips, 2015)»

### **6.3.Ασφαλιστική εταιρία ANY TIME**

Η Anytime είναι η 1η direct ασφάλιση στην Ελλάδα. Μέσω της Anytime υπάρχει η δυνατότητα να ασφαλιστεί όποιος επιθυμεί απευθείας από το internet ή τηλεφωνικά, επιλέγοντας το πρόγραμμα που του ταιριάζει (anytimeonline, 2015).

Με την Anytime εξασφαλίζεται:

- **Απλότητα**

Οι διαδικασίες είναι εύκολες και γρήγορες και τα προϊόντα απλά και κατανοητά.

- **Αξία στην επιλογή**

Τα ασφάλιστρα όπως και τα προϊόντα είναι ανταγωνιστικά και χαρακτηρίζονται από υψηλή ποιότητα υπηρεσιών.

- **Εξυπηρέτηση**

Η εταιρία είναι στη διάθεση του κοινού κάθε στιγμή, 24 ώρες το 24ωρο.

- **Εμπιστοσύνη**

Υπάρχει αξιοπιστία και σιγουριά, γιατί τα προγράμματα ασφάλισης της Anytime προσφέρονται από την INTERAMERICAN, μέλος του ομίλου Achmea.

#### **6.3.1.Ασφάλεια Προσωπικών Δεδομένων**

##### **6.3.1.1 Προσωπικά Δεδομένα**

Οι επισκέπτες και οι χρήστες του [www.anytime.gr](http://www.anytime.gr), για να αποκτήσουν πρόσβαση σε ορισμένες υπηρεσίες που προσφέρονται από το συγκεκριμένο δικτυακό τόπο, είναι απαραίτητο να γνωστοποιήσουν κάποιες από τις προσωπικές τους πληροφορίες, οι οποίες χαρακτηρίζονται ως «δεδομένα προσωπικού χαρακτήρα» (anytimeonline, 2015).

«Δεδομένο προσωπικού χαρακτήρα» ορίζεται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων και μπορεί να προσδιορίσει την

ταυτότητά του ή τα στοιχεία επικοινωνίας του. Η γνωστοποίηση των παραπάνω πληροφοριών από τον επισκέπτη ή και τον χρήστη, σημαίνει την αποδοχή του για επιπλέον επεξεργασία τους.

Οι Εταιρίες: «INTERAMERIKAN ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΙΑ ΑΣΦΑΛΙΣΕΩΝ ΖΗΜΙΩΝ Α.Ε.», «INTERAMERIKAN ΕΛΛΗΝΙΚΗ ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ ΖΩΗΣ Α.Ε.» και «INTERAMERIKAN ΒΟΗΘΕΙΑΣ ΑΝΩΝΥΜΟΣ ΕΤΑΙΡΙΑ ΓΕΝΙΚΩΝ ΑΣΦΑΛΕΙΩΝ», με έδρα στην Αγ. Κωνσταντίνου 57, 15124, Μαρούσι και αριθμό τηλεφωνικού κέντρου 210 94 60000, θα τηρούν και θα επεξεργάζονται αρχεία με προσωπικά δεδομένα που παρέχουν με τη θέλησή τους οι επισκέπτες του δικτυακού τόπου.

Η συλλογή και η χρήση προσωπικών δεδομένων περιορίζεται στα απολύτως αναγκαία για την επίτευξη του σκοπού που αναφέρεται στα στοιχεία συλλογής τους (όνομα, επώνυμο, φύλο, e-mail, αριθμός σταθερού & κινητού τηλεφώνου, κ.α.).

Η συλλογή και η χρήση των παραπάνω δεδομένων πραγματοποιείται με βάση την ελληνική και κοινοτική νομοθεσία, σύμφωνα με τους Νόμους 2472/97 & 3471/2006, όπως ισχύουν σήμερα. Σκοπός της συλλογής των προσωπικών δεδομένων είναι η βελτίωση των υπηρεσιών που παρέχεται στους επισκέπτες ή και στους χρήστες του [www.anytime.gr](http://www.anytime.gr), προκειμένου να διαπιστωθούν οι ανάγκες, επιθυμίες και προσδοκίες τους.

Κάθε χρήστης μπορεί οποιαδήποτε στιγμή να ασκήσει τα δικαιώματα πρόσβασης, διόρθωσης ή και αντίρρησης που αναφέρονται στα Άρθρα 12 και 13 του Νόμου 2472/1997.

Η άσκηση των παραπάνω δικαιωμάτων γίνεται με γραπτή δήλωση:

- Μέσω fax στο 210 94 62 078
- Μέσω e-mail στο [anytime@interamerican.gr](mailto:anytime@interamerican.gr)

Εκτός από τις Εταιρίες του Ομίλου INTERAMERICAN, αποδέκτες των συγκεκριμένων δεδομένων μπορεί να είναι μόνο οι Δημόσιες αρχές, έπειτα από υποβολή νόμιμου αιτήματος.

### 6.3.2.Cookies

Για την καλύτερη εξυπηρέτηση των επισκεπτών του δικτυακού τόπου [www.anytime.gr](http://www.anytime.gr), σε ορισμένες περιπτώσεις πλοήγησης γίνεται η χρήση «cookies» και καταγράφονται οι περίοδοι σύνδεσης του επισκέπτη. Το cookie είναι μία πληροφορία, την οποία μια ιστοσελίδα μπορεί να αποθηκεύσει στην εφαρμογή πλοήγησης του επισκέπτη και στη συνέχεια να την ανακτήσει.

Σε καμία περίπτωση τα cookies δεν περιέχουν προσωπικές πληροφορίες ή πληροφορίες, οι οποίες θα επιτρέψουν σε οποιονδήποτε να επικοινωνήσει με τον επισκέπτη του δικτυακού τόπου, μέσω τηλεφώνου, e-mail, κ.λπ. Ωστόσο, τα cookies μπορούν να χρησιμοποιηθούν από δικτυακούς τόπους εταιρειών των οποίων το μετοχικό κεφάλαιο συμμετέχει, με οποιοδήποτε ποσοστό πέραν του 10%, ο Ολλανδικός Όμιλος Εταιρειών με την επωνυμία «Achmea» στον οποίο άλλωστε ανήκουν και οι εταιρείες του Ομίλου INTERAMERICAN.

Ο επισκέπτης του δικτυακού τόπου, μπορεί με την κατάλληλη ρύθμιση στην εφαρμογή πλοήγησης που χρησιμοποιεί, να ειδοποιείται κάθε φορά που του αποστέλλονται cookies, ώστε να αποτρέψει την εγκατάστασή τους. Η αποτροπή εγκατάστασης cookies μπορεί να έχει επιπτώσεις στη δυνατότητα λήψης πληροφοριών ή και υπηρεσιών από την INTERAMERICAN.

Το περιεχόμενο της συγκεκριμένης πολιτικής «Προστασίας Προσωπικών Δεδομένων» μπορεί να μεταβληθεί οποιαδήποτε στιγμή, με σκοπό την αναβάθμιση των παρεχόμενων υπηρεσιών που προσφέρει ο δικτυακός τόπος [www.anytime.gr](http://www.anytime.gr). Ο επισκέπτης ή και ο χρήστης οφείλει να ελέγχει συχνά το περιεχόμενο της συγκεκριμένης ιστοσελίδας, ώστε να είναι ενήμερος κάθε στιγμή για την πολιτική που ισχύει.



## 6.4 Μελέτη περίπτωσης τράπεζας ALPHA BANK

«Η Alpha Bank χρησιμοποιεί το προαναφερόμενο πρωτόκολλο. Συγκεκριμένα μέσω αυτού δίνει τη δυνατότητα στους πελάτες της να εκτελούν, εντελώς δωρεάν, τραπεζικές συναλλαγές μέσω Internet 24 ώρες το 24ωρο.

Ο συνδρομητής μπορεί να παρακολουθεί τα υπόλοιπα των καταθετικών λογαριασμών, των στεγαστικών δανείων, των ανοικτών προσωπικών δανείων και των πιστωτικών καρτών, να πραγματοποιεί μεταφορές κεφαλαίων και πληρωμές οφειλών σε τρίτους, να πληροφορείται για τιμές συναλλάγματος και μετοχών κ.λπ. μέσω του Alpha Web Banking» (Αλφα., 2015).

Συγκεκριμένα ο χρήστης έχει την ικανότητα μέσω του πρωτόκολλου να προγραμματίζει μεταφορές κεφαλαίων που επιθυμεί να πραγματοποιήσει σε συγκεκριμένη ημερομηνία. Ακόμα δίνεται η δυνατότητα απεριόριστων συναλλαγών με οποιαδήποτε τράπεζα. Ο χρήστης μπορεί να μεταφέρει κεφάλαια σε λογαριασμούς καταθέσεων της Alpha Bank ή άλλης τράπεζας εσωτερικού που δεν έχουν δηλωθεί στο χρήστη (Αλφα., 2015).

Ακόμα δίνεται η δυνατότητα πληρωμών οφειλών σε δεδομένη ημερομηνία όπου αφορούν Προσωπικές πιστωτικές κάρτες (Alpha Bank Visa, American Express, Alpha Bank MasterCard κ.λ.π.) και κάρτες Επιχειρήσεων εκδόσεως Alpha Bank., Ανοικτά Προσωπικά Δάνεια Alpha 700, Alpha 702 Προσωπικά Δάνεια, Alpha 710 Καταναλωτικά Δάνεια, Alpha 702 «Προσωπικά Δάνεια Πρώτων Εξόδων Εγκαταστάσεως», Alpha Auto loan, Εκχώρηση Απαιτήσεων, Alpha Auto, Alpha 1|2|3 Προσωπικά Δάνεια, Alpha 1|2|3 Καταναλωτικά Δάνεια, Alpha1|2|3 Δάνεια Μεταπτυχιακών Σπουδών, Alpha 1|2|3 Φοιτητικών Εξόδων. (Αλφα., 2015).

- ο Άλλες εταιρίες του Ομίλου (π.χ. ALPHA ΑΣΦΑΛΙΣΤΙΚΗ).
- ο Λογαριασμούς κοινής ωφελείας (Δ.Ε.Η., Ε.ΥΔ.ΑΠ.).
- ο Δημόσιο (π.χ. Φ.Π.Α., Ι.Κ.Α., Τ.Ε.Β.Ε., Τέλη κυκλοφορίας).
- ο Λογαριασμούς σταθερής και κινητής τηλεφωνίας
- ο Λοιπές εταιρίες (π.χ. MULTICHOICE, ALLIANZ ΖΩΗΣ, ALLIANZ ΑΕΓΑ, κάρτες Diners).

Σε κάθε μεταφορά ή πληρωμή σε επιλεγμένη ημερομηνία υπάρχει η δυνατότητα επιλογής δέσμευσης του αντίστοιχου ποσού από το λογαριασμό μέχρι την ημερομηνία εκτελέσεως (χωρίς απώλεια τόκων) ή όχι. Η δυνατότητα δέσμευσης δίνεται σε συναλλαγές που καταχωρούνται από τις 7:30 π.μ. έως τις 11:00 μ.μ. Ο χρήστης μπορεί επίσης να χρησιμοποιήσει το πρωτόκολλο για κάποια από τα ακόλουθα δεδομένα (Lawnet.,2006):

- Για τα υπόλοιπα και τις κινήσεις των προδηλωμένων λογαριασμών καταθέσεων σε ευρώ ή συνάλλαγμα και στεγαστικών δανείων.
- Για τα στοιχεία των βιβλιαρίων επιταγών.
- Για τις μεταφορές σε προδηλωμένους ή μη λογαριασμούς που έχουν πραγματοποιηθεί ή καταχωρηθεί προς εκτέλεση μέσω των εναλλακτικών δικτύων της Alpha Bank (Alpha Web Banking, Alpha phone Banking και Alpha Bank m-Banking).
- Για τις πληρωμές οφειλών που έχουν καταχωρηθεί μέσω των εναλλακτικών δικτύων της Alpha Bank (Alpha Web Banking, Alpha phone Banking και Alpha Bank m-Banking).
- Για το ανώτατο ημερήσιο ποσό μεταφορών σε μη προδηλωμένους λογαριασμούς (για την εκτέλεση της συναλλαγής απαιτείται η χρήση του πρόσθετου κωδικού ασφαλείας).
- Για τους λογαριασμούς καταθέσεων, δάνεια και κάρτες που είναι συνδεδεμένες μέσω του Alpha Web Banking ή/και του Alpha phone Banking (με τη βοήθεια εκπροσώπου της τράπεζας).
- Για την «Κάρτα Συνδρομητή» στο Alpha phone Banking, δηλ. τους λογαριασμούς και τις πληρωμές που μπορεί να διαχειρίζεται ο χρήστης μέσω συναλλαγών του Alpha phone στο αυτόματο σύστημα εκτέλεσης συναλλαγών με επιλογή πλήκτρων-IVR.
- Για τις τιμές συναλλάγματος και ξένων χαρτονομισμάτων (αγορά - πώληση).

- Για τις τιμές μετοχών επιλεγμένων εταιριών του ΧΑΑ καθώς και για τους δείκτες τιμών μετοχών του ΧΑΑ, όπως διαμορφώνονται κατά τη διάρκεια συνεδρίασης με διαφορά ενημέρωσης 25 λεπτών περίπου.
- Για τις τιμές κλεισίματος των μετοχών του ΧΑΑ.
- Για την αναλυτική θέση και αποτίμηση του χαρτοφυλακίου στην Alpha Finance με βάση τις τιμές κλεισίματος των μετοχών της τελευταίας συνεδρίασης του ΧΑΑ καθώς και για τη χρηματική θέση στην Alpha Finance, όπως αυτή έχει διαμορφωθεί την αμέσως προηγούμενη της ερώτησης.
- Για τα υπόλοιπα των επενδυτικών λογαριασμών Αμοιβαίων Κεφαλαίων.  
Ο χρήστης έχει τη δυνατότητα να διαχειρίζεται τον κωδικό συνδρομητή στο Alpha Web Banking και το μυστικό κωδικό. Επίσης μπορεί:
  - Να μεταβάλλει τους καταθετικούς λογαριασμούς (προσθήκη, μεταβολή δικαιωμάτων χρήσης, διαγραφή).
  - Να προσθέτει ή να διαγράφει τα στεγαστικά δάνεια.
  - Να προσθέτει ή να διαγράφει κάρτες έκδοσης Alpha Bank και δάνεια Alpha 700.
  - Να προσθέτει λογαριασμούς ΕΥΔΑΠ, προκειμένου να τους πληρώνει μέσω των εναλλακτικών δικτύων της Alpha Bank (Alpha Web Banking, Alphaphone Banking και Alpha Bank m-Banking) ή να τους διαγράφει.
  - Να προσθέτει ή να διαγράφει επενδυτικούς λογαριασμούς αμοιβαίων κεφαλαίων.
  - Να αλλάζει την ονομασία των προδηλωμένων λογαριασμών καταθέσεων, καρτών, δανείων, λογαριασμών ΕΥΔΑΠ καθώς και των επενδυτικών λογαριασμών.
  - Να προσθέτει χαρτοφυλάκιο μετοχών που τηρείται στην Alpha Finance.
  - Να αλλάζει τα στοιχεία επικοινωνίας (αριθμούς τηλεφώνων, ηλεκτρονική διεύθυνση).

- Να ενεργοποιήσει την υπηρεσία για λήψη μηνυμάτων (μέσω e-mail ή SMS) που αφορούν στην ανεπιτυχή εκτέλεση εντολών που έχει καταχωρήσει μέσω των εναλλακτικών δικτύων της Alpha Bank (Alpha Web Banking, Alphaphone Banking και Alpha Bank m-Banking) ή να μεταβάλλει τον τρόπο λήψης των μηνυμάτων αυτών.

Ο χρήστης μπορεί επιπλέον να διαχειρίζεται:

- Τον πρόσθετο κωδικό ασφαλείας (ενεργοποίηση, μεταβολή, απενεργοποίηση) που απαιτείται για την εκτέλεση ορισμένων συναλλαγών.
- Το ανώτατο ημερήσιο ποσό μεταφορών σε μη προδηλωμένους λογαριασμούς.
- Τα βιβλιάρια επιταγών (καταχώρηση αίτησης για έκδοση βιβλιαρίου επιταγών, ερώτηση για την κατάσταση μιας αίτησης, ακύρωση αίτησης).

Η υπηρεσία e-banking της Alpha παρέχει στον πελάτη τη δυνατότητα να ακυρώνει:

- Μεταφορές κεφαλαίων που έχει καταχωρήσει προς εκτέλεση μέσω των εναλλακτικών δικτύων της Alpha Bank.
- Πληρωμές που έχει καταχωρήσει προς εκτέλεση μέσω των εναλλακτικών αυτών δικτύων.
- Αιτήσεις για έκδοση βιβλιαρίων επιταγών που έχει καταχωρήσει.
- Τη λήψη μηνυμάτων που αφορούν στην ανεπιτυχή εκτέλεση εντολών που έχει καταχωρήσει μέσω των εναλλακτικών δικτύων της τράπεζας.
- Τη χρήση του πρόσθετου κωδικού ασφαλείας.

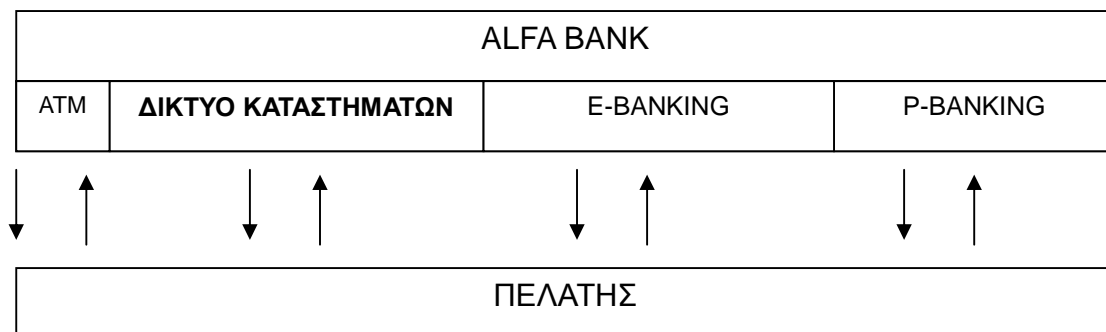
Από τις 07:30 το πρωί μέχρι τις 11:00 το βράδυ μπορούν επίσης να πραγματοποιηθούν ηλεκτρονικά:

- Μεταφορές κεφαλαίων μεταξύ προδηλωμένων λογαριασμών καταθέσεων της τράπεζας, του ίδιου νομίσματος.
- Πληρωμές Τελών Κυκλοφορίας.

#### 6.4.1 Πλαίσιο εφαρμογής e-banking από την ALPHA BANK

Τα Εναλλακτικά Δίκτυα της Alpha Bank παρέχουν στους ιδιώτες πελάτες (Φυσικά Πρόσωπα) έναν εύκολο- εναλλακτικό τρόπο διενέργειας τραπεζικών συναλλαγών μέσω των Υπηρεσιών e-Banking και Phone Banking. Οι Υπηρεσίες e-Banking και Phone Banking υποστηρίζουν το κεντρικό κανάλι επικοινωνίας της Τράπεζας με τους Πελάτες της, που είναι το Δίκτυο των Καταστημάτων.

Πίνακας 6.1 Εναλλακτικά Δίκτυα της Alpha Bank



Πηγή: Αλφα.,(2015),Τραπεζικές Υπηρεσίες, Ανάκτηση από [http://www.go-online.gr/ebusiness/specials/article.html?article\\_id=754](http://www.go-online.gr/ebusiness/specials/article.html?article_id=754) [2015]

Τα οφέλη για τους πελάτες σε σχέση με την εφαρμογή του e-banking αναφέρονται:

1. Οικονομία χρόνου.
2. Διενέργεια συναλλαγών με ελάχιστη προσπάθεια στο χώρο τους.
3. Δυνατότητα παροχής εξελιγμένων υπηρεσιών.
4. Μειωμένες-μηδενικές προμήθειες συναλλαγών.

Το πλαίσιο λειτουργίας SET της τράπεζας βασίζεται σε μια συμμετρική πληροφόρηση, όπου ο χρήστης λαμβάνει έναν κωδικό από την ίδια τη τράπεζα τον οποίο και χρησιμοποιεί προκειμένου να κάνει τις τραπεζικές του συναλλαγές μέσω του Internet. Παρακάτω παραθέτουμε το πλαίσιο υλοποίησης των συναλλαγών με βάση τη μεθοδολογία SET.

Πίνακας 6.2 πλαίσιο υλοποίησης των συναλλαγών με βάση τη μεθοδολογία

Θα ήθελα	Καλώς ήλθατε e-banking Επιχειρήσεων
1. ΠΛΗΡΟΦΟΡΙΕΣ	Εδώ παραθέτονται γενικά στοιχεία για τις προηγούμενες προσπάθειες εισόδου του χρήστη με την εξής μορφή: Αποτυχημένες προηγούμενες συνδέσεις: 7/5/2008 1:55:12 Επιτυχημένες προηγούμενες συνδέσεις 7/4/2008 5:07:56
2. ΕΠΕΝΔΥΣΕΙΣ	
3. ΜΕΤΑΦΟΡΕΣ	
4. ΠΛΗΡΩΜΕΣ	Εδώ υπάρχει ενημέρωση συναλλαγών και γενικά για τις οικονομικές σχέσεις της τράπεζας με το χρήστη. Παρακαλώ επιλέξτε εδώ για να ενημερωθείτε για τις συναλλαγές
5. ΔΙΑΧΕΙΡΙΣΗ ΣΥΝΑΛΛΑΓΩΝ	
6. ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΦΙΛ.	Εδώ ενημερώνεται ο χρήστης σε σχέση με την ασφαλή πρόσβαση του το κωδικό του τι πρέπει να προσέχει και κυρίως να μην εμπιστεύεται άγνωστα τηλέφωνα ή email από άτομα που δεν έχουν σχέση με τη τράπεζα.
7. ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ	
8. ΕΞΟΔΟΣ	
9. ΠΡΟΣΩΠΙΚΑ ΜΥΝΗΜΑΤΑ	Εδώ η τράπεζα με το χρήστη ανταλλάσσουν μηνύματα σ' ένα πεδίο ασφαλής από τρίτους.

Πήγη: Αλφα.,(2015), Τραπεζικές Υπηρεσίες, Ανάκτηση από [http://www.go-online.gr/ebusiness/specials/article.html?article\\_id=754](http://www.go-online.gr/ebusiness/specials/article.html?article_id=754) [2015]

Τα πλεονεκτήματα του παραπάνω πλαισίου για το χρήστη είναι τα ακόλουθα:

1. **Φιλικά Ονόματα:** Δυνατότητα ορισμού Φιλικών Ονομάτων για λογαριασμούς που ορίζονται από τον Πελάτη, αντί των αριθμών Λογαριασμών, Δανείων και Πιστωτικών Καρτών. Για παράδειγμα «Αποταμίευση» αντί του «9800123456».
2. **Υποστήριξη σε πολλές γλώσσες:** Ελληνικά, Αγγλικά, Γαλλικά, Αλβανικά.
3. **Συντομεύσεις:** Δυνατότητα αποθήκευσης των συχνά χρησιμοποιούμενων συναλλαγών, ώστε να μπορούν να χρησιμοποιηθούν ξανά με ελάχιστες κινήσεις.
4. **Απλή διαδικασία εγγραφής:** Μόνο με την Αστυνομική Ταυτότητα και το ΑΦΜ, γίνεται άμεσα η εγγραφή και η παραλαβή των κωδικών πρόσβασης.
5. **Συσκευή ασφαλείας e-Token & Ψηφιακές Υπογραφές:** Παροχή μέγιστου επιπέδου ασφαλείας που δεν παρέχεται από τον ανταγωνισμό στην Ελλάδα (δύο λειτουργίες με την χρήση της ίδιας συσκευής eToken –το eToken χρησιμοποιείται και για την ασφάλεια των συναλλαγών μέσω του ALPHA e-Banking και για την ασφάλεια των συναλλαγών μέσω του ALPHA Phone Banking).
6. **Δια-υπηρεσιακή Εξυπηρέτηση Πελατών:** Μία πολύ-ειδικευμένη ομάδα εξυπηρέτησης Πελατών εξυπηρετεί αποτελεσματικά τον Πελάτη με την χρήση κοινών εφαρμογών και πληροφοριών.

Η τράπεζα έχει αναπτύξει ένα πλαίσιο e-banking το οποίο έχει κατηγοριοποιηθεί σε 5 ενότητες. Αναλυτικά:

1. Υπόλοιπο και ανάλυση καταθετικών λογαριασμών
2. Κινήσεις λογαριασμών έως και 1 χρόνο πίσω
3. Υπόλοιπο, ανάλυση και κινήσεις πιστωτικών καρτών (έως και 3 statement)
4. Συνολική εικόνα προϊόντων (λογαριασμοί, δάνεια, εταιρικές κάρτες)

5. Υπόλοιπο και ανάλυση προθεσμιακών καταθέσεων, δανείων και Αμοιβαίων Κεφαλαίων (λεπτομέρειες Αμοιβαίου Κεφαλαίου και πληροφορίες απόδοσης)

Παρακάτω παραθέτουμε σχετικό παράδειγμα:

1. ΠΛΗΡΟΦΟΡΙΕΣ	Λογαριασμός κάρτες δάνεια συνολική εικόνα προϊόντων
2. ΕΠΕΝΔΥΣΕΙΣ	Πληροφορίες Λογαριασμών
3. ΜΕΤΑΦΟΡΕΣ	Φιλικό Όνομα Αρ. Λογαριασμού Τύπος Λογαρ. Νόμισμα Υπόλοιπο
4. ΠΛΗΡΩΜΕΣ	9800171408 Σε συνάλλαγμα UBD 0,00

### Μεταφορές

1. Μεταφορές χρημάτων μεταξύ προσωπικών λογαριασμών ή σε λογαριασμούς τρίτων στη ALPHA
2. Bank ή σε άλλες Ελληνικές τράπεζες
3. Μαζικές μεταφορές χρημάτων σε λογαριασμούς της ALPHA Bank(μέσω δημιουργίας λίστας ή αποστολής αρχείου).
4. Προγραμματισμένες Μεταφορές σε προσωπικούς λογαριασμούς ή λογαριασμούς τρίτων στη ALPHA Bank ή σε άλλες Ελληνικές τράπεζες, με δυνατότητα δέσμευσης ή όχι του ποσού κατά την καταχώρηση.



Πίνακας 6.3 Προγραμματισμένες Μεταφορές σε προσωπικούς λογαριασμούς ή λογαριασμούς τρίτων στη ALPHA Bank ή σε άλλες Ελληνικές τράπεζες

	Προσωπικούς Λογαριασμούς	Λογαριασμούς τρίτων	Άλλες Ελληνικές Τράπεζες	Μαζικές Μεταφορές
ΠΛΗΡΟΦΟΡΙΕΣ				
ΜΕΤΑΦΟΡΕΣ	Μεταφορές μεταξύ Προσωπικών μου Λογαριασμών			
ΠΛΗΡΩΜΕΣ	1. Επιλέξτε Λογαριασμό	Από	Προς Φιλικό Λογαριασμό	Νόμισμα
ΔΙΑΧΕΙΡΙΣΗ ΣΥΝΑΛΛΑΓΩΝ				
ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΦΙΛ.	Ποσό			
ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ	Αιτιολογία			
ΕΞΟΔΟΣ	Να προστεθεί αυτή η συναλλαγή στις συντομεύσεις μου.			
ΠΡΟΣΩΠΙΚΑ ΜΥΝΗΜΑΤΑ	Φιλικό Όνομα			

Πήγη: Αλφα.,(2015),Τραπεζικές Υπηρεσίες, Ανάκτηση από [http://www.go-online.gr/ebusiness/specials/article.html?article\\_id=754](http://www.go-online.gr/ebusiness/specials/article.html?article_id=754) [2015]

Οι δυνατότητες που δίνονται είναι:

1. Μεταφορές μεταξύ προσωπικών Λογαριασμών.
2. Μεταφορές σε λογαριασμούς τρίτων στη τράπεζα.
3. Μεταφορά σε λογαριασμούς άλλων τραπεζών.
4. Μαζικές μεταφορές χρημάτων σε πολλούς λογαριασμούς ταυτόχρονα με τη χρήση αρχείου.

### **Πληρωμές**

1. Προσωπικών πιστωτικών καρτών ή τρίτου στη τράπεζα ή άλλες Ελληνικές τράπεζες, online ή προγραμματισμένες.
2. Τηλεφωνίας (ΟΤΕ, Tellas ,Vivodi, Forthnet), online ή προγραμματισμένες.
3. Φόρων(ΦΠΑ, φόρος εισοδήματος) online ή προγραμματισμένες.
4. Ασφαλειών(ΙΚΑ, ΤΕΒΕ), online ή προγραμματισμένες.
5. Λοιπών Υπηρεσιών (BMWFS, FIREN, SERFIN, VWBANK, Πλαίσιο), online ή προγραμματισμένες.
6. Καταχώρηση παγίων εντολών πληρωμής (ΟΤΕ, Tellas, Vivodi, Forthnet, ΤΕΒΕ, BMWFS, FIREN, SERFIN, VWBANK).

### **Διαχείριση συναλλαγών**

1. Ενημέρωση για συναλλαγές σε αναμονή εκτέλεσης (έχουν ληφθεί από την τράπεζα και εκκρεμεί η εκτέλεσή τους).
2. Ακύρωση των συναλλαγών σε αναμονή εκτέλεσης.
3. Ενημέρωση για ακυρωμένες και αποτυχημένες συναλλαγές, καθώς και του λόγου αποτυχίας, έως και 7 ημέρες πίσω.
4. Ενημέρωση για τις εκκρεμείς πληρωμές ΔΙΑΣ με δυνατότητα ακύρωσης (ΟΤΕ, Tellas, Vivodi, ΦΠΑ, Φόρος εισοδήματος, ΙΚΑ, ΤΕΒΕ, BMWFS, FIREN, SERFIN).

### **Διαχείριση προφίλ**

1. Διαχείριση ψηφιακού πιστοποιητικού (ενημέρωση, έκδοση, ακύρωση).
2. Αλλαγή προσωπικών κωδικών e-Banking (User ID, Password, Certificate password).
3. Δήλωση και διαγραφή φιλικών ονομάτων λογαριασμών.
4. Προσθήκη και διαγραφή από το ευρετήριο, προσωπικών λογαριασμών και καρτών ή λογαριασμών και καρτών τρίτου στην Alpha Bank ή άλλες Ελληνικές τράπεζες.
5. Διαγραφή συντομεύσεων συναλλαγών.
6. Προσθήκη νέων προϊόντων.
7. Δυνατότητα ρύθμισης Token για την παραγωγή κωδικών μίας χρήσης (για χρήση στο Alpha Phone Banking).
8. Διαχείριση προσωπικών στοιχείων επικοινωνίας (π.χ. καταχώρηση νέου τηλεφώνου) ή διεύθυνσης επικοινωνίας.

Πίνακας 6.4 Διαχείριση προφίλ

	Certificate to password	Αλλαγή password	Μαζικές μεταφορές	Αρχικοποίηση opt
ΠΛΗΡΟΦΟΡΙΕΣ				
ΕΠΕΝΔΥΣΕΙΣ	Αλλαγή password			
ΜΕΤΑΦΟΡΕΣ	Σ' αυτή τη σελίδα ο χρήστης μπορεί να αλλάξει κωδικούς οι κωδικοί θα πρέπει να αποτελούνται από 6 χαρακτήρες.			
ΠΛΗΡΩΜΕΣ	Επιλέξτε	User ID	Προς Φιλικό Λογαριασμό	Νόμισμα
ΔΙΑΧΕΙΡΙΣΗ ΣΥΝΑΛΛΑΓΩΝ	Παλιό User ID			
ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΦΙΛ.	Νέο User ID			
ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ	Επιβεβαίωση νέου User ID			
ΕΞΟΔΟΣ				

Πήγη: Αλφα.,(2015),Τραπεζικές Υπηρεσίες, Ανάκτηση από [http://www.go-online.gr/ebusiness/specials/article.html?article\\_id=754](http://www.go-online.gr/ebusiness/specials/article.html?article_id=754) [2015]

1. Μέσω της Υπηρεσίας e-Banking η ALPHA Bank σας προσφέρει 80% έκπτωση στο υπάρχον τιμολόγιο της τράπεζας
2. Οι προμήθειες εντολών μεταφοράς χρημάτων σε λογαριασμούς άλλων Ελληνικών τραπεζών εξαρτάται από την επιλογή της κατηγορίας χρέωσης (BEN, SHA, OUR)
3. Όλες οι συναλλαγές και πληρωμές σε λογαριασμούς και κάρτες στη ALPHA Bank είναι δωρεάν
4. Οι πληρωμές λογαριασμών τηλεφωνίας, φόρων, ασφαλειών, και λοιπών υπηρεσιών είναι δωρεάν

## Κεφάλαιο 7<sup>ο</sup> Συμπεράσματα

Οι περισσότεροι μελετητές θεωρούν τα blog ως μια μορφή εναλλακτικής δημοσιογραφίας καθώς συμπληρώνουν ουσιαστικά τις υπόλοιπες –κλασικές- πρακτικές του δημοσιογραφικού λόγου και συμβάλλουν στον εκδημοκρατισμό της δημόσιας επικοινωνίας και ενημέρωσης.

Επιπλέον, ανάμεσα στα χαρακτηριστικά τους συγκαταλέγονται και τα τρία βασικά χαρακτηριστικά της δημοσιογραφίας – η υπερκειμενικότητα, η διαδραστικότητα και η πολυμεσικότητα - ενώ η λειτουργία τους είναι ταυτόσημη με τον κύριο σκοπό της δημοσιογραφίας, που δεν είναι άλλος από το να παρέχει στους πολίτες τις πληροφορίες που χρειάζονται ώστε να είναι ελεύθεροι και αυτοκυβερνώμενοι .

Τα blogs έχουν εισχωρήσει στην ελληνική κοινωνία, ως μέσω κοινωνικής επικοινωνίας αλλά και ως μέσω διεύρυνσης της εμπορικής λειτουργίας που αναπτύσσεται μεταξύ των επιχειρήσεων και των πελατών τους. Οι Έλληνες bloggers αυξάνονται συνεχώς κατά χιλιάδες και οι ενασχολούμενες ηλικίες αναφέρονται σ' όλα τα ηλικιακά επίπεδα. Συγκεκριμένα η πλειοψηφία των bloggers βρίσκεται στις νέες και παραγωγικές ηλικίες. Συγκεκριμένα το 38% είναι μεταξύ των ηλικιών 25 και 34 και το 28% μεταξύ των ηλικιών 35-44.

Τα δεδομένα στο Web2.0 δημοσιοποιούνται πράγμα που δε συνάδει με τη τάση του να παραμένουν κρυφά, πράγμα που συνηθιζόταν στο παρελθόν από τις εταιρείες.

## Βιβλιογραφία

- Andrew S.Tanenbaum, “Computer Networks”, Prentice Hall Inc 1989.
- Barger, J. Top Ten Tips for New Bloggers From Original Blogger Jorn Barger, Wired Magazine 2007.
- Carolina M. Laborde, 2010, “Electronic Signatures in International Contracts”, Peter Lang.
- CNET.,(2007), Blogs Turn 10-Who’s the father, Ανάκτηση από <http://www.news.cnet.com>.
- Deuze, M.,(2003), The Web and its Journalisms: Considering the consequences of Different Types of News media Online, New Media & Society, Vol.5, No2 (2003).
- Douglas E. Comer, “Internetworking with TCP/IP, Principles, Protocols and Architecture, Vol 1”, Prentice Hall Inc 2000.
- FaceBook.,(2008), Η έρευνα για τους Bloggers στην Ελλάδα, Ανάκτηση από <http://el-gr.facebook.com/note.php>.
- Furst K, Lang WW, Nolle DE (2002) Internet banking. J Financ Serv Res, Vol.22, No.12,pp.95–117.
- Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP)*, 4(2), 36-48.
- nailtips (2015) Ανάκτηση από:  
<http://www.nailtips.gr/%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD/>, [2015]
- Eatonweb (2015) Ανάκτηση από: <http://www.portal.eatonweb.com> [2015]

- Saferinternet (2015) Ανάκτηση από:  
<http://www.saferinternet.gr/index.php?objId=Category62&parentobjId=Page5-Text165> [2015]
- Anytimeonline (2015) Ανάκτηση από:  
<https://www.anytimeonline.gr/portal/anytime-online-about> [2015].
- John E. Canavan, 2001, “Fundamentals of Network Security”, Artech House
- Johnson G.,(2006), e-banking services, Harvard Business Review.
- Kailash N. Gupta, Kamalesh N. Agarwala, Prateek Amar Agarwala, 2005, ”Digital Signature: Network Security Practices”, PHI Learning Pvt. Ltd.
- Lawnet.,(2006), Ηλεκτρονικές Πληρωμές, Ανάκτηση από:  
<http://www.lawnet.gr> [2015].
- Len Sassaman, 2000, “Email Security”, No Starch Press, Incorporated.
- Mark D. Ciampa, 2011, “Security+ Guide to Network Security Fundamentals, 4ed”, Cengage Learning.
- Matyas, V., & Zdenek, J.R. (2000). *Biometric authentication systems*. Technical report, ECOM-Monitor.
- Nancy Flynn, Randolph Kahn, 2003, “Email Rules”, AMACOM Div American Mgmt Assn.
- Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.
- Peterson P.,(2007), The new Banking services, McGraw Hill.
- Phillip J. Windley, 2008, “Digital Identity”, O'Reilly Media, Inc.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 34(3), 503-522.
- Summers, R.,”Secure Computing Threats and Safeguards”, McGraw-Hill 1997.

- T. Bradley, 2006 “Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security”, Syngress.
- Tipton, H. F., & Krause, M. (2012). *Information security management handbook*. CRC Press.
- Wenbo, M.(2003), *Modern Cryptography: Theory and Practice*. Prentice Hall.
- Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.
- [www.microsoft.com/security](http://www.microsoft.com/security).
- Αλφα.,(2015), Τραπεζικές Υπηρεσίες, Ανάκτηση από [http://www.go-online.gr/ebusiness/specials/article.html?article\\_id=754](http://www.go-online.gr/ebusiness/specials/article.html?article_id=754) [2015].
- Γιαννόπουλος Γ.Ν.,(2001), Προστασία Προσωπικών Δεδομένων και διανοσυριακή ροή πληροφοριών, Τόμος 11, Εκδόσεις Σάκουλας, σελ. 733.
- Εργαστήριο Εκπαιδευτικής και Γλωσσικής Τεχνολογίας.,(2010), Token Ring, <http://hermes.di.uoa.gr/RETUDIS/Token%20ring/Main.htm>.
- Πατέλη Δ.,(2000), Η δημοσιογραφία στον Ιστό, Σημειώσεις Οικονομικού Πανεπιστημίου Αθηνών.
- Σπύρου Ν.,(2007), Υπηρεσίες ηλεκτρονικής τραπεζικής, Ελευθεροτυπία.