Είδη – Μορφές και Ασφάλεια Ηλεκτρονικού Εμπορίου

Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Διοίκησης και Οικονομίας

Τμήμα Διοίκησης Επιχειρήσεων

Επιβλέπων Καθηγητής
Ρομπογιαννάκης Ι.

Μαυρομουστακάκη Αντιγόνη
Α.Μ. 4006

« If your business is not on the Internet,
Then your business will be out of business »
Bill Gates

ΑΘΗΝΑ,
ΟΚΤΩΒΡΙΟΣ 2018

COPYRIGHT

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Ρομπογιαννάκη Ιωάννη, PhD για την βοήθεια και την στήριξη του καθ' όλη τη διάρκεια εκπόνησης της εργασίας, την Co-Founder and Head of HR & Culture, Ανθουλάκη Αγγέλα, καθώς και τον Chief Technology Officer, Βαβίλη Παναγιώτη της εταιρίας Enartia Group of Brands με έδρα την Βιομηχανική Περιοχή Ηρακλείου Κρήτης, για την βοήθεια στο ερευνητικό κομμάτι της εργασίας, χωρίς τη συμβολή τους το 5ο Κεφάλαιο εκτός από υπόσταση δεν θα είχε τόσο αξιόπιστες πληροφορίες. Εν συνεχεία την μητέρα μου για την υπομονή της και τέλος τον Λιναρδάκη Χαράλαμπο για την συνεχή του στήριξη και τον περίγυρο μας, που χωρίς αυτούς η δειγματοληψία του ερωτηματολογίου δεν θα ήταν τόσο εύκολη.

ΠΕΡΙΛΗΨΗ

Το ηλεκτρονικό εμπόριο είναι μια μορφή εμπορίου που επιτρέπει αφενός στις επιχειρήσεις να διαφημίζουν και να πωλούν τα προϊόντα τους στο ευρύτερο κοινό μέσω του διαδικτύου και αφετέρου επιτρέπει στους καταναλωτές να διευρύνουν τους αγοραστικούς τους ορίζοντες πέρα από τις τοπικές αγορές και να ανακαλύπτουν προϊόντα και υπηρεσίες που παλαιότερα ήταν εντελώς άγνωστα. Όλα αυτά διέπονται από διάφορες τεχνικές και ζητήματα ασφαλείας προκειμένου μια τέτοια ηλεκτρονική συναλλαγή να είναι win-win τόσο για τον ηλεκτρονικό πωλητή όσο και για τον αγοραστή.

Ο σκοπός καθώς και τα ερωτήματα που απαντώνται στην παρούσα εργασία είναι να γίνουν κατανοητά τόσο τα είδη και οι μορφές του ηλεκτρονικού εμπορίου καθώς επίσης και οι μηχανισμοί ασφαλείας που προηγούνται προκειμένου να επέλθει η τελική μορφή του εκάστοτε ηλεκτρονικού εμπορίου. Ποιά είναι τα βήματα που απαιτούνται για να γίνει μια ηλεκτρονική συναλλαγή; Πώς καθίσταται μια τέτοια συναλλαγή ασφαλής και ποιες είναι οι διενέργειες που πρέπει να γίνουν μέχρι την πληρωμή του προϊόντος ή της υπηρεσίας;

Αυτά τα ζητήματα και άλλα πολλά θα διερευνηθούν στην εκπόνηση της παρούσας ερευνητικής εργασίας με τη χρήση διάφορων μεθόδων ανάπτυξης.

Λέξεις κλειδιά : Ηλεκτρονικό εμπόριο, είδη ηλεκτρονικού εμπορίου, ασφάλεια ηλεκτρονικού εμπορίου, πρωτόκολλο ασφαλείας, νομικό πλαίσιο

ABSTRACT

E-commerce is a form of commerce that allows businesses to advertise and sell their products to the general public via the internet and allows the customers to broaden their purchasing horizons beyond the local markets and discover products and services that previously were completely unknown. All of this actions governed by various security techniques and issues in order for the online transaction to be win-win for both the vendor and the buyer.

The objective of this research is to understand both the types and forms of e-commerce, as well as the security actions that came before the final form of the e-commerce. What are the steps required to make an online transaction? How does such a transaction become safe and what are the actions to be taken until the payment of the product or service?

Those matters and much more will be explored in this research by using various development methods.

Keywords: E-commerce, forms of e-commerce, e-commerce security, security protocol

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1^{Ο} : ΕΙΣΑΓΩΓΙΚΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

1.1 ΕΙΣΑΓΩΓΗ

Διανύουμε μια εποχή όπου εύκολα θα χαρακτηριζόταν ως ‘’διαδικτυακή’’, καθώς δεν υφίσταται νοικοκυριό που να μην έχει υπολογιστή ή κινητό τηλέφωνο στην κατοχή του που να μην είναι συνδεδεμένα στο διαδίκτυο λιγότερο από 1 με 2 ώρες ημερησίως. Η κατάσταση αυτή δίνει ένα γερό πάτημα στον επιχειρηματικό τομέα να εξελιχθεί από τον παραδοσιακό τρόπο εμπορίου στον ηλεκτρονικό.

Στο 1ο κεφάλαιο αναπτύσσεται ο ορισμός του ηλεκτρονικού εμπορίου έτσι ώστε να γίνει κατανοητή η έννοια σ’ ένα μεγάλο βαθμό. Παρατίθεται μία σύντομη ιστορική αναδρομή για να γίνει αντιληπτή η διαφορά του παραδοσιακού από το ηλεκτρονικό εμπόριο καθώς επίσης αναφέρεται αναλυτικά το θεσμικό πλαίσιο που διέπει τις διαδικασίες του ηλεκτρονικού εμπορίου. Τέλος όπως κάθε τι καινούριο είναι φυσιολογικό να έχει τα υπέρ και τα κατά του για όλους τους τομείς στους οποίους απευθύνεται πχ. Κοινωνία, καταναλωτές κτλ.

Προχωράμε στο 2ο κεφάλαιο στο οποίο μας δίνεται η δυνατότητα να διαχωρίσουμε τα είδη αυτής της κατηγορίας ανάλογα με τα συναλλασσόμενα μέρη στα οποία απευθύνονται. Θα μελετήσουμε με ενδελεχή λεπτομέρεια τις 4 κατηγορίες που ο **απευθυνόμενος είναι η επιχείρηση** προς τους καταναλωτές, άλλες επιχειρήσεις, το κράτος και το εμπόριο στα μέλη εντός της επιχείρησης. Στη συνέχεια θα εντρυφήσουμε σε 3 κατηγορίες όπου ο **απευθυνόμενος είναι το κράτος** προς τους καταναλωτές, τα άλλα κράτη και τις επιχειρήσεις και τέλος έχουμε ακόμα 3 κατηγορίες με **απευθυνόμενο τον πελάτη** προς αντίστοιχα τους άλλους πελάτες, το κράτος και τις επιχειρήσεις.

Στα μέσα της εργασίας θα συναντήσουμε το 3ο κεφάλαιο στο οποίο γίνεται λόγος για τις μορφές ηλεκτρονικού εμπορίου με τις οποίες άλλοι ερχόμαστε σε επαφή καθημερινά και άλλοι εξυπηρετούμαστε ιδιαίτερα. Οι μορφές αυτές εν συντομία είναι : α) το ηλ. κατάστημα, β) η ηλ. Αγορά, γ) το ηλ. Επιχειρήν, δ) η ηλ. Επιχείρηση, ε) η ηλ. Μεσιτεία, στ) η ηλ. Δημοπρασία, ζ) το ηλ. Σύστημα προμηθειών, η) το ηλ. Εμπορικό κέντρο.

Κλείνοντας, στο 4ο και σημαντικότερο κεφάλαιο της παρούσας εργασίας μελετούμε τους τρόπους συναλλαγής για τις ηλεκτρονικές αγορές, τα τεχνικά ζητήματα ασφαλείας

καθώς και τους κινδύνους που διέπουν αυτού του είδους τις συναλλαγές χρησιμοποιώντας εικόνες και προσωπική επίθεση προκειμένου να γίνει περισσότερο κατανοητή η έννοια και το πόσο εύκολα μπορεί να πραγματοποιηθεί μία απάτη .

Πάνω σε αυτό το κομμάτι θα πραγματοποιηθεί και αντίστοιχη έρευνα την οποία βλέπουμε αναλυτικά στο 5ο και τελευταίο κεφάλαιο και είναι βασισμένη στις μεθόδους του ερωτηματολογίου σε ευρύ κοινό για την προτίμηση αυτού του είδους εμπορίου και της συνέντευξης από τον CTO System Administrator Βαβίλη Παναγιώτη της Enartia Group of Brands, πάνω στα ζητήματα ασφαλείας.

Στη συνέντευξη θα καλυφτούν θέματα πάνω στον τομέα της ασφάλειας του Web Hosting ,E-mail Hosting & Word Press Hosting καθώς και στην δημιουργία, διαχείριση και ασφάλεια ενός e–shop.

1.2 ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Καλπάζουσα ανάπτυξη παρατηρείται στον επιχειρηματικό τομέα ιδίως σε επιχειρήσεις που χρησιμοποιούν ένα από τα πιο διαδεδομένα εργαλεία του INTERNET που τους επιτρέπει να διεισδύουν σε αγορές και πελατολόγιο που παλαιότερα ήταν αν όχι ανέφικτο, σίγουρα απρόσιτο.

Ο λόγος γίνεται για το Ηλεκτρονικό Εμπόριο ή Ηλεκτρονικό Επιχειρήν. Ο τίτλος υιοθετήθηκε προκειμένου να είναι διακριτός ο τρόπος με τον οποίο δραστηριοποιείται η εκάστοτε επιχείρηση, από αυτές που ακολουθούν την πεπατημένη οδό και κρατάνε τα παραδοσιακά μοτίβα ανάπτυξης.

Υπάρχουν αρκετοί γενικοί όροι για την περιγραφή του ηλεκτρονικού εμπορίου αλλά στην ουσία ηλεκτρονικό εμπόριο είναι η δυνατότητα των καταναλωτών και των εμπορικών καταστημάτων να διεξάγουν εμπορικές συναλλαγές μέσω του Διαδικτύου.

Το ηλεκτρονικό εμπόριο ορίζεται ως «η διαδικασία της αγοράς και πώλησης ή ανταλλαγής αγαθών, υπηρεσιών και πληροφοριών μέσω δικτύων υπολογιστών, συμπεριλαμβανομένου και του διαδικτύου» (Turban, 2006).

Παρότι δείχνει απλός, θα πρέπει να επικεντρωθούμε σε τρία βασικά σημεία του:

Το πρώτο σημαντικό σημείο του ορισμού που αναφέρεται παραπάνω, αφορά τα μέσα πραγματοποίησης του ηλεκτρονικού εμπορίου. Το διαδίκτυο αποτελεί ένα από αυτά, αυτό όμως δεν το καθιστά μοναδικό. Στα μέσα του ηλεκτρονικού εμπορίου συγκαταλέγονται, επίσης, το τηλέφωνο, η τηλεόραση, η τηλεομοιοτυπία. (Bacchetta,

1998) Το διαδίκτυο παρέχει διάφορα πλεονεκτήματα κατά την πραγματοποίηση μιας εμπορικής συναλλαγής κάτι το οποίο έχει ως αποτέλεσμα να συνδέεται άρρηκτα με τον όρο ‘’Ηλεκτρονικό εμπόριο’’. Το διαδίκτυο επιτρέπει την ταυτόχρονη μετάδοση φωνής, εικόνας και κειμένου με εφαρμογές πολυμέσων και για αυτό το λόγο διευρύνει το φάσμα των αγαθών και υπηρεσιών από απόσταση ενώ επιτρέπει την πραγματοποίηση του συνόλου μιας εμπορικής συναλλαγής μέσω αυτού.

Το δεύτερο βασικό σημείο του ορισμού που αναφέρθηκε είναι η έννοια της διαδικασίας. Μια εμπορική συναλλαγή έχει μια πορεία με τρεις διακριτές φάσεις:

- την παραγγελία,
- την πληρωμή και
- την παράδοση του προϊόντος.

Ανάλογα με το βαθμό της ψηφιοποίησης κάθε μιας από τις φάσεις αυτές μπορεί να γίνει λόγος για άμεσο ή έμμεσο ηλεκτρονικό εμπόριο. (Turban, 2006)

Το τρίτο σημαντικό σημείο του ορισμού αφορά την υπόσταση της συναλλαγής. Με λίγα λόγια δεν περιορίζεται στα αγαθά, αλλά συμπεριλαμβάνει τις υπηρεσίες και τις πληροφορίες. Επισημαίνεται ότι στη διεθνή επιστημονική κοινότητα επικρατεί η τάση να χρησιμοποιείται ο όρος «προϊόν» για να περιγράψει τόσο αγαθά όσο και υπηρεσίες.

Το ηλεκτρονικό εμπόριο διακρίνεται σε έμμεσο και άμεσο. Ο πρώτος όρος χρησιμοποιείται όταν πρόκειται για την ηλεκτρονική παραγγελία υλικών αγαθών που μπορούν να παραδοθούν μόνο με παραδοσιακούς τρόπους όπως είναι το ταχυδρομείο. Άμεσο είναι το ηλεκτρονικό εμπόριο που περιλαμβάνει παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την αρωγή πάντα και τη σύμπραξη των τραπεζών.

1.3 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ *(ΑΠΟ ΤΟ ΠΑΡΑΔΟΣΙΑΚΟ → ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ)*

Η εξέλιξη και η πορεία του ηλεκτρονικού εμπορίου είναι άρρηκτα συνδεδεμένη με την ανάπτυξη των δικτύων υπολογιστών και του internet. Οι πρώτες μορφές του Ηλεκτρονικού Εμπορίου εμφανίζονται στις αρχές του 1970, όταν οι τράπεζες χρησιμοποίησαν την Ηλεκτρονική Μεταφορά Κεφαλαίων (EFT) για τις συναλλαγές τις οποίες πραγματοποιούσαν μέσω ασφαλών ιδιωτικών δικτύων, βελτιώνοντας τα συστήματα πληρωμών.

Στις αρχές του ‘80 το ηλεκτρονικό εμπόριο διαδόθηκε μεταξύ των επιχειρήσεων, αρχικά ως τεχνολογία ηλεκτρονικής μετάδοσης μηνυμάτων, όπως η ηλεκτρονική ανταλλαγή δεδομένων (EDI) και το ηλεκτρονικό ταχυδρομείο (email) για να επικοινωνούν οι εταιρίες μεταξύ τους. Οι τεχνολογίες του EDI συντελέσαν στον εκσυγχρονισμό των διεργασιών μεταξύ των επιχειρήσεων, αφού αυξήθηκε η αυτοματοποίηση, μειώνοντας έτσι τα έγγραφα και τα δεδομένα σε χαρτί, επιτρέποντας στις επιχειρήσεις να επικοινωνούν ηλεκτρονικά.

Η κορύφωση του πραγματοποιείται από το 1990 και μετά, όταν το διαδίκτυο εξελίσσεται σημαντικά και γίνεται γνωστό και προσιτό σε ολοένα και περισσότερους χρήστες με την εμφάνιση του παγκόσμιου ιστού. Η εμφάνισή του παρείχε την δυνατότητα για διαφορετικές μορφές ηλεκτρονικού εμπορίου, όπως για παράδειγμα υπηρεσίες σε απευθείας σύνδεση και νέες μορφές άντλησης πληροφοριών και επικοινωνίας μεταξύ των χρηστών. Από τότε και μετά εμφανίζονται οι μορφές B2C, C2C, G2C, G2B και το ηλεκτρονικό εμπόριο επεκτείνεται σε νέους τομείς. Μία επιχείρηση πλέον μπορεί να απευθυνθεί σε ένα ευρύτατο αγοραστικό κοινό το οποίο μπορεί να βρίσκεται σε οποιοδήποτε σημείο του πλανήτη χωρίς να είναι υποχρεωτική η φυσική παρουσία του καταναλωτή στον χώρο πώλησης. Αυτό το γεγονός από μόνο του παρέχει σημαντική δυναμική για το εμπόριο και για τις διεθνείς αλλά και εγχώριες οικονομικές αγορές. Στις μέρες μας νέες μορφές ηλεκτρονικού εμπορίου δημιουργούνται και εξελίσσονται χάρη στην εξέλιξη της τεχνολογίας τέτοιες είναι το κινητό εμπόριο (m- commerce) και το «πανταχού παρόν» ηλεκτρονικό εμπόριο (u-commerce).

1.4 ΕΓΧΩΡΙΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ & ΝΟΜΟΕΣΙΑ ΗΛ. ΕΜΠΟΡΙΟΥ

Το ηλεκτρονικό εμπόριο είναι μια μορφή εμπορίου και, συνεπώς, βρίσκουν εφαρμογή σε αυτό όλες οι κοινοτικές οδηγίες (το κοινοτικό δίκαιο) και οι εθνικές διατάξεις, για την προστασία του Καταναλωτή, που αφορούν το εμπόριο γενικότερα. Έχοντας υπόψη τον διασυνοριακό χαρακτήρα του παγκόσμιου ιστού και των δυνατοτήτων αυτού, κάθε κράτος θεσπίζει μια σειρά νομοθετημάτων, είτε προσαρμόζοντας υφιστάμενα, είτε εκδίδοντας νέα, προκειμένου αφενός μεν, να ενισχυθούν οι ηλεκτρονικές συναλλαγές, αφετέρου δε αυτές να τυγχάνουν νόμιμες κατά το εσωτερικό δίκαιο και ασφαλείς για τους συναλλασσομένους.

Κάθε μέλος κράτος της Ευρωπαϊκής Ένωσης υποχρεούται να ενσωματώνει τις διάφορες νομοθετικές ρυθμίσεις της Ευρωπαϊκής Ένωσης στην εθνική νομοθεσία. Έτσι η Ελλάδα ενσωμάτωσε αρκετές από αυτές τις ρυθμίσεις στο εθνικό της δίκαιο.

Κυριότερη είναι το Προεδρικό Διάταγμα 131/2003 που αποτελεί προσαρμογή της οδηγίας 2000/31/ΕΚ σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.

Παράλληλα με το προεδρικό διάταγμα 131/2003 σε ειδικότερους τομείς, ισχύουν και άλλα νομοθετήματα. Αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα παροχών υπηρεσιών πιστοποίησης των προϊόντων ηλεκτρονικής υπογραφής έχει οριστεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ., 2018).

Οι κοινοτικές οδηγίες και οι διατάξεις που διέπουν την προστασία του καταναλωτή έχουν αναρτηθεί από την ανωτέρω επιτροπή.

- Ο νόμος 2251/94 περί προστασίας καταναλωτών στο άρθρο 4 ρυθμίζει τις συμβάσεις από απόσταση. Εδώ ανατρέχει και το ηλεκτρονικό εμπόριο. Ο νόμος 2472/97 περί προστασίας προσωπικών δεδομένων και ο νόμος 2774/99που αφορά την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.
- Το προεδρικό διάταγμα 150/2001, ΦΕΚ Α’125 για τις ηλεκτρονικές υπογραφές δείχνει την προσπάθεια του κράτους να προσφέρει μια σωστή βάση νομοθετικών πλαισίων. Το προεδρικό διάταγμα που εκδόθηκε την 22 Νοεμβρίου 2002, καθορίζει τις καταστάσεις στις οποίες είναι απαραίτητη μια ψηφιακή υπογραφή. Δηλώνει ξεκάθαρα ότι μια ψηφιακή υπογραφή είναι απαραίτητη σε ένα ηλεκτρονικό έγγραφο εάν αυτό το έγγραφο έχει νομική συνέπεια. Αυτό σημαίνει ότι μόνο «αβλαβή» έγγραφα μπορούν να παραδοθούν στους δημόσιους διαχειριστές, ενώ σχεδόν όλες οι σημαντικές συναλλαγές πρέπει να χρησιμοποιούν έναν μηχανισμό ψηφιακής υπογραφής.
- Το προεδρικό διάταγμα 131/2003 για το ηλεκτρονικό εμπόριο δίνει έμφαση στην εξώδικη επίλυση διαφορών, στη συνεργασία των κρατών μελών της Ευρωπαϊκής ένωσης, στην επίλυση των προβλημάτων των καταναλωτών, στη θέσπιση κανόνων δεοντολογίας με υποχρεωτική ισχύ για τους αποδέκτες τους, στην σύναψη ηλεκτρονικών συμβάσεων, στην ευθύνη των ενδιάμεσων, στον τόπο εγκατάστασης των φορέων παροχής υπηρεσιών, στις πληροφορίες που πρέπει να παρέχονται στις εμπορικές επικοινωνίες.
- Οι καταναλωτές όταν αγοράζουν από χώρες εκτός Ευρωπαϊκής Ένωσης πρώτα απ’ όλα πρέπει να αναζητούν το νομοθετικό κανονιστικό πλαίσιο που θα διέπει τις αγορές τους.
- Η σύμβαση των Βρυξελών προβλέπει ότι σε περίπτωση διαφοράς που θα προκύψει με έμπορο ή εταιρεία εκτός της χώρας του καταναλωτή αλλά εντός της

Ευρωπαϊκής Ένωσης, ο καταναλωτής θα μπορεί να προσφύγει στο δικαστήριο του τόπου κατοικίας του. Το δίκαιο που θα εφαρμόσει το δικαστήριο καθορίζεται από τη σύμβαση της Ρώμης και ως επί το πλείστον είναι το δίκαιο της χώρας του. Το Υπουργείο Ανάπτυξης γνωρίζοντας τη σημαντική αύξηση του ηλεκτρονικού εμπορίου στην Ελλάδα και θέλοντας να εξασφαλίσει την ασφάλεια των συναλλαγών, ενσωμάτωσε στην Ελληνική νομοθεσία με την Κοινή Υπουργική Απόφαση Ζ1-891 του 2013 (ΦΕΚ Β'2144/30.08.13), τις διατάξεις της Οδηγίας 2011/83/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου του 2011 σχετικά με τα δικαιώματα των καταναλωτών, την τροποποίηση της οδηγίας 93/13/ΕΟΚ του Συμβουλίου και της οδηγίας1999/44/ΕΚ. Τα βασικότερα σημεία αυτής της απόφασης η οποία τέθηκε σε ισχύ στις 13Ιουνίου του 2014 είναι τα εξής:

- ✓ Ο καταναλωτής έχει προθεσμία 14 ημερολογιακών ημερών για να υπαναχωρήσει εάν έχει κάνει αγορές εξ' αποστάσεως, χωρίς να αναφέρει τους λόγους επιβαρυνόμενος μόνο τη δαπάνη επιστροφής του προϊόντος. Ο προμηθευτής από τη μεριά του υποχρεούται να επιστρέψει τα χρήματα, μαζί με τα έξοδα αποστολής εντός 14 ημερολογιακών ημερών από την ημέρα που ενημερώθηκε από τον καταναλωτή ότι υπαναχωρεί. Εάν ο προμηθευτής δεν έχει ενημερώσει τον καταναλωτή για το δικαίωμα υπαναχώρησης, τότε η προθεσμία υπαναχώρησης λήγει 12 μήνες μετά την κανονική προθεσμία των 14 ημερών.
- ✓ Ο προμηθευτής οφείλει να έχει παραδώσει το προϊόν εντός 30 ημερών από την παραγγελία, εκτός και αν έχει συμφωνηθεί άλλη ημερομηνία παραλαβής.
- ✓ Ο καταναλωτής ευθύνεται για τυχόν μείωση της αξίας του προϊόντος μόνο εάν ο ίδιος προέβη σε κακή χρήση αυτού π.χ. εάν αποσυσκευάσει το προϊόν για να δει πως είναι και αυτό λειτουργεί δεν σημαίνει ότι μειώνει την αξία του.
- ✓ Θεσπίζεται υποχρέωση λεπτομερούς και σαφούς ενημέρωσης των καταναλωτών για το συνολικό κόστος του προϊόντος ή της υπηρεσίας πριν την πραγματοποίηση της αγοράς, στις συναλλαγές που γίνονται μέσω διαδικτύου, μέσω ηλεκτρονικού ταχυδρομείου, μέσω fax, μέσω τηλεφώνου και εκτός εμπορικού καταστήματος.
- ✓ Ειδικότερα, οι προμηθευτές οφείλουν να αναφέρουν το συνολικό κόστος του προϊόντος ή της υπηρεσίας, όπως και κάθε άλλη πρόσθετη δαπάνη (έξοδα μεταφοράς, δασμοί, ΦΠΑ κλπ.), πριν την πραγματοποίηση της αγοράς ενώ ο καταναλωτής που αγοράζει ηλεκτρονικά δεν θα υποχρεούται να πληρώνει επιβαρύνσεις ή άλλες δαπάνες, εάν δεν έχει ενημερωθεί πλήρως και λεπτομερώς πριν κάνει την παραγγελία.

- ✓ Δημιουργείται ενιαίο πανευρωπαϊκό έντυπο υπαναχώρησης που καθιστά απλή τη διαδικασία υπαναχώρησης σε διασυνοριακές συναλλαγές.
- ✓ Αναφέρονται με σαφήνεια τα δικαιώματα και οι υποχρεώσεις του καταναλωτή και του προμηθευτή σε περίπτωση ακύρωσης μιας σύμβασης.
- ✓ Ο καταναλωτής ενημερώνεται με σαφήνεια για το ποιος πληρώνει τα έξοδα σε περίπτωση επιστροφής των προϊόντων.
- ✓ Παρέχεται ειδική προστασία των καταναλωτών σε περίπτωση συμβάσεων που συνάπτονται δια τηλεφώνου (cold calling).

  Η σύμβαση είναι έγκυρη και ισχύει από τη στιγμή που ο καταναλωτής υπογράψει ότι αποδέχεται την προσφορά, ενώ μέχρι σήμερα αρκούσε η προφορική συναίνεση δια τηλεφώνου για την εγκυρότητα της σύμβασης.
- ✓ Απαγορεύεται να επιβαρύνονται οι καταναλωτές με επιπλέον κόστος όταν πληρώνουν με πιστωτική κάρτα. Επίσης απαγορεύεται οποιαδήποτε επιπρόσθετη χρέωση των καταναλωτών πέραν της βασικής τιμής χρέωσης όταν καλούν σε γραμμή εξυπηρέτησης.
- ✓ Ενισχύεται η προστασία των καταναλωτών σε ότι αφορά στα ψηφιακά προϊόντα (υποχρέωση παροχής ενημέρωσης σχετικά με τη συμβατότητα του περιεχομένου, τις τεχνικές προδιαγραφές του hardware και του software).
- ✓ Θεσπίζεται υποχρέωση ενημέρωσης των καταναλωτών, πριν την πραγματοποίηση της αγοράς, για τα βασικά στοιχεία που αφορούν μία συναλλαγή π.χ. το συνολικό κόστος, τον τρόπο πληρωμής, τη διάρκεια της σύμβασης, για αγορές που γίνονται εντός εμπορικών καταστημάτων. (Ναυτεμπορική, 2018, Ε.Ε.Α., 2018)

1.5 ΤΑ ΥΠΕΡ ΚΑΙ ΤΑ ΚΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

1.5.1 ΤΑ ΥΠΕΡ ΤΟΥ ΗΛ. ΕΜΠΟΡΙΟΥ ΑΝΑ ΚΑΤΗΓΟΡΙΑ

ΓΙΑ ΤΟΥΣ ΚΑΤΑΝΑΛΩΤΕΣ

Ένας δικτυακός τόπος αρχίζει να υφίσταται από την ώρα που ξεκινάει να έχει απήχηση στο αγοραστικό κοινό, συνεχόμενα και όχι παροδικά. Τα πλεονεκτήματα που εντοπίζονται είναι τα εξής :

- **Τα ηλεκτρονικά καταστήματα είναι ανοιχτά 24 ώρες το 24ωρο.**

Σύμφωνα με έρευνες που έχουν διεξαχθεί σε πολλές ανεπτυγμένες χώρες, οι άνθρωποι σήμερα παραπονιούνται περισσότερο για την έλλειψη χρόνου παρά για την έλλειψη χρημάτων. Με άλλα λόγια οποιαδήποτε στιγμή επιθυμεί ο καταναλωτής μπορεί

να αγοράσει οτιδήποτε. Τα δικτυακά καταστήματα είναι ανοιχτά όλο το εικοσιτετράωρο και μπορούν να αποδειχθούν πολύ χρήσιμα σε χρονικά πιεσμένες κατηγορίες ανθρώπων.

- **Μειωμένο Κόστος**

Το κόστος των προϊόντων που διατίθενται στους δικτυακούς τόπους είναι αισθητά πιο χαμηλό απ' ότι στα φυσικά καταστήματα, αφού ένα ηλεκτρονικό κατάστημα είναι απαλλαγμένο από ένα μεγάλο μέρος του λειτουργικού κόστους ενός πραγματικού καταστήματος. Για παράδειγμα δεν υπάρχουν τα κόστη που σχετίζονται με την ενοικίαση χώρου και αέρα, το ηλεκτρικό, το νερό, κλπ και γενικά απαιτεί πολύ λιγότερο υπαλληλικό προσωπικό.

- **Η αγορά είναι παγκόσμια.**

Οι ορίζοντες του καταναλωτή διευρύνονται αφού μέσω του υπολογιστή μπορεί κανείς να αγοράσει ακόμα και κάτι το οποίο δεν κυκλοφορεί στην Ελλάδα.

- **Η συναλλαγή είναι γρήγορη και άμεση.**

Αυτό σημαίνει ότι από τη στιγμή που ολοκληρώνεται η παραγγελία το αργότερο σε 3- 4 ημέρες θα γίνει η λήψη της, ακόμη και αν το κατάστημα βρισκόταν στην άλλη άκρη του πλανήτη. Ο κάθε καταναλωτής βρίσκει αυτό που θέλει, χωρίς κόπο και χωρίς καμία σπατάλη χρόνου.

- **Καλύτερη εξυπηρέτηση των πελατών**

Το ηλεκτρονικό εμπόριο μπορεί να βελτιώσει σε πολύ μεγάλο βαθμό την εξυπηρέτηση των πελατών, αυτοματοποιώντας τη διαδικασία απάντησης στις πιο συχνές και συνηθισμένες ερωτήσεις, επιτρέποντας έτσι στο ανθρώπινο δυναμικό της επιχείρησης να ασχοληθεί με τις περιπτώσεις που πραγματικά απαιτούν ιδιαίτερη προσοχή. Η διαθεσιμότητα της υποστήριξης των πελατών σε εικοσιτετράωρη βάση και όλες τις ημέρες του χρόνου είναι ένα πολύ ισχυρό ανταγωνιστικό εργαλείο.

- **Μείωση του λειτουργικού κόστους για τους προμηθευτές, με τα αντίστοιχα οφέλη και για τους πελάτες**

Δηλαδή υπάρχει μείωση κόστους και δυνατότητα εξασφάλισης καλύτερων τιμών. Επίσης, κάθε επικοινωνία που είναι απαραίτητη για μια εμπορική συναλλαγή κοστίζει και διαρκεί λιγότερο αν πραγματοποιηθεί ηλεκτρονικά.

- **Μεγαλύτερη εξοικονόμηση χρόνου.**

Ο χρόνος που απαιτείται για την εκτύπωση των τιμολογίων εξοικονομείται στο μεγαλύτερο μέρος του, ενώ η τιμολόγηση λαμβάνει χώρα 24 ώρες το 24ωρο. Εν

κατακλείδι το e-invoice συντελεί στη βελτίωση του επιπέδου συνεργασίας μεταξύ προμηθευτή και εφεξής αμφότερα μπορούν να απολαμβάνουν υπηρεσίες προστιθέμενης αξίας, που καθιστούν την εργασία του ευκολότερη, αποδοτικότερη και παραγωγικότερη. (Πασχόπουλου & Σκαλτσάς, 2001)

ΓΙΑ ΤΗΝ ΚΟΙΝΩΝΙΑ

Αναφορικά με το παρελθόν, κοινωνίες κυρίως σε απομακρυσμένες περιοχές, ορεινά χωριά ή νησιά άγονης γραμμής με δύσκολη πρόσβαση δεν είχαν την δυνατότητα να εκμεταλλευτούν προϊόντα και υπηρεσίες όπως αυτές που ήταν διαθέσιμες στις μεγαλουπόλεις.

Πλέον αυτό έχει αλλάξει και όλοι έχουν ίσες ευκαιρίες στην αγορά και εκμετάλλευση υπηρεσιών και παροχών σε όποιο μέρος του πλανήτη κι αν βρίσκονται. Αυτή είναι μια πολύ σημαντική δυνατότητα, από αυτές που στο παρελθόν ήταν αδύνατο να πραγματοποιηθούν.

ΓΙΑ ΤΟΥΣ ΟΡΓΑΝΙΣΜΟΥΣ

- **Αγορά χωρίς σύνορα**

Κάθε εταιρία που έχει ηλεκτρονική παρουσία μπορεί να παρουσιάσει τον κύκλο εργασιών της επεκτείνοντας τα γεωγραφικά όρια των συναλλαγών της. Αυτό σημαίνει πως κάθε επιχείρηση που διαθέτει τα προϊόντα της onlineμπορεί και αποκτά πελάτες σε περιοχές που βρίσκονται μακριά από την έδρα της ακόμη και στο εξωτερικό και μάλιστα με ελάχιστο λειτουργικό κόστος.

- **Βελτιωμένη ανταγωνιστικότητα**

Κάθε εταιρία που χρησιμοποιεί τις νέες τεχνολογίες όπως το Διαδίκτυο γίνεται πιο ανταγωνιστική, αφού μπορεί να ενημερώνεται πιο εύκολα για τις τρέχουσες εξελίξεις στο χώρο της. Με άλλα λόγια και δεδομένου ότι σε λίγα χρόνια όλες οι εμπορικές δραστηριότητες θα γίνονται μέσω διαδικτύου. Το ηλεκτρονικό εμπόριο είναι η νέα μεγάλη πρόκληση για κάθε εταιρία που θέλει να είναι ανταγωνιστική. Το ηλεκτρονικό εμπόριο διευκολύνει σε μεγάλο βαθμό τη διερεύνηση της αγοράς και τον εντοπισμό του κατάλληλου προϊόντος στην κατάλληλη τιμή σε συντομότερο χρόνο και με σχεδόν μηδενικό κόστος.

- **Βελτίωση της δημόσιας εικόνας της επιχείρησης**

Το ηλεκτρονικό εμπόριο μπορεί να αποτελέσει ένα θετικό στοιχείο της δημόσιας εικόνας μιας επιχείρησης, ιδιαίτερα όταν η επιχείρηση αυτή απευθύνεται σε τμήματα

της αγοράς με ευνοϊκή στάση απέναντι στη νέα τεχνολογία. Η δημόσια εικόνα είναι ένα από τα πολυτιμότερα άυλα κεφάλαια μιας επιχείρησης. Μάλιστα, πολλές επιχειρήσεις επενδύουν τεράστια κεφάλαια για την καλλιέργεια και τη διατήρηση μιας ισχυρής επωνυμίας. Αυτό ισχύει κυρίως στις ανταγωνιστικές αγορές, όπου οι διαφορές μεταξύ των προϊόντων είναι μικρές και δεν επαρκούν για να κερδίσουν την προτίμηση των καταναλωτών.

- **Αμφίδρομη σχέση μεταξύ επιχείρησης και καταναλωτή**

Η εταιρία μέσω των ηλεκτρονικών συναλλαγών μπορεί να συλλέξει πολλά στοιχεία για τις συνήθειες, τις ανάγκες και τα γούστα των καταναλωτών και σύμφωνα με αυτά να αναπροσαρμόσει την πολιτική της προς το θετικότερο. Γνωρίζοντας τις ανάγκες των πελατών τους, οι εταιρίες μπορούν να προχωρήσουν στη δημιουργία προϊόντων είτε ανταποκρινόμενων σε έναν καταναλωτή είτε σε μια ομάδα καταναλωτών που χρειάζονται ένα προϊόν το οποίο δεν υπάρχει ακόμη στην αγορά.

- **Ελαχιστοποίηση Κόστους**

Η επιχείρηση που υποχρεούται στην έκδοση των τιμολογίων (προμηθευτής) μειώνει σημαντικά δαπάνες της για αναλώσιμα υλικά (μελάνι, χαρτί, ειδικοί εκτυπωτές κλπ.). Συγχρόνως και ο λιανέμπορος ευνοείται καθώς δεν υποχρεώνεται να τυπώνει τα τιμολόγια. Μπορεί δηλαδή να διατηρηθεί σε ηλεκτρονική μορφή, αρχειοθετούμενα σε κάποιο ψηφιακό αποθηκευτικό μέσο εργασιών.

- **Μείωση δυσλειτουργιών**

Οι δυσλειτουργίες που υπήρχαν στο παραδοσιακό εμπόριο, όπως η απώλεια τιμολογίων, φθορά παραστατικών κατά την διάρκεια της παράδοσης ή ακόμα και λανθασμένα στοιχεία στα παραστατικά που την ώρα της εργασίας δεν γίνονταν αντιληπτά, πλέον εκμηδενίζονται και είναι γεγονός το κέρδος που αποφέρει ένας δικτυακός τόπος είναι πραγματικό.

- **Ευρύ πεδίο δραστηριοτήτων**

Το ηλεκτρονικό εμπόριο βρίσκει εφαρμογή σε ένα ευρύ πεδίο δραστηριοτήτων, πυρήνας των οποίων αποτελεί ο κύκλος των εμπορικών συναλλαγών. Κατά συνέπεια γίνεται λόγος για την ηλεκτρονική εμπορευματοποίηση των φυσικών αγαθών και υπηρεσιών, τη διαφήμιση και προώθηση αυτών, την διευκόλυνση της επικοινωνίας μεταξύ των εμπόρων, την υποστήριξη πελάτη (πριν και μετά την πώληση), την εξαγγελία δημόσιας προμήθειας και την υποστήριξη κοινών επιχειρηματικών διαδικασιών. (Porter, 1985)

- **Καλύτερος έλεγχος αποθεμάτων**

Οι ηλεκτρονικές επικοινωνίες επιταχύνουν την ολοκλήρωση των συναλλαγών, αυξάνοντας έτσι την ευελιξία στις προμήθειες των επιχειρήσεων. Πολλές επιχειρήσεις αξιοποιούν τη δυνατότητα αυτή με την εφαρμογή του συστήματος JIT (Just-In-Time), που μειώνει τα περιθώρια ανανέωσης των αποθεμάτων, περιορίζοντας έτσι το κόστος παραγωγής και διάθεσης των προϊόντων τους. Στην πραγματικότητα πάντοτε υπάρχει ανάγκη για ένα ελάχιστο απόθετα ασφαλείας.

Ο χρόνος είναι ο παράγοντας που επιτρέπει τον περιορισμό της ελάχιστης απαραίτητης ποσότητας αποθεμάτων. Όσο λιγότερος χρόνος απαιτείται για την ολοκλήρωση μιας παραγγελίας, τόσο πιο μικρό απόθεμα είναι υποχρεωμένη να κρατά μια επιχείρηση.

Η συνεχής παρακολούθηση των αποθεμάτων από το σύστημα μηχανογράφησης επιτρέπει την πραγματοποίηση προβλέψεων για το επίπεδο των αναγκών στο μέλλον. Υπάρχει η δυνατότητα σύνδεσης των συστημάτων της επιχείρησης με τον προμηθευτή, ώστε ο τελευταίος να χρησιμοποιεί τις προβλέψεις για τον έλεγχο των δικών του αποθεμάτων και να καλύπτει αυτόματα τις ανάγκες της επιχείρησης. (Παρασχόπουλος & Σκαλτσάς, 2000)

1.5.2 ΤΑ ΚΑΤΑ ΤΟΥ ΗΛ. ΕΜΠΟΡΙΟΥ ΑΝΑ ΚΑΤΗΓΟΡΙΑ

ΓΙΑ ΤΟΥΣ ΚΑΤΑΝΑΛΩΤΕΣ

- **Πλαστοπροσωπία**

Ένας σοβαρός αλλά όχι ιδιαίτερα γνωστός κίνδυνος για τον καταναλωτή που επιλέγει να κάνει χρήση του ηλεκτρονικού εμπορίου είναι η πλαστοπροσωπία. Έγκειται στο να χρησιμοποιήσει κάποιος τη δικτυακή ταυτότητα κάποιου άλλου με κακόβουλο σκοπό. Η λύση είναι περίπλοκη, τόσο τεχνικά όσο και διαδικαστικά και νομικά.

Μια ιδιόμορφη περίπτωση που μοιάζει με πλαστοπροσωπία είναι η χρήση ενός ονόματος κάποιου δικτυακού τόπου που να διαφέρει μόνο σε ένα γράμμα από το άλλο. Αν τα δύο αυτά γράμματα βρίσκονται κοντά στο πληκτρολόγιο τότε ένας χρήστης κάνοντας ένα απλό ορθογραφικό λάθος βρίσκεται σε μια άλλη σελίδα συνήθως όμοιας μορφής με την σωστή και μπορεί να πραγματοποιήσει συναλλαγές χωρίς να γίνει αντιληπτό το λάθος του.

- **Ανυπαρξία ασφάλειας στις ηλεκτρονικές πληρωμές**

Λόγω του ότι οι πληρωμές είναι απρόσωπες και χωρίς να είναι γνωστή η γεωγραφική θέση των μερών, είναι εύκολο να χρησιμοποιηθούν κλασικά μοτίβα εξαπάτησης. Στις πληρωμές μέσω διαδικτύου είναι δύσκολο να φτιάξει κανείς εγγυητική αρχή. Ο

κίνδυνος που υπάρχει είναι να εγγραφεί ένας μεγάλος αριθμός πληρωμών, να μην συμψηφιστεί άμεσα και η εταιρία να μην αποστείλει το προϊόν. Σε αυτή την περίπτωση ο έχων λαμβάνειν θα βρεθεί να έχει δώσει χρήματα χωρίς ποτέ να λάβει το προϊόν για το οποίο πλήρωσε.

- **Έλλειψη επαφής πωλητή-πελάτη**

Με την έλλειψη επαφής μεταξύ πωλητή – πελάτη, δημιουργείται δυσπιστία από την πλευρά του καταναλωτή καθώς δεν του προσφέρεται η δυνατότητα να δει το προϊόν και να διαπιστώσει τη φερεγγυότητα του πωλητή. Συνεπώς, δεν νιώθει το αίσθημα της ασφάλειας αν αυτό που βλέπει στον υπολογιστή ανταποκρίνεται στη πραγματικότητα. (Σκαλίδης, 2000)

ΓΙΑ ΤΗΝ ΚΟΙΝΩΝΙΑ

Υπάρχει η πιθανότητα δημιουργίας δύο ταχυτήτων καταναλωτών. Πρόκειται για ένα εν δυνάμει σοβαρό κοινωνικό πρόβλημα που αφορά τους καταναλωτές. Ειδικά σε κοινωνίες με σημαντικές οικονομικές ανισότητες ο κίνδυνος είναι ότι οι χρήστες του διαδικτύου θα γίνουν πλουσιότεροι αγοράζοντας την «φθηνή» παγκόσμια αγορά του διαδικτύου, ενώ, οι φτωχοί θα παγιδευτούν σε μια πρωτόγονη και ακριβή οικονομία. (Σκαλίδης, 2000)

ΓΙΑ ΤΟΥΣ ΟΡΓΑΝΙΣΜΟΥΣ

- **Ανυπαρξία ασφάλειας στις ηλεκτρονικές πληρωμές**

Η έλλειψη εμπιστοσύνης του καταναλωτή προς το διαδίκτυο με αποτέλεσμα να υπάρχει δισταγμός στην πληρωμή του προϊόντος ή της υπηρεσίας μέσω πιστωτικής κάρτας.

- **Αδυναμία στην παρουσίαση των προϊόντων**

Μερικά είδη επιχειρήσεων όπως για παράδειγμα εταιρίες με είδη ρούχων, ευαίσθητων τροφίμων, κοσμημάτων είναι σχεδόν αδύνατον, προς το παρόν τουλάχιστον, να ελεγχθούν επαρκώς για την ποιότητα που προσφέρουν, από μια απομακρυσμένη τοποθεσία, αν και υπάρχουν εξαιρέσεις.

- **Υψηλά κόστη υλοποίησης και βελτιστοποίησης ηλεκτρονικού καταστήματος.**

Οι τεχνολογίες αλλάζουν και εξελίσσονται καθημερινά και αυτό έχει ως αποτέλεσμα το κόστος για την υλοποίηση ενός απλού ηλεκτρονικού καταστήματος να αυξηθεί δραματικά πολύ. Εν συνεχεία η διατήρηση ενός τέτοιου καταστήματος που θέλει να πληρεί όλες τις σύγχρονες προϋποθέσεις απαιτεί επένδυση μεγάλων χρηματικών ποσών από τις επιχειρήσεις η τα φυσικά πρόσωπα που τα διαθέτουν.

ΚΕΦΑΛΑΙΟ 2^{Ο} : ΕΙΔΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Το ηλεκτρονικό εμπόριο διαχωρίζεται σε δύο κατηγορίες. Το άμεσο και το έμμεσο. Με τον όρο άμεσο εννοούμε το ηλεκτρονικό εμπόριο το οποίο από την ώρα που γίνεται η ηλεκτρονική παραγγελία, η πληρωμή και η παράδοση του αγαθού γίνεται απευθείας σε ψηφιακή μορφή.

Έμμεσο ηλεκτρονικό εμπόριο είναι αυτό το οποίο χρειάζεται κάποια διαδικασία προκειμένου το αγορασθέν προϊόν να φτάσει στον πελάτη. Η διαδικασία αυτή π.χ. είναι το ταχυδρομείο.

Βέβαια τα είδη του ηλεκτρονικού εμπορίου διευρύνονται σε μια πιο μεγάλη γκάμα από αυτή του άμεσου και του έμμεσου και αυτό οφείλεται στα διάφορα συναλλασσόμενα μέρη που υπάρχουν όπως θα τα διαχωρίσουμε παρακάτω :

2.1 ΗΛ. ΕΜΠΟΡΙΟ ΠΡΟΣ ΤΟΥΣ ΚΑΤΑΝΑΛΩΤΕΣ (B2C)

Το Business to Consumer (B2C) είναι ένα από τα πιο δημοφιλή και ευρέως γνωστά μοντέλα πωλήσεων. Η ιδέα του B2C χρησιμοποιήθηκε για πρώτη φορά από τον Michael Aldrich το 1979, ο οποίος χρησιμοποίησε την τηλεόραση ως το κύριο μέσο για να προσεγγίσει τους καταναλωτές. Η παραδοσιακή προσέγγιση του B2C αναφέρεται στον παραδοσιακό τρόπο αγορών. Ωστόσο, η άνοδος του διαδικτύου δημιούργησε ένα εντελώς νέο επιχειρηματικό κανάλι B2C με τη μορφή ηλεκτρονικού εμπορίου ή πώλησης αγαθών και υπηρεσιών μέσω του Διαδικτύου.

Ο όρος B2C έγινε πολύ δημοφιλής μετά την εξαιρετικά μεγάλη ανοδική πορεία του DOTCOM στα τέλη της δεκαετίας του ’90, όταν η κύρια χρήση του έγινε προκειμένου να εξυπηρετούνται ηλεκτρονικοί έμποροι λιανικής πώλησης, καθώς και άλλες εταιρίες που έκαναν εμπόριο αγαθών μέσω διαδικτύου.

Οι επιχειρήσεις που βασίζονται στο B2C πρέπει να κάνουν τον καταναλωτή να έχει μια συναισθηματική ανταπόκριση στο μάρκετινγκ που χρησιμοποιούν και να διατηρούν τόσο καλές σχέσεις με αυτούς όσο και καλό κλίμα εντός του χώρου για να έχει πάντα λόγο ο πελάτης να επιστρέφει

Εταιρίες B2C με παρουσία στο διαδίκτυο που συνεχίζουν να κυριαρχούν πάνω από τους παραδοσιακούς ανταγωνιστές τους είναι το Amazon, η Priceline, ο Zappos (που

αγοράστηκαν από την Amazon το 2009), το eBay και το Victoria's Secret αναφερόμενοι ως επιζώντες της πρώιμης έκρηξης της DOTCOM καθώς συνεχίζουν να επεκτείνονται με επιτυχία και να διαταράσσουν συνεχώς την παγκόσμια βιομηχανία. Υπάρχουν πέντε τύποι επιχειρηματικών μοντέλων B2C που οι περισσότερες εταιρείες χρησιμοποιούν ηλεκτρονικά για να στοχεύουν τους καταναλωτές:

Απευθείας πωλητές: Είναι το πιο γνωστό είδος μοντέλου, όπου οι καταναλωτές αγοράζουν αγαθά από ιστότοπους ηλεκτρονικής λιανικής πώλησης. Αυτές μπορεί να περιλαμβάνουν μικρές επιχειρήσεις ή σε απευθείας σύνδεση μεγάλα πολυκαταστήματα που πωλούν προϊόντα από διαφορετικούς κατασκευαστές.

Διαδικτυακοί διαμεσολαβητές: Πρόκειται για διαμεσολαβητές μέσω των οποίων οι καταναλωτές αγοράζουν τις υπηρεσίες ή τα προϊόντα που επιλέγουν. Στην πραγματικότητα οι διαμεσολαβητές δεν διαθέτουν δικά τους προϊόντα ή υπηρεσίες που συνδέουν αγοραστές και πωλητές. Σκεφτείτε περιοχές όπως η Expedia, Trivago ή Etsy.

B2C με βάση τη διαφήμιση: Αυτό το μοντέλο χρησιμοποιεί δωρεάν περιεχόμενο για να προσελκύσει επισκέπτες σε έναν ιστότοπο. Αυτοί οι επισκέπτες, με τη σειρά τους, συναντούν ψηφιακές ή online διαφημίσεις. Για να καταλήξουμε στην πώληση των αγαθών και των υπηρεσιών χρησιμοποιούνται μεγάλοι όγκοι διαδικτυακής κυκλοφορίας προκειμένου να πολωθούν διαφημίσεις που τα προβάλουν. Ένα παράδειγμα θα ήταν οι χώροι των μέσων ενημέρωσης όπως το Huffington Post, ένα site υψηλής επισκεψιμότητας που αναμειγνύεται στη διαφήμιση με το εγγενές του περιεχόμενο.

Κοινοτική βάση: Οι ιστότοποι όπως το Facebook, το οποίο χτίζει τις διαδικτυακές κοινότητες βάσει κοινών συμφερόντων, βοηθούν τους εμπόρους και τους διαφημιζόμενους να μεταφέρουν τα προϊόντα τους απευθείας στους καταναλωτές. Οι ιστότοποι στοχεύουν τις διαφημίσεις τους βάσει των δημογραφικών στοιχείων και της γεωγραφικής θέσης των χρηστών.

Free-Based: Είναι ιστότοποι που απευθύνονται απευθείας στους καταναλωτές, όπως το Netflix, που χρεώνουν ένα τέλος, ώστε οι καταναλωτές να έχουν πρόσβαση στο περιεχόμενό τους. Μερικές φορές, ο ιστότοπος μπορεί να προσφέρει δωρεάν, αλλά για περιορισμένο περιεχόμενο ή χρονικό διάστημα, ενώ χρεώνει το μεγαλύτερο μέρος του. Οι New York Times και άλλες μεγάλες εφημερίδες συχνά χρησιμοποιούν ένα επιχειρηματικό μοντέλο B2C που βασίζεται σε αμοιβές. (Investopedia, 2018)

2.2 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΠΡΟΣ ΤΗΝ ΕΠΙΧΕΙΡΗΣΗ (B2B)

Αναφερόμαστε σε συνεργασίες που διεξάγονται μεταξύ εταιριών και όχι μεταξύ εταιρίας και μεμονωμένων καταναλωτών. Τέτοιες είναι συναλλαγές μεταξύ κατασκευαστών και χονδρέμπορων ή μεταξύ χονδρέμπορων και λιανοπωλητών.

Οι συναλλαγές μεταξύ επιχειρήσεων είναι κοινές σε μια τυπική αλυσίδα εφοδιασμού, καθώς στηρίζονται σε εταιρίες που αγοράζουν προϊόντα και πρώτες ύλες για χρήση στις παραγωγικές διαδικασίες. Τα τελικά προϊόντα μπορούν στη συνέχεια να πωληθούν σε ιδιώτες μέσω συναλλαγών μεταξύ επιχειρήσεων και καταναλωτών.

Η ερευνητική εταιρεία Forrester εκτιμά ότι το 2014, το αμερικανικό λιανικό εμπόριο στις ΗΠΑ αντιπροσώπευε περίπου το ήμισυ του ακαθάριστου εγχώριου προϊόντος της οικονομίας των ΗΠΑ, που πωλούσε πάνω από 8 τρισεκατομμύρια δολάρια σε αγαθά. Το 2017, ο Forrester δήλωσε ότι αναμένει από την αγορά **ηλεκτρονικού εμπορίου B2B** να φτάσει τα 1,1 τρισεκατομμύρια δολάρια στις ΗΠΑ έως το 2021, αντιπροσωπεύοντας το 13% όλων των πωλήσεων B2B στο έθνος.

Το διαδίκτυο παρέχει ένα ισχυρό περιβάλλον στο οποίο οι επιχειρήσεις μπορούν να ανακαλύψουν προϊόντα και υπηρεσίες και να θέσουν τις βάσεις για μελλοντικές συναλλαγές μεταξύ επιχειρήσεων. Οι ιστοσελίδες των εταιριών επιτρέπουν στα ενδιαφερόμενα μέρη να μάθουν για τα προϊόντα και τις υπηρεσίες μιας επιχείρησης πριν ξεκινήσουν την επαφή μαζί τους και οι ιστοσελίδες ηλεκτρονικής ανταλλαγής προϊόντων και πρώτων υλών επιτρέπουν στις επιχειρήσεις να αναζητούν προϊόντα και υπηρεσίες και να κλείνουν συμφωνίες μέσω της πλατφόρμας **ηλεκτρονικής προμήθειας**.

Προκειμένου να γίνει περισσότερο κατανοητή η κατηγορία του B2B, παραθέτουμε τα ακόλουθα παραδείγματα :

1. Οι συναλλαγές μεταξύ επιχειρήσεων και οι μεγάλοι εταιρικοί λογαριασμοί είναι συνηθισμένο φαινόμενο για τις επιχειρήσεις παραγωγής. Η **Samsung,** για παράδειγμα, είναι ένας από τους μεγαλύτερους προμηθευτές της **Apple** στην παραγωγή του iPhone. Οι αναφορές στα τέλη του 2017 εκτιμούν ότι η Samsung θα μπορούσε εισπράξει έως 22 δισεκατομμύρια δολάρια από τις οθόνες OLED που προμηθεύει την Apple για τα iPhone εν έτει 2018. Η Apple διατηρεί επίσης σχέσεις B2B με εταιρείες όπως η **Intel**, η **Panasonic** και η **Micron Technology** .
2. Οι συναλλαγές B2B είναι επίσης η ραχοκοκαλιά της **αυτοκινητοβιομηχανίας**. Πολλά από τα εξαρτήματα των οχημάτων κατασκευάζονται ανεξάρτητα, και οι

κατασκευαστές αυτοκινήτων τα αγοράζουν για να συναρμολογήσουν τα παραγόμενα αυτοκίνητα. Τα ελαστικά, οι μπαταρίες, τα ηλεκτρονικά, οι εύκαμπτοι σωλήνες και οι κλειδαριές των θυρών, για παράδειγμα, κατασκευάζονται συνήθως από διάφορες εταιρείες και πωλούνται απευθείας στους κατασκευαστές αυτοκινήτων.

3. Οι πάροχοι υπηρεσιών πραγματοποιούν επίσης συναλλαγές B2B. Οι εταιρείες που ειδικεύονται στη διαχείριση ακινήτων, την καθαριότητα και τη βιομηχανική εξυγίανση, πωλούν συχνά αυτές τις υπηρεσίες αποκλειστικά σε άλλες επιχειρήσεις, και όχι σε μεμονωμένους καταναλωτές. (Investodepia, 2018)

2.3 ΗΛ. ΕΜΠΟΡΙΟ ΜΕΤΑΞΥ ΕΤΑΙΡΙΩΝ& ΚΡΑΤΟΥΣ (B2G)

Η κατηγορία B2G καλύπτει συμβάσεις κάθε είδους-για αγαθά, υπηρεσίες και πληροφορίες-μεταξύ επιχειρήσεων κάθε μεγέθους και κυβέρνησης σε όλα τα επίπεδα (κρατικό, τοπικό και ομοσπονδιακό). Το κράτος ενημερώνει τις επιχειρήσεις ηλεκτρονικά για διαγωνισμούς, προκηρύξεις, δημοπρασίες και αυτές υποβάλλουν ηλεκτρονικά τις αιτήσεις τους. Γίνεται πλέον ηλεκτρονική έκδοση πιστοποιητικών, προμηθειών δημοσίου, αυτοματοποίησης των συναλλαγών, ηλεκτρονική πιστοποίηση της επιχείρησης, δυνατότητα ηλεκτρονικής πληρωμής κ.α.

Η μορφή αυτή του ηλεκτρονικού εμπορίου έχει σαν αποτέλεσμα την μείωση των λειτουργικών εξόδων, την παροχή καλύτερων και πιο γρήγορων υπηρεσιών και τον αποτελεσματικότερο έλεγχο εσόδων και διαφάνειας. Οι κυβερνήσεις χρειάζονται περισσότερο χρόνο απ’ ότι οι ιδιωτικές εταιρίες για να εγκρίνουν κι να αρχίσουν να εργάζονται σ’ ένα συγκεκριμένο έργο, αυτό οφείλεται εν μέρει επειδή το κίνητρο κέρδους απουσιάζει και εν μέρει στις γραφειοκρατικές αυστηρότητες.

Οι κυβερνητικές συμβάσεις είναι συχνά μεγάλες και συχνά πιο σταθερές από τις ανάλογες εργασίες του ιδιωτικού τομέα. Παράδειγμα πάλι στη χώρα μας το πρόγραμμα TAXIS με την ηλεκτρονική υποβολή δηλώσεων Φ.Π.Α, e-παράβολο, υποβολή Φ.Μ.Υ, e-Α.Π.Α.Α, e-Κ.Β.Σ κ.α. Οι εφαρμογές αυτές γίνονται μέσα στους γνωστούς σε όλους ιστότοπους όπως www.gsis.gov.gr, www.ika.gr, www.oga.gr κλπ. (Investopedia, 2018)

2.4 ΕΝΔΟΕΠΙΧΕΙΡΗΣΙΑΚΟ ΗΛ. ΕΜΠΟΡΙΟ (B2E)

Ένας άλλος τύπος πώλησης που οι εταιρείες αρχίζουν να βρίσκουν πιο ελκυστικό, ιδιαίτερα οι μεγάλες εταιρείες είναι το B2E ή η πώληση σε επιχειρήσεις. Αυτό

περιλαμβάνει την πώληση προϊόντων και υπηρεσιών εντός της εταιρείας και τη διαφήμιση αυτών στους υπαλλήλους μέσω διάφορων εταιρικών εφαρμογών όπως τα intranets και το ηλεκτρονικό ταχυδρομείο. Συχνά εφαρμόζονται ειδικές εκπτώσεις ή συμφωνίες προς τους υπαλλήλους για να παρακινηθούν και να αγοράσουν από την εταιρεία. Το B2E έχει ως στόχο την εξάπλωση πληροφοριών και χρήσιμων υπηρεσιών μεταξύ των εργαζομένων για να ενθαρρυνθεί η συνολική ανάπτυξη της εταιρείας.

Στην κατηγορία των μη κερδοσκοπικών υπηρεσιών, οι πρωτοβουλίες B2E συνήθως εμπίπτουν σε δύο ομάδες που λειτουργούν ως ηλεκτρονικές εφαρμογές μέσω του intranet της εταιρείας ή του διαδικτύου. Η πρώτη ομάδα ασχολείται κυρίως με τις λειτουργίες ανθρώπινου δυναμικού (HR), προσφέροντας στους εργαζόμενους πολλές δυνατότητες και πληροφορίες. Ενημερώσεις σχετικά με τις δυνατότητες υγειονομικής περίθαλψης, μισθοδοσίας και άλλων μορφών αποζημίωσης, μαζί με όλους τους τύπους online εταιρικής κατάρτισης. Η διάδοση μηνυμάτων ή ανακοινώσεων σε ολόκληρη την εταιρεία ανήκει επίσης στο πρώτο κομμάτι. Η δεύτερη ομάδα περιλαμβάνει πιο εκτεταμένες μορφές παροχών σε εργαζόμενους, όπως κρατήσεις για ταξίδια, αποζημίωση για ορισμένα είδη δαπανών προσωπικού, υπηρεσίες πίστωσης και διαχείριση ασφάλισης.

Ένας ξεχωριστός τύπος μη κερδοσκοπικών υπηρεσιών B2E επιτρέπει στους υπαλλήλους να έχουν πρόσβαση σε εξειδικευμένους ιστοχώρους που περιέχουν τις απαραίτητες πληροφορίες για αυτούς και τα καθήκοντά τους. Αυτό μπορεί να περιλαμβάνει δεδομένα, λειτουργίες αναζήτησης δεδομένων και ορισμένες πληροφορίες που είναι διαθέσιμες μόνο σε συγκεκριμένους υπαλλήλους. Ακόμη υπάρχουν στατιστικά που επιτρέπουν στους αναλυτές να συλλέγουν δεδομένα σχετικά με το ποιοι υπάλληλοι χρησιμοποιούν υπηρεσίες B2E, ποιες ευκαιρίες επιλέγονται περισσότερο και ποιες υπηρεσίες είναι οι πιο επιτυχημένες. (Simon & Shaffer, 2001)

2.5 ΗΛ. ΕΜΠΟΡΙΟ ΜΕΤΑΞΥ ΚΡΑΤΟΥΣ & ΚΑΝΑΝΑΛΩΤΩΝ (G2C)

Η κυβέρνηση προς καταναλωτή (G2C) περιλαμβάνει πρωτοβουλίες που αποσκοπούν στη διευκόλυνση της αλληλεπίδρασης των ανθρώπων με την κυβέρνηση ως καταναλωτές δημοσίων υπηρεσιών. Αυτό περιλαμβάνει τις αλληλεπιδράσεις που σχετίζονται με την παροχή δημόσιων υπηρεσιών καθώς και με τη συμμετοχή στη διαδικασία διαβούλευσης και λήψης αποφάσεων. (Public Institutions and Digital Government Department of Economic and Social Affairs, 2018)

2.6 ΗΛ. ΕΜΠΟΡΙΟΜΕΤΑΞΥ ΚΡΑΤΩΝ (G2G or E-GOVERNANCE)

Η ηλεκτρονική διακυβέρνηση χρησιμοποιείται για δραστηριότητες που αφορούν από τις «ηλεκτρονικές κυβερνητικές υπηρεσίες» έως την «ηλεκτρονική ανταλλαγή πληροφοριών και υπηρεσιών με πολίτες, επιχειρήσεις και άλλα όργανα της κυβέρνησης». Παραδοσιακά, η ηλεκτρονική διακυβέρνηση θεωρείται ως η χρήση των τεχνολογιών πληροφορίας και επικοινωνίας (ΤΠΕ) για τη βελτίωση των κυβερνητικών υπηρεσιών και την παροχή κρατικών υπηρεσιών μέσω διαδικτύου. Εν συνεχεία το πλαίσιο της ηλεκτρονικής διακυβέρνησης διευρύνεται ώστε να περιλαμβάνει τη χρήση των ΤΠΕ από την κυβέρνηση για τη διεξαγωγή ευρέος φάσματος αλληλεπιδράσεων με τους πολίτες και τις επιχειρήσεις, καθώς και ανοικτά κυβερνητικά δεδομένα και χρήση των ΤΠΕ για να καταστεί δυνατή η καινοτομία στη διακυβέρνηση.

Επομένως, η ηλεκτρονική διακυβέρνηση μπορεί να οριστεί ως η χρήση των ΤΠΕ για αποτελεσματικότερη παροχή κυβερνητικών υπηρεσιών στους πολίτες και τις επιχειρήσεις. Η εφαρμογή των ΤΠΕ σε αυτές τις επιχειρήσεις, επιτυγχάνει τους δημόσιους στόχους που τίθενται μέσω των ψηφιακών μέσων, καθώς η βασική αρχή της ηλεκτρονικής διακυβέρνησης, υποστηριζόμενη από ένα αποτελεσματικό θεσμικό πλαίσιο, είναι η βελτίωση της εσωτερικής λειτουργίας του δημόσιου τομέα με τη μείωση του οικονομικού κόστους και των χρόνων συναλλαγής, έτσι ώστε να ενσωματωθούν καλύτερα οι ροές εργασίας και οι διαδικασίες και να καταστεί δυνατή η αποτελεσματικότερη χρήση των πόρων από τους διάφορους οργανισμούς του δημόσιου τομέα που στοχεύουν σε βιώσιμες λύσεις. Μέσω της καινοτομίας και της ηλεκτρονικής διακυβέρνησης, οι ανά τον κόσμο κυβερνήσεις μπορούν να είναι πιο αποτελεσματικές, να παρέχουν καλύτερες υπηρεσίες, να ανταποκρίνονται στις απαιτήσεις του κοινού, να είναι πιο περιεκτικές και έτσι να αποκαθίσταται η εμπιστοσύνη των πολιτών στις κυβερνήσεις τους. (Public Institutions and Digital Government Department of Economic and Social Affairs, 2018)

2.7 ΗΛ. ΕΜΠΟΡΙΟ ΜΕΤΑΞΥ ΚΡΑΤΟΥΣ & ΕΠΙΧΕΙΡΗΣΕΩΝ (G2B)

Το G2B είναι το επιχειρηματικό μοντέλο που αναφέρεται στην παροχή κρατικών υπηρεσιών ή πληροφοριών στην οργάνωση επιχειρήσεων. Η κυβέρνηση χρησιμοποιεί τον ιστότοπο μοντέλου B2G για να προσεγγίσει επιχειρηματικούς οργανισμούς. (Siingh, 2018)

Τέτοιες ιστοσελίδες υποστηρίζουν :

- προσφορές
- λειτουργίες υποβολής αιτήσεων
- δημόσιες συμβάσεις
- ηλεκτρονικές αγορές προμηθειών
- ηλεκτρονικές δημοπρασίες
- αποστολή συμπληρωμένων ηλεκτρονικών εντύπων (π.χ. έντυπα φόρου, κοινωνικής ασφάλισης)
- αποστολή ηλεκτρονικών πληρωμών
- αποστολή – λήψη απαντήσεων ηλεκτρονικά

2.8 ΗΛ. ΕΜΠΟΡΙΟ ΜΕΤΑΞΥ ΚΑΤΑΝΑΛΩΤΩΝ (C2C)

Το επιχειρηματικό μοντέλο ‘’πελάτης προς τον πελάτη’’ (C2C) επιτρέπει στους πελάτες να μπορούν να πραγματοποιούν συναλλαγές μεταξύ τους συνήθως στο ηλεκτρονικό περιβάλλον. Ένας τρόπος που μπορεί να υλοποιηθεί το εμπόριο C2C είναι οι δημοπρασίες. Το C2C έχει πάρει μεγάλες διαστάσεις και είναι πλέον πολύ δημοφιλές από την άφιξη του διαδικτύου. Τέτοιες εταιρίες με ανοδική πορεία είναι το eBay και το Craigslist.

Στην βάση του το C2C αντιπροσωπεύει ένα περιβάλλον αγοράς όπου ένας πελάτης αγοράζει αγαθά από άλλον πελάτη χρησιμοποιώντας μια επιχείρηση ή μια πλατφόρμα τρίτου για τη διευκόλυνση της συναλλαγής αυτής. Οι επιχειρήσεις C2C είναι ένας νέος τύπος μοντέλου που έχει προκύψει με την τεχνολογία ηλεκτρονικού εμπορίου. Το πλεονέκτημα για τους πελάτες είναι ότι επωφελούνται από τον ανταγωνισμό για προϊόντα και συχνά βρίσκουν αντικείμενα που είναι δύσκολο να βρεθούν αλλού. Επιπλέον, τα περιθώρια είναι υψηλά για τους πωλητές, επειδή υπάρχει ελάχιστο κόστος λόγω της έλλειψης λιανοπωλητών ή χονδρεμπόρων. Οι τοποθεσίες C2C είναι εύκολα προσβάσιμες επειδή δεν υπάρχει ανάγκη να επίσκεψης ενός φυσικού καταστήματος. Οι καταναλωτές απλά διαφημίζουν τα προϊόντα τους στο διαδίκτυο και οι αγοραστές ανταποκρίνονται. Στην περίπτωση του eBay, τα αντικείμενα αποστέλλονται απευθείας από τον πωλητή στον αγοραστή. (Investopedia, 2018)

2.9 ΗΛ. ΕΜΠΟΡΙΟ ΜΕΤΑΞΥ ΚΑΤΑΝΑΛΩΤΩΝ & ΚΡΑΤΟΥΣ (C2G)

Το C2G μαζί με το B2G είναι οι πιο πρόσφατες κατηγορίες ηλεκτρονικού εμπορίου, δημιουργήθηκαν τα τελευταία χρόνια και αποτελούν μέρος ενός νέου αναπτυσσόμενου κλάδου της ηλεκτρονικής διακυβέρνησης (e-government).

Η εν λόγω συναλλαγή αφορά όλες τις ενέργειες που γίνονται μεταξύ καταναλωτή και κράτους (C2G). Είναι ακόμα σε αρχικό στάδιο αλλά επεκτείνεται ραγδαία. Ήδη αναπτύσσονται πολλές εφαρμογές οι οποίες εξυπηρετούν τις συναλλαγές των πολιτών με τους δημόσιους φορείς. Σε αυτές εντάσσονται δραστηριότητες όπως ηλεκτρονική παροχή πληροφοριών, ηλεκτρονική έκδοση πιστοποιητικών, ηλεκτρονική πιστοποίηση πολιτών και ηλεκτρονική πληρωμή. Το κυριότερο παράδειγμα αυτής της συναλλαγής είναι το πρόγραμμα TAXIS το οποίο τα τελευταία χρόνια αναπτύσσεται αλματωδώς στην Ελλάδα και μέσω του οποίου γίνονται πλέον όλες οι φορολογικές συναλλαγές των πολιτών με το κράτος (φορολογικές δηλώσεις κλπ).

2.10 ΗΛ. ΕΜΠΟΡΙΟ ΜΕΤΑΞΥ ΚΑΤΑΝΑΛΩΤΩΝ & ΕΠΙΧΕΙΡΗΣΕΩΝ (C2B)

Σε αντίθεση με το πιο παραδοσιακό μοντέλο των επιχειρήσεων προς τον καταναλωτή, το μοντέλο C2B (καταναλωτής προς επιχείρηση) επιτρέπει στις επιχειρήσεις να δίνουν αξία στους καταναλωτές-και αντίστροφα. Στο πρότυπο C2B, οι επιχειρήσεις επωφελούνται από την προθυμία των καταναλωτών να ζητούν τη δική τους τιμή, ενώ οι καταναλωτές επωφελούνται από την ευελιξία, την άμεση πληρωμή των αγαθών που διαθέτουν και ακόμα επωφελούνται από τα προϊόντα ή τις υπηρεσίες με δωρεάν ή με μειωμένη τιμή.

Το μοντέλο C2B έχει αναπτυχθεί στην εποχή του Διαδικτύου λόγω της εύκολης πρόσβασης στους καταναλωτές που είναι "συνδεδεμένοι" με τα εμπορικά σήματα. Όταν η επιχειρηματική σχέση υπήρξε αυστηρά μονόδρομη, με τις εταιρείες να προωθούν τις υπηρεσίες και τα προϊόντα στους καταναλωτές, το νέο αμφίδρομο δίκτυο επέτρεψε στους καταναλωτές να δημιουργήσουν δικές τους επιχειρήσεις. Οι μειώσεις στο κόστος των τεχνολογιών όπως οι βιντεοκάμερες, οι εκτυπωτές υψηλής ποιότητας και οι υπηρεσίες ανάπτυξης ιστοσελίδων παρέχουν στους καταναλωτές πρόσβαση σε εργαλεία προώθησης και επικοινωνίας που κάποτε περιορίζονταν μόνο σε μεγάλες εταιρείες. Ως αποτέλεσμα, τόσο οι καταναλωτές όσο και οι επιχειρήσεις μπορούν να επωφεληθούν από το μοντέλο C2B. (Arline, 2015)

ΚΕΦΑΛΑΙΟ 3^{Ο}: ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

3.1 E – SHOP (ΗΛΕΚΤΡΟΝΙΚΟ ΚΑΤΑΣΤΗΜΑ)

Το ηλεκτρονικό κατάστημα χαρακτηρίζεται από εφαρμογές που επιτρέπουν στους καταναλωτές να κάνουν συναλλαγές και να αλληλεπιδρούν ανάμεσα στην επιχείρηση και τον τελικό καταναλωτή μέσω του διαδικτύου. Χαρακτηριστικά της κατηγορίας αυτής είναι: η συσσώρευση περιεχομένου με σκοπό την πώληση αγαθών και την παροχή υπηρεσιών στον καταναλωτή, η προσπάθεια για δημιουργία φίρμας από τις επιχειρήσεις. (Βασιλικοπούλου, Σιώμκος, 2005)

Αντιπροσωπευτικές επιχειρήσεις: eBay, Aemazon.com, Cdnow.com, Priceline.com.

3.2 E – MARKETPLACE (ΗΛΕΚΤΡΟΝΙΚΗ ΑΓΟΡΑ)

Ένα e-Marketplace είναι μια ηλεκτρονική πλατφόρμα όπου απαντώνται προμηθευτές και αγοραστές και λαμβάνουν χώρα αγοραπωλησίες διαφόρων ειδών ή υπηρεσιών. Τα εμπλεκόμενα μέρη στις ηλεκτρονικές αγορές είναι τρία: οι προμηθευτές, οι αγοραστές και αυτός που έχει δημιουργήσει την πλατφόρμα της ηλεκτρονικής αγοράς. Η πλατφόρμα αυτή επιτρέπει στους συμμετέχοντες αγοραστές και πωλητές να ανταλλάσσουν πληροφορίες για τιμές και προσφορές προϊόντων και να συνεργάζονται μεταξύ τους μέσω πληροφοριακών portals και εργαλείων εμπορικής συνεργασίας. (Bloomberg, 2018)

3.3 E – BUSINESS (ΗΛΕΚΤΡΟΝΙΚΟ ΕΠΙΧΕΙΡΗΝ)

Στο ηλεκτρονικό Επιχειρήν (e-business) περιλαμβάνονται όλες οι επιχειρηματικές πρωτοβουλίες που επικεντρώνονται σε εφαρμογές και δράσεις που υποστηρίζονται με τη χρήση ηλεκτρονικών μέσων και νέων τεχνολογιών. Συχνά δημιουργείται σύγχυση μεταξύ του ‘’ Ηλεκτρονικού Επιχειρήν ’’ και του ‘’Ηλεκτρονικού Εμπορίου’’ γι αυτό το λόγο είναι επιτακτικός ο διαχωρισμός των δύο αυτών όρων καθώς το ηλεκτρονικό εμπόριο απευθύνεται σε ευρύ αγοραστικό κοινό και συμβάλει στη ροή της επικοινωνίας αγοραστή – επιχείρησης. (Δεληγιάννης, 2006)

Χαρακτηριστικά της κατηγορίας αυτής των μοντέλων είναι:

- η εστίαση της επιχειρηματικότητας στις βασικές ικανότητες του οργανισμού
- ο προσανατολισμός στη συσσώρευση διαδικασιών (Βλαχοπούλου, 1999)

Αντιπροσωπευτικές επιχειρήσεις : Cisco Systems, General Electric, MetalSite.com, Chem Connect

3.4 E – ENTERPRISE (ΗΛΕΚΤΡΟΝΙΚΗ ΕΠΙΧΕΙΡΗΣΗ)

Έως τώρα έχει γίνει αναφορά στα B2C και B2B επιχειρηματικά μοντέλα, με παραδείγματα εταιριών που κάνουν χρήση των μοντέλων αυτών. Παρατηρείται όμως μια συνάντηση των παραπάνω μοντέλων σε εταιρίες που δραστηριοποιούνται τόσο σε αγορές με τελικούς καταναλωτές όσο και σε αγορές με εταιρικούς πελάτες.

Ο συνδυασμός αυτός δίνει μια νέα οπτική στον τρόπο διεξαγωγής των επιχειρηματικών δραστηριοτήτων χρησιμοποιώντας το διαδίκτυο κατά κύριο λόγο στις ηλεκτρονικές επιχειρήσεις. Από την προμήθεια πρώτων υλών μέχρι την πώληση του προϊόντος, στις επιχειρήσεις αυτές, η βασική αξία στηρίζεται στον συνδυασμό των παραδοσιακών μεθόδων της εταιρίας και της σαφούς επικοινωνίας με το ενδιαφερόμενο κοινό (καταναλωτές, πελάτες, διανομείς, συνεργάτες και ανταγωνιστές). (Καρανικόλας, 2006)

Αντιπροσωπευτικές επιχειρήσεις: American Express, Dell Computers, Healtheon

3.5 E – INFOBROKERS (ΗΛΕΚΤΡΟΝΙΚΗ ΜΕΣΙΤΕΙΑ)

Κάθε επιχείρηση χρειάζεται άτομα τα οποία να είναι ικανά να συλλέγουν πληροφορίες τέτοιες έχοντας ως στόχο την δημιουργία της υπεραξίας για την επιχείρηση. Τέτοια άτομα ονομάζονται Infobrokers και ανήκουν στον τομέα του μάρκετινγκ στην κατηγορία των συμβούλων. Αυτή η ειδικότητα αξιοποιείται κυρίως από εταιρίες όπως οι τραπεζικοί οργανισμοί, αναλυτές αγοράς και γενικότερα εταιρίες που για να λειτουργήσουν χρειάζονται σαν ‘’καύσιμο’’ όσες περισσότερες πληροφορίες και στοιχεία, για τον τομέα που απασχολούνται, είναι δυνατό προκειμένου να υλοποιήσουν το στόχο τους. Σε περιβάλλον ηλεκτρονικού εμπορίου οι ηλεκτρονικοί μεσίτες (E-Infobrokers) είναι απαραίτητοι καθώς το καθήκον τους είναι όχι μόνο να βρίσκουν τα στοιχεία αλλά να την επεξεργάζονται με τέτοιο τρόπο ώστε να δημιουργούν το κέρδος και λύσεις ακριβής και άμεσα εκμεταλλεύσιμες στους πελάτες τους. (Καρανικόλας, 2006)

3.6 E – AUCTION (ΗΛΕΚΤΡΟΝΙΚΗ ΔΗΜΙΟΡΑΣΙΑ)

Το μοντέλο ηλεκτρονικών δημοπρασιών ή αλλιώς e-Auctions ενδιαφέρει το σύνολο των επιχειρήσεων που επιθυμούν να καλύπτουν τις ανάγκες τους σε προϊόντα και υπηρεσίες με το χαμηλότερο κόστος. Μέσα από αυτή τη δράση μπορεί να δημιουργηθεί για την επιχείρηση ένας νέος δρόμος για την προώθηση των αγαθών της, υλικών και μη. Ακόμη μέσα από το e-auction μία εταιρία μπορεί να εκποιήσει ή γενικότερα να εκμεταλλευτεί την ακίνητη περιουσία της. Οι κατηγορίες προϊόντων ή υπηρεσιών που μπορούν να αποτελέσουν αντικείμενο ηλεκτρονικού διαγωνισμού στην παρούσα δράση είναι απεριόριστες καθώς μπορεί να αγοράσει προϊόντα και υπηρεσίες από τον πιο συμφέροντα προμηθευτή είτε να πουλήσει δικά της εμπορεύματα και υπηρεσίες στον πιο συμφέροντα αγοραστή. Τέλος τα οφέλη που προκύπτουν είναι η ελαχιστοποίηση του κόστους καθώς επιτυγχάνονται οι βέλτιστες τιμές σε αγορά και σε πώληση συνδυαστικά με την ελαχιστοποίηση του χρόνου που απαιτείται για την εκάστοτε διαπραγμάτευση. (Eurobank, 2019)

Αντιπροσωπευτικές επιχειρήσεις : iBid, FleaMarket, eBazar

3.7 E – PROCUREMENT (ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΡΟΜΗΘΕΙΕΣ)

Με το μοντέλο των ηλεκτρονικών προμηθειών (e-Procurement) δύνεται η δυνατότητα της δημιουργίας μιας ηλεκτρονικής αγοράς για την επιχείρηση. Δεν απαιτούνται επενδύσεις σε υποδομές και ειδικευμένο προσωπικό. Ακόμα στο μοντέλο e-Procurement παρατηρείται βελτίωση της εφοδιαστικής αλυσίδας και χρήση σύγχρονων συστημάτων αναφορών. Μέσα από το εν λόγω μοντέλο μπορούμε να δημιουργήσουμε ένα κύκλωμα αγορών επιλέγοντας τους προμηθευτές που θέλουμε κι έτσι επιτυγχάνεται η ηλεκτρονική προμήθεια των βασικών προϊόντων (πρώτες ύλες, είδη προς μεταπώληση, βιομηχανικό εξοπλισμό) καθώς και των δευτερευόντων προϊόντων (είδη γραφείου, αναλώσιμα, υπολογιστές). Τέλος ακόμα μία ευκολία είναι η δημιουργία ενός ακόμα κυκλώματος αλλά αυτή τη φορά στις πωλήσεις οι οποίες απευθύνονται στους αντιπροσώπους, διανομείς και πελάτες της επιχείρησης που βρίσκονται εντός ή εκτός Ελλάδας. Με αυτόν τον τρόπο επιτυγχάνεται η καλύτερη λήψη και παρακολούθηση των παραγγελιών, ανεξάρτητα από την τοποθεσία. (Eurobank, 2019)

3.8 E – MALL (ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΚΟ ΚΕΝΤΡΟ)

Είναι μια συλλογή από ηλεκτρονικά καταστήματα με παρόμοια λογική με αυτή των συγκεντρωμένων φυσικών καταστημάτων (π.χ MALL ATHENS). Σε αντίθεση με τα μεμονωμένα ηλεκτρονικά καταστήματα, τα E malls είναι μια συλλογή ηλεκτρονικών καταστημάτων μέσα από την οποία ο πελάτης μπορεί να ψωνίσει έχοντας διαφορετικές επιλογές σε κατηγορίες και καταστήματα. Το E mall χρεώνει μια προμήθεια στους πωλητές από τους οποίους απαρτίζεται η οποία εξαρτάται από τον όγκο των πωλήσεων που πραγματοποιούν. Υπάρχουν πολλά τοπικά E malls τα οποία έχουν ως στόχο την προώθηση των τοπικών προμηθευτών και κατ' επέκταση των τοπικών προϊόντων και υπηρεσιών. Τέτοια malls έχουμε συναντήσει στις Σέρρες, το Λασίθι, στο Ρέθυμνο κτλ. Άλλα ηλεκτρονικά εμπορικά κέντρα είναι οι επωνυμίες GLAMI.GR, Z – MALL.GR κ.α. όπου παρέχουν πρόσβαση σε πολλά ανεξάρτητα ηλεκτρονικά καταστήματα. (Turban, Whiteside, King, Outland, 2017)

3.9 M – COMMERCE (ΚΙΝΗΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ)

Οι εμπορικές συναλλαγές που πραγματοποιούνται μέσω φορητών ηλεκτρονικών συσκευών (κινητά τηλέφωνα) στο διαδίκτυο είναι ευρέως γνωστές ως m -commerce ή Mobile Commerce. Η άνοδος αυτού του είδους συναλλαγών είναι συνεχόμενα αυξανόμενη και περιλαμβάνει τόσο αγορές όσο και πωλήσεις μιας μεγάλης γκάμας προϊόντων και υπηρεσιών, όπως τραπεζικές συναλλαγές, εξοφλήσεις λογαριασμών σταθερής και κινητής τηλεφωνίας, αγορά ενδυμάτων και υποδημάτων κ.ο.κ. Όλα αυτά συνήθως πραγματοποιούνται με τη χρήση του Google, των e mails, των μέσων κοινωνικής δικτύωσης κ.τ.λ. μέσα από συνδέσμους που οδηγούν τον καταναλωτή σε προγράμματα περιήγησης ειδικά για κινητά. Προκειμένου ο καταναλωτής να έχει μια ολοκληρωμένη εικόνα για της αγορές μέσω κινητού τηλεφώνου καλό θα ήταν να υπάρχει συνδυασμός των εφαρμογών αλλά και των ιστότοπων που είναι σχεδιασμένοι γι αυτό το σκοπό. (Investopedia, 2019)

3.10 E – INVOICING (ΗΛΕΚΤΡΟΝΙΚΗ ΤΙΜΟΛΟΓΗΣΗ)

Με τον όρο Ηλ. Τιμολόγηση, ο οποίος εμφανίστηκε με το άρθρο 1 του Ν.3193/2003 (Φ.Ε.Κ 266/Α'/20.11.2003) και το άρθρο 18/α παρ. 5 έως 9 και 10 έως 15, αναφερόμαστε στην κατάργηση της εκτύπωσης των παραστατικών πώλησης σε χαρτί και πλέον θα έχουμε μόνο την ηλεκτρονική αποστολή αυτών μέσω mail στον

ενδιαφερόμενο, που είναι ο λήπτης – επιχείρηση ή ιδιώτης, της παροχής υπηρεσίας ή του εμπορεύματος.

Το Ηλ. τιμολόγιο δεν είναι απλά η αποστολή ενός παραστατικού με email ως αρχείο PDF ή μιας φωτογραφίας ενός χειρόγραφου τιμολογίου. Υλοποιείται μέσω μιας εφαρμογής ηλεκτρονικής τιμολόγησης η οποία σε συνεργασία με κάποιες επιπλέον τεχνολογίες (hardware και software) εγκεκριμένες από το κράτος (πχ. Φορολογικός μηχανισμός και ψηφιακή υπογραφή), εγγυάται την γνησιότητα της προέλευσης και την διασφάλιση των δεδομένων του ηλεκτρονικού παραστατικού. Ταυτόχρονα πρέπει να γίνεται και η ηλεκτρονική αρχειοθέτηση από την εφαρμογή ηλεκτρονικής τιμολόγησης, ώστε να επιτυγχάνεται η ανάκληση των ηλεκτρονικών τιμολογίων ανά πάσα στιγμή από τις αρχές ή την επιχείρηση. (Ναυτεμπορική, 2018)

Τα επιτεύγματα της ηλεκτρονικής τιμολόγησης κατά κράτος είναι : α) Η εξάλειψη της διαφθοράς στις οικονομικές υπηρεσίες που υπήρχε με την θεώρηση των βιβλίων στην Ελλάδα, β) η εξοικονόμηση χρόνου στις επιχείρησες, γ) η αποφυγή λαθών από την καταχώρηση των παραστατικών, δ) η αμεσότητα στην πληροφόρηση του κράτους για φόρους και ε) η διευκόλυνση ελέγχου των παραστατικών από το κράτος.

Ενώ σε μια πιο οικολογική βάση τα επιτεύγματα που ξεχωρίζουν είναι : α) η εξοικονόμηση των φυσικών πόρων από την καταστροφή δέντρων για χαρτοπολτό, β) η μείωση της ρύπανσης του περιβάλλοντος, γ) η αποφυγή της σπατάλης για χώρους που διατηρούσαν φυσικό αρχείο με χαρτιά και φακέλους (έντυπα, τιμολόγια) ενώ σε ένα πιο πρακτικό παράδειγμα παρακάτω βλέπουμε την εξοικονόμηση που επιτυγχάνεται με την ηλ. τιμολόγηση.

Παράδειγμα εξοικονόμησης για εκτύπωση ενός παραστατικού την ημέρα σε κόστος/ανά έτος= 1488 € 0.15 Δέντρα 0.04 Τόνοι CO2 0.47 Τόνοι Νερό

ΚΕΦΑΛΑΙΟ 4^{Ο} : ΚΙΝΔΥΝΟΙ & ΑΣΦΑΛΕΙΑ ΗΛ. ΕΜΠΟΡΙΟΥ

4.1 ΤΡΟΠΟΙ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΧΡΗΜΑ

Το κρισιμότερο σημείο κάθε εμπορικής συναλλαγής είναι η πληρωμή. Εμπόριο χωρίς χρήμα δεν έχει νόημα. Το internet παρουσιάζει την ιδιομορφία να μην υπάρχει προσωπική επαφή μεταξύ του εμπόρου και του πελάτη, ιδιαίτερα στις λιανικές συναλλαγές. Κατά συνέπεια το θέμα των πληρωμών είναι ένα σημαντικό κομμάτι του ηλεκτρονικού εμπορίου. Το μεγαλύτερο μέρος της παρακάτω συζήτησης θα αναφέρεται κυρίως στις πληρωμές λιανικών πωλήσεων, οι οποίες έχουν και το σημαντικότερο πρόβλημα καθώς τις περισσότερες φορές η επαφή πελάτη – εμπόρου είναι πολύ σπάνια. (Πομπορτσης & Τσουλφας, 2002)

4.1.1 ΜΕΣΑ ΠΛΗΡΩΜΗΣ

Σύμφωνα με την εγκύκλιο του Υπουργείου Οικονομικών ΠΟΛ. 1005/2017 «Καθορισμός δαπανών για τις οποίες απαιτείται η χρήση ηλεκτρονικών μέσων πληρωμής ή/και συλλογής αποδείξεων για το φορολογικό έτος 2017» ως ηλεκτρονικά μέσα πληρωμής νοούνται τα ακόλουθα: **α) οι πληρωμές που πραγματοποιούνται μέσω καρτών** (χρεωστικών ή/και πιστωτικών), **β) οι πληρωμές που πραγματοποιούνται μέσω λογαριασμού πληρωμών Παροχών Υπηρεσιών Πληρωμών** του ν. 3862/2010 (μεταφορά πίστωσης, εντολές άμεσης χρέωσης, πάγιες εντολές), και διενεργούνται μέσω **ηλεκτρονικής τραπεζικής (e-banking)**, **ηλεκτρονικού πορτοφολιού (e-wallet)** κ.λπ. Ενδεικτικά, ηλεκτρονικές πληρωμές θεωρούνται οι μεταφορές από λογαριασμό ηλεκτρονικής τραπεζικής (e-Banking), μέσω χρήσης πιστωτικής ή χρεωστικής κάρτας καθώς και μέσω οποιουδήποτε άλλου ηλεκτρονικού μμέσου πληρωμών, όπως ενδεικτικά αλλά όχι περιοριστικά, ηλεκτρονικό πορτοφόλι, κτλ. (HSBC, 2018)

4.1.2 ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ

Πιστωτική κάρτα είναι ένα μέσο πληρωμής το οποίο παρέχει στον κάτοχο της τη δυνατότητα να δανειστεί κεφάλαια τα οποία καλείται να αποπληρώσει αργότερα με κάποιο τόκο ή σε κάποιες περιπτώσεις άτοκα. Ο εκδότης της κάρτας είναι συνήθως κάποιο χρηματοπιστωτικό ίδρυμα και χρησιμοποιείται για βραχυπρόθεσμη χρηματοδότηση, ενώ δίνει την δυνατότητα στον κάτοχο να συνεχίζει να δανείζεται μέχρι ένα συγκεκριμένο πιστωτικό όριο κάθε μήνα. Οι παρεχόμενες από τις ελληνικές

τράπεζες πιστωτικές κάρτες, είναι συνδεδεμένες με κάποιον από τους παγκόσμιους οργανισμούς πιστωτικών καρτών (American Express, Mastercard, Maestro, VISA). Αυτό κυρίως δίνει την δυνατότητα στον πελάτη και κάτοχο της τράπεζα να την χρησιμοποιεί και σε άλλες χώρες. (Ευρετήριο οικονομικών όρων, 2018)

4.1.3 ΧΡΕΩΣΤΙΚΕΣ ΚΑΡΤΕΣ

Χρεωστική κάρτα είναι μια κάρτα που εκδίδεται από τράπεζες ή άλλα χρηματοπιστωτικά ιδρύματα και η οποία επιτρέπει στους πελάτες τους να έχουν ηλεκτρονική πρόσβαση στους τραπεζικούς λογαριασμούς τους για να τραβήξουν χρήματα ή να πληρώσουν για αγαθά και υπηρεσίες. Η χρεωστική κάρτα, ως μέσο πληρωμής, καταργεί επίσης την ανάγκη ύπαρξης μετρητών ή επιταγών και καρτών ανάληψης μετρητών, καθώς χρησιμοποιώντας την, τα κεφάλαια μεταφέρονται άμεσα από το λογαριασμό της τράπεζας του πελάτη στον εκάστοτε επιχειρηματικό. (Ευρετήριο οικονομικών όρων, 2018)

4.1.4 ΠΡΟΠΛΗΡΩΜΕΝΕΣ ΚΑΡΤΕΣ

Οι προπληρωμένες κάρτες θεωρούνται παρόμοιες με τις χρεωστικές κάρτες καθώς παρέχουν ένα συγκεκριμένο ποσό διαθέσιμο στον κάτοχο της κάρτας. Η διαφορά τους είναι ότι γενικά οι προπληρωμένες κάρτες είναι ανώνυμες ενώ οι χρεωστικές κάρτες είναι συνδεμένες με τον τραπεζικό λογαριασμό ενός ατόμου. Επίσης συνήθως οι χρεωστικές κάρτες προσφέρουν κάποια προστασία έναντι απώλειας, κλοπής, ή μη εξουσιοδοτημένης χρήσης, ενώ οι προπληρωμένες όχι. (Ευρετήριο οικονομικών όρων, 2018)

4.1.5 ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΟ EDI (FEDI)

Η Χρηματοοικονομική Ανταλλαγή Δεδομένων, δεν είναι τίποτε περισσότερο από χρήση EDI για οικονομικές συναλλαγές. Αποτελεί δηλαδή μια εξειδικευμένη μορφή EDI, στις περιπτώσεις όπου ο ένας από τους δυο συναλλασσόμενους είναι τράπεζα ή άλλο χρηματοπιστωτικό ίδρυμα. Εφαρμογές αυτής της τεχνολογίας έχουν ήδη αναπτυχθεί για διεξαγωγή τραπεζικών συναλλαγών από το σπίτι (home banking) καθώς και για την πληρωμή εμπορικών συναλλαγών (όπου πελάτης και προμηθευτής δίνουν αντίστοιχες οδηγίες στις τράπεζές τους για τη διευθέτηση των λογαριασμών). Για να είναι ασφαλής ως μέθοδος πληρωμής, πρέπει να υιοθετούνται οι μηχανισμοί ασφαλείας που χρησιμοποιούνται στο πρωτόκολλο SSL. Επίσης η χρήση extranet είναι ένας άλλος τρόπος υλοποίησης ασφαλούς FEDI και μπορεί να χρησιμοποιηθεί για περισσότερη ασφάλεια στις συναλλαγές μεταξύ οικονομικών οργανισμών και επιχειρήσεων. Τα

extranet κρυπτογραφούν τα πακέτα που ανταλλάσσονται ανάμεσα σε αποστολείς και παραλήπτες χρησιμοποιώντας κρυπτογράφηση δημοσίου κλειδιού (Turban, Lee,, King, Chung, σελ. 291).

4.1.6 ΗΛΕΚΤΡΟΝΙΚΗ ΜΕΤΑΦΟΡΑ ΚΕΦΑΛΑΙΩΝ (EFT)

Η ηλεκτρονική μεταφορά κεφαλαίων εμφανίστηκε τη δεκαετία του 1970 και αναφέρεται στην επικοινωνία μεταξύ δυο τραπεζών για την διεκπεραίωση των μεταξύ τους δοσοληψιών. Η επικοινωνία αυτή μπορεί να γίνεται μέσω EDI ή άλλων τεχνολογιών. Η Ηλεκτρονική Μεταφορά Κεφαλαίων, με τη χρήση EDI, αποτελεί ακόμα μια πολύ διαδεδομένη εφαρμογή του ΗΕ καθώς εδώ και αρκετά χρόνια όλες σχεδόν οι μεταφορές κεφαλαίων γίνονται με ηλεκτρονικό τρόπο. Πιο συγκεκριμένα η EFT είναι μια δημοφιλής μέθοδος ηλεκτρονικών πληρωμών με την οποία μπορεί κάποιος να μεταφέρει ένα χρηματικό ποσό από ένα τραπεζικό λογαριασμό σ' ένα άλλο, στην ίδια ή σε διαφορετική τράπεζα. Επίσης με την EFT μπορεί κάποιος ηλεκτρονικά και αυτόματα να καταθέσει χρήματα στο προσωπικό του λογαριασμό (μισθοί, συντάξεις κ.α.). Σήμερα μπορούμε να χρησιμοποιούμε την EFT μέσω διαδικτύου πράγμα που υπονοεί ότι σύνδεση ανάμεσα σε κυβερνοτράπεζες και σε προστασία ασφαλείας κατά τη διάρκεια της μετάδοσης είναι υποχρεωτική. (Turban, Lee,, King, Chung, σελ. 277).

Η προστασία του λογισμικού που χρησιμοποιείται είναι αναγκαία και αυτό μπορεί να γίνει με μεθόδους κρυπτογράφησης. Η ηλεκτρονική μεταφορά κεφαλαίων χρησιμοποιείται όλο και περισσότερο στις μέρες μας ως συνέπεια της ανάπτυξης του ηλεκτρονικού εμπορίου και των ηλεκτρονικών συναλλαγών. Τέλος, θα μπορούσαμε να πούμε πως η Ηλεκτρονική Μεταφορά Κεφαλαίων (EFT) αποτελεί ένα πολύ σημαντικό βήμα στην ανάπτυξη του ηλεκτρονικού εμπορίου, έχοντας προσφέρει πολύ σημαντικές υπηρεσίες στους χρήστες. Η χρήση της προσφέρει ταχύτητα, υψηλό επίπεδο ασφάλειας, μειώνει το κόστος συναλλαγής, προσφέρει 24ωρη εξυπηρέτηση και τέλος συμβάλει στην αποφυγή γραφειοκρατίας και συνωστισμού.

4.2 ΤΕΧΝΙΚΑ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΗΛ. ΕΜΠΟΡΙΟΥ

Με βάση λοιπόν τους παραπάνω στόχους κάποιος που ενδιαφέρεται να διασφαλίσει τις συναλλαγές του στο δίκτυο και να αποφύγει τους κινδύνους που αναφέρθηκαν παραπάνω, εκτός από τις λύσεις που προτάθηκαν, εφαρμόζει επιπλέον και τα ακόλουθα πρωτόκολλα και εφαρμογές βασισμένες και αυτές σε τεχνικές κρυπτογράφησης προκειμένου να είναι πλήρως προστατευμένος .

4.2.1 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια ώστε αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

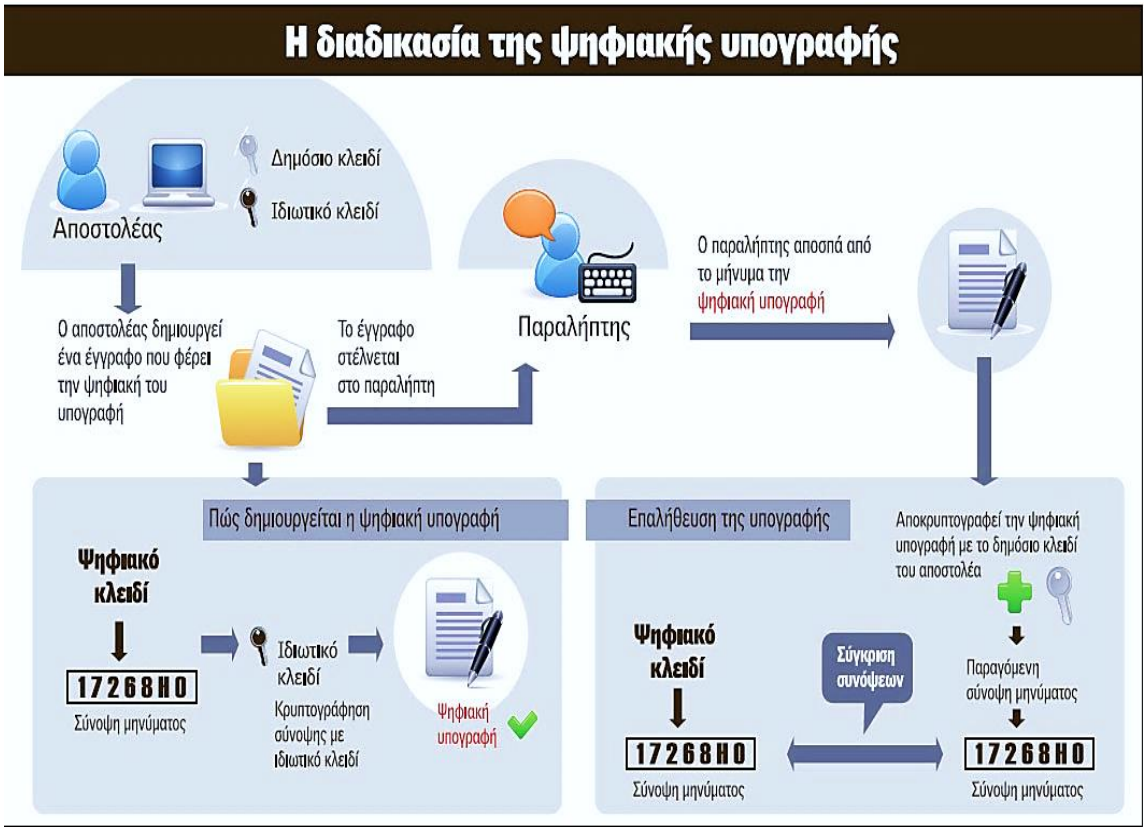
Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος και μοναδική για το μήνυμα και το αντιπροσωπεύει.

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

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

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

Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. απολέσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί). (ΕΕΤΤ, 2018)



Εικόνα 4.1 : Διαδικασία Ψηφιακής υπογραφής

(Πηγή :ΕΛ/ΛΑΚ, 2018)

4.2.2 COOKIES

Τα «cookies» είναι μικρά αρχεία με πληροφορίες που μια ιστοσελίδα (συγκεκριμένα ο εξυπηρετητής ιστού-web server) αποθηκεύει στον υπολογιστή ενός χρήστη, ώστε κάθε φορά που ο χρήστης συνδέεται στην ιστοσελίδα, να ανακτά τις εν λόγω πληροφορίες και να προσφέρει στο χρήστη σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει ο χρήστης στη συγκεκριμένη ιστοσελίδα (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, διαφημίσεων, κλπ).

Η εγκατάσταση των «cookies» επιτρέπεται μόνο με τη συγκατάθεση του χρήστη και μετά από κατάλληλη ενημέρωσή του.

Ειδικότερα, η παράγραφος 5 του άρθρου 4 ν. 3471/2006, όπως αυτή τροποποιήθηκε από το ν. 4070/2012 ορίζει ότι η εγκατάσταση των «cookies» επιτρέπεται μόνο αν ο συνδρομητής ή χρήστης «έχει δώσει τη συγκατάθεση του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει».

Αυτό το σύστημα είναι γνωστό και ως «opt-in», σε αντιδιαστολή με το σύστημα «opt-out» που ίσχυε πριν από την τροποποίηση της Οδηγίας 2002/58/ΕΚ και επέτρεπε την εγκατάσταση των «cookies» χωρίς τη συγκατάθεση του συνδρομητή ή χρήστη, εφόσον ο τελευταίος έχει προηγουμένως ενημερωθεί και δεν έχει εναντιωθεί στην επεξεργασία.

Επομένως, σύμφωνα με τα παραπάνω, ο πάροχος μιας υπηρεσίας διαδικτύου (π.χ. ένα on-line κατάστημα) ή κάποιος τρίτος (π.χ. διαφημιστικό δίκτυο που προωθεί προϊόντα του μέσω της ιστοσελίδας ενός on-line καταστήματος) μπορεί να εγκαταστήσει ένα «cookie» μόνο εφόσον έχει εξασφαλίσει τη συγκατάθεση του συνδρομητή ή χρήστη μετά από προηγούμενη κατάλληλη ενημέρωσή του. (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2018)

4.2.3 ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ

Το **ψηφιακό πιστοποιητικό** είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για την αναγνώριση μίας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός κοκ) και την ανάκτηση του δημοσίου κλειδιού αυτής.

Η έκδοση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση του ενδιαφερομένου σε μία Αρχή Πιστοποίησης. Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, το οποίο συνοπτικά περιλαμβάνει τα εξής στοιχεία:

- Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.

Το πιο διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών είναι το X.509.

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται ευρέως για διάφορες κρυπτογραφημένες ηλεκτρονικές συναλλαγές μέσω του διαδικτύου. Παραδείγματα τέτοιων συναλλαγών είναι: Σύνοδοι με βάση το πρωτόκολλο SSL (Client /Server SSL Certificates),

κρυπτογραφημένο και υπογεγραμμένο ηλεκτρονικό ταχυδρομείο (S/MIME Certificates), υπογραφή αντικειμένων (Object-signing Certificates) κοκ.

Η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), παρέχει την δυνατότητα στον πολίτη και στον δημόσιο υπάλληλο να εκδώσει δωρεάν προσωπικά ψηφιακά πιστοποιητικά αυθεντικοποίησης / υπογραφής και κρυπτογράφησης.

Εικόνα 4.2: Διαδικασία έκδοσης ψηφιακού πιστοποιητικού

(Πηγή : Αρχή Πιστοποίησης του Ελληνικού Δημοσίου, 2018)

Η ψηφιακή υπογραφή που δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο (κάρτα ή ειδική συσκευή usb) είναι αυτή που σύμφωνα με το άρθρο 2 του ΠΔ 150/2001 ορίζεται ως «Προηγμένη ηλεκτρονική υπογραφή» ή «ψηφιακή υπογραφή».

Η χρήση ψηφιακών πιστοποιητικών προσθέτει επιπλέον ασφάλεια στις ηλεκτρονικές συναλλαγές των πολιτών ενώ στις περιπτώσεις των δημοσίων υπαλλήλων είναι υποχρεωτική σε αρκετές διαδικασίες όπως οι ηλεκτρονικές προμήθειες. (Αρχή πιστοποίησης Ελληνικού δημοσίου, 2018)

4.2.4 ΠΡΟΤΥΠΟ ISO 17799 : 2005

Το ISO / IEC 17799: 2005 θεσπίζει κατευθυντήριες γραμμές και γενικές αρχές για την έναρξη, την εφαρμογή, τη διατήρηση και τη βελτίωση της διαχείρισης της ασφάλειας των πληροφοριών σε έναν οργανισμό. Στόχος είναι η παροχή γενικών οδηγιών για τη διαχείριση της ασφάλειας των πληροφοριών. Το ISO / IEC 17799: 2005 περιλαμβάνει τις βέλτιστες πρακτικές ελέγχου στους ακόλουθους τομείς διαχείρισης της ασφάλειας των πληροφοριών:

- Της πολιτική ασφαλείας
- Της οργάνωση της ασφάλειας των πληροφοριών
- Της διαχείρισης περιουσιακών στοιχείων
- Της ασφάλειας των ανθρώπινων πόρων
- Της φυσικής και περιβαλλοντικής ασφάλειας
- Της επικοινωνίας και διαχείρισης λειτουργιών
- Του ελέγχου πρόσβασης
- Της απόκτησης, ανάπτυξης και συντήρησης των συστημάτων πληροφορικής.
- Της διαχείρισης των περιστατικών ασφάλειας των πληροφοριών
- Της διαχείρισης των επιχειρηματικών κινδύνων

Οι στόχοι ελέγχου και οι έλεγχοι στο πρότυπο ISO / IEC 17799: 2005 εφαρμόζονται προκειμένου να ικανοποιηθούν οι απαιτήσεις που προκύπτουν από την αξιολόγηση του κινδύνου. Σκοπός του προτύπου ISO / IEC 17799: 2005 είναι να αποτελέσει κοινή βάση και κατευθυντήρια γραμμή για την οργάνωση των προτύπων ασφαλείας καθώς και για την αποτελεσματικότερη διαχείριση αυτής. Με αυτόν τον τρόπο κτίζεται η εμπιστοσύνη μεταξύ οργανισμών που συνεργάζονται μεταξύ τους. (International Organization for Standardization – ISO, 2018)

4.2.5 S – HTTP (SECURE BROWSER)

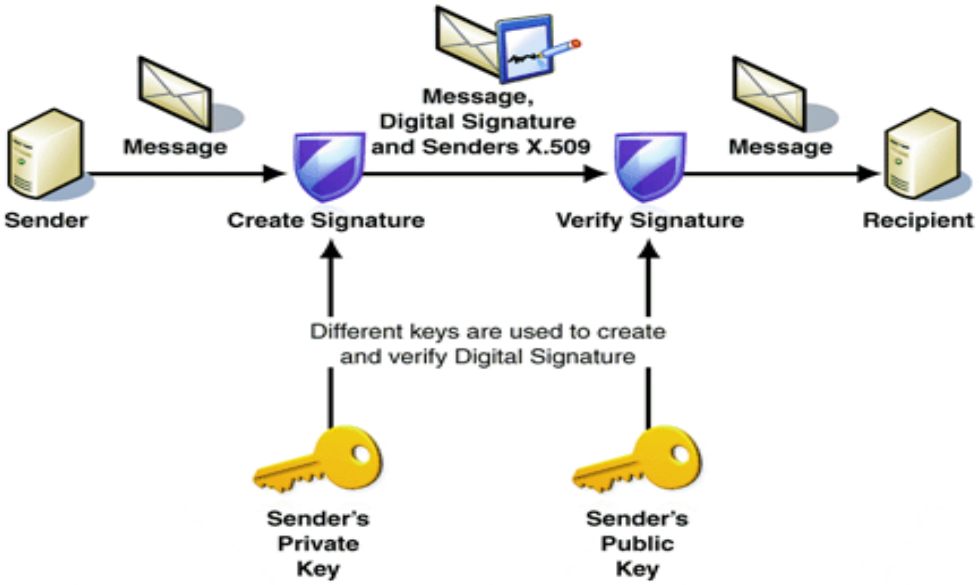
Το ασφαλές πρωτόκολλο υπερκειμένου (S-HTTP) είναι μια παρωχημένη εναλλακτική λύση από το πρωτόκολλο HTTPS για την κρυπτογράφηση των επικοινωνιών ιστού που μεταφέρονται μέσω HTTP. Αναπτύχθηκε από τους Eric Rescorla και Allan M. Schiffman και δημοσιεύθηκε το 1999 ως RFC 2660.

Τα προγράμματα περιήγησης Web συνήθως χρησιμοποιούν HTTP για να επικοινωνούν με διακομιστές ιστού, αποστέλλοντας και λαμβάνοντας πληροφορίες χωρίς κρυπτογράφηση. Για ευαίσθητες συναλλαγές, όπως το δικτυακό ηλεκτρονικό

εμπόριο ή η ηλεκτρονική πρόσβαση σε χρηματοοικονομικούς λογαριασμούς, το πρόγραμμα περιήγησης και ο διακομιστής πρέπει να κρυπτογραφούν αυτές τις πληροφορίες. Τα HTTPS και S-HTTP εφαρμόστηκαν και τα δύο στα μέσα της δεκαετίας του 1990 για την αντιμετώπιση αυτής της ανάγκης. Το S-HTTP χρησιμοποιήθηκε από τον διακομιστή ιστού του Spyglass, ενώ το Netscape και η Microsoft υποστήριζαν το HTTPS παρά το S-HTTP, οδηγώντας στο HTTPS να γίνει ο κυρίαρχος τυποποιημένος μηχανισμός για την εξασφάλιση επικοινωνιών στο διαδίκτυο. (Sheldon, 2001)

4.2.6 S – MIME (SECURE MAIL ATTACHMENT)

Το S/MIME (Multipurpose Internet Mail) είναι μια βάση για την αποστολή αρχείων με binary attachments μέσω του internet. Το Secure/MIME είναι μια επέκταση της βάσης MIME για την αναγνώριση των κρυπτογραφημένων email. Το S/MIME δεν εφαρμόσθηκε σαν ένα αυτόνομο πρόγραμμα, αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου. Επειδή το εργαλείο προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγόριθμους και όλες τις πατέντες και επειδή οι μμεγαλύτερες εταιρείες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security, είναι πιθανό το S/MIME να υιοθετηθεί περισσότερο από τους πωλητές e-mail προγραμμάτων. Το S/MIME προσφέρει **α)** εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη **β)** προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη **γ)** προσφέρει αναγνώρισης γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων. Το σύστημα μπορεί να χρησιμοποιηθεί με δυνατή ή αδύνατη κρυπτογράφηση . Για να στείλουμε κρυπτογραφημένα μμηνύματα σε κάποιον με το S/MIME ,πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του . Τα περισσότερα προγράμματα που χρησιμοποιούν το S/MIME κάνουν χρήση των X.509 v3 Public Key Infrastructures σαν και αυτές που δημιουργούνται από την VeriSign και άλλες αρχές πιστοποίησης . (Canter,1998)



Εικόνα 4.3 : Ψηφιακό κλειδί X.509

(Πηγή : Wordpress.com, 2018)

4.2.7 SET (SECURE ELECTRONIC TRANSACTION)

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

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

- εγγραφή κατόχου κάρτας
- εγγραφή εμπόρου
- αιτήσεις αγοράς
- εξουσιοδότηση πληρωμής
- σύλληψη πληρωμής
- επιστροφές χρεώσεων
- πιστώσεις
- αντιστροφή πίστωσης
- συναλλαγές χρεωστικής κάρτας

Τα μόνα εμπορικά προϊόντα που παρέχουν σήμερα συναλλαγές SET είναι η εφαρμογή Wallet της Verifone Corporation για καταναλωτές και η επέκταση vPOS για τον Εμπορικό Web Server της Microsoft. Στο μέλλον, τα προγράμματα πλοήγησης της Netscape και της Microsoft θα παρέχουν υποστήριξη για SET. (Investopedia, 2018)

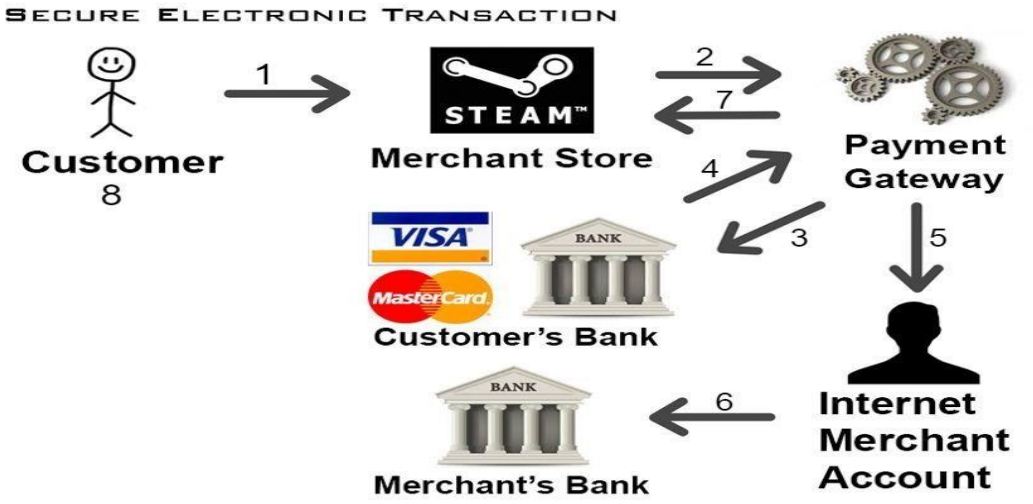
Ασφάλεια

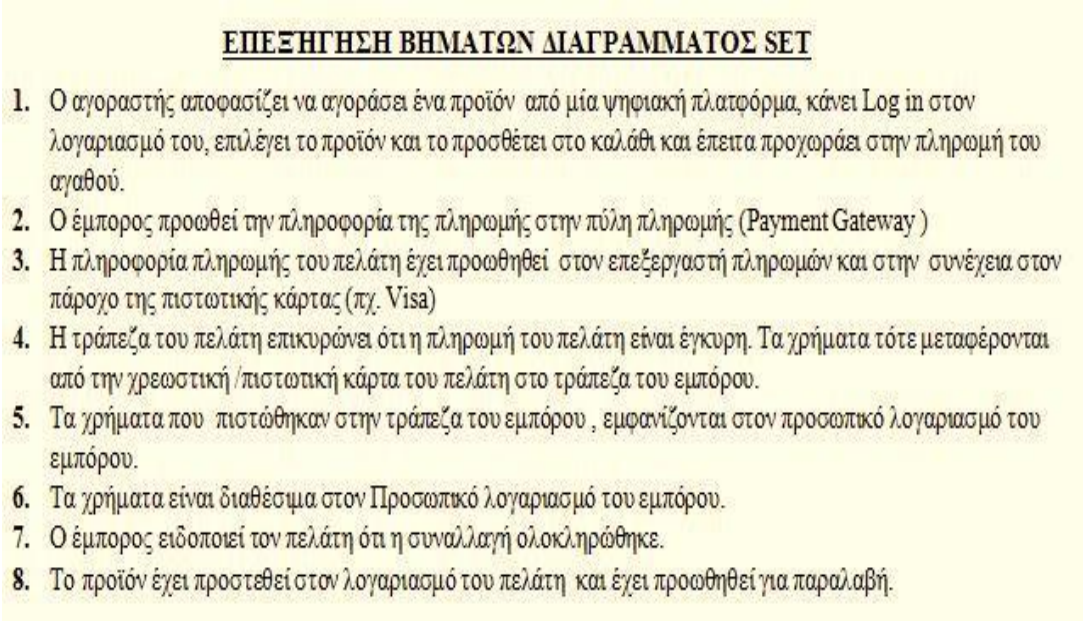
Η πιο δραματική βελτίωση του Secure Electronic Transaction Protocol πέρα από το πρωτόκολλο εντολών τηλεφώνων και ταχυδρομείου για τις Mastercard είναι ότι ο έμπορος παίρνει αρκετές πληροφορίες για μόνο μια αγορά. Οι έμποροι δεν μπορούν να χρησιμοποιήσουν το Secure Electronic Transaction Protocol για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

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

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

Η διεύθυνση του καταναλωτή (customer) και τα δεδομένα παραγγελίας προσφέρονται στους εμπόρους (merchants) σε ένα ξεχωριστό κανάλι από το Secure Electronic Transaction Protocol μέσω των πελατών. Γι' αυτό το λόγο αυτή η πληροφορία είναι διαθέσιμη στους παρατηρητές (observers). (Investopedia, 2018)





ΕΠΕΞΗΓΗΣΗ ΒΗΜΑΤΩΝ ΔΙΑΓΡΑΜΜΑΤΟΣ SET

1. Ο αγοραστής αποφασίζει να αγοράσει ένα προϊόν από μία ψηφιακή πλατφόρμα, κάνει Log in στον λογαριασμό του, επιλέγει το προϊόν και το προσθέτει στο καλάθι και έπειτα προχωράει στην πληρωμή του αγαθού.
2. Ο έμπορος προωθεί την πληροφορία της πληρωμής στην πύλη πληρωμής (Payment Gateway)
3. Η πληροφορία πληρωμής του πελάτη έχει προωθηθεί στον επεξεργαστή πληρωμών και στην συνέχεια στον πάροχο της πιστωτικής κάρτας (πχ. Visa)
4. Η τράπεζα του πελάτη επικυρώνει ότι η πληρωμή του πελάτη είναι έγκυρη. Τα χρήματα τότε μεταφέρονται από την χρεωστική /πιστωτική κάρτα του πελάτη στο τράπεζα του εμπόρου.
5. Τα χρήματα που πιστώθηκαν στην τράπεζα του εμπόρου , εμφανίζονται στον προσωπικό λογαριασμό του εμπόρου.
6. Τα χρήματα είναι διαθέσιμα στον Προσωπικό λογαριασμό του εμπόρου.
7. Ο έμπορος ειδοποιεί τον πελάτη ότι η συναλλαγή ολοκληρώθηκε.
8. Το προϊόν έχει προστεθεί στον λογαριασμό του πελάτη και έχει προωθηθεί για παραλαβή.

Εικόνα 4.4 : Secure Electronic Transaction Steps

(Πηγή : Digitalbusiness.com, 2018)

4.3 ΚΙΝΔΥΝΟΙ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

4.3.1 MAN – IN – THE MIDDLE ATTACK

Στην κρυπτογράφηση, η Man-In-The–Middle-Attack (συχνά MITM), είναι μια μορφή υποκλοπής στην οποία ο επιτιθέμενος κάνει ανεξάρτητες συνδέσεις με τα θύματα και προωθεί μηνύματα μεταξύ τους, καθιστώντας τους να πιστεύουν ότι μιλούν απευθείας ο ένας στον άλλο σε μια ιδιωτική σύνδεση, όταν στην πραγματικότητα ολόκληρη τη ‘’συζήτηση’’ ελέγχεται από τον εισβολέα. Ο εισβολέας είναι σε θέση να παρακολουθεί όλα τα μηνύματα μεταξύ των δυο θυμάτων και να τα τροποποιεί, με αυτό τον τρόπο μπορεί να υποκλέψει ό,τι πληροφορίες έχουν ανταλλαχθεί με το εκάστοτε Ηλεκτρονικό Κατάστημα, συμπεριλαμβανομένων όλων των προσωπικών στοιχείων του αγοραστή . Για παράδειγμα, ένας εισβολέας στο εύρος της λήψης μίας μη κρυπτογραφημένης σύνδεσης Wi-Fi, μπορεί ο ίδιος να εισαχτεί ως Man-in-the-middle εφόσον το site δεν χρησιμοποιεί κάποιο τρόπο κρυπτογράφησης και ταυτοποίησης του server (SSL).

Μία Man -In -The –Middle-Attack μπορεί να επιτύχει μόνο όταν ο εισβολέας μπορεί να μιμηθεί κάθε παράμετρο για να ‘’ξεγελάσει’’ τα δύο άκρα της σύνδεσης, είναι μια επίθεση σε αμοιβαίο έλεγχο ταυτότητας. Τα περισσότερα κρυπτογραφικά πρωτόκολλα περιλαμβάνουν κάποια μορφή ελέγχου ταυτότητας για να βεβαιώσουνε την αυθεντικότητα της σύνδεσης, ειδικά προκειμένου να αποτραπούν οι επιθέσεις MITM.

Για παράδειγμα, το SSL* ελέγχει την ταυτότητα του διακομιστή χρησιμοποιώντας μια αμοιβαία αξιόπιστη αρχή πιστοποίησης.(Hjelmvik, 2011)

***SSL**: Το πρωτόκολλο SSL επιτρέπει στον client / server να επικοινωνούν μέσω δικτύου με έναν τρόπο που αποσκοπούν στην πρόληψη υποκλοπών και παραβιάσεων.

Δεδομένου ότι τα περισσότερα πρωτόκολλα μπορούν να χρησιμοποιηθούν είτε με είτε χωρίς SSL είναι απαραίτητο να φαίνεται στον server αν ο πελάτης έχει μια σύνδεση SSL ή όχι. Για να επιτευχθεί αυτό, μια επιλογή είναι να χρησιμοποιηθεί ένας διαφορετικός αριθμός θύρας για SSL συνδέσεις (για παράδειγμα port 443 για HTTPS).

Μόλις ο πελάτης και ο διακομιστής αποφασίζουν να χρησιμοποιήσουν το πρωτόκολλο SSL, αρχίζει η διαπραγμάτευση μιας σταθερής σύνδεσης με τη χρήση μίας διαδικασίας ‘’γνωριμίας της σύνδεσης (handshake). Κατά τη διάρκεια αυτής της ‘’γνωριμίας’’ ο πελάτης και ο διακομιστής συμφωνούν σε διάφορες παραμέτρους που χρησιμοποιούνται για την εδραίωση της ασφάλειας της σύνδεσης.

Η ‘Γνωριμία’’ της σύνδεσης (handshake) αρχίζει όταν ένας πελάτης συνδέεται σε έναν SSL-enabled διακομιστή που παρέχει μία ασφαλή σύνδεση και παρουσιάζει μια λίστα με τους αλγόριθμους κρυπτογράφησης και τις λειτουργίες που χρησιμοποίει. Από τον κατάλογο αυτό, ο διακομιστής επιλέγει το ισχυρότερο αλγόριθμο κρυπτογράφησης και λειτουργίας που υποστηρίζει και ειδοποιεί τον πελάτη γι’ αυτή την απόφαση.

Ο server στέλνει πίσω την ταυτοποίησή της με τη μορφή ενός ψηφιακού πιστοποιητικού. Το πιστοποιητικό περιέχει συνήθως το όνομα του διακομιστή, την αξιόπιστη αρχή έκδοσης πιστοποιητικών (CA) και το δημόσιο κλειδί κρυπτογράφησης του server.

Ο πελάτης μπορεί να επικοινωνήσει με το διακομιστή που εξέδωσε το πιστοποιητικό (η αξιόπιστη αρχή, όπως παραπάνω) και να επιβεβαιώσει την εγκυρότητα του πιστοποιητικού πριν συνεχίσει. Για να δημιουργηθούν τα κλειδιά που χρησιμοποιούνται για την ασφαλή σύνδεση, ο πελάτης κρυπτογραφεί έναν τυχαίο αριθμό με το public key του server και στέλνει το αποτέλεσμα με το διακομιστή. Το αποτέλεσμα αυτό μόνο ο διακομιστής πρέπει να μπορεί να το αποκρυπτογραφήσει, με το private key του. Από τον τυχαίο αριθμό, τα δύο μέρη παράγουν τα βασικά υλικά για την κρυπτογράφηση και την αποκρυπτογράφηση.

Εδώ ολοκληρώνεται το Handshake και αρχίζει η ασφαλής σύνδεση, η οποία είναι κρυπτογραφημένη και αποκρυπτογραφείται με τα keys έως ότου η σύνδεση κλείσει.

Εάν κάποιο από τα παραπάνω βήματα αποτύχει, το SSL Handshake αποτυγχάνει και η σύνδεση δεν έχει δημιουργείται. (Dan, 2009)

Τύποι πρωτοκόλλου SSL :

- Domain Validation SSL

  Πρόκειται για πιστοποίηση βασικού επιπέδου. Ο οργανισμός που αιτείται το πιστοποιητικό πρέπει απλά να επιβεβαιώσει ότι το domain name είναι έγκυρο και του ανήκει.
- Organization Validation SSL

  Ψηλότερου επιπέδου πιστοποίηση. Ο οργανισμός ή η επιχείρηση που αιτείται το πιστοποιητικό πρέπει, εκτός από την ιδιοκτησία του domain name, να επιβεβαιώσει εταιρικά στοιχεία όπως: επωνυμία, πόλη, νομός, χώρα που εδρεύει η επιχείρηση.
- Extended Validation SSL

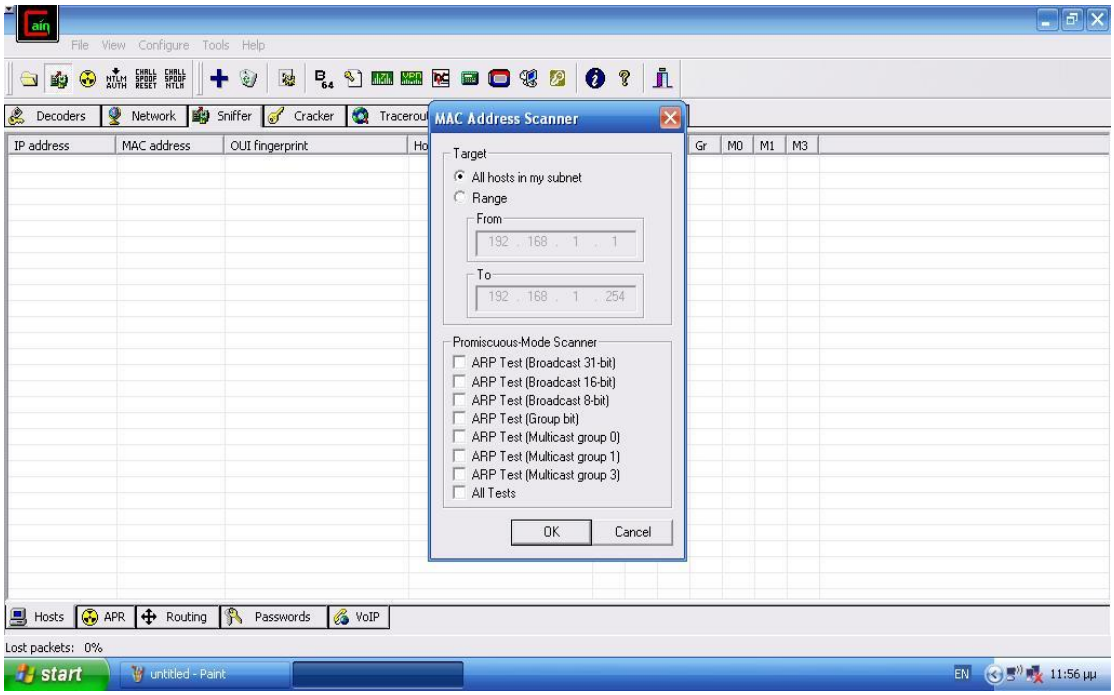
  Πρόκειται για την αυστηρότερη διαδικασία ελέγχων. Η διαδικασία αποτελείται από 7 επίπεδα και αφορά: την αποκλειστική ιδιοκτησία του domain name, την έδρα του οργανισμού, τη φυσική και νόμιμη υπόστασή του, τη λειτουργία του, την επιβεβαίωση ότι ο ίδιος ο οργανισμός αιτήθηκε την έκδοση του SSL καθώς και τη φυσική και νόμιμη ύπαρξη του νομίμου εκπροσώπου. (Papaki, 2018)

Παράδειγμα επίθεσης Man -In -The –Middle-Attack (όταν δεν χρησιμοποιείται SSL):

1. Στο παρακάτω παράδειγμα χρησιμοποιήθηκε δικός μας λογαριασμός στην ιστοσελίδα zortal.gr και όλες οι ενέργειες καθώς και η επίθεση έγιναν στο προσωπικό μας δίκτυο.

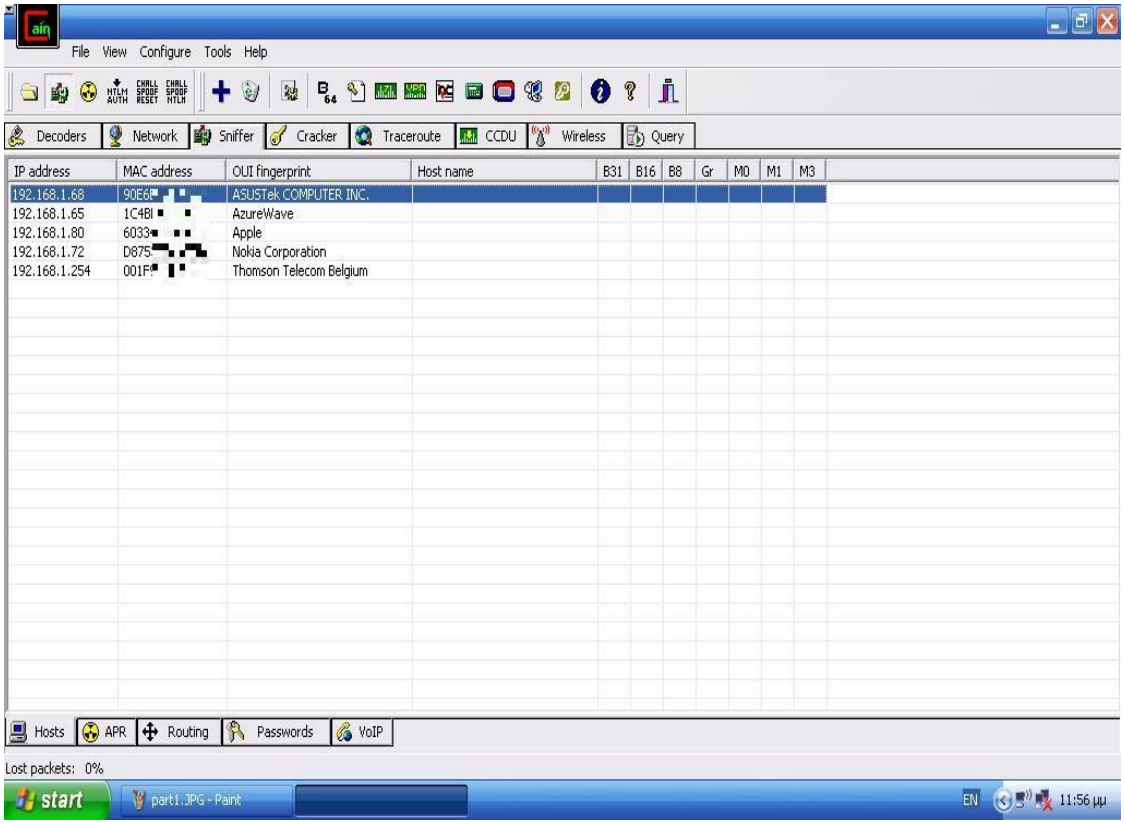
Εικόνα 4.5 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 1

2. Είσοδος στο site από τον αρχικό υπολογιστή (θύμα)



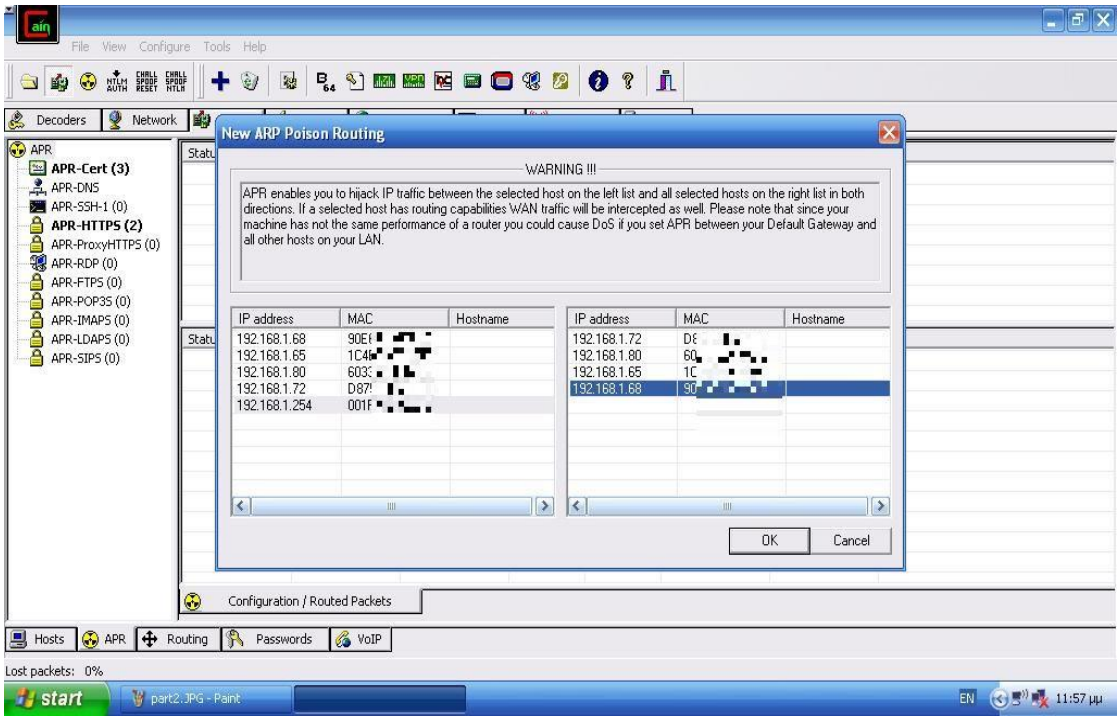
Εικόνα 4.6 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 2

3. Σ' έναν άλλο υπολογιστή που είναι συνδεδεμένος στο ίδιο δίκτυο χρησιμοποιούμε έναν ανιχνευτή για να σαρώσουμε το τοπικό μας δίκτυο για να βρούμε τον αρχικό υπολογιστή (θύμα).



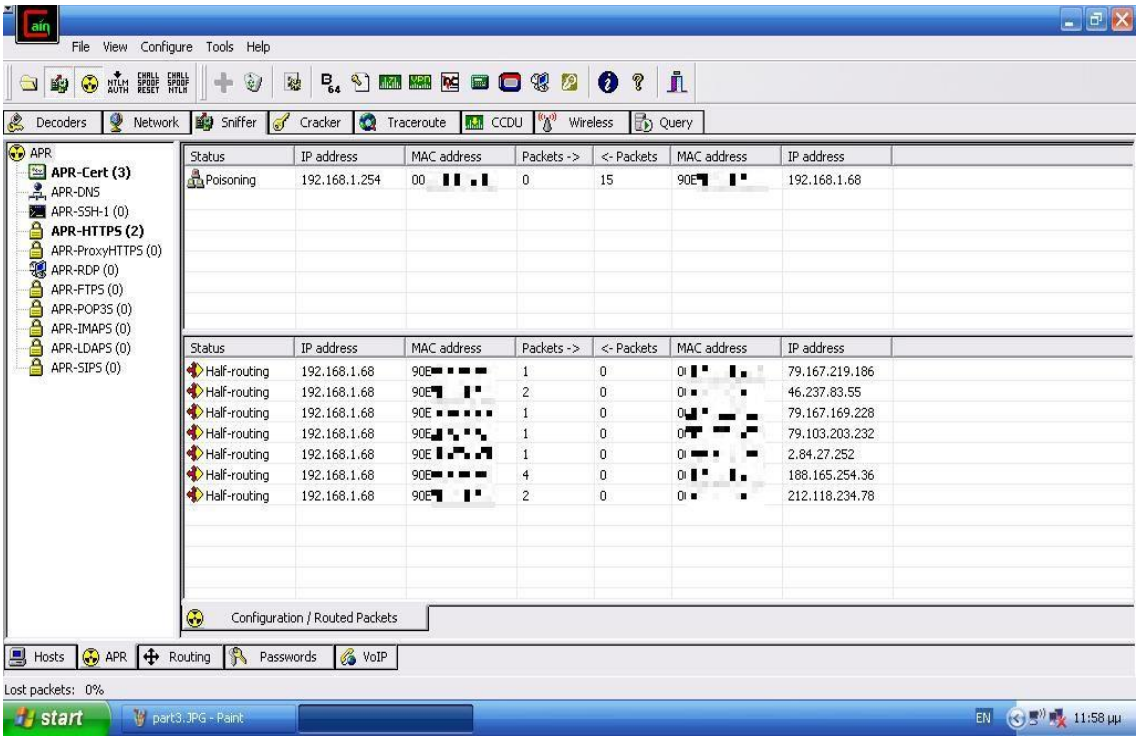
Εικόνα 4.7 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 3

4. Βλέπουμε τους υπολογιστές που είναι στο δίκτυο (Ο επιλεγμένος υπολογιστής είναι ο υπολογιστής-θύμα)



Εικόνα 4.8 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 4

5. Επιλέγουμε την IP του Router (αριστερά) και του υπολογιστή (δεξιά) και ξεκινάμε την διαδικασία επίθεσης ARP Poisoning.



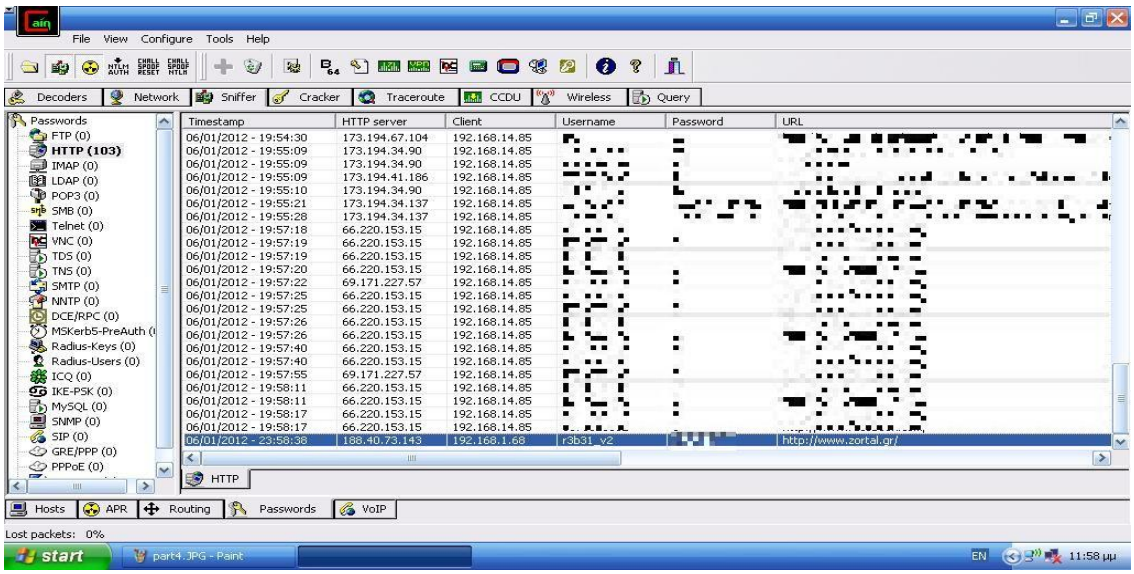
Εικόνα 4.9 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 5

6. Πλέον λειτουργούμε σαν Ενδιάμεσος (Man-In – The-Middle) όλες οι συνδέσεις περνάνε από εμάς.

Καλωσήλθες στην σελίδα μας r3b31_v2.
Εαν η σελίδα δεν ανανεώνεται αυτόματα, παρακαλούμε πατήστε εδώ

Εικόνα 4.10 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 6

7. Μπαίνουμε στη σελίδα από τον υπολογιστή – θύμα.



Εικόνα 4.11 : Προσωπικό παράδειγμα Επίθεσης – Βήμα 7

8. Τέλος στην επιλεγμένη γραμμή βλέπουμε το username και το password που μόλις χρησιμοποιήθηκε από τον υπολογιστή – θύμα για την είσοδο του στο site.

Αυτή η επίθεση δεν θα ήταν δυνατή άμα το site χρησιμοποιούσε SSLγια την login form του.

4.3.2 PHISING

Όπως το ίδιο το όνομά του υπονοεί ως παραλλαγή του αγγλικού «fishing» (ψάρεμα), το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου **spam email**, το οποίο ισχυρίζεται –ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα

χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων-παράνομων οικονομικών συναλλαγών.

Τα **email** αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά websites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή που και ο ίδιος ο internet browser «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας. (Spring, 2001)

Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου –σύντομου- χρονικού διαστήματος ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος.

Χρειάζεται ιδιαίτερη προσοχή ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω Phishing. Τα **email** που αποστέλλονται μοιάζουν αρκετά επίσημα και οι πλαστές σελίδες είναι τις περισσότερες φορές πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικά τους.

Το Phishing μπορεί να αντιμετωπιστεί με σωστή ενημέρωση του πελάτη μέσω μίας ξεκάθαρης εταιρικής πολιτικής η οποία θα υπενθυμίζει ότι ποτέ δεν πρόκειται να αποσταλεί οποιουδήποτε είδους ηλ. Μήνυμα προς τον πελάτη που θα ζητάει οποιοδήποτε προσωπικό του στοιχείο (πχ. Eurobank) . Οι απάτες ψαρέματος μπορεί επίσης να γίνουν και αυτοπροσώπως ή μέσω τηλεφώνου. Στην τελευταία περίπτωση, σε αντίθεση με τα κοινά **phishing e-mails**, δεν υπάρχει διεύθυνση ή URL για να απαντήσει κανείς, αλλά ένα τηλεφωνικό νούμερο, όπου πρέπει ο παραλήπτης να τηλεφωνήσει και να παράσχει τις ζητούμενες πληροφορίες. Καλώντας το νούμερο αυτό, τους χρήστες καλωσορίζει συνήθως ένα ηχογραφημένο μήνυμα, το οποίο τους καθοδηγεί στην συνέχεια στην παραχώρηση των προσωπικών τους στοιχείων.(Metropolitan Police, 2005)

4.3.3 ΙΟΊ ΥΠΟΛΟΓΙΣΤΩΝ

Ένας ιός υπολογιστών είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς την άδεια του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, όπως πχ. από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως οπτικό δίσκο ή μνήμη USB. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (Trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε Τοπικό δίκτυο υπολογιστών, και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC, 2018).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων. Ακόμη και οι η **μη καταστροφικοί ιοί** μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών, όπως : καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και κατά συνέπεια προκαλούν συχνά, ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του. Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων μέσω ενός key logger ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη που συνήθως χρησιμοποιείται **σε επιθέσεις DDOS**. (McAfee Press, 2018)

Τρόποι αντιμετώπισης

Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη-ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά

προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία, τους νέο-δημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται να συμβεί, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.(Symantec Security Summary, 2018)

4.3.4 CROSS – SITE SCRIPTING (XSS)

Με τον όρο **Cross-site scripting** ή XSS (δεν είναι CSS γιατί αλλιώς θα υπήρχε πρόβλημα ονομασίας) αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) των υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστοχώρο. Κάποιος κακόβουλος χρήστης, θα μπορούσε να εισάγει τον κώδικα σε έναν ιστοχώρο, μέσω ενός κειμένου εισόδου, για παράδειγμα, ο οποίος αφού δεν θα φιλτραριζόταν από τον ιστοχώρο σωστά, θα μπορούσε να προκαλέσει προβλήματα στον διαχειριστή ή επισκέπτη του ιστοχώρου. (Amit, 2005)

Οι τρύπες τις οποίες εκμεταλλεύεται το Cross-site scripting είναι κενά ασφαλείας web-εφαρμογών που επιτρέπουν στους επιτιθέμενους να παρακάμψουν την ασφάλεια από την πλευρά του πελάτη. Με την εισαγωγή του κώδικα ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση με αυξημένα δικαιώματα σε ευαίσθητα περιεχόμενα της σελίδας όπως τα session cookies, και μια ποικιλία από άλλες πληροφορίες που διατηρούνται από το πρόγραμμα περιήγησης για λογαριασμό του χρήστη. Το Cross-site scripting είναι επομένως μια ειδική περίπτωση επίθεσης με εισαγωγή κώδικα (code injection).

Η έκφραση «cross-site scripting» αρχικά αναφερόταν στην πράξη κατά την οποία μία web εφαρμογή δεχόταν επίθεση και εκτελούσε μετά από εισαγωγή κώδικα (code injection), scripts γραμμένα σε Java Script από κάποια άσχετη ιστοσελίδα, ελεγχόμενη από τον επιτιθέμενο (non-persistent XSS vulnerability). Ο ορισμός σταδιακά επεκτάθηκε για να συμπεριλάβει άλλους τρόπους εισαγωγής κώδικα (code injection), συμπεριλαμβανομένων των persistent και non-Java Script vectors (Java, ActiveX, VBScript, Flash, HTML, και SQL Queries), προκαλώντας σύγχυση στους νεοεισερχόμενους στον τομέα της ασφάλειας των πληροφοριών.

Γνωστές ιστοσελίδες έχουν πληγεί κατά το παρελθόν από XSS περιλαμβανομένων των Twitter, Facebook, MySpace, και Orkut. Σύμφωνα με ορισμένους ερευνητές το 2007, το 68% των δικτυακών τόπων μπορεί να δεχτεί επιθέσεις XSS.(Grossman, 2006)

ΠΑΡΑΔΕΊΓΜΑΤΑ ΕΚΜΕΤΑΛΕΥΣΗΣ ΚΕΝΩΝ ΑΣΦΑΛΕΙΑΣ

Οι επιτιθέμενοι που προτίθενται να εκμεταλλευτούν το Cross-site scripting πρέπει να προσεγγίσουν κάθε κατηγορία τρωτότητας με διαφορετικό τρόπο. Για κάθε κατηγορία, ένας συγκεκριμένος φορέας της επίθεσης περιγράφεται εδώ. Τα ονόματα των παρακάτω είναι τεχνικοί όροι, που λαμβάνονται από το cast των χαρακτήρων που χρησιμοποιούνται συνήθως στην ασφάλεια των υπολογιστών.

ΠΡΟΣΩΡΙΝΑ ΜΕΤΡΑ

1) Η Μαρία επισκέπτεται συχνά μια συγκεκριμένη ιστοσελίδα ενός ηλεκτρονικού καταστήματος, η οποία φιλοξενείται από το Νίκο.
2) Ιστοσελίδα του Νίκου επιτρέπει στην Μαριάννα συνδεθεί με έναusername / password και να αποθηκεύει ευαίσθητα δεδομένα, όπως πληροφορίες χρέωσης.
3) Η Ειρήνη παρατηρεί ότι η ιστοσελίδα του Νίκου περιέχει μια ευπάθεια XSS.
4) Η Ειρήνη δημιούργησε μια διεύθυνση URL για να εκμεταλλευτεί την ευπάθεια και στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στην Μαρία, προκαλώντας τη να επιλέξει ένα σύνδεσμο για τη διεύθυνση URL με ψευδείς παραστάσεις. Αυτό το URL θα την κατευθύνει στην ιστοσελίδα του Νίκου (είτε άμεσα είτε μέσω ενός iframe ή ajax), αλλά θα περιέχει τον κακόβουλο κώδικα της Ειρήνης και η ιστοσελίδα θα είναι ευπαθής.
5) Η Μαρία επισκέπτεται το URL που παρέχεται από την Ειρήνη ενώ είναι συνδεδεμένη στην ιστοσελίδα του Νίκου.
6) Το κακόβουλο script ενσωματώνεται στη διεύθυνση URL στο πρόγραμμα περιήγησης που εκτελεί η Μαρία, σαν να ήρθε κατευθείαν από το διακομιστή του Νίκου (αυτό είναι το πραγματικό θέμα ευπάθειας XSS). Το σενάριο μπορεί να χρησιμοποιηθεί για την αποστολή του session cookie της Μαρίας στην Ειρήνη. Η Ειρήνη μπορεί να χρησιμοποιήσει στη συνέχεια το cookie για την κλοπή ευαίσθητων στοιχείων της Μαρίας (διαπιστευτήρια ελέγχου ταυτότητας, πληροφορίες τιμολόγησης, κ.λπ.) χωρίς τη γνώση της Μαρίας.

ΜΟΝΙΜΗ ΕΠΙΘΕΣΗ

1) Η Ειρήνη δημοσιεύει ένα μήνυμα με κακόβουλο payload από κάποιο ηλεκτρονικό κατάστημα σε ένα κοινωνικό δίκτυο.

2) Όταν ο Νίκος ανοίξει το σύνδεσμο, μέσω του XSS exploit η Ειρήνη κλέβει τα cookies του Νίκου.
3) Η Ειρήνη μπορεί να χρησιμοποιήσει το session cookie του Νίκου, οπότε μπορεί να μπει στο κατάστημα σαν αυτόν.

ΜΕΙΩΣΗ ΚΙΝΔΥΝΟΥ

1) Escaping of string input

Ο κύριος μηχανισμός άμυνας για να σταματήσει η XSS είναι το ‘’escaping’’ το οποίο είναι μια τεχνική που χρησιμοποιείται για να εξασφαλίσει ότι χαρακτήρες αντιμετωπίζονται ως δεδομένα, και όχι ως χαρακτήρες. Υπάρχουν πολλοί διαφορετικοί τύποι ‘’escaping’’, μερικές φορές λανθασμένα ονομάζεται “ output encoding” Μερικές από αυτές τις τεχνικές καθορίζουν έναν συγκεκριμένο “escape character” (χαρακτήρα), και άλλες τεχνικές έχουν μια πιο σύνθετη σύνταξη που περιλαμβάνει διάφορους χαρακτήρες.

Το “escaping” αποτελεί το κύριο μέσο για να βεβαιωθούμε ότι η τα μη αξιόπιστα δεδομένα δεν μπορούν να χρησιμοποιηθούν για μια επίθεση . Μέσω του “escaping” απλά ενημερώνετε ο interpreter ότι τα δεδομένα δεν πρόκειται να εκτελεστούν, και ως εκ τούτου οι τυχόν επιθέσεις δεν δουλεύουν. Να σταματήσουμε τις επιθέσεις XSS ενώ δεχόμαστε εισαγωγή HTML κώδικα από τους χρήστες είναι πολύ πιο περίπλοκο. Ο κώδικας θα πρέπει να ελεγχτεί από μία “HTML policy engine” για να σιγουρευτούμε ότι δεν περιέχει κακόβουλο κώδικα που μπορεί να χρησιμοποιηθεί για επιθέσεις XSS. (Microsoft, 2007).

2) Cookie security

Εκτός από το φιλτράρισμα περιεχομένου, υπάρχουν κι άλλες ατελής μέθοδοι για την αντιμετώπιση του cross-site scripting. Ένα παράδειγμα είναι η χρήση πιο αυστηρών τρόπων διαχείρισης των cookies των πελατών. Πολλές διαδικτυακές εφαρμογές βασίζονται στα session cookies προκειμένου να ελέγξουν την ταυτότητα μεταξύ των επιμέρους HTTP συνδέσεων και επειδή τα client-side scripts γενικά έχουν πρόσβαση σε αυτά, υπάρχει εκμετάλλευση του XSS έτσι ώστε να επιτευχτεί η επίθεση και η κλοπή των session cookies. Για να περιοριστεί η συγκεκριμένη απειλή (και όχι το XSS πρόβλημα σε γενικές γραμμές), πολλές web εφαρμογές αντιστοιχούν τα session cookies με τη διεύθυνση IP του χρήστη όταν αρχικά συνδεθεί και επιτρέπουν συνδέσεις μόνο στην IP που χρησιμοποιήσει το cookie. Αυτό είναι αποτελεσματικό στις περισσότερες περιπτώσεις (όταν ένας εισβολέας έχει καταφέρει να υποκλέψει μόνο το session cookie), αλλά προφανώς είναι αναποτελεσματικό σε περιπτώσεις όπου ο επιτιθέμενος πλαστογραφεί τη διεύθυνση IP και είναι πίσω από την ίδια NAT

διεύθυνση IP ή web proxy. Ένα άλλο σύστημα που υποστηρίζεται : στον Internet Explorer (από την έκδοση 6), στον Firefox (από την έκδοση 2.0.0.5), στο Safari (από την έκδοση 4), στον Opera (από την έκδοση 9.5) και στην Google Chrome, είναι ένα Http Only flag, το οποίο επιτρέπει σε ένα διακομιστή Web να ορίσει ότι ένα cookie δεν είναι διαθέσιμο για client-side scripts. Παρόλο που αυτό ωφελεί, δεν αποκλείει εντελώς την κλοπή των cookies ούτε μπορεί να αποτρέψει τις επιθέσεις στο πρόγραμμα περιήγησης.

*3) Απενεργοποίηση των **scripts***

Τέλος, οι σχεδιαστές Web 2.0 και Ajax ευνοούν τη χρήση της Java Script, για ορισμένες εφαρμογές Ιστού που λειτουργούν πλήρως χωρίς την ανάγκη για client-side scripts. Αυτό επιτρέπει στους χρήστες, αν το επιλέξουν, να απενεργοποιήσουν το scripting στον υπολογιστή τους πριν από τη χρήση της εφαρμογής. Με αυτόν τον τρόπο, έστω και δυνητικά τα κακόβουλα client-side scripts που θα μπορούσαν να έχουν εισαχθεί σε μια σελίδα, δεν πρόκειται να εκτελεστούν και οι χρήστες δεν θα είναι επιρρεπείς σε επιθέσεις XSS.

Ορισμένα προγράμματα περιήγησης ή πρόσθετα προγράμματος περιήγησης μπορεί να ρυθμιστούν για να απενεργοποιήσουν τα client-side scripts ανά όνομα χώρου (domain name). Αν το scripting επιτρέπεται από προεπιλογή, τότε αυτή η προσέγγιση έχει περιορισμένη αξία, δεδομένου ότι μπλοκάρει κακά sites μόνο αφού ο χρήστης γνωρίζει ότι είναι κακά, το οποίο είναι πολύ αργά. Η λειτουργικότητα που μπλοκάρει όλες τις δέσμες ενεργειών από προεπιλογή και στη συνέχεια να επιτρέπει στο χρήστη να το ενεργοποιήσει αυτή τη λειτουργία ανά όνομα χώρου (domain name) είναι πιο αποτελεσματική. Αυτό κατέστη δυνατό για μεγάλο χρονικό διάστημα στον Internet Explorer (από την έκδοση 4), με τη δημιουργία λεγόμενες «ζώνες ασφαλείας» της και στον Opera (από την έκδοση 9) χρησιμοποιώντας “Site specific preferences” του. Μια λύση για τον Firefox και άλλα Gecko Based προγράμματα περιήγησης είναι το open source Add-on No Script το οποίο, εκτός από τη δυνατότητα να επιτρέπει σενάρια για κάθε τομέα-βάση, παρέχει και κάποια αντί-XSS προστασία ακόμη και όταν έχουν ενεργοποιηθεί οι δέσμες ενεργειών.

Το πιο σημαντικό πρόβλημα με τον αποκλεισμό όλων των scripts σε όλες τις ιστοσελίδες από προεπιλογή είναι η ουσιαστική μείωση της λειτουργικότητας και της ανταπόκρισης (Το client-side scripting μπορεί να είναι πολύ πιο γρήγορο από server-side scripting, επειδή δεν χρειάζεται να συνδεθεί σε ένα απομακρυσμένο server και η σελίδα ή το πλαίσιο δεν χρειάζεται να ξαναφορτωθεί). Ένα άλλο πρόβλημα με το σενάριο αποκλεισμού είναι ότι πολλοί χρήστες δεν το καταλαβαίνουν, και δεν ξέρουν πώς να προστατεύσουν κατάλληλα τα προγράμματα περιήγησης που διαθέτουν. Ακόμα

ένα μειονέκτημα είναι ότι πολλές περιοχές δεν λειτουργούν χωρίς scripting client-side, αναγκάζοντας τους χρήστες να απενεργοποιήσουν την προστασία για αυτήν την τοποθεσία και το άνοιγμα των συστημάτων τους για τρωτά σημεία. Το No Script του Firefox επιτρέπει στους χρήστες να επιτρέψουν επιλεκτικά τα scripts που θα τρέξουν από μια συγκεκριμένη σελίδα, ενώ δεν αφήνει όλα τα υπόλοιπα στην ίδια σελίδα. Για παράδειγμα, scripts από example.com θα μπορούσαν να επιτρέπονται, ενώ scripts από το advertisingagency.com που προσπαθούν να εκτελεστούν μέσω της ίδιας σελίδας μπορούν να αποκλειστούν. (Mozilla Firefox, 2012)

4.3.5 FIREWALLS

Ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο, σύμφωνα με ένα σύνολο κανόνων με το οποίο είναι προγραμματισμένα.

Τα firewalls βασίζονται στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI (Open Systems Interconnection). Το κύριο χαρακτηριστικό αυτής είναι ότι μπορεί να αντιλαμβάνεται ποια προγράμματα και πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση (πχ FTP-File Transfer Protocol, DNS-Domain Name System, περιήγηση στο Διαδίκτυο κοκ). Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μιας υπηρεσίας.

Η χρήση τους είναι απαραίτητη προκειμένου να προστατευτούν οι servers και το intranet της εκάστοτε εταιρίας από επιθέσεις.(Ingham&Forrest, 2002)

4.4 ΚΙΝΔΥΝΟΙ & ΑΣΦΑΛΕΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΗΛ. ΕΜΠΟΡΙΟ

Ακόμα κι αν έχουμε ασφαλίσει το site μας από την υποκλοπή δεδομένων, τα προσωπικά στοιχεία εξακολουθούν να είναι στην βάση δεδομένων του site πράμα που σημαίνει ότι η βάση αποτελεί στόχο και έχει πολύ μεγάλη αξία στην ‘’μαύρη’’ αγορά του Διαδικτύου. Πχ. Η Κλεμμένη βάση δεδομένων της Sony που περιείχε δεκάδες εκατομμύρια πελατών μαζί με όλα τα προσωπικά τους στοιχεία, είχε αξία στην ‘’μαύρη’’ αγορά περίπου 3000 ευρώ το αντίτυπο και ανάγκασε την εταιρία να κλείσει το PSN(δίκτυο Playstation) για δύο εβδομάδες προκειμένου να αναβαθμίσει την ασφάλεια των server τους.

ΕΠΙΘΕΣΗ ΜΕ SQL INJECTION

Μια SQL injection χρησιμοποιείται συχνά για να επιτεθεί στην ασφάλεια μιας ιστοσελίδας με την εισαγωγή SQL statements σε μια ηλεκτρονική φόρμα για να εκτελέσει σε μία κακώς σχεδιασμένη βάση δεδομένων κακόβουλες συνήθως λειτουργίες. Η SQL injection είναι μια τεχνική κατά την εισαγωγή του κώδικα που εκμεταλλεύεται ένα κενό ασφαλείας στο λογισμικό στον δικτυακό τόπο προκειμένου να τροποποιήσει το περιεχόμενο της βάσης δεδομένων όπως αριθμών πιστωτικών καρτών ή κωδικούς πρόσβασης για τον εισβολέα. Η SQL injection είναι περισσότερο γνωστή ως φορέας της επίθεσης για ιστοσελίδες, αλλά μπορεί να χρησιμοποιηθεί για να επιτεθεί σε οποιοδήποτε τύπο βάσης δεδομένων SQL.

Η SQL injection μπορεί να αποτραπεί χρησιμοποιώντας μία καλά σχεδιασμένη βάση (πχ. Με την χρήση VIEWS) .Έχει παρατηρηθεί ότι κατά μέσω όρο μια βάση δεδομένων η οποία είναι συνδεδεμένη στο Διαδίκτυο δέχεται κατά μέσο όρο, 71 επιθέσεις ανά ώρα. Όταν, γίνεται οργανωμένη επίθεση το νούμερο μπορεί να φτάσει τις 800-1300 φορές ανά ώρα. Ακόμα και στην περίπτωση που η βάση κλαπεί θα πρέπει να αποτραπεί η άμεση έκθεση των στοιχείων του πελάτη με την χρήση κρυπτογράφησης (πχ. SaltedMD5), όπως και με την μη αποθήκευση ορισμένων στοιχείων τα οποία ο πελάτης θα πρέπει να επιβεβαιώνει σε κάθε αγορά (πχ. Αποθήκευση του αριθμού της πιστωτικής κάρτας και όχι του CVV έτσι και μετά από επιτυχημένη αποκρυπτογράφηση της κλεμμένης βάσης η πιστωτική του πελάτη δεν μπορεί να χρεωθεί). Αυτό αποτελεί μια επιπλέον δικλείδα ασφαλείας. Ακόμη υπάρχει και η πιθανότητα της αντικαταβολής ως εναλλακτικός τρόπος πληρωμής έτσι ώστε οι πελάτες οι οποίοι φοβούνται τυχόν υποκλοπή των δεδομένων τους να μπορούν να κάνουν τις αγορές τους με μεγαλύτερη άνεση. (Clarke,2009).

ΚΕΦΑΛΑΙΟ 5^{Ο} : ΕΡΕΥΝΑ

5.1 ΕΙΣΑΓΩΓΙΚΑ ΓΙΑ ΤΗΝ ΕΡΕΥΝΑ

Το σύνολο της παρούσας έρευνας αποτελείται από 2 διαφορετικές μεθόδους συλλογής πληροφοριών, μία ποιοτική και μια ποσοτική.

Η ποιοτική μέθοδος παίρνει μορφή στην παρούσα εργασία με την διαδικασία της Συνέντευξης από τον Chief Technology Officer της εταιρίας Enartia Group of Brands σε μια αντιπροσωπευτική συνέντευξη πάνω στα τεχνικά ζητήματα ασφαλείας που κρύβονται από πίσω από όλες τις κινήσεις που κάνει ένας μέσος άνθρωπος κατά την διάρκεια της περιήγησης του στο Ίντερνετ, Κο Βαβίλη Παναγιώτη.

Εν συνεχεία προχωράμε σε μια πιο μαζική έρευνα, η οποία στηρίζεται στην διαδικασία του Ερωτηματολογίου σε ευρύ δείγμα χρηστών.

5.2 ΠΕΡΙΓΡΑΦΗ ΕΡΕΥΝΑΣ

5.2.1 ΣΥΝΕΝΤΕΥΞΗ

Στις δύο πρώτες ερωτήσεις της συνέντευξης θα αναλυθεί η διασφάλιση μιας συναλλαγής σ’ ένα ηλεκτρονικό κατάστημα και οι διαδικασίες ασφαλείας που είναι αναγκαίες να τηρηθούν για να έχει υπόσταση το κατάστημα αυτό.

Συνεχίζουμε με τις επόμενες δύο ερωτήσεις στις οποίες αναφερόμαστε στην κρυπτογράφηση των ιστοσελίδων και των email και πως μπορούμε να ξεχωρίζουμε τις ασφαλείς συνδέσεις από τις υπόλοιπες.

Στις εναπομένουσες ερωτήσεις έως το τέλος της συνέντευξης αναλύουμε τους κινδύνους των ηλεκτρονικών συναλλαγών και των βάσεων δεδομένων των ιστοσελίδων που πραγματοποιούνται οι ηλεκτρονικές συναλλαγές, καθώς επίσης και τους τρόπους αντιμετώπισης αυτών μέσα από τα διάφορα πρωτόκολλα ασφαλείας . Στόχος είναι να μάθουμε πως μπορούμε να διακρίνουμε αν εκτιθέμαστε σε κίνδυνο έτσι ώστε να αποφεύγουμε αυτού του είδους σελίδες.

5.2.2 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Το ερωτηματολόγιο που χρησιμοποιήθηκε για το συγκεκριμένο κομμάτι της έρευνας συμπληρώθηκε από πραγματικό δείγμα φυσικών προσώπων το οποίο ανέρχεται στα 160 άτομα.

Ο χρόνος ανταπόκρισης στην παρούσα έρευνα ανέρχεται στα 3 εικοσιτετράωρα και οι ερωτηθέντες βρέθηκαν κατά κύριο λόγο από γνωστή σελίδα κοινωνικής δικτύωσης (Facebook) και από τους χώρους εργασίας της ερευνήτριας (Ιατρικό Διαγνωστικό κέντρο και Αλυσίδα γυμναστηρίων στην Αττική).

Εν περιλήψει στην 1η ενότητα του ερωτηματολογίου (Ερώτηση 1 έως 5) ο ερωτώμενος μας συστήνεται παραθέτοντας μας ανώνυμα τα δημογραφικά του στοιχεία.

Στην 2η ενότητα (Ερώτηση 6 έως 8) ο ερωτώμενος καλείται να απαντήσει σε ζητήματα που αφορούν την ενασχόληση του γενικότερα με το διαδίκτυο .

Εν συνεχεία στην 3η (Ερώτηση 9 έως 16) ενότητα ζητούνται να απαντηθούν ερωτήματα για τις ηλεκτρονικές αγορές με σκοπό να καταλήξουμε στην 4η ενότητα (Ερώτηση 17 έως 20) όπου γίνεται κατανοητό αν οι καταναλωτές έχουν αίσθηση του κινδύνου που ελλοχεύουν πίσω από τα Διαδικτυακά καταστήματα και τις ιστοσελίδες που απευθύνονται.

5.3 ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

5.3.1 ΣΥΝΈΝΤΕΥΞΗ – ΠΟΙΟΤΙΚΗ ΕΡΕΥΝΑ

ΣΤΟΙΧΕΊΑ ΕΡΩΤΩΜΕΝΟΥ

Ονοματεπώνυμο :	Βαβίλης Παναγιώτης
Εταιρία Εργασίας :	Enartia Group of Brands
Θέση Εργασίας :	CTO – Senior System Administrator
Έδρα:	Βιομηχανική Περιοχή Ηρακλείου, Οδός Σ, 71 601, Κρήτη

ΠΑΡΑΘΕΣΗ ΕΡΩΤΑΠΑΝΤΗΣΕΩΝ

1η Ερώτηση : Ποιά είναι τα πρωτόκολλα και οι τεχνικές που εφαρμόζονται προκειμένου να διασφαλιστεί η έκβαση μιας συναλλαγής σ' ένα ηλεκτρονικό κατάστημα ;

Απάντηση : Καταρχήν η συναλλαγή λαμβάνει χώρα μεταξύ Client και Server. Δηλαδή υπάρχει ένας Server που τρέχει τις υπηρεσίες και ο Client ο οποίος τις χρησιμοποιεί. Η οποιαδήποτε συναλλαγή με ένα ηλεκτρονικό κατάστημα γίνεται κατά κύριο λόγο μέσω του HTTP(s) πρωτοκόλλου. Για την διασφάλιση της ομαλής

αλλά και ασφαλούς συναλλαγής θα πρέπει τόσο ο server όσο και ο client να πληρούν κάποιες προδιαγραφές. Βασική προδιαγραφή και για τους 2 είναι να βασίζονται σε τελευταίες εκδόσεις υπηρεσιών, τεχνολογιών και λειτουργικών συστημάτων. Επίσης είναι σημαντικό να ακολουθούνται και τηρούνται οι ενημερώσεις ασφαλείας που κατά καιρούς ανακοινώνονται. Ένας client για παράδειγμα με Windows XP έχει σταματήσει να ενημερώνεται και να διορθώνονται τα κενά ασφαλείας του εδώ και αρκετά χρόνια. Η οποιαδήποτε συναλλαγή γίνει με αυτόν τον client θα είναι κατώτερη σε ασφάλεια λόγω παλαιότητας εκδόσεων και μη συμβατότητας με τις τελευταίες, χαρακτηριστική είναι η υποστήριξη μόνο TLS V1.0

2η Ερώτηση : Ποιες είναι οι διαδικασίες ασφαλείας που πρέπει να τηρηθούν στο background ενός ηλεκτρονικού καταστήματος ;

Απάντηση : Ας το δούμε από την πλευρά του Server. Ένα ηλεκτρονικό κατάστημα είναι μια web εφαρμογή την οποία σερβίρει ο server μέσω του HTTP(s) πρωτοκόλλου. Η εφαρμογή αυτή μπορεί να είναι γραμμένη σε PHP, .NET, javascript, nodejs κτλ. όπου η αποθήκευση των δεδομένων γίνεται, τις περισσότερες φορές, σε μια SQL βαση. Για την ασφάλεια της συναλλαγής και των δεδομένων που ανταλλάσσονται μας ενδιαφέρει η επικοινωνία του Client – Πελάτης με τον Server να είναι κωδικοποιημένη. Για να πραγματοποιηθεί αυτό θα πρέπει το ηλεκτρονικό κατάστημα να έχει ενεργοποιημένο SSL και να ανακατευθύνει όλες τις συναλλαγές σε HTTPs. Στην συνέχεια είναι εξίσου σημαντικό η πλατφόρμα που βασίζεται το ηλεκτρονικό κατάστημα να είναι ενημερωμένη και να ακολουθεί τελευταίες και σύγχρονες τεχνικές. Να είμαστε σίγουροι ότι δεν φιλοξενείται κακόβουλος κώδικας που σκοπό έχει υποκλέψει ή αλλοιώσει δεδομένα τις συναλλαγής. Τέλος για την ολοκλήρωση και πληρωμή της συναλλαγής θα πρέπει το ηλεκτρονικό κατάστημα να χρησιμοποιεί εγκεκριμένο μηχανισμό διαχείρισης πιστωτικών καρτών και γενικά στοιχείων πληρωμής. Συνήθως τα περισσότερα ηλεκτρονικά καταστήματα χρησιμοποιούν έτοιμους μηχανισμούς της τράπεζας που συνεργάζονται ή του Paypal. Στις περιπτώσεις αυτές το site ανακατευθύνει στο μηχανισμό αυτό όπου πραγματοποιείται η εγχρήματη συναλλαγή και στην συνέχεια επιστρέφει στο ηλεκτρονικό κατάστημα.

Επιπλέον επειδή όλα διέπονται από το GPTR (Κανονισμός προστασίας προσωπικών δεδομένων) πρέπει το site να κρατά μόνο τα απαραίτητα στοιχεία κι όχι περαιτέρω πληροφορία (πχ. Ημερομηνία γέννησης, φύλο, σεξουαλικότητα κτλ.) κι αυτά να είναι διασφαλισμένα προκειμένου να μην υπάρχουν διαρροές σε τρίτους.

3η Ερώτηση : Πόσο σημαντική θεωρείτε την ύπαρξη του HTTP-S πρωτοκόλλου για τις Ιντερνετικές συναλλαγές ; Που αλλού θα ήταν καλό να χρησιμοποιείται και ποιος είναι ο λόγος που πρέπει να προτιμούμε τέτοιες συνδέσεις ;

Απάντηση : Το HTTPS πρωτόκολλο είναι το νούμερο 1 για την διαδικτυακή επικοινωνία καθώς και η χρήση γενικότερα του SSL. Αυτό πρέπει να λαμβάνει χώρα σε οποιαδήποτε συναλλαγή, είτε είναι συναλλαγή με χρήματα, είτε απλή περιήγηση, είτε η ανταλλαγή ηλεκτρονικής αλληλογραφίας. Γενικά όλη η ανταλλαγή πληροφορίας που προκύπτει πρέπει να είναι κωδικοποιημένη, αν δεν είναι, θα έμοιαζε με το να

φωνάζεις κάθε φορά σε δημόσιο χώρο το οτιδήποτε σκέφτεσαι ή λες ιδιωτικά σε κάποιον.

Το αν είναι κωδικοποιημένη ή όχι μία σύνδεση το καταλαβαίνουμε στον Browser πάνω αριστερά όπου γράφουμε την ηλεκτρονική διεύθυνση, URL. Εκεί πρέπει να βλέπουμε HTTPS και τη λέξη Secure (αυτό κατά καιρούς αλλάζει, παλαιότερα ήταν πράσινο, τώρα είναι γκρίζο, αλλά σε καμία περίπτωση δεν πρέπει να είναι κόκκινο ή να βλέπουμε Not secure ή σκέτο HTTP). Ο Chrome έχει ανακοινώσει ότι το επόμενο διάστημα δεν θα αφήνει να μπούμε σε διευθύνσεις που δεν θα είναι Secure.

4η Ερώτηση : Πως επιτυγχάνεται η κρυπτογράφηση των e-mails και ειδικότερα όσων περιλαμβάνουν επισυναπτόμενα αρχεία ; Πώς μπορούμε να καταστήσουμε μια συνομιλία ασφαλή και ακόμη υπάρχει τρόπος να προστατεύσουμε τον υπολογιστή μας από κάποιο επιθετικό e-mail;

Απάντηση : Η απάντηση σ' αυτή την ερώτηση βρίσκεται κατά κύριο λόγο στις ρυθμίσεις που έχουν πραγματοποιηθεί στο πρόγραμμα του εκάστοτε mail client. Σε κάθε περίπτωση τόσο για την εισερχόμενη όσο και για την εξερχόμενη αλληλογραφία θα πρέπει να έχετε επιλέξει SSL σύνδεση. Αυτό γίνεται μέσω secure IMAP (port 993), secure POP3 (port 995) και secure SMTP (port 465 ή 587) αντίστοιχα. Από εκεί και πέρα και εφόσον έχουμε διασφαλίσει το απόρρητο της επικοινωνίας θα πρέπει ο server που φιλοξενεί την e-mails υπηρεσία να έχει τους κατάλληλους μηχανισμούς ώστε να απορρίπτει ή να χαρακτηρίζει τυχόν κακόβουλη αλληλογραφία. Τέλος ο υπολογιστής μας, που λαμβάνει τα e-mails, θα πρέπει να τρέχει κατάλληλο λογισμικό προστασίας ώστε να σκανάρονται επιπλέον τα e-mails σε τοπικό επίπεδο για κακόβουλο κώδικα ή μη επιτρεπτό περιεχόμενο.

5η Ερώτηση : Ποιοί είναι οι πιο διαδεδομένοι κίνδυνοι που διέπουν τις ηλεκτρονικές συναλλαγές ;

Απάντηση : Το πιο συχνό που παρατηρούμε στις ηλεκτρονικές συναλλαγές είναι ότι το ηλ. Κατάστημα, η τράπεζα, το site το οποίο πάει να επισκεφτεί ο πελάτης είναι πλαστό, οπότε ο κίνδυνος με τον οποίο ερχόμαστε αντιμέτωποι είναι το Phising. Σ' αυτή την περίπτωση έρχεται στον πελάτη ένα mail όπου λέει ότι είναι από το αντίστοιχο site και ότι πρέπει μέσα από αυτό να μπει στον λογαριασμό του και να ανανεώσει τα στοιχεία του. Με το που κλικάρει τον σύνδεσμο εμφανίζεται ένα site ακριβώς το ίδιο με το πραγματικό, εισάγοντας τα στοιχεία του εκεί ο πελάτης το μόνο που καταφέρνει είναι να έχουν υποκλαπεί όλα.

Άλλος κίνδυνος είναι τα Man – in – the middle attacks, όπου κάποιος μπαίνει ενδιάμεσα σε μια μη κωδικοποιημένη συναλλαγή και υποκλέπτει ή αλλοιώνει τα δεδομένα που ανταλλάσσονται.

Κλείνοντας την ερώτηση αυτή ένας άλλος συχνός κίνδυνος είναι τα μη ενημερωμένα ηλεκτρονικά καταστήματα. Υπάρχουν περιπτώσεις αρκετά παλιού και μη ενημερωμένου λογισμικού με γνωστά κενά ασφαλείας ή custom κώδικα που έχει σταματήσει για διάφορους λόγους να αναπτύσσεται και βελτιώνεται από τον εκάστοτε προγραμματιστή. Αυτό έχει σαν συνέπεια τα ηλεκτρονικά αυτά

καταστήματα να φιλοξενούν κακόβουλο κώδικα και συμμετέχουν άμεσα ή έμμεσα σε κακόβουλες ενέργειες.

6η Ερώτηση : Αναφερόμενοι σε μια ασφαλή ηλεκτρονική συναλλαγή, ποιά είναι τα σημεία στα οποία επεμβαίνουν τα πρωτόκολλα ασφαλείας από την ώρα που ο πελάτης θα εξοφλήσει στον ηλεκτρονικό έμπορο το προϊόν που επίλεξε, έως την στιγμή που το προϊόν θα είναι έτοιμο για αποστολή προς τον αγοραστή ;

Απάντηση : Από την αρχή που ένα άτομο επισκέπτεται μία σελίδα επεμβαίνει το HTTP με την πόρτα 80 κι έτσι η ίδια η σελίδα εφόσον έχει ενεργοποιημένο SSL πρέπει να γυρίσει την σύνδεση σε HTTP – S. Αυτή είναι η διαδικασία κωδικοποίησης μεταξύ του φυσικού προσώπου με τον Server.

Τώρα, στο τελικό στάδιο της ηλ. Συναλλαγής ο Server για να πάρει τα χρήματα εκτελεί διάφορους μηχανισμούς, με κάποιους από τους οποίους εφόσον έχει διαπιστευτεί από κάποια τράπεζα μπορεί να πάρει τα στοιχεία της πιστωτικής κάρτας και να μπαίνει ο ίδιος να εκτελεί τη συναλλαγή. Βέβαια αυτό είναι πιο δύσκολο πλέον, διότι οι τράπεζες θέλουν κάποια προαπαιτούμενα για να δώσουν σ' έναν Server τη δυνατότητα να χρεώνει πιστωτικές κάρτες ηλεκτρονικά. Αν η σελίδα έχει μόνιμους πελάτες κι υπάρχουν συνδρομές που είναι ανανεωνόμενες, σημαίνει ότι έχει περαστεί η πιστωτική και τα στοιχεία αυτά υπάρχουν κάπου αποθηκευμένα για να γίνεται Auto -Update και να τραβιούνται τα χρήματα αυτόματα. Σ' αυτές τις περιπτώσεις η πιστωτική κάρτα δεν αποθηκεύεται στη σελίδα τοπικά αλλά ανιχνεύεται η τράπεζα στην οποία ανήκει και από 'κει και πέρα η τράπεζα εξουσιοδοτεί ,για το συγκεκριμένο ID συναλλαγής, τη σελίδα για να ζητούνται χρήματα όποτε πρέπει.

Άλλος μηχανισμός είναι κατά την εξόφληση της συναλλαγής ο πελάτης να μεταφέρεται αυτόματα στο site της τράπεζας κι εκεί πάλι αναφερόμαστε σε HTTP – S.

7η Ερώτηση : Αναφορικά με το πρωτόκολλο SSL : Ποιός είναι ο ρόλος του, ποιοι τύποι υπάρχουν και πως καταλαβαίνουμε ότι η σελίδα που απευθυνόμαστε διέπεται από τον εκάστοτε τύπο ;

Απάντηση : Κατά την γνώμη μου υπάρχουν 4 τύποι κι όχι 3 που αναφέρονται γενικά. Ο 4ος είναι τα Self-Signed SSL πιστοποιητικά που τα έχει φτιάξει ο εκάστοτε προγραμματιστής, τα οποία δεν είναι Valid και πιστοποιημένα από κάποια εταιρία, αλλά υπάρχουν. Αυτά συνήθως τα βλέπουμε όταν ένας προγραμματιστής σηκώνει ένα Site και σηκώνει παράλληλα και ένα SSL και βάζει ένα πιστοποιητικό που το έχει φτιάξει ο ίδιος, εννοείται ότι δεν είναι Secure (Πράσινο ή Γκρίζο) και Valid αλλά έχει υπόσταση. Το αν θα το δεχθεί ο πελάτης ή όχι είναι στην κρίση του αν εμπιστεύεται τον προγραμματιστή. Παρόλα αυτά η επικοινωνία είναι κωδικοποιημένη και δεν μπορεί να κλαπεί.

Οι υπόλοιποι 3 τύποι είναι : 1ον) Ο πιο απλός τύπος το DOMAIN VALIDATE CERTIFICATE καθώς και ο πιο οικονομικός και δεν απαιτείται τίποτα περισσότερο από το να ανήκει απλά στον ενδιαφερόμενο το Domain και αποδεικνύεται απλά μέσω ενός mail το οποίο θα λάβει και θα πρέπει να πατήσει Verified.

Καταλαβαίνουμε ότι γίνεται χρήση αυτού, αν πατήσουμε πάνω στον Browser και γράφει απλά Secure και τα μόνα στοιχεία που δίνει είναι το όνομα του Domain και τα στοιχεία της εταιρίας που το έχει εκδώσει πχ. Comodo SSL Certificates

2ον) Λίγο ανώτερο είναι το ORGANISATION CERTIFICATE VALIDATION το οποίο απαιτεί και κάποια γραφειοκρατία για να εκδοθεί. Δηλαδή έγγραφα που αποδεικνύουν ότι όχι απλά ανήκει στον ενδιαφερόμενο το Domain αλλά και βεβαίωση ότι έχει και το δικαίωμα χρήσης του. Επιπλέον το διακρίνουμε γιατί όταν θα πατήσουμε πάνω στον Browser αναφέρονται και τα στοιχεία της εταιρίας στην οποία ανήκει κι όχι μόνο το Domain.

3ον) Τέλος έχουμε το πιο ενισχυμένο SSL, το EXTENDED VALIDATION που αναφέρεται κυρίως σε μεγάλους οργανισμούς και τράπεζες. Απαιτείται πολύ γραφειοκρατία καθώς πρέπει να πιστοποιηθεί εγγράφως η φυσική και νομική υπόσταση του προσώπου στο οποίο ανήκει το Domain και πρέπει να πιστοποιηθεί και το δικαίωμα χρήσης αυτού. Κατέχοντας ένα τέτοιο πιστοποιητικό αυτόματα πιστοποιείται ότι έχει κατατεθεί κάθε απαραίτητο έγγραφο και όλα τα αποδεικτικά για την ταυτοπροσωπία του κατόχου του. Γενικότερα είναι το πιο μεγάλο και είναι και το πιο ακριβό πιστοποιητικό. Το διακρίνουμε γιατί όταν θα πατήσουμε πάνω στον Browser δεν θα λέει απλά Secure λέει και το όνομα του οργανισμού που ανήκει.

8η Ερώτηση : Πως αντιμετωπίζεται μια επίθεση στα κενά ασφαλείας μιας web εφαρμογής και πως ένας απλός επισκέπτης ενός site μπορεί να καταλάβει ότι τα στοιχεία του είναι εκτεθειμένα σε κίνδυνο ;

Απάντηση : Η απάντηση σ' αυτή την ερώτηση δεν είναι εύκολη. Ένας μέσος χρήστης δεν μπορεί να το καταλάβει. Κατ' αρχήν όταν επισκεπτόμαστε μία σελίδα όπως λέμε από την αρχή της συνέντευξης, πρέπει να ελέγχουμε πάντα αν έχει SSL. Πρέπει το μάτι να πηγαίνει αυτόματα στον Browser να λέει Valid – Secure κτλ.

Εν συνεχεία όταν θα μας έρθει ένα mail πχ. Από την τράπεζα Πειραιώς και πατήσουμε πάνω στον σύνδεσμο που περιέχεται, θα πρέπει μετακινώντας το ποντίκι μας χαμηλά στον Browser που έχει ανοίξει, το URL που εμφανίζεται να είναι σχετικό με την τράπεζα Πειραιώς και να μην είναι κάτι άσχετο, δηλαδή ένα χακαρισμένο Site με ένα Phising πάνω – ομοίωμα της Πειραιώς. Είναι σημαντικό να λαμβάνουμε σοβαρά υπόψη τυχόν προειδοποιητικά μηνύματα του browser ή του λογισμικού προστασίας του υπολογιστή μας ώστε να διακόπτουμε τυχόν επισφαλείς ή ύποπτες συναλλαγές.

Γενικότερα σημαντικό ρόλο παίζει και το είδος της συναλλαγής που θέλουμε να κάνουμε. Αν πάμε να κατεβάσουμε μία σπασμένη ταινία ή ένα σπασμένο πρόγραμμα από ένα site είναι σίγουρο ότι εμπεριέχονται πολλά κακόβουλα στοιχεία σ' αυτά. Οπότε όταν εξ' αρχής η IP είναι περίεργη είναι φυσιολογικό να πέσουμε σε παγίδα και ακόμα πιο πιθανό είναι να μην το καταλάβουμε.

Τέλος θα πρέπει να είμαστε προσεκτικοί που βάζουμε τα στοιχεία μας (αριθμός κάρτας κτλ.) και γενικά αποφεύγουμε να ψωνίζουμε από σελίδες που δεν έχουν πληρωμή μέσω διαπιστευμένου μηχανισμού (πχ Paypal).

9η Ερώτηση : Μελετώντας σε βάθος το θέμα των επιθέσεων στο διαδίκτυο, με ποιόν τρόπο μπορούμε να προστατέψουμε μια βάση δεδομένων SQL, δεδομένου ότι αποτελεί δέλεαρ καθώς όλα τα στοιχεία των πελατών των ηλεκτρονικών καταστημάτων, σελίδων κτλ είναι αποθηκευμένα εκεί ;

Απάντηση : Η απάντηση στην ερώτηση αυτή είναι ένα μεγάλο κεφάλαιο και μπορεί να καλυφτεί πλήρως συγκεντρώνοντας απαντήσεις από διάφορες ειδικότητες και κυρίως αυτή του Developer. Εγώ είμαι System Administrator και Μηχανικός δικτύου και θα δώσω την απάντηση από την δική μου σκοπιά. Αυτό το λέω γιατί σ' ότι έχουμε πει μέχρι στιγμής, υπάρχει μια δόση κι από άλλες ειδικότητες. Το ίδιο ισχύει και για την βάση δεδομένων.

Ένας SQL Server που φιλοξενεί μία βάση δεδομένων, είτε είναι My SQL που είναι ο πιο συνηθισμένος για τα διαδικτυακά καταστήματα, είτε σπανιότερα είναι Postgre SQL ή Oracle SQL Server πρέπει να τηρεί συγκεκριμένες αρχές. Πρέπει να είναι απομονωμένος – Isolated, δηλαδή πρέπει να επιτρέπει συνδέσεις μόνο από συγκεκριμένα δίκτυα και συγκεκριμένες IPs. Ακόμα καλύτερο θα ήταν αν είναι δυνατό ο Server να επιτρέπει συνδέσεις μόνο από την IP του Site ή ο ίδιος ο TP Server να είναι στον ίδιο Server με τον Web, γιατί όταν επιτρέπει Local Host συνδέσεις στην Local διεύθυνση καθίσταται ακόμα πιο ασφαλής η επικοινωνία.

Αν δεν υπάρχει περιορισμός στις IPs και ο Server δέχεται συνδέσεις από παντού, θα πρέπει να υπάρχει ένα πάρα πολύ ισχυρό ADMIN Password και επιπλέον θα πρέπει και οι λογαριασμοί που υπάρχουν μέσα να έχουν κι αυτοί πάρα πολύ δυνατά Passwords, αλλά θα ήταν προτιμότερο να μην επιτρέπονται συνδέσεις από παντού.

Βέβαια το πρόβλημα στην βάση δεδομένων δεν είναι να χτυπηθεί η ίδια η βάση. Τα στοιχεία της ίδιας της βάσης αντλούνται από κενά ασφαλείας που έχει το ίδιο το Site και είναι αυτά που προκαλούν τα λεγόμενα SQL Injections. Δηλαδή το Site τρέχει κώδικα ο οποίος αναγκάζει τη βάση δεδομένων να επιστρέφει στοιχεία τα οποία δεν θα έπρεπε κι αυτό δεν μπορεί να αποφευχθεί διότι είναι απαραίτητο η σελίδα να έχει πρόσβαση στη βάση δεδομένων και δεν μπορεί να περιοριστεί με κάποιο Firewall. Για να προστατευτούν τα δεδομένα της βάσης πρέπει το site να είναι κατάλληλα γραμμένο και υπάρχουν τεχνικές όπως θα μας εξηγούσε καλύτερα ένας Developer που περιορίζουν τα SQL injections. Κάποιες από αυτές τις τεχνικές είναι οι Storage Procedures και ουσιαστικά μας διασφαλίζουν ότι η εφαρμογή μας δεν θα επιτρέψει σε κάποιο κώδικα να τρέξει ερωτήματα – SQL Queries στην βάση διότι μεσολαβούν άλλες διαδικασίες πριν.

Κλείνοντας λοιπόν, το πρόβλημα της βάσης δεδομένων είναι τα SQL Injections και όχι τόσο τα κενά ασφαλείας στον TP Server. Πάντα είναι αυτονόητο ότι πρέπει να είναι ενημερωμένος με τελευταίες εκδόσεις λογισμικού κτλ. Η Αχίλλειος πτέρνα είναι το Site και ο τρόπος που είναι γραμμένο αυτό, διότι αν είναι γραμμένο με τρόπο που επιτρέπονται τα απευθείας ερωτήματα στην βάση, τότε η πληροφορία θα διαρρεύσει από εκεί.

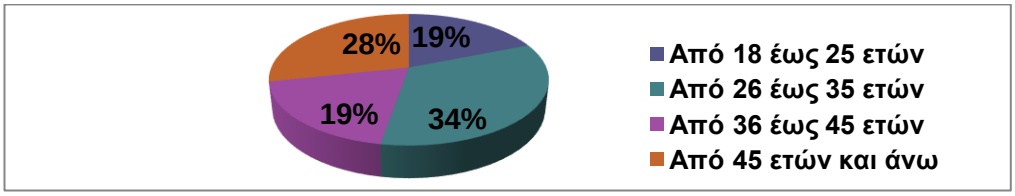
5.3.2 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ – ΠΟΣΟΤΙΚΗ ΕΡΕΥΝΑ

Ενότητα 1η : Δημογραφικές Ερωτήσεις

Διάγραμμα 5.1 : Φύλο

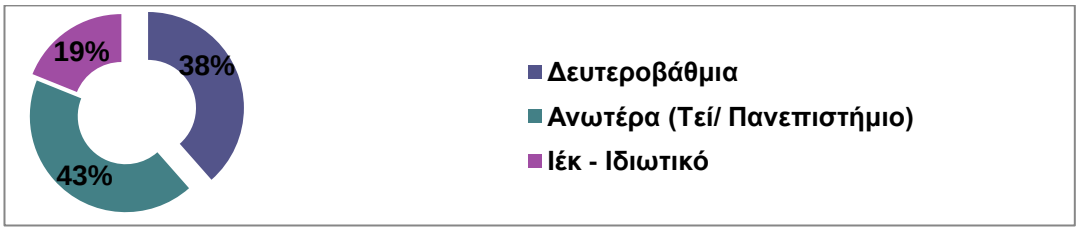
Σχόλια : Στα πλαίσια αυτής της έρευνας το κοινό το οποίο ανταποκρίθηκε ανέρχεται στα 150 άτομα από τα οποία το 41% είναι άνδρες και το 59% είναι γυναίκες.

Διάγραμμα 5.2 : Ηλικία



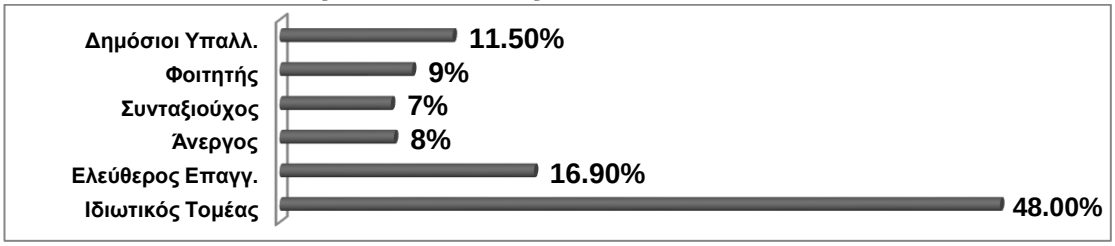
Σχόλια : Οι ηλικίες που κερδίζουν τα ποσοστά συμμετοχής στο επί μελέτη δείγμα είναι από 26 έως 35 ετών με ποσοστό 34% και αμέσως μετά από 45 ετών και άνω με ποσοστό 28% . Τέλος με μικρότερο ίδιο ποσοστό έρχονται οι ηλικίες από 18 έως 25 και από 36 έως 45 ετών με 19% η κάθε κατηγορία.

Διάγραμμα 5.3 : Εκπαίδευση



Σχόλια : Το μορφωτικό επίπεδο των ατόμων που συμμετείχαν στο ερωτηματολόγιο αφορά άτομα που κατά 43% έχουν αποφοιτήσει από Ανώτερο εκπαιδευτικό Ίδρυμα, εν συνεχεία το 38% είναι άτομα που έχουν σταματήσει στην Δευτεροβάθμια εκπαίδευση και τέλος με 19% απαντώνται άτομα που έχουν αποφοιτήσει από Ιέκ ή Ιδιωτικό Κολέγιο.

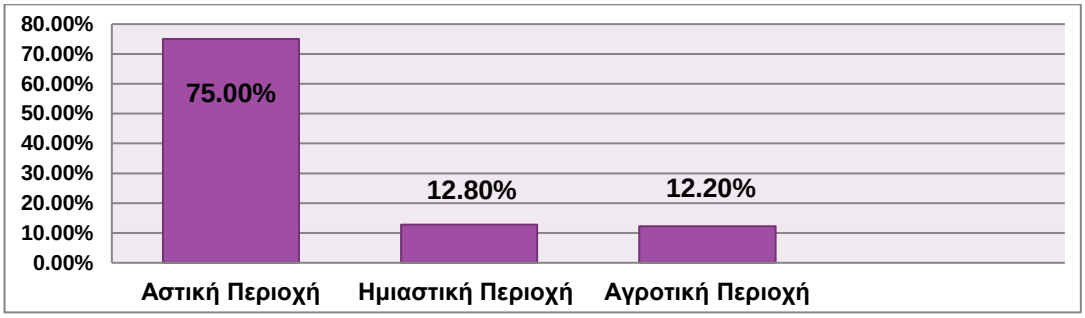
Διάγραμμα 5.4 : **Τομέας Απασχόλησης**



Σχόλια : Στο διαθέσιμο δείγμα βλέπουμε ότι η πλειοψηφία των ερωτηθέντων ανήκουν στον ιδιωτικό τομέα με 48%, συνεχίζουμε με το 16,9% που αντιστοιχεί στους

ελεύθερους επαγγελματίες και σε μικρότερα ποσοστά απάντησαν με 8% Άνεργοι, με 8,8% Φοιτητές, με 11,5 % Υπάλληλοι του Δημοσίου και τέλος με 7,4% Συνταξιούχοι.

Διάγραμμα 5.5 : Καταγωγή



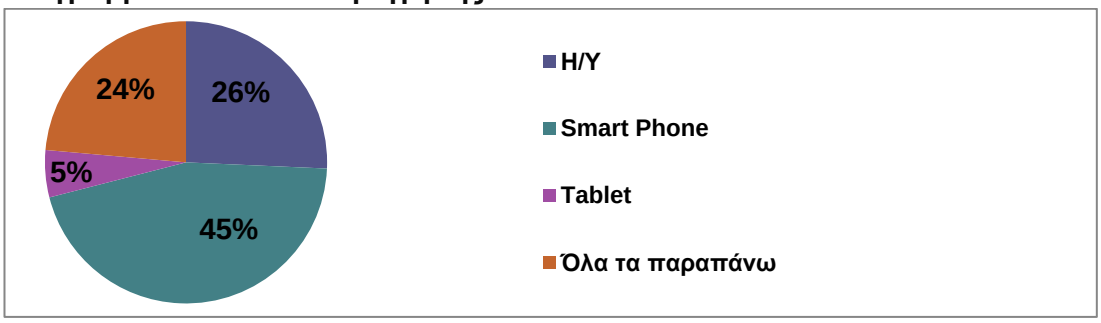
Σχόλια : Το μεγαλύτερο ποσοστό ατόμων από εκείνους που ερωτήθηκαν ανέρχεται σε 75% ανήκει σε κάτοικους Αστικής περιοχής, το 12,8% σε κάτοικους ημιαστικής περιοχής και το 12,2% σε κάτοικους αγροτικής περιοχής.

Ενότητα 2η : Ενασχόληση Ερωτώμενου με το Διαδίκτυο

Διάγραμμα 5.6 : Χρήση Διαδικτύου Ημερησίως

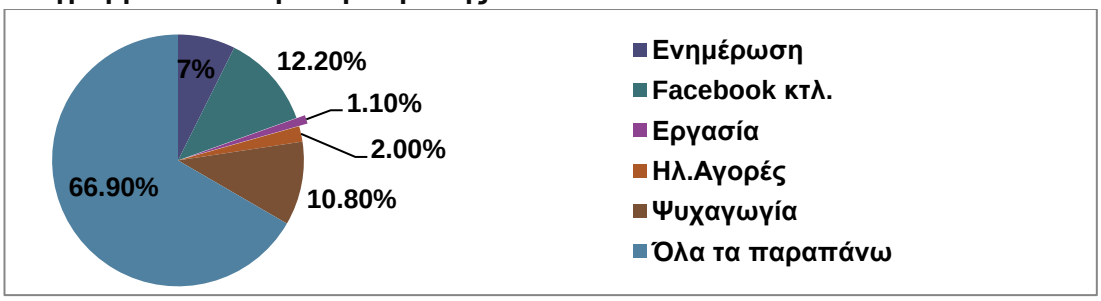
Σχόλια : Στο παραπάνω διάγραμμα παρατηρούμε ότι το μεγαλύτερο μέρος του δείγματος απασχολείται στο διαδίκτυο από 2 έως 4 ώρες με 50% και από 4 έως 8 ώρες το 26%. Τέλος σε μικρότερα ποσοστά από 8 ώρες και άνω το 17%, με 7% έως 1 ώρα.

Διάγραμμα 5.7 : Μέσα Περιήγησης στο Διαδίκτυο



Σχόλια : Η τεχνολογία που μπορεί κάποιος να χρησιμοποιήσει για να περιηγηθεί στο διαδίκτυο ποικίλει έτσι παρατηρούμε ότι το μεγαλύτερο ποσοστό 45% σε σύνολο 150 ατόμων χρησιμοποιεί Smart Phoneτο 26% Η/Υτο 5% Tablet και τέλος το 24% κάνει χρήση όλων των παραπάνω.

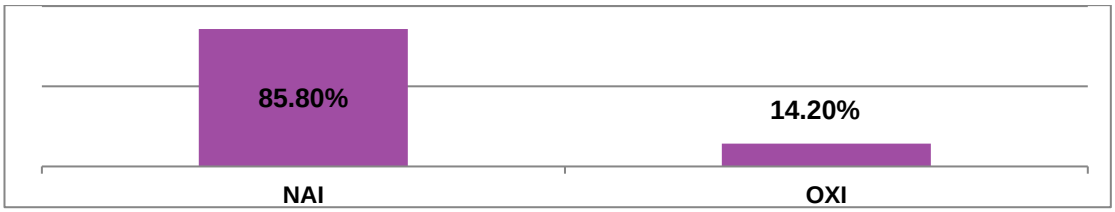
Διάγραμμα 5.8 : Λόγοι Πρόσβασης στο Διαδίκτυο



Σχόλια : Οι λόγοι για τους οποίους μπορεί κάποιος να περιηγηθεί στο διαδίκτυο είναι πολλοί και το 12,2 % το χρησιμοποιεί για λόγους κοινωνικής δικτύωσης το 10.8% για ψυχαγωγία το 7% για Ενημέρωση το 1,10% για Εργασία το 2% αποκλειστικά για Ηλ. Αγορές και τέλος το 66,9% για όλους τους παραπάνω λόγους.

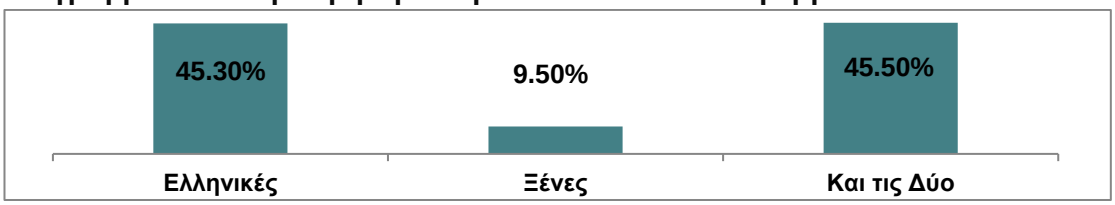
Ενότητα 3η : Ηλεκτρονικές Αγορές

Διάγραμμα 5.9 : Προτίμηση Ηλεκτρονικών αγορών



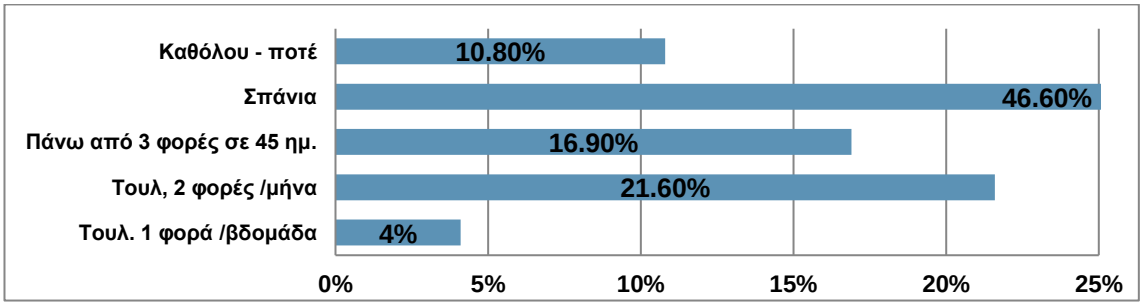
Σχόλια : Στα 150 άτομα που ερωτήθηκαν το 85,8% δήλωσαν ότι προτιμούν τις ηλεκτρονικές αγορές ενώ σε μικρότερο ποσοστό μόλις 14,2% ότι δεν πραγματοποιούν καθόλου.

Διάγραμμα 5.10 : Προτίμηση Ελληνικών / Ξένων Πλατφορμών



Σχόλια : Σε 45,3% ανέρχεται η προτίμηση Ελληνικών πλατφορμών και σε 9,5% οι Ξένες, ενώ η προτίμηση και των δύο απαντάται σε ποσοστό 45,5%.

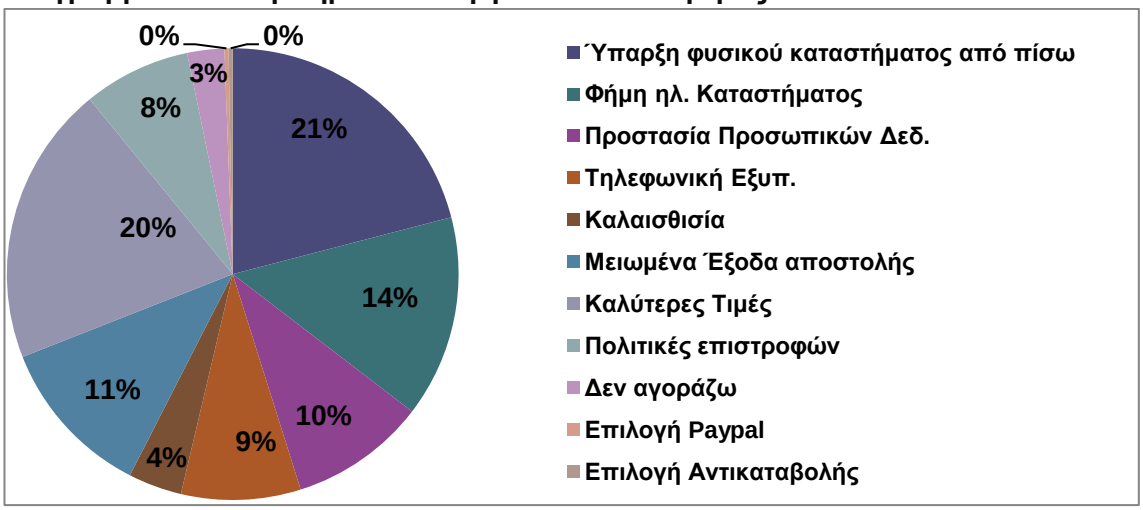
Διάγραμμα 5.11 : Συχνότητα Ηλ. Αγορών



Σχόλια : Η συχνότητα των διαδικτυακών αγορών τουλάχιστον 2 φορές μέσα σ' ένα μήνα ανέρχεται στο 21,6%με ποσοστό 16,9% συναντάμε την κατηγορία 'Πάνω από 3

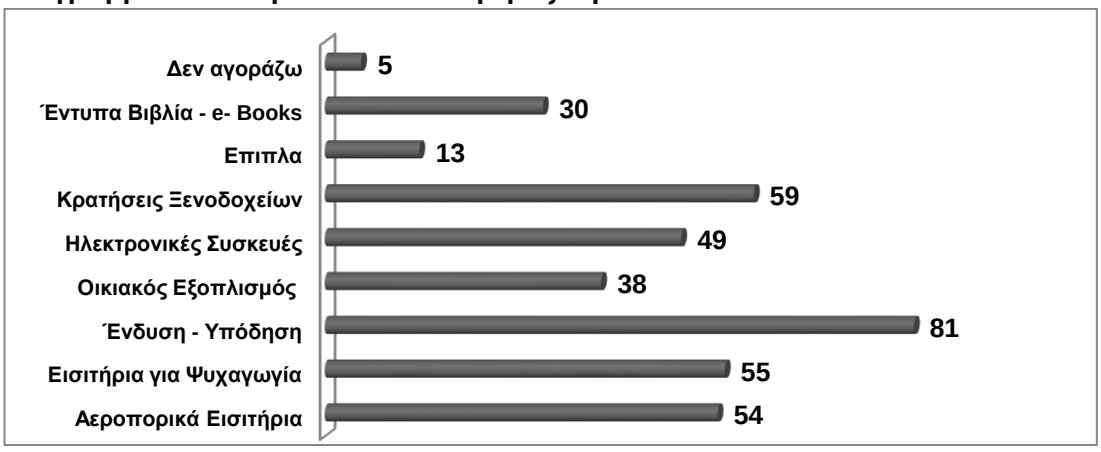
φορές μέσα σε 45 μέρες' και την κατηγορία του κοινού που δεν πραγματοποιεί καθόλου αγορές την απαντάμε με ποσοστό 10,8%. Κλείνουμε με 46,6% αυτοί που αγοράζουν Σπάνια μέσω διαδικτύου και με 4% εκείνοι που αγοράζουν τουλάχιστον 1 φορά την εβδομάδα.

Διάγραμμα 5.12 : Κριτήρια Επιλογή Ιστότοπου αγοράς



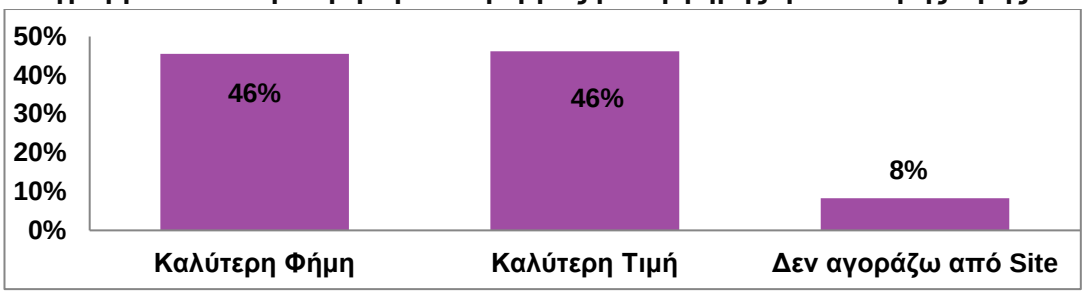
Σχόλια : Ενδιαφέρον παρουσίασαν τα ποσοστά των κριτηρίων με τα οποία ένας διαδικτυακός αγοραστής επιλέγει την σελίδα που θα πραγματοποιήσει τις αγορές του. Με 21% κερδίζει η Ύπαρξη φυσικού καταστήματος από πίσω, με 20% έρχεται δεύτερη η κατηγορία ''Καλύτερη Τιμή'' και Τρίτη με 14% η κατηγορία '' Φήμη''. Με μικρότερα ποσοστά ακολουθούν με 10% όσες σελίδες παρέχουν προστασία προσωπικών δεδομένων και μειωμένα έξοδα αποστολής, με 8% όσες έχουν ορθή πολιτική επιστροφών με 9% όσες έχουν σωστή τηλεφωνική εξυπηρέτηση, με 4% όσες έχουν καλαίσθητο site και κλείνουμε με αυτούς που δεν έχουν κριτήριο γιατί δεν αγοράζουν.

Διάγραμμα 5.13 : Προϊόντα που αγοράζουμε από το διαδίκτυο



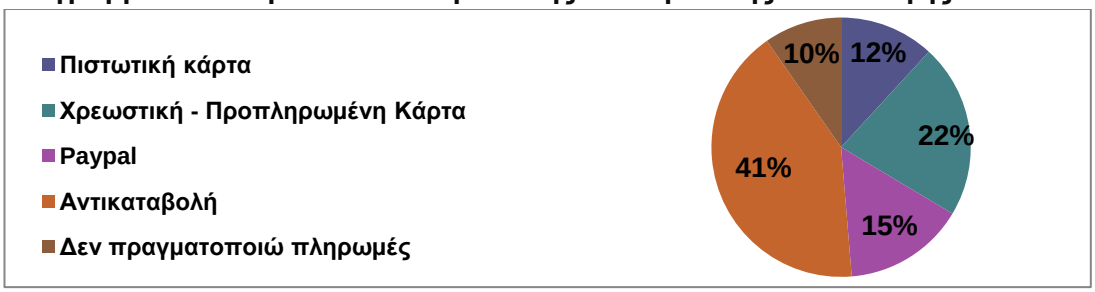
Σχόλια : Οι προτιμήσεις των καταναλωτών στα προϊόντα και τις υπηρεσίες που εμπορεύονται διαδικτυακά έρχονται ως εξής καθώς κάθε ερωτώμενος είχε τη δυνατότητα να επιλέξει περισσότερα από 1 προϊόντα : 81 άτομα επέλεξαν ρούχα και παπούτσια55 εισιτήρια για ψυχαγωγία και αντίστοιχα για αεροπορικά εισιτήρια59 για κρατήσεις ξενοδοχείων, 49 για αγορά ηλεκτρονικών συσκευών, 38 για οικιακό εξοπλισμό και αντίστοιχα 30 για βιβλία13 για έπιπλα και 5 δεν αγοράζουν τίποτα .

Διάγραμμα 5.14 : Προτίμηση Πλατφόρμας βάση φήμης ή καλύτερης τιμής



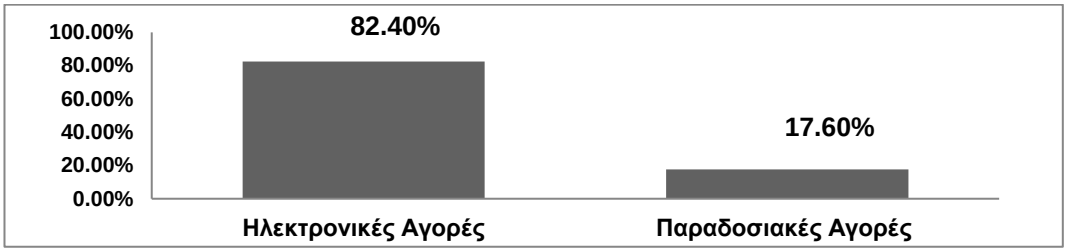
Σχόλια : Ισοπαλία έχουμε στην επιλογή πλατφόρμας ηλεκτρονικής αγοράς με 46% η κάθε επιλογή. Τέλος το 8% δεν αγοράζει από Site.

Διάγραμμα 5.15 : Τρόποι διεκπεραίωσης Ηλεκτρονικής Συναλλαγής



Σχόλια : Πρώτη σε προτίμηση έρχεται η επιλογή της αντικαταβολής με 41% και εν συνεχεία με 22% η χρήση της χρεωστικής κάρτας. Κλείνοντας το 12% θα χρησιμοποιούσε την πιστωτική του ενώ το 10% δεν πραγματοποιεί πληρωμές μέσω διαδικτύου.

Διάγραμμα 5.16 : Παραδοσιακή ή Ηλεκτρονική Αγορά?



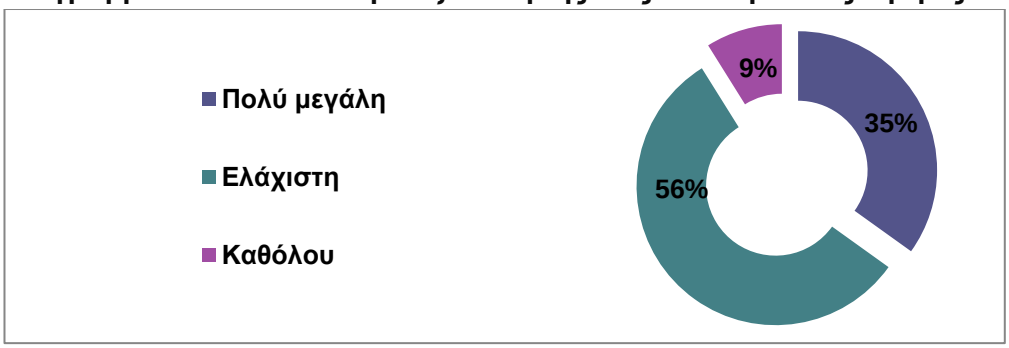
Σχόλια : Το 82,4% του πληθυσμού επιλέγει Ηλεκτρονικές αγορές ενώ μόνο το 17,6% παραμένει στον παραδοσιακό τρόπο αγορών.

Ενότητα 4η : Κίνδυνοι Ηλεκτρονικών Αγορών

Διάγραμμα 5.17 : Ειλικρίνεια Ηλεκτρονικών Καταστημάτων

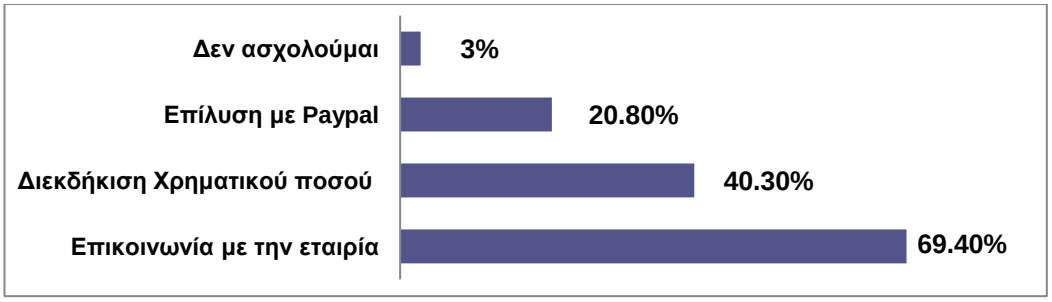
Σχόλια : Με μεγάλη διαφορά στα νούμερα βλέπουμε ότι το 35% του δείγματος πιστεύει στην απόλυτη ειλικρίνεια των ηλεκτρονικών Καταστημάτων ενώ το 65% εμφανίζει δυσπιστία ως προς αυτού του είδους τις συναλλαγές.

Διάγραμμα 5.18 : Πιθανότητα εξαπάτησης στις Ηλεκτρονικές Αγορές



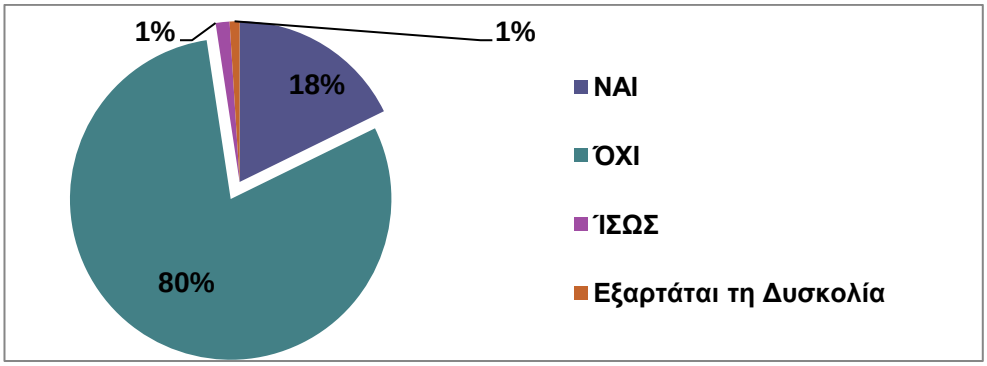
Σχόλια : Οι απόψεις έρχονται και επαληθεύονται αναλυτικότερα στο παρόν ερώτημα καθώς το 56% πιστεύει ότι οι πιθανότητες εξαπάτησης είναι ελάχιστεςενώ με 35% έρχονται οι δύσπιστοι που υποστηρίζουν ότι είναι πολύ μεγάλη και τέλος το 9% που πιστεύει ότι δεν κινδυνεύει καθόλου.

Διάγραμμα 5.19 : Πως αντιμετωπίζουμε μια κακή ηλεκτρονική συναλλαγή ;



Σχόλια : Οι περισσότεροι καταναλωτές καταφεύγουν στην επικοινωνία με την εταιρία προκείμενου να αντιμετωπίσουν ένα πρόβλημα στις συναλλαγές τους ,ενώ το 40,3% διεκδικεί το τα χρήματα τους πίσω. Τέλος το 20,8% χρησιμοποιεί σαν ενδιάμεσο το Paypal ενώ το 3% δεν ασχολείται καν.

Διάγραμμα 5.20 : Θα προτιμούσατε ξανά το ηλ. Κατάστημα που σας δυσκόλεψε στην συναλλαγή ;



Σχόλια : Το 80% δεν θα προτιμούσε ξανά το ηλεκτρονικό κατάστημα που τους δημιούργησε πρόβλημα ενώ το 18% θα έδινε μια 2η ευκαιρία. Τέλος το 1% θα αποφάσιζε ανάλογα με τη δυσκολία που αντιμετώπισε.

ΚΕΦΑΛΑΙΟ 6^{Ο} : ΣΥΜΠΕΡΑΣΜΑΤΑ

ΣΚΟΠΟΣ ΕΡΓΑΣΙΑΣ

Η παρούσα πτυχιακή εργασία δημιουργήθηκε με σκοπό την σε βάθος μελέτη του Ηλεκτρονικού Εμπορίου και των στοιχείων που το απαρτίζουν. Η βασική παράμετρος πάνω στην οποία εστίασε η μελέτη και βασίστηκε η δευτερογενής έρευνα είναι το κομμάτι της ασφάλειας που διέπει οποιαδήποτε ηλεκτρονική δραστηριότητα (είτε απλή περιήγηση ,είτε πιο σύνθετη συναλλαγή).

Σύμφωνα με την βιβλιογραφική ανασκόπηση που προηγήθηκε έγινε διακριτό το κατά πόσο το ηλεκτρονικό εμπόριο είναι προσαρμοσμένο στην καθημερινότητα της κοινωνίας σε σημείο ώστε να υπερτερεί του παραδοσιακού. Αρωγός της ραγδαίας αυτής εξέλιξης είναι η έλλειψη χρόνου τόσο σε προσωπικό επίπεδο όσο και σε επίπεδο εργασιακού τομέα.

Όλη αυτή η έξαρση του ηλεκτρονικού εμπορίου ως επί το πλείστον οφείλεται στην επικέντρωση στα θετικά που έχει τόσο για τους καταναλωτές και την κοινωνία όσο και για τους οργανισμούς. Τα μειονεκτήματα αν και υπάρχουν δεν φαίνεται να απασχολούν ιδιαίτερα καθώς το ενδιαφέρον παραμένει σταθερά αμείωτο σύμφωνα με το ερωτηματολόγιο που συμπληρώθηκε στα πλαίσια της δευτερογενούς έρευνας.

Κατά την πρόοδο της έρευνας διαπιστώθηκε ότι η εκμετάλλευση του ίντερνετ και η χρήση του για τις επιχειρησιακές δραστηριότητες δημιούργησε την ανάγκη πολλών ηλεκτρονικών ειδών όπως : το **B2C (Business to Consumer)**το **B2B (Business to Business)**το **B2G (Business to Government)**το **B2E (Business to Enterprise)**το **G2C (Government to Consumer)**το **E – Governance** και το **G2B (Government to Business)**το **C2C (Consumer to Consumer)** και το **Consumer to Business (C2B)**. Εν κατακλείδι ερχόμαστε σε επαφή με πολυάριθμους συνδυασμούς ηλεκτρονικών συναλλαγών για την εξυπηρέτηση διαφορετικών σκοπών στην κάθε περίπτωση.

Φυσικό επακόλουθο ήταν η εμφάνιση ποικίλων μορφών με τις οποίες κάποιος μπορεί ηλεκτρονικά να πραγματοποιήσει συναλλαγές. Έχουμε λοιπόν τα **E – shops,** τα **E – Marketplaces**, το **Ηλ. Επιχειρήν,** τις **Ηλ. Επιχειρήσεις,** τους **E – infobrokers,** τις **Ηλ. Δημοπρασίες,** τις **Ηλ. Προμήθειες,** τα **E – Malls**, το **E – Invoice** και τέλος το **ηλεκτρονικό εμπόριο** που πραγματοποιείται **μέσω Κινητού τηλεφώνου**.

Όπως περιγράφεται και στο 4ο κεφάλαιο της εργασίας, οι κυριότεροι μηχανισμοί διεκπεραίωσης ηλεκτρονικών συναλλαγών είναι η πιστωτική – προπληρωμένη – χρεωστική κάρτα, το ηλεκτρονικό χρήμα κ.ο.κ ενώ η διασφάλιση των παραπάνω συναλλαγών γίνεται με την χρήση τεχνικών όπως είναι : η ψηφιακή υπογραφή, τα cookies, το ψηφιακό πιστοποιητικό, το πρότυπο ISO 17799 : 2005, το πρωτόκολλο S – HTTP, τα S – MIME και το πρωτόκολλο SET.

Βασιζόμενοι στη μελέτη των τεχνικών ζητημάτων ασφαλείας ως άνω αναφέρθη, συνεχίζουμε με τους κίνδυνους που προκύπτουν από την μη τήρηση τους. Στην υποκλοπή **Man in the Middle Attack** αναφερόμαστε σε απόσπαση στοιχείων η οποία επιτυγχάνεται μόνο όταν ο εισβολέας είναι σε θέση να μιμηθεί κάθε παράμετρο της σύνδεσης. Στην δευτερογενή έρευνα αναλύσαμε επαρκώς την προστασία των συνδέσεων μέσω του πρωτόκολλου ασφαλείας SSL το οποίο είναι υπεύθυνο για το μεγαλύτερο μέρος της αποφυγής των ηλεκτρονικών απατών στις συναλλαγές. Στο ανωτέρω κεφάλαιο έχει δημιουργηθεί προσωπικό παράδειγμα επίθεσης προκειμένου να γίνει κατανοητός ο τρόπος της επίθεσης και έχει μελετηθεί αναλυτικά κάθε είδους πρωτόκολλο SSL και τα γνωρίσματα του καθώς επίσης και πως εμείς οι απλοί χρήστες μπορούμε να γνωρίζουμε ανά πάσα ώρα και στιγμή αν η σύνδεση μας είναι προστατευμένη. Ακόμα μια απάτη είναι αυτή του **Phising** η οποία σαν δόλωμα χρησιμοποιεί συνήθως πλαστές URL και η αρκετά συνηθισμένη μέθοδο των **Ιών των Υπολογιστών**.

Ακόμα πιο ειδικά στις επιθέσεις συναντάμε τις **Cross Site Scripting** επιθέσεις και τέλος τις **επιθέσεις που γίνονται στις βάσεις δεδομένων με την χρήση των SQL Injections.** Τρόποι αποφυγής των συγκεκριμένων επιθέσεων δεν είναι άλλοι όπως έχει σημειωθεί παραπάνω παρά ένας καλός σχεδιασμός της βάσης δεδομένων και πέρα από αυτό η καλή συντήρηση και έγκαιρη ενημέρωση αυτής από τον δημιουργό της.

ΘΕΣΗ ΕΡΕΥΝΗΤΗ ΚΑΙ ΠΡΟΤΆΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

Η επιθυμία εκπόνησης του συγκεκριμένου θέματος προέκυψε από τη πρώιμη επαφή με το αντικείμενο στο πλαίσιο των σπουδών μου. Αυτό ήταν αρκετό για να ξέρω εκ τότε το θέμα που θα ήθελα να ερευνήσω περισσότερο δοθείσης ευκαιρίας.

Τα αποτελέσματα που προκύπτουν από τη μελέτη είναι πλήρως ικανοποιητικά ώστε να μάθει ο αναγνώστης – καταναλωτής πόσοι μηχανισμοί τίθενται σε λειτουργία πίσω από μια απλή περιήγηση και αρκετά ικανά ώστε να δώσουν κατευθυντήριες γραμμές τόσο στους έμπειρους χρήστες και διαχειριστές για την εξασφάλιση μιας ασφαλούς ηλ.

συναλλαγής όσο και στους απλούς περιηγητές για μια ασφαλή αγορά πλοήγηση και οικονομική συναλλαγή.

Η ανάλυση των ερωτηματολογίων ανέδειξε την ιδιαίτερη προτίμηση των νέων και μεσήλικων (η κατηγορία 18-45 ετών εκπροσωπείται στο δείγμα σε ποσοστό 72%) για τις ηλεκτρονικές αγορές (85.8%) έναντι των παραδοσιακών. Οι ερωτώμενοι συνδέονται στο δίκτυο για τουλάχιστον 2ώρες ημερησίως σε ποσοστό 93% ενώ δεν είναι λίγοι αυτοί που ξεπερνούν τις 8ώρες καθημερινής χρήσης (17%). Οι ηλεκτρονικές αγορές ωστόσο φαίνεται να μην αποτελούν βασικό λόγο πρόσβασης στο διαδίκτυο (κύριος λόγος πρόσβασης στο διαδίκτυο για το 2%). Σε ότι αφορά στις προτιμήσεις πλατφόρμων ηλεκτρονικών αγορών η τάση είναι να επιλέγουν ελληνικά καταστήματα, χωρίς όμως να αποκλείουν και καταστήματα του εξωτερικού (45.3% μόνο ελληνικές πλατφόρμες, 45.5% ελληνικές και ξένες πλατφόρμες). Η δυσπιστία των αγοραστών είναι έκδηλη εφόσον η πλειοψηφία (65%) θεωρεί πως τα ηλεκτρονικά καταστήματα δεν είναι ειλικρινή και ένα σημαντικό ποσοστό (35%) πιστεύει πως οι ηλεκτρονικές αγορές ενέχουν σε μεγάλο βαθμό κίνδυνο εξαπάτησης. Παρόλο που οι χρήστες φαίνεται να αμφιταλαντεύονται μεταξύ φήμης και τιμής για την επιλογή πλατφόρμας αγορών, οι επιλογές τους δείχνουν την προσπάθειά τους να προστατευτούν από τις πιθανές απάτες μέσω της προτίμηση ιστοτόπων αγοράς που παρέχουν επικοινωνία με τον πωλητή (π.χ. φυσικό κατάστημα, τηλεφωνική εξυπηρέτηση) και της επιλογής μεθόδου πληρωμής. Πιο συγκεκριμένα, η ύπαρξη φυσικού καταστήματος, η φήμη, η προστασία προσωπικών δεδομένων και η τηλεφωνική εξυπηρέτηση αποτελούν παράγοντες που επηρεάζουν την επιλογή ηλεκτρονικών καταστημάτων. Σχετικά με την πληρωμή, το 41% προτιμά τη μέθοδο της αντικαταβολής ενώ το υπόλοιπο 37% καλύπτει την ανάγκη του για προστασία από ενδεχόμενη οικονομική απάτη με την πληρωμή μέσω paypal ή χρεωστικής/προπληρωμένης κάρτας. Τέλος, οι πελάτες δηλώνουν πως οι δυσκολίες στη συναλλαγή μπορούν να οδηγήσουν στην απόρριψη μία πλατφόρμας ηλεκτρονικών αγορών στο μέλλον.

Από το κομμάτι της συνέντευξης τα αποτελέσματα που προέκυψαν μέσα από την έμπειρη ματιά του κου Βαβίλη μας οδηγούν κυριολεκτικά από την θεωρία στην πράξη καθώς στις περισσότερες απαντήσεις τονίζεται τόσο η σημαντικότητα της ενεργής ύπαρξης των πρωτόκολλων ασφαλείας σε μία ηλεκτρονική ενέργεια όσο και το συνεχές update των συστημάτων μέσα από τα οποία πραγματοποιούνται οι εκάστοτε συνδέσεις προκειμένου η ‘’δουλειά’’ των πρωτόκολλων ασφαλείας να διεξάγεται με επιτυχία.

Μας διαφώτισε για τους τύπους των SSL καθώς και για τα ιδιαίτερα χαρακτηριστικά του καθενός και για το πώς ακόμα εμείς οι απλοί περιηγητές μπορούμε να καταλάβουμε ποιο χρησιμοποιείται κάθε φορά και κατά πόσο ασφαλής είναι η σύνδεση

στην οποία βρισκόμαστε. Προς το τέλος μας έδωσε TIPS για την αποφυγή ηλεκτρονικών απατών μέσω e-mail καθώς και για την αποφυγή έκθεσης των προσωπικών μας στοιχείων από χακαρισμένα site πάλι μέσω της απάτης με τη μέθοδο των πλαστών mail. Η συνέντευξη έκλεισε με μια αναφορά από τη σκοπιά του System Administrator στο πραγματικό πρόβλημα των βάσεων δεδομένων που δεν είναι άλλο από τα SQL injections και διευκρινίστηκε ότι πιο σαφή απάντηση παρόλα αυτά θα μπορούσε να μας δοθεί από την ειδικότητα του Developer.

Πολλάκις στη μελέτη έχουμε αναφερθεί στους κινδύνους και στα κενά ασφαλείας όπου αυτοί χτυπάνε και έτσι θα ήταν καλό βασιζόμενοι στην αποκτηθείσα γνώση σχετικά με τα τρωτά αυτά σημεία, να διεξαχθεί περεταίρω έρευνα για τις πιθανότητες της εξ ολοκλήρου αντιμετώπισης τους. Η δημιουργία της αίσθησης αλλά και της βεβαιότητας για την ασφάλεια πίσω από μία ηλεκτρονική συναλλαγή συνιστά έναν από τους σημαντικότερους παράγοντες για την βιωσιμότητα των ηλεκτρονικών επιχειρήσεων.

Ακόμη για την επίτευξη της μέγιστης ασφάλειας θα μπορούσε να αναπτυχθεί μια εφαρμογή η οποία να σαρώνει κάθε σελίδα που καταλήγει σε ηλεκτρονική συναλλαγή πριν ο πελάτης προχωρήσει σε αυτή. Τα αποτελέσματα της σάρωσης θα μπορούσαν να δείχνουν σε ποσοστό κατά πόσο ασφαλής είναι η μετάβαση στην πληρωμή καθώς επίσης και τα διάφορα τεχνικά στοιχεία (SSLενημερώσεις κτλ.) που τρέχουν στο background αυτής.

Επιπροσθέτως ενδείκνυται η υλοποίηση νέων ερευνών για την αντίληψη που έχουν οι καταναλωτές απέναντι στην ηλεκτρονική αγορά καθώς επίσης και σε κάτι αντίστοιχο που να αφορά στην προστασία των καταναλωτών, τόσο σε επίπεδο προσωπικών δεδομένων, όσο και σε επίπεδο προστασίας από ηλεκτρονικές οικονομικές απάτες.

Κλείνοντας επί 6 συναπτά έτη κάθε Μάρτιο έχουμε τον θεσμό της Εβδομάδας Ηλεκτρονικού Εμπορίου στα πλαίσια της οποίας κάθε ηλεκτρονική επιχείρηση διαθέτει τα προϊόντα της σε πολύ ελκυστικές τιμές. Πέρα από αυτό, που δεν λέω, είναι ένα πολύ γερό κίνητρο για τον καταναλωτή να ξεφύγει από την παραδοσιακή μέθοδο και να στραφεί στην διαδικτυακή θα ήταν χρήσιμο να πραγματοποιούνταν ημερίδες προσαρμοσμένες στα νέα δεδομένα που προκύπτουν κάθε χρόνο έτσι ώστε κάθε ενδιαφερόμενος να ξέρει με τι έχει να κάνει καθώς επίσης αυτό θα ήταν ιδιαίτερα καλή γνώση για τους μαθητές στα σχολεία.

ΒΙΒΛΙΟΓΡΑΦΊΑ

1Ο ΚΕΦΑΛΑΙΟ

📖 Bachetta, M et al, 1998. *Electronic Commerce and the role of the WTO*. World Trade Organization (WTO) : Geneva

📖 Porter, M., 1985. *Technology and Competitive Advantage*,.*Journal of Business Strategy*, Vol. 33, σελ. 23-31

📖 Turban, E, King, D& Lee, Kyu Jae, 2006. *Electronic Commerce: A managerial perspective.* Prentice Hall : Upper Saddle River, NJ

📖 Παρασχόπουλος, Α. & Σκαλτσάς, Π., 2000. *Ηλεκτρονικό εμπόριο – Ανάπτυξη και εφαρμογή επιχειρηματικής στρατηγικής στο διαδίκτυο*. Κλειδάριθμος : Αθήνα

📖 Πασχοπούλου, Α. & Σκαλτσάς, Π.2001. *Ηλεκτρονικό εμπόριο.* Κλειδάριθμος : Αθήνα

📖 Πομπορτσής, Α. &Τσούλφας, Α.2002. *Εισαγωγή στο Ηλεκτρονικό Εμπόριο.* Τζιόλα : Αθήνα

📖 Σκαλίδης, Λ., 2000. Δίκαιο εμπορικών εταιριών. Ius : Θεσσαλονίκη

Εθνική επιτροπή τηλεπικοινωνιών και ταχυδρομείων
https://www.eett.gr/opencms/opencms/EETT/
Ημερομηνία τελευταίας πρόσβασης : 24/09/2018

Εμπορικό βιομηχανικό επιμελητήριο Αθηνών
http://www.acci.gr/acci/articles/article.jsp?context=103&categoryid=433&articleid=775
Ημερομηνία τελευταία πρόσβασης : 24/09/2018

Επαγγελματικό επιμελητήριο Αθηνών http://www.eea.gr/gr/el/articles/ypoxreotiki-i-eggrafi-se-eea-kai-gemi-gia-ilektroniko-emporio Ημερομηνία τελευταίας πρόσβασης : 24/09/2018

Ναυτεμπορική https://www.naftemporiki.gr/story/810401/ti-allazei-stous-kanones-gia-to-ilektroniko-emporio Ημερομηνία τελευταίας πρόσβασης : 29/09/2018

2Ο ΚΕΦΑΛΑΙΟ

📖 Simon, Alan R. & Shaffer, Steven L.2001. *Data Warehousing and Business Intelligence for E-commerce.* Morgan Kaufmann : San Fransisco

Arline, K., 2015. What is C2B?.*Business news daily* [Διαδίκτυο], Ιανουάριος. Διαθέσιμο στο : http://www.businessnewsdaily.com/5001-what-is-c2b.html Ημερομηνία τελευταίας πρόσβασης : 25/10/2018

Siingh, A. 2018. What are the best examples of G2B E-commerce? *Quora* [Διαδίκτυο], 13 Αυγούστου, Διαθέσιμο στο : https://www.quora.com/What-are-the-best-examples-of-G2B-E-commerce Ημερομηνία τελευταίας πρόσβασης : 06/11/2018

- Business to Business-B2B https://www.investopedia.com/terms/b/btob.asp

Ημερομηνία τελευταίας πρόσβασης : 20/09/2018

- Business to Consumer-B2C https://www.investopedia.com/terms/b/btoc.asp

Ημερομηνία τελευταίας πρόσβασης: 20/09/2018

- Business To Government-B2G https://www.investopedia.com/terms/b/business-to-government.asp Ημερομηνία τελευταίας πρόσβασης : 10/10/2018
- Consumer To Consumer-C2C https://www.investopedia.com/terms/c/ctoc.asp

Ημερομηνία τελευταίας πρόσβασης: 16/10/2018

- United Nations https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework#whatis Ημερομηνία τελευταίας πρόσβασης : 16/10/2018

ΚΕΦΑΛΑΙΟ 3^{Ο}

- Turban, E., Whiteside, J., King, D., Outland, J., 2017. *Introduction to Electronic Commerce and Social Commerce.* Pg. 42. Springer : New York
- Βασιλικοπούλου, Α. & Σιώμκος, Γ.2005. *Εφαρμογή Μεθόδων Ανάλυσης στην Έρευνα Αγοράς.* Σταμούλης : Αθήνα
- Βλαχοπούλου, Μ.1999*. E-Marketing*. Rosili : Αθήνα
- Δεληγιάννης, Γ., 2006. *Η κοινωνία της πληροφορίας και ο ρόλος των διαδραστικών πολυμέσων.* Fagotto : Αθήνα
- Καρανικόλας, Ν., 2006. *Τεχνολογίες Διαδικτύου και Ηλεκτρονικό Εμπόριο*. Νέων Τεχνολογιών : Αθήνα
- Παλαιτσάκης, Γ.2018e-τιμολόγια υποχρεωτικά από 1ης-1-2020. *Ναυτεμπορική* [Διαδίκτυο], 18 Οκτωβρίου 2018, Διαθέσιμο στο: https://www.naftemporiki.gr/finance/story/1403594/e-timologia-upoxreotika-apo-1is-1-2020 Ημερομηνία Τελευταίας πρόσβασης : 13/03/2019
- Eurobank, 2009. Υπηρεσίες Ε – auctions. Διαθέσιμο στο : https://www.eurobank.gr/el/business/ilekronikes-upiresies/ilektronikes-upiresies/special-b2b-services/b2b-services/e-auctions

Ημερομηνία Τελευταίας πρόσβασης : 27/02/2019

- Eurobank, 2009. Υπηρεσία Ε – Procurement.

Διαθέσιμο στο : https://www.eurobank.gr/el/business/ilekronikes-upiresies/ilektronikes-upiresies/special-b2b-services/b2b-services/e-procurements

Ημερομηνία τελευταίας πρόσβασης : 27/02/2019

- M – Commerce https://www.investopedia.com/terms/m/mobile-commerce.asp

Ημερομηνία Τελευταίας Πρόσβασης : 05/03/2019

Tozzi, J., 2008. Determining Where to Sell Online. *Bloomberg* [Διαδίκτυο], 7 Νοεμβρίου 2008. Διαθέσιμο στο : https://www.bloomberg.com/news/articles/2008-11-07/determining-where-to-sell-onlinebusinessweek-business-news-stock-market-and-financial-advice Ημερομηνία τελευταίας πρόσβασης : 17/10/2018

ΚΕΦΑΛΑΙΟ 4Ο

Clarck, J., 2009. *SQL Injection Attacks and Defense.* Elsevier Science : UK

Turban, E., Lee J., King, D. & Chung, M., 2000. *Electronic Commerce: A Managerial Perspective.*Σελ. 291. Prentice Hall : Upper Saddle River, NJ

Turban, E., Lee J., King, D. & Chung, M.,2002. *Ηλεκτρονικό εμπόριο: Αρχές, Εξελίξεις, Στρατηγική από τη σκοπιά του manager*, σελ. 277. Μ. Γκιούρδας : Αθήνα

Πομπορτσής, Α. & Τσούλφας, Α., 2002. *Εισαγωγή στο Ηλεκτρονικό Εμπόριο.* Τζιόλα : Αθήνα

Canter, S., 1998. Making e-mailsecure. *Pc Magazine,* 17 (15), σελ. 263

Amit, Y., 2005. Google.comUTF-7 XSS Vulnerabilities. *Securiteam* [Διαδίκτυο], 21 Δεκεμβρίου 2006, Διαθέσιμο στο :
http://www.securiteam.com/securitynews/6Z00L0AEUE.html
Ημερομηνία τελευταίας πρόσβασης: 24/09/2018

Goodin, D., 2009. SSL spoof bug still haunts IE, Safari, Chrome. *The Register* [Διαδίκτυο], 1 Οκτωβριου 2009,
Διαθέσιμο στο : https://www.theregister.co.uk/2009/10/01/microsoft_crypto_ssl_bug/
Ημερομηνία τελευταίας πρόσβασης: 27/10/2018

Grossman, J., 2006. The origins of Cross-Site Scripting (XSS). *Jeremiah Grossman* [Διαδίκτυο], 30 Ιουλίου 2006, Διαθέσιμο στο :
https://blog.jeremiahgrossman.com/2006/07/origins-of-cross-site-scripting-xss.html
Ημερομηνία τελευταίας πρόσβασης: 27/10/2018

Hjelmvik, E., 2011. Network Forensic Analysis of SSL MITM Attacks. *Net Resec* [Διαδίκτυο], 27 Μαρτίου 2011, Διαθέσιμο στο :
https://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis- of-SSL-MITM-Attacks Ημερομηνία τελευταίας πρόσβασης : 24/10/2018

Ingham, K., Forrest, S., 2002. A History and Survey of Network Firewalls.
http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf
Ημερομηνία τελευταίας πρόσβασης: 30/10/2018

Sheldon, T., 2001. S-HTTP (Secure Hypertext Transfer Protocol). *Tom Sheldon's Linktionary* [Διαδίκτυο], Διαθέσιμο στο : http://www.linktionary.com/s/shttp.html
Ημερομηνία τελευταίας πρόσβασης: 17/10/2018

- Spring, T., 2003. Spam Slayer: Do You Speak Spam? . *PC World* [Διαδίκτυο], 17 Νοεμβρίου 2003, Διαθέσιμο στο : https://www.pcworld.com/article/113431/article.html Ημερομηνία τελευταίας πρόσβασης: 25/10/2018
- PC stripper helps spam to spread, *BBC News* [Διαδίκτυο], 30 Οκτωβρίου 2007, Διαθέσιμο στο : http://news.bbc.co.uk/2/hi/technology/7067962.stm Ημερομηνία τελευταίας πρόσβασης: 25/10/2018
- HSBC https://www.hsbc.gr/1/PA_esf-ca-app-content/content/greece/personal/common/pdf/HSBC_FAQ_TAX_FREE.pdf. Σελ.6 Ημερομηνία τελευταίας πρόσβασης: 01/10/2018
- McAfee Press, *McAfee discovers first Linux virus,* Διαθέσιμο στο : http://math-www.uni-paderborn.de/~axel/bliss/mcafee_press.html Ημερομηνία τελευταίας πρόσβασης: 20/09/2018
- Metropolitan Police ServiceInternet Banking Targeted Phishing Attack, [Διαδίκτυο], 3 Ιουνίου 2005, Διαθέσιμο στο : http://www.webcitation.org/5ndG8erWg Ημερομηνία τελευταίας πρόσβασης : 23/09/2018
- Papaki.com www.papaki.com/el/ssl.htm?gclid Ημερομηνία τελευταίας πρόσβασης : 07/11/2018
- Secure Electronic Transaction (SET) https://www.investopedia.com/terms/s/secure-electronic-transaction-set.asp Ημερομηνία τελευταίας πρόσβασης: 20/09/2018
- Symantec Security Corporation, *Summary W32.Gammima. AG,* Διαθέσιμο στο : http://www.symantec.com/security_response/writeup.jsp?docid=2007-082706-1742-99 Ημερομηνία τελευταίας πρόσβασης : 20/09/2018
- I. S. O. https://www.iso.org/standard/39612.html Ημερομηνία τελευταίας πρόσβασης: 20/09/2018
- IRC Security (Internet relay Chat) http://www.irchelp.org/security/trojan.html Ημερομηνία τελευταίας πρόσβασης : 29/09/2018
- Αρχή Πιστοποίησης Ελληνικού Δημοσίου http://www.aped.gov.gr/procedures.html Ημερομηνία τελευταίας πρόσβασης: 19/10/2018
- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα http://www.dpa.gr/portal/page?_pageid=33,146950&_dad=portal&_schema=PORTAL Ημερομηνία τελευταίας πρόσβασης: 26/10/2018
- Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html Ημερομηνία τελευταίας πρόσβασης: 25/09/2018
- Ευρετήριο Οικονομικών όρων https://www.euretirio.com/pistotiki-karta-credit-card/ Ημερομηνία τελευταίας πρόσβασης: 01/10/2018