ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Πρόγραμμα Μεταπτυχιακών Σπουδών στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με Διεθνή Προσανατολισμό

"Ασφάλεια και Διαχείριση Ηλεκτρονικών Συναλλαγών - Προβλέψεις"

Διπλωματική Εργασία

Φοιτήτρια: **Κούτση Φιορεντίνα**

Α.Μ.: ***ΜΔΕ-ΟΠ 1411***

E-mail: fiorentina.koutsi@gmail.com

Επιβλέπων Καθηγητής: κος Μ. Σφακιανάκης

Πειραιάς, 2016

Περίληψη

Η αλματώδης αύξηση της χρήσης των ηλεκτρονικών υπολογιστών, καθώς και η έκρηξη του Mobile Internet, προσφέρουν πλέον απεριόριστες δυνατότητες σε όλους τους τομείς της σύγχρονης οικονομικής και κοινωνικής ζωής. Η χρήση προηγμένων λειτουργικών συστημάτων επιτρέπει στους χρήστες να είναι συνδεδεμένοι συνεχώς στο Διαδίκτυο επηρεάζοντας με αυτόν τον τρόπο το βαθμό χρήσης των ηλεκτρονικών συναλλαγών.

Η νέα πραγματικότητα πλέον βασίζεται στις οικονομικές δομές του διαδικτύου καθώς και σε οργανώσεις και άτομα που απολαμβάνουν την ευκολία αγοράς εμπορευμάτων και υπηρεσιών πέραν από τα σύνορα. Οι πραγματοποιούμενες συναλλαγές όμως φέρουν πληροφορίες που σε αρκετές περιπτώσεις είναι πιο σημαντικές απ' ότι το ίδιο το χρήμα, καθώς και η τάση εκμετάλλευσης της δυνατότητας πρόσβασης στις πληροφορίες αυτές αλλά και στα χρήματα που κινούνται στο διαδίκτυο, «σπάζοντας» τον κώδικα, είναι υπαρκτή.

Η παρούσα διπλωματική πραγματεύεται τις ηλεκτρονικές απάτες που έχουν γίνει στην Ελλάδα χρησιμοποιώντας δεδομένα από την Ηλεκτρονική Δίωξη Εγκλήματος και μελετά τις τάσεις αυτών μέσω της πρόβλεψης των αναμενόμενων ηλεκτρονικών εγκλημάτων για το διάστημα Μάρτιο με Ιούλιο του έτους 2016.

Οι ηλεκτρονικές απάτες τελούνται πλέον αντί της χρήσης όπλων. Η σημαντικότητα αυτού του θέματος, δηλαδή η απασχόληση της χώρας με τα ηλεκτρονικά εγκλήματα, μπορεί να υποδηλώσει το κατά πόσο ο συνδυασμός τεχνικών μέσων μαζί με την εξειδίκευση του ανθρώπινου παράγοντα είναι στο επιθυμητό επίπεδο στην Ελλάδα.

Τα αποτελέσματα υποδεικνύουν σημαντική μείωση στις καταγγελίες που σχετίζονται με ηλεκτρονικές απάτες. Όμως, η ηλεκτρονική εγκληματικότητα εμπλουτίζεται μέρα με τη μέρα και η πιθανότητα εμφάνισης νέων μορφών στο μέλλον επιβάλλει την πραγματοποίηση επενδύσεων από τους αντίστοιχους φορείς στο θέμα αυτό.

ABSTRACT

The rapid increase in the use of computers and the explosion of Mobile Internet offers unlimited possibilities in all the areas of modern economic and social life. Advanced operating systems allow users to be constantly connected to the Internet, thus having impact on the use of electronic transactions.

Nowadays, the new reality is based on the financial web structures, and organizations and individuals who enjoy the convenience of buying and offering goods and services across the borders. Electronic transactions carry out information that in many cases are more important than money itself and the tendency to exploit the accessibility to such information, and money as well, by just "breaking" codes, is our current reality.

This thesis deals with the online scams that have been transpired in Greece by using data from the Electronic Crime Prosecution and studying these trends by the expected electronic crimes for the period of March to July, 2016.

In general, online fraud is committed instead of the use of arms. The importance of this issue, how the country deals with electronic crimes, can indicate whether the combination of technical resources with the expertise of the human factor is at the desired level in Greece.

Results indicate a significant decrease in the incidents related to online scams. But the electronic criminality is advancing day by day and the possibility of new kind of crimes in the future requires investment by the respective institutions.

Ευχαριστίες

Η επιτυχημένη ολοκλήρωση της εν λόγω διπλωματικής εργασίας που εκπονήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με Διεθνή Προσανατολισμό δε θα ήταν δυνατή χωρίς την ουσιαστική αρωγή ορισμένων προσώπων, τα οποία κι επιθυμώ να ευχαριστήσω.

Πρωτίστως, θα επιθυμούσα να ευχαριστήσω τον επιβλέποντα καθηγητή και εισηγητή του θέματος, κύριο Μιχάλη Σφακιανάκη, Πρόεδρο του Τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων του Πανεπιστημίου Πειραιώς. Θέλω να εκφράσω τη βαθιά ευγνωμοσύνη μου στο πρόσωπό του αφού με εμπιστεύτηκε και μου έδωσε ουσιαστική βοήθεια κατά την εκπόνηση της εργασίας.

Ιδιαίτερα χρήσιμες ήταν και οι συμβουλές, η καθοδήγηση και η βοήθεια του Διδάκτορα του Τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων του Πανεπιστημίου Πειραιώς, κύριου Ιωάννη Κατσανάκη, τον οποίο ευχαριστώ πολύ.

Επίσης, ευχαριστώ θερμά για την υπομονή του και τη βοήθειά του τον Γιώργο Γέρμανο, Υπαστυνόμο της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, και κυρίως ευχαριστώ τον κ. Μανώλη Σφακιανάκη, Υποστράτηγο και Βοηθό Προϊσταμένου Επιτελείου του Αρχηγείου της Ελληνικής Αστυνομίας, που υποστήριξε την εκπόνηση αυτής της διπλωματικής. Θα ήταν παράλειψή μου να μην τους ευχαριστήσω και για τη φιλοξενία τους κατά τις επισκέψεις μου στο γραφείο τους.

Ευχαριστώ τα μέλη της επιτροπής κύριο Νικόλαο Γεωργόπουλο, Πρύτανη του Πανεπιστημίου Πειραιώς, και τον κύριο Πέτρο Μαραβελάκη, Επίκουρο Καθηγητή του Τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων, για το ενδιαφέρον τους.

Τέλος, επιθυμώ να ευχαριστήσω τους γονείς μου και τον αδερφό μου για την απεριόριστη υπομονή, συμπαράσταση και κατανόηση καθ' όλα αυτά τα χρόνια των σπουδών μου.

Κατάσταση Πινάκων

Κατάσταση Γραφημάτων

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Ο τρόπος διεξαγωγής των συναλλαγών πλέον έχει αλλάξει κι αυτό οφείλεται σε σημαντικό βαθμό στο Ηλεκτρονικό Εμπόριο το οποίο έχει αναπτυχθεί με ταχύτατους ρυθμούς. Το ηλεκτρονικό εμπόριο έχει να κάνει με εμπορικές συναλλαγές που πραγματοποιούνται με ηλεκτρονικά μέσα και βασίζεται ουσιαστικά στην ηλεκτρονική μετάδοση δεδομένων. Αφορά την αγοραπωλησία αγαθών, πληροφοριών κι υπηρεσιών μέσα από δίκτυα ηλεκτρονικών μέσων.

Η παρούσα διπλωματική εργασία διαμορφώθηκε με σκοπό τη μελέτη των παραγόντων που επηρεάζουν την ασφάλεια των ηλεκτρονικών συναλλαγών, όπως και τη διερεύνηση της τάσης του ηλεκτρονικού εγκλήματος στην Ελλάδα στην κατηγορία των ηλεκτρονικών απατών.

Η αλματώδης αύξηση της χρήσης των ηλεκτρονικών υπολογιστών προσφέρει πλέον απεριόριστες δυνατότητες σε όλους τους τομείς της σύγχρονης οικονομικής και κοινωνικής ζωής. Η έκρηξη του Mobile Internet (MI) μαζί με την ανάπτυξη των smartphones που χρησιμοποιούν προηγμένα λειτουργικά συστήματα και επιτρέπουν στους χρήστες να εγκαταστήσουν νέες εφαρμογές, να είναι συνδεδεμένοι συνεχώς στο Διαδίκτυο και να παρέχουν πολυσχιδείς λειτουργίες αποτελούν ένα συνδυασμό που έχει επηρεάσει και το βαθμό χρήσης των ηλεκτρονικών συναλλαγών. Το τελευταίο διάστημα έχει κάνει την εμφάνισή του και «Το Ίντερνετ των Πραγμάτων» (Internet of Things – IoT), το οποίο αποτελεί ένα αναπτυσσόμενο δίκτυο καθημερινών αντικειμένων που μπορεί να μοιράζεται πληροφορίες και να ολοκληρώνει εργασίες. Ωστόσο, όλα τα παραπάνω έχουν οδηγήσει κι αναμένεται εκθετικά να οδηγούν σε ανησυχίες που αφορούν την ασφάλεια.

Η παρούσα πρόταση για την ανάληψη της διπλωματικής εργασίας αναπτύσσεται σε εφτά κεφάλαια. Στο πρώτο κεφάλαιο, αναφέρεται ο σκοπός της εργασίας, καθώς και οι θεωρητικοί και ερευνητικοί στόχοι που έχουν τεθεί. Στο δεύτερο κεφάλαιο γίνεται μια σύντομη θεωρητική ανασκόπηση των εννοιών που πρόκειται να διερευνηθούν, όπως αυτή του ηλεκτρονικού εμπορίου με σκοπό την τεκμηρίωση των θεωρητικών στόχων της εργασίας. Στο τρίτο κεφάλαιο γίνεται αναφορά στις ηλεκτρονικές συναλλαγές, τους μηχανισμούς ηλεκτρονικών πληρωμών και τους τρόπους συναλλαγών στα ηλεκτρονικά καταστήματα. Στο τέταρτο και πέμπτο κεφάλαιο γίνεται ανάλυση της ασφάλειας στο διαδίκτυο και της διαχείρισης ασφάλειας των πληροφοριών. Στο έκτο κεφάλαιο παρουσιάζεται η έννοια του ηλεκτρονικού εγκλήματος και στο τελευταίο κεφάλαιο παρουσιάζεται η τάση του ηλεκτρονικού εγκλήματος στην Ελλάδα σύμφωνα με τη βάση

δεδομένων της Ελληνικής Δίωξης Ηλεκτρονικού Εγκλήματος κι επιλογικά, αναφέρονται τα συμπεράσματα που προέκυψαν από την εργασία.

Κεφάλαιο 1: Σκοποί και στόχοι της ερευνητικής εργασίας

1.1. Σκοπός της εργασίας

Αρχικά, να επισημανθεί ότι το *Ηλεκτρονικό Εμπόριο* ορίζεται ως το σύνολο των ηλεκτρονικών συναλλαγών μεταξύ μιας επιχείρησης και ενός τρίτου με τον οποίο αυτή συναλλάσσεται. Με βάση αυτόν τον ορισμό, οι μη οικονομικές συναλλαγές (π.χ. η ζήτηση περαιτέρω πληροφοριών) θεωρούνται επίσης μέρος του ηλεκτρονικού εμπορίου[1]. Οι κυριότεροι λόγοι διάδοσης του ηλεκτρονικού εμπορίου είναι η παγκοσμιοποίηση, η οικονομική κρίση και ιδίως η εξάπλωση του Διαδικτύου[2].

Η αλματώδης αύξηση της χρήσης των ηλεκτρονικών υπολογιστών προσφέρει πλέον απεριόριστες δυνατότητες σε όλους τους τομείς της σύγχρονης οικονομικής και κοινωνικής ζωής μας πλέον. Πιο συγκεκριμένα, στην Ελλάδα, σύμφωνα με την έρευνα WebID της Focus Bari για το διάστημα Ιανουάριο – Μάρτιο 2015, φαίνεται ότι 7 στους 10 πολίτες χρησιμοποιούν το Διαδίκτυο. Η χρήση είναι ακόμα μεγαλύτερη στις νεαρές ηλικίες (13-17 ετών) με το ποσοστό τους να αγγίζει το 96,9%, ενώ στις ηλικίες 18-24 το αντίστοιχο ποσοστό διαμορφώνεται σε 98,1%[3]. Αυτά τα ποσοστά οφείλονται και στο γεγονός ότι η χρήση διαδικτύου από τα κινητά τηλέφωνα έχει αυξηθεί σημαντικά τα τελευταία χρόνια. Ο αριθμός των συνδρομητών κινητής τηλεφωνίας έχει ξεπεράσει τα 7 δισεκατομμύρια και είναι πολύ κοντά στο να φτάσει το σύνολο του παγκόσμιου πληθυσμού[4].

Η έκρηξη του Mobile Internet (MI) μαζί με την ανάπτυξη των smartphones που χρησιμοποιούν προηγμένα λειτουργικά συστήματα κι επιτρέπουν στους χρήστες να εγκαταστήσουν νέες εφαρμογές, να είναι συνδεδεμένοι συνεχώς στο Διαδίκτυο και να παρέχουν πολυσχιδείς λειτουργίες αποτελούν ένα συνδυασμό που έχει επηρεάσει κιόλας τον βαθμό χρήσης των ηλεκτρονικών συναλλαγών[5]. Επιπλέον, ο αριθμός των έξυπνων τηλεφωνικών συνδέσεων προβλέπεται ότι θα αυξηθεί κατά 136% μέσα στα επόμενα 5 χρόνια και θα φθάσει τα 3,9 δισεκατομμύρια συνδέσεις σε όλο τον κόσμο το 2018[6].

---

[1] Bocij, Chaffey D., Greasley A. and Hichie S., Business Information Systems,Prentice Hall, 2006, 3rd Edition

[2] Μπατσίνης Ν., Δέλιας Π., Τσαφαράκης Σ., Ηλεκτρονικό εμπόριο και εικονικές επιχειρήσεις. Εκδόσεις Πολυτεχνείου Κρήτης «Χανιά», 2006

[3] www.FocusBari.gr

[4] Patricio E. Ramirez-Correa, F. Javier Rondan-Cataluna, Jorge Arenas-Gaitan, Elsevier, 2015

[5] Norazah Mohd, S., Students' demand for smartphones. Campus-Wide Inform. Syst. 30 (4), 236–248, 2013

[6] de Renesse, R., 2014. Research Forecast Report: Smartphone markets: worldwide trends, forecasts and strategies 2014–2018. http://www.analysysmason.com/smartphone-forecasts-2014

Όλη αυτή η έντονη χρήση οφείλεται στις δυνατότητες που προσφέρει πλέον η τεχνολογία. Το τελευταίο διάστημα έχει κάνει την εμφάνισή του και «Το Ίντερνετ των Πραγμάτων» (Internet of Things – IoT) που αποτελεί ένα αναπτυσσόμενο δίκτυο των καθημερινών αντικειμένων που μπορεί να μοιράζεται πληροφορίες και να ολοκληρώνει εργασίες. Αποτελείται από εκατομμύρια αισθητήρες και συσκευές που παράγουν συνεχείς ροές δεδομένων. Σύμφωνα με την Intel, οι πόλεις επρόκειτο να δαπανήσουν $41 τρισεκατομμύρια μέσα στα επόμενα 20 χρόνια στην αναβάθμιση των υποδομών του Internet of Things, ενώ σύμφωνα με την Gartner η συνολική προστιθέμενη αξία από το IoT σε όλους τους κλάδους θα φτάσει τα 1.9 τρισεκατομμύρια δολάρια έως το 2020 παγκοσμίως[7]. Το «Διαδίκτυο των Πραγμάτων» (Internet of Things ή IoT) θεωρείται η επόμενη καταλυτική μετάλλαξη της ψηφιακής επανάστασης. Το ποσοστό των «πραγμάτων» που δεν είναι πλέον απλά μόνο tablets, κινητά ή υπολογιστές αναμένεται να αυξηθεί από χαμηλότερα του 10% το 2010 σε 50% το 2020[8].

Στο βιβλίο «The Zero Marginal Cost Society», ο Τζέρεμι Ρίφκιν γράφει: «Το Διαδίκτυο των Πραγμάτων θα συνδέσει τα πάντα με τους πάντες, σε ένα ενιαίο παγκόσμιο δίκτυο. Άνθρωποι, μηχανές, φυσικοί πόροι, γραμμές παραγωγής, δίκτυα εφοδιασμού, καταναλωτικές συνήθειες, ροές ανακύκλωσης και σχεδόν κάθε άλλη πτυχή της οικονομικής και κοινωνικής ζωής θα διασυνδεθούν μέσω αισθητήρων και λογισμικού στην πλατφόρμα του IoT, και θα παρέχουν Μεγάλα Δεδομένα σε κάθε κόμβο -επιχειρήσεις, σπίτια, οχήματα- λεπτό προς λεπτό, σε πραγματικό χρόνο.»

Ωστόσο, όλα τα παραπάνω έχουν οδηγήσει, κι αναμένεται εκθετικά να οδηγούν, σε ανησυχίες που αφορούν την ασφάλεια. Τελικά, η επιλογή θα γίνεται μεταξύ των επί πληρωμή υπηρεσιών που θα την εγγυώνται οι επιχειρήσεις, και των δωρεάν υπηρεσιών τις οποίες όμως θα πληρώνουν οι καταναλωτές με τα προσωπικά τους δεδομένα.

Η ασφάλεια των αγορών μέσω διαδικτύου είναι ένας από τους παράγοντες που δρουν ανασταλτικά προς τους καταναλωτές για την πραγματοποίηση αγορών. Υπάρχουν περιπτώσεις όπου η έλλειψη προστασίας των προσωπικών δεδομένων του αγοραστή και η ασφάλεια των συναλλαγών αποτελεί ανασταλτικό παράγοντα. Επιπλέον, ένα κλίμα δυσπιστίας δημιουργείται κι από την ύπαρξη ιών στους υπολογιστές. Οι ιοί προκαλούν περιττές καθυστερήσεις, καταστρέφουν αρχεία, δημιουργούν προβλήματα αποθήκευσης, καθώς και άλλες παρόμοιες δυσκολίες. Περισσότερο άγχος προστίθεται κι από τον κίνδυνο πρόσβασης των χάκερς σε αρχεία και λογαριασμούς τόσο στις επιχειρήσεις όσο και στους

[7] http://www.sas.com/el_gr/insights/big-data/internet-of-things.html
[8] www.sepe.gr

καταναλωτές. Ο καταναλωτής που ψωνίζει διαδικτυακά θα πρέπει να αναζητά όλες τις πληροφορίες που αφορούν στη συναλλαγή του. Από την άλλη, ο προμηθευτής είναι υποχρεωμένος να αναφέρει στην ιστοσελίδα όλα τα απαραίτητα στοιχεία του, όπως την ταυτότητα, την κύρια δραστηριότητά του, τη γεωγραφική διεύθυνση στην οποία δραστηριοποιείται, το εμπορικό μητρώο στο οποίο είναι εγγεγραμμένος, αν είναι καταχωρημένος σε μητρώο, τον αριθμό καταχώρησής του καθώς και τα στοιχεία της αρμόδιας εποπτεύουσας αρχής. Τέλος, είναι απαραίτητο να μπορεί να επιβεβαιωθεί η ταυτότητα του αποστολέα ενός μηνύματος, ώστε ο αποδέκτης να είναι σίγουρος πως το μήνυμα προέρχεται πράγματι από το πρόσωπο που φέρεται να το υπογράφει και δεν έχει παραποιηθεί ή πλαστογραφηθεί από κάποιον άλλον τρίτο.

1.2. Πτυχές Ηλεκτρονικού Εμπορίου

Οι Kalakota και Whinston αναφέρουν τέσσερις διαφορετικές πτυχές του ηλεκτρονικού εμπορίου: α) την *επικοινωνιακή* πτυχή, δηλαδή την παροχή πληροφοριών, προϊόντων/υπηρεσιών ή πληρωμών με ηλεκτρονικά μέσα, β) την πτυχή της *επιχειρησιακής διαδικασίας*, δηλαδή την εφαρμογή της τεχνολογίας για τον αυτοματισμό των εμπορικών συναλλαγών και των ροών εργασίας, γ) την πτυχή της *παροχής υπηρεσιών*, που επιτρέπει τη μείωση του κόστους με παράλληλη αύξηση της ποιότητας και της ταχύτητας των παρεχόμενων υπηρεσιών και δ) τη *δικτυακή πτυχή,* δηλαδή την αγορά και την πώληση προϊόντων και πληροφοριών μέσω Διαδικτύου[9].

Όσον αφορά στο «Διαδίκτυο των Πραγμάτων», για τα ελληνικά δεδομένα αυτός ο όρος είναι αρκετά καινούριος και οι αναφορές είναι αρκετά λίγες, επομένως στο ερευνητικό κομμάτι δε θα υπάρξει κάποια πρόβλεψη μιας και δεν απασχολεί ακόμα την Ελλάδα. Όμως, έχει αρχίσει να κάνει ήδη την εμφάνισή του και πρέπει να επιστήσουμε την προσοχή μας και προς τα εκεί. Σε συνέδριο που πραγματοποίησε η SAP τον Ιούνιο του 2015 ο Β. Νικολόπουλος (PhD, CEO και co-founder της Intelen) μίλησε για τη *μελλοντολογία* κι αναφέρθηκε στη Θεωρία της 5ης Διάστασης (πρόσφατο άρθρο του) που έχει να κάνει με την ανθρώπινη φυσιολογία που θα αλληλεπιδρά με το κοινωνικό κυβερνοχώρο σε πραγματικό χρόνο[10]. Συνεπώς, η λήψη μέτρων για περαιτέρω ασφάλεια καθίσταται αναγκαία.

[9] Kalakota Ravi-Whinston B. Andrew, “Electronic Commerce: A Manager’s Guide”, Addison-Wesley 1997

[10] http://www.vnikolopoulos.com/?p=194

1.3. Ερευνητικοί στόχοι

Οι ερευνητικοί στόχοι της εργασίας περιλαμβάνουν τη μελέτη των παραγόντων που επηρεάζουν την ασφάλεια των ηλεκτρονικών συναλλαγών, αλλά και τη διερεύνηση της πρόβλεψης των μελλοντικών τιμών του ηλεκτρονικού εγκλήματος στην Ελλάδα. Μέσω της χρήσης του στατιστικού πακέτου Statgraphics θα εξεταστούν και θα πραγματοποιηθούν οι σχετικές προβλέψεις και τα δεδομένα για τις χρονοσειρές οι οποίες θα ληφθούν από τη βάση δεδομένων της Ελληνικής Δίωξης Ηλεκτρονικού Εγκλήματος. Απώτερος στόχος είναι η εφαρμογή τεχνικών προβλέψεων και να διερευνηθεί αν υπάρχει κάποιου είδους εποχικότητα στην Ελλάδα που μπορεί μελλοντικά να προϊδεάζει για λήψη κατάλληλων προληπτικών μέτρων.

Κεφάλαιο 2: Ηλεκτρονικό Εμπόριο

2.1. Το Διαδίκτυο - Ιστορική Αναδρομή

Η τεχνολογική πρόοδος ξεκίνησε να προκύπτει από τον 20ο αιώνα καθώς και την πρώτη δεκαετία του 21ου αιώνα σηματοδοτώντας σημαντικά κοινωνικοοικονομικά αποτελέσματα. Η ανάπτυξη των ηλεκτρονικών υπολογιστών, του διαδικτύου καθώς και η παγκοσμιοποίηση της αγοράς έχουν επιφέρει ουσιαστικές αλλαγές στην εποχή αυτή[11].

Ερευνητές του Υπουργείου Άμυνας των Η.Π.Α. στα τέλη της δεκαετίας το ΄60, πειραματιζόμενοι με τη διασύνδεση απομακρυσμένων υπολογιστών, δημιούργησαν το ARPA-net με στόχο την παροχή ενός καναλιού επικοινωνίας ανάμεσα στους οργανισμούς που δραστηριοποιούνταν σε θέματα άμυνας. Για αυτόν τον σκοπό, απαραίτητη ήταν η ύπαρξη ενός πρότυπου και πιο εξεζητημένου πρωτοκόλλου, δηλαδή της τεχνολογίας IP (Internet Protocol), η οποία καθόριζε τη διαχείριση και την αποστολή ηλεκτρονικών μηνυμάτων μέσω του δικτύου. Το 1977 εφευρέθηκε ένα νέο πρωτόκολλο, το TCP/IP (Transmission Control Protocol/Internet Protocol). Αυτό έδινε τη δυνατότητα στους χρήστες να συνδέονται μέσα από διάφορα σύνθετα δίκτυα[12] στο ARPA-net. Σταδιακά το δίκτυο απέκτησε πρόσβαση και σε άλλα ακαδημαϊκά ιδρύματα κι άρχισε να αναπτύσσεται και να εξελίσσεται σε ένα δίκτυο που υποστηριζόταν από τους κόμβους, δηλαδή από μεγάλους σταθμούς υπολογιστών, το οποίο στη συνέχεια εξελίχθηκε στο γνωστό διαδίκτυο - Internet.

Συνοπτικά, το διαδίκτυο είναι μία τεχνολογική πλατφόρμα στην οποία εντάσσονται ασύρματα και ενσύρματα μέσα σύνδεσης και ηλεκτρονικοί υπολογιστές που επικοινωνούν με τη βοήθεια εφαρμογών λογισμικού. Το μέγεθος του συνεχώς μεταβάλλεται μιας και κάθε στιγμή κάποιος μπορεί να συνδέεται ή να αποσυνδέεται στο διαδίκτυο από οποιοδήποτε μέσο έχει. Οι πρώτες εμπορικές διαδικτυακές συναλλαγές πραγματοποιήθηκαν στα τέλη της δεκαετίας του 1980. Με το πέρασμα των χρόνων, ο αριθμός των υπολογιστών αυξήθηκε εκθετικά, αποτελώντας ερέθισμα για την εμφάνιση κι αξιοποίηση των ηλεκτρονικών συναλλαγών. Αναπτύχθηκαν τα προγράμματα περιήγησης στο διαδίκτυο (web browsers) και ταυτόχρονα πολλές επιχειρήσεις έψαχναν τρόπους εκμετάλλευσης αυτού του μέσου μετατρέποντάς το σε ένα σημαντικό εργαλείο για τα φυσικά και τα νομικά πρόσωπα[13].

---

[11] Focus Bari, ELTRUN-Ηλεκτρονικό Εμπόριο B2C στην Ελλάδα, Ιούνιος 2009, http://www.focus.gr/default.asp?id=200050049&lcid=1032

[12] http://wdvl.com/internet/history

[13] Hossein, Electronic commerce: principles and practice, Academic Press, 2002

Νέοι όροι όπως το ηλεκτρονικό ταχυδρομείο (e-mail) (δεκαετία 1990), η ηλεκτρονική τραπεζική (e-banking), το ηλεκτρονικό εμπόριο (e-commerce), η ηλεκτρονική ανταλλαγή δεδομένων (EDI), έκαναν την εμφάνισή τους παρέχοντας μία σειρά από νέες δυνατότητες, όπως η επικοινωνία τόσο για τους χρήστες όσο και για τις επιχειρήσεις. Το διαδίκτυο και ο παγκόσμιος ιστός έχουν φέρει επανάσταση στις εμπορικές συναλλαγές σε όλον τον κόσμο.

Στα μέσα της δεκαετίας του 1990, η εμφάνιση του Παγκόσμιου Ιστού (WWW) στο Internet και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών (PC) που χρησιμοποιούν λειτουργικά συστήματα τύπου Windows προσφέρουν μεγάλη ευκολία χρήσης λύνοντας το πρόβλημα της δημοσίευσης και της εύρεσης πληροφοριών στο διαδίκτυο. Το ηλεκτρονικό εμπόριο γίνεται ένας πολύ φτηνότερος τρόπος για την πραγματοποίηση μεγάλου όγκου συναλλαγών, ενώ συγχρόνως διευκολύνει την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών δραστηριοτήτων επιτρέποντας σε μικρές επιχειρήσεις να ανταγωνιστούν μεγαλύτερες, με πολύ ευνοϊκότερες προϋποθέσεις[14].

Στα τέλη της δεκαετίας του 1990, η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και εξακρίβωσης της ταυτότητας του αποστολέα ηλεκτρονικών μηνυμάτων, καθώς και η σχετική προσαρμογή της νομοθεσίας στους τομείς των εισαγωγών-εξαγωγών και των επικοινωνιών, καθιστούν δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών[15].

Οι τεχνολογίες του EDI συντέλεσαν 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[16]. Η κορύφωσή 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 τη 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 (Business to Consumer), C2C (Consumer to Consumer), B2G (Business to Government), B2B (Business to Business) και το ηλεκτρονικό εμπόριο επεκτείνεται σε νέους τομείς. Έτσι, οι επιχειρήσεις μπορούν κι απευθύνονται σε ένα ευρύτατο αγοραστικό κοινό το οποίο μπορεί να βρίσκεται σε οποιοδήποτε σημείο του

[14] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., (1998), σελ. 18 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών

[15] A. Zorayda, E-commerce and e-Business, e-ASEAN Task Force and the UNDP Asia Pacific Development Information Programme (UNDP-APDIP), 2003.

[16] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., (1998), σελ. 18 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών

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. Νέες μορφές ηλεκτρονικού εμπορίου δημιουργούνται χάρη στην εξέλιξη της τεχνολογίας, όπως είναι το κινητό εμπόριο (m-commerce) και το «πανταχού παρόν» ηλεκτρονικό εμπόριο.

2.2. Ορισμός ηλεκτρονικού εμπορίου

Η τεχνολογία του διαδικτύου δημιουργεί τεράστιες ευκαιρίες επέκτασης των υπαρχουσών επιχειρήσεων και σχηματίζει αυτό που ονομάζεται Νέα Οικονομία, Παγκόσμια Οικονομία ή Ηλεκτρονικό Εμπόριο (E-Commerce). Το Ηλεκτρονικό Εμπόριο[17] περιγράφει τις επιχειρηματικές συναλλαγές, τις υπηρεσίες εξυπηρέτησης πελατών, τις παραγγελίες, την παράδοση και πληρωμή, καθώς και τις ενδο-επιχειρηματικές εργασίες που κάνουν χρήση του δημόσιου διαδικτύου και του ψηφιακού δικτυωμένου υπολογιστικού περιβάλλοντος που συνδέει τις οργανώσεις και τα άτομα στην επιχείρηση, στη βιομηχανία, στην κυβέρνηση και στο σπίτι. Ωστόσο, πολλοί οργανισμοί εκφοβίζονται από τις νέες τεχνολογίες, χωρίς να είναι σίγουροι για το πώς θα επωφεληθούν από αυτές, και αναρωτιούνται πώς θα υποστηρίξουν τις υφιστάμενες επενδύσεις σε δεξιότητες κι υποδομές. Επιπλέον, αυτό το νέο είδος της οικονομίας ή του εμπορίου έρχεται με πολλές προκλήσεις, ιδίως εκείνες που σχετίζονται με θέματα εμπιστοσύνης και ασφάλειας[18].

Το Ηλεκτρονικό Εμπόριο είναι κάθε μορφής επιχειρηματική συναλλαγή και επικοινωνία που γίνεται με ηλεκτρονικά μέσα. Έχει να κάνει με τις δυνατότητες για επανακαθορισμό του τρόπου με τον οποίο πραγματοποιείται το εμπόριο, που γίνεται εφικτός με τη χρήση νέων τεχνολογιών από τις σύγχρονες επιχειρήσεις[19]. Βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων που αποτελεί έκφανση των λεγόμενων υπηρεσιών εξ αποστάσεως (ΠΔ 39/2001). Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά ή πώληση αγαθών ή υπηρεσιών[20].

Το Ηλεκτρονικό Εμπόριο είναι μια νέα επιχειρηματική πρακτική που ορίζεται ως ένα σύνολο επιχειρηματικών στρατηγικών για την αγοραπωλησία αγαθών, πληροφοριών και υπηρεσιών μέσα από δίκτυα ηλεκτρονικών υπολογιστών. Ο όρος αυτός είναι ευρύτερος,

[17] https://books.google.gr/books?hl=en&lr=&id=EOjG84UvrHMC&oi=fnd&pg=PR13&dq=E-commerce+definition&ots=X8EKb7TFwq&sig=TP9tNQEHwnLLk50rRkj8wHGkPbU&redir_esc=y#v=onepage&q=E-commerce%20definition&f=false

[18] 10.1109/FiCloud.2014.39 , IEEE, Conference at Barcelona, 2014, INSPEC Accession Number: 14846900

[19] Αλευρομαγείρου, Σ., Ηλεκτρονικό εμπόριο και νομικά θέματα. ΑΤΕΙ Κρήτης, Πτυχιακή εργασία, 2007

[20] Ρουμελιώτης Α., (2006), Ανάπτυξη πλατφόρμας ηλεκτρονικού εμπορίου. ΑΤΕΙ Ηρακλείου, πτυχιακή εργασία

καθώς περιλαμβάνει όχι μόνο τις διαδικασίες της αγοραπωλησίας, αλλά επίσης την εξυπηρέτηση πελατών, τη συνεργασία μεταξύ εμπορικών εταίρων, καθώς και τη διεξαγωγή ηλεκτρονικών διαδικασιών[21].

Ηλεκτρονικό εμπόριο είναι ο διαμοιρασμός επιχειρηματικών πληροφοριών, η διατήρηση επιχειρηματικών σχέσεων και η διεξαγωγή επιχειρηματικών συναλλαγών χρησιμοποιώντας ως μέσο το διαδίκτυο[22]. Επίσης, το ηλεκτρονικό εμπόριο ορίζεται ως το σύνολο των διαδραστικών υπηρεσιών που παραδίδονται μέσω του διαδικτύου κάνοντας χρήση ανεπτυγμένων τεχνολογιών, τηλεπικοινωνιών, πληροφορικής και πολυμέσων[23]. Ειδικότερα, το ηλεκτρονικό εμπόριο μπορεί να οριστεί μέσω τεσσάρων διαφορετικών οπτικών γωνιών[24]:

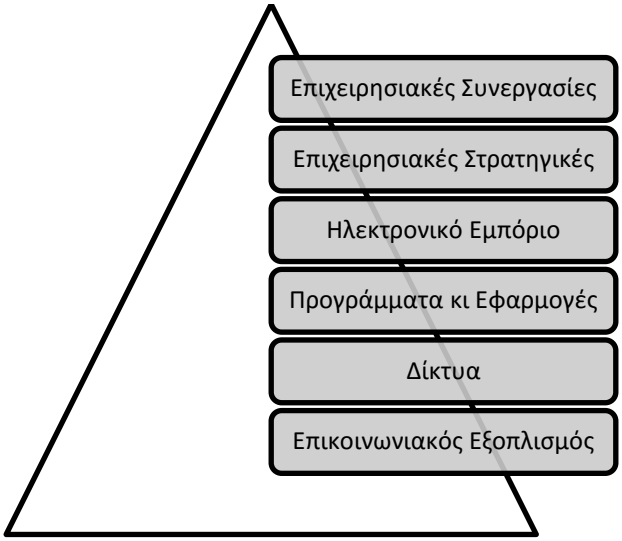
- *Επιχειρήσεις*: Εφαρμογή νέων τεχνολογιών ως προς τον αυτοματισμό των συναλλαγών και τη ροή εργασιών.
- *Υπηρεσίες*: Μηχανισμός που ικανοποιεί την κοινή επιθυμία προμηθευτών και πελατών για καλύτερη ποιότητα υπηρεσιών, μεγαλύτερη ταχύτητα εκτέλεσης συναλλαγών και μικρότερο κόστος.
- *Απόσταση*: Δυνατότητα αγοραπωλησίας προϊόντων και υπηρεσιών ανεξαρτήτως γεωγραφικής απόστασης μέσω του διαδικτύου.
- *Επικοινωνία*: Δυνατότητα παροχής πληροφοριών, προϊόντων ή υπηρεσιών, και πληρωμών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.

2.3. Η πυραμίδα του ηλεκτρονικού εμπορίου

Ακολουθεί η δομή του όλου συστήματος του ηλεκτρονικού εμπορίου, από τη βάση που είναι οι τηλεπικοινωνίες οι οποίες στην ουσία κάνουν δυνατές τις συναλλαγές μέσω του διαδικτύου, έως την κορυφή που εμφανίζονται οι συνεργασίες των επιχειρήσεων μεταξύ τους διαδικτυακά.

[21] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., (1998), 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών
[22] Barnes, S.J., Vidgen, R.T., "An integrative approach to the assessment of e-commerce quality", Journal o f Electronic Commerce Research, Vol.3, No.3, pp.114-127, 2003
[23] A. Kaponen, "E-Commerce Electronic Payments, Helsinki University of Technology", Telecommunications Software and Multimedia Laboratory, 2006
[24] Σαλτσογλίδης Α., Ανάπτυξη συστήματος ηλεκτρονικού εμπορίου, ΑΤΕΙ Κρήτης, Πτυχιακή εργασία, 2007

Γράφημα 2.1: Πυραμίδα ηλεκτρονικού εμπορίου



Πηγή: Πασχόπουλος Α, Σκάλτσας Π., 2006 και Φωτακοπούλου Δ., 2011

Ειδικότερα:

- Στη βάση παρουσιάζονται οι ***τηλεπικοινωνίες*** καθώς σχετίζονται με όλες τις υλικές υποδομές και είναι αυτές που επιτρέπουν τη δημιουργία δικτύων. Περιλαμβάνουν το παραδοσιακό τηλεφωνικό καλώδιο της καλωδιακής τηλεόρασης, το δορυφορικό δίκτυο τηλεπικοινωνιών και ασύρματες συνδέσεις υψηλής ταχύτητας. Από τις τελευταίες εξελίξεις στον επικοινωνιακό εξοπλισμό είναι το triple play, η ταυτόχρονη μετάδοση δηλαδή φωνής (τηλέφωνο), δεδομένων (διαδίκτυο) και τηλεοπτικού σήματος μέσα από ένα δίκτυο[25].
- Τα ***δίκτυα*** αναλύονται σε κλειστά δίκτυα μέσα στο χώρο ενός κτιρίου, μιας πόλης, μιας περιοχής και σε ανοικτά δίκτυα. Τα πρώτα πλεονεκτούν στο γεγονός ότι είναι ασφαλή όμως δε μπορούν να έρθουν σε επαφή με τους καταναλωτές. Χρησιμοποιούνται ιδίως μέσα σε μια επιχείρηση ή μεταξύ επιχειρήσεων. Σε αυτά τα δίκτυα εφαρμόζονται τα προγράμματα κάνοντας πραγματικότητα το Ηλεκτρονικό Εμπόριο[26]. Πιο συγκεκριμένα, υπάρχουν τα κάτωθι δίκτυα:
    1. *Τοπικά* (Local Area Networks ή LANs): Είναι δίκτυα εντός ενός ή περισσοτέρων γειτονικών κτιρίων. Χρησιμοποιούνται ενδοεπιχειρησιακά και μπορούν να χρησιμοποιηθούν από τους εργαζόμενους της επιχείρησης για ανταλλαγή μηνυμάτων και για κοινή χρήση εφαρμογών. Είναι ο μόνος

[25] Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001
[26] Πασχοπουλος Α., Σκαλτσας Π., Ηλεκτρονικό Εμπόριο, εκδόσεις «Κλειδάριθμος» 2η έκδοση, 2000

τύπος δικτύου που δεν παρέχει δυνατότητα επικοινωνίας με άλλες επιχειρήσεις.

2. *Μητροπολιτικά* (Metropolitan Area Networks ή MANs): Είναι δίκτυα εντός των ορίων της πόλεως. Μπορούν να χρησιμοποιηθούν όπως και τα LNAs, αλλά σε ευρύτερη κλίμακα και αν περιλάβουν πάνω από μια επιχειρήσεις. Το κόστος τους, όμως, είναι μεγαλύτερο.
3. *Ευρείας περιοχής* (Wide Area Networks ή WANs): Χρησιμοποιούνται όπως και τα MANs, αλλά χωρίς περιορισμό όσον αφορά στη γεωγραφική περιοχή των μελών του δικτύου. Έχουν μεγάλο κόστος κατασκευής και συντήρησης, αλλά παρέχουν μεγάλη ασφάλεια στους χρήστες τους.
4. *Δίκτυα Προστιθέμενης Αξίας* (Value Added Networks ή VANs): Είναι τα ασφαλέστερα για τη μεταφορά εμπορικών δεδομένων μεταξύ επιχειρήσεων. Έχουν όμως περιορισμένη δυνατότητα μεταφοράς δεδομένων και πολύ υψηλό κόστος[27].

- Το ***Ηλεκτρονικό Εμπόριο*** με τη σειρά του γίνεται εργαλείο διαθέσιμο για εκμετάλλευση απ' την επιχείρηση με σκοπό τη διαμόρφωση στρατηγικής και την ανάπτυξη πλεονεκτημάτων έναντι των ανταγωνιστών της. Τα προγράμματα για την επίτευξη του Ηλεκτρονικού Εμπορίου περιλαμβάνουν το ηλεκτρονικό ταχυδρομείο, το φωνητικό ταχυδρομείο, τους ηλεκτρονικούς καταλόγους, τις ηλεκτρονικές φόρμες στοιχείων, την ανταλλαγή στοιχείων. Οι εφαρμογές Ηλεκτρονικού Εμπορίου αφορούν την ανταλλαγή πληροφοριών, την παραγγελία, παράδοση, πληρωμή του προϊόντος, την ηλεκτρονική ανταλλαγή παραστατικών, την εξυπηρέτηση των πελατών μετά την πώληση. Αναλυτικότερα:
    1. *Ηλεκτρονικό Ταχυδρομείο* (Electronic Mail — E-mail): Αποτελεί ένα γρήγορο, οικονομικό και αποδοτικό τρόπο επικοινωνίας μεταξύ μεμονωμένων χρηστών στο δίκτυο σε ολόκληρο τον κόσμο, αφού συνδυάζει άμεση διαπροσωπική επικοινωνία αλλά και ευελιξία στη μεταφορά μηνυμάτων και αρχείων. Το Ηλεκτρονικό Ταχυδρομείο είναι το άμεσο αντίστοιχο του παραδοσιακού σε ηλεκτρονική μορφή, επιτρέποντας την επικοινωνία μεταξύ χρηστών για την ανταλλαγή οποιουδήποτε είδους πληροφορίας.
    2. Το *Φωνητικό Ταχυδρομείο* (Voice Mail): Οι χρήστες στέλνουν φωνητικά μηνύματα με τη βοήθεια μικροφώνου μέσω του υπολογιστή τους. Μια από

[27] Πασχόπουλος Α., Σκάλτσας Π., Ηλεκτρονικό Εμπόριο, εκδόσεις «Κλειδάριθμος» 2η έκδοση, 2000

τις μεγαλύτερες εταιρείες του χώρου της τηλεφωνίας μέσω διαδικτύου (web telephony) είναι η Skype η οποία προσφέρει φωνητικό ταχυδρομείο για τους συνδρομητές της για 15 δολάρια το χρόνο.

3. *Ηλεκτρονικοί Κατάλογοι* (E-catalogues): Πρόκειται στην ουσία για ηλεκτρονικές σελίδες στο Internet που περιλαμβάνουν πληροφορίες για τα προϊόντα τους και τις υπηρεσίες που προσφέρει μια εμπορική επιχείρηση. Ένας τυπικός ηλεκτρονικός κατάλογος περιλαμβάνει λεπτομερή πληροφόρηση για τη συσκευασία, τη μορφή και την τιμή των προϊόντων, ενώ στις περισσότερες περιπτώσεις υπάρχει δυνατότητα ηλεκτρονικής παραγγελίας, αγοράς και πληρωμής. Στα σημαντικά πλεονεκτήματα των ηλεκτρονικών καταλόγων μπορούμε να συμπεριλάβουμε: την αυξημένη δυνατότητα αλληλεπίδρασης, τη δυναμική αναβάθμισή τους, τη δυνατότητα ενσωμάτωσης υπερσυνδέσμενων στο κείμενο, και τη δυνατότητα για παγκόσμια παρουσίαση του υλικού τους.
4. *Ηλεκτρονικές Φόρμες Στοιχείων και Παραγγελιών* (Electronic Forms): Οι Ηλεκτρονικές Φόρμες παρέχουν λύση στο αδιέξοδο που δημιουργούσε ανέκαθεν η διαχείριση των έντυπων φορμών. Εκτός από τις κλασικές λειτουργίες της εκτύπωσης και της συμπλήρωσης οι ηλεκτρονικές φόρμες υποστηρίζουν και πιο ευφυείς πρακτικές αφού πολλές φορές αποτελούν διεπαφές που συνδέονται με βάσεις δεδομένων για αναζήτηση, ολοκλήρωση και χρήση πληροφοριών. Οι ηλεκτρονικές φόρμες παρέχουν τη δυνατότητα ηλεκτρονικής συμπλήρωσης και υποβολής δεδομένων μέσα από ένα εύχρηστο γραφικό περιβάλλον. Για παράδειγμα, με τη χρήση τέτοιων φορμών οι πελάτες μιας επιχείρησης μπορούν να παραγγείλουν ηλεκτρονικά τα προϊόντα, να συμπληρώσουν ερωτηματολόγια (δίνοντας έτσι πολύτιμες πληροφορίες στις επιχειρήσεις), να υποβάλλουν ερωτήματα, και γενικά να επικοινωνήσουν με τις επιχειρήσεις με δομημένο τρόπο[28].
5. *Το EDI*: Είναι η ανταλλαγή στοιχείων (τιμολογίων, τιμοκαταλόγων) μεταξύ επιχειρήσεων. Η διάδοση του EDI οφείλεται στο ότι μειώνει τα λειτουργικά κόστη και αποτελεί προθάλαμο για τη δημιουργία συμμαχιών μεταξύ των επιχειρήσεων. Από την άλλη πλευρά, αν και οι εφαρμογές του EDI μπορούν να "τρέξουν" σε εφαρμογές ασύμβατες μεταξύ τους, υπάρχει μεγάλο

[28] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών, 1998

κόστος στο να ενσωματωθούν οι δυνατότητες των EDI εφαρμογών στις ήδη υπάρχουσες εφαρμογές μιας επιχείρησης.

6. *Το FEDI*: Το FEDI (Financial EDI) είναι η χρηματοοικονομική μορφή του EDI, κατά το οποίο ένα από τα συναλλασσόμενα μέρη είναι τράπεζα ή άλλος χρηματοπιστωτικός οργανισμός.
7. *Η Ηλεκτρονική Διαχείριση Εγγράφων*: Είναι η διαχείριση παντός είδους εγγράφου μέσω λογισμικού, το οποίο "διαβάζει" όλα τα έγγραφα προς την επιχείρηση και τα διαχειρίζεται ανάλογα με τον παραλήπτη και τη μορφή τους. Είναι σαν τον διαχειριστή εισερχομένων κλήσεων, αλλά ο διαχωρισμός γίνεται με βάση το είδος της κλήσης: αν είναι τηλεφώνημα, χτυπά το τηλέφωνο, αν είναι ηλεκτρονικό ταχυδρομείο (e-mail) αποστέλλεται ηλεκτρονικό μήνυμα κι αν είναι fax, μπαίνει σε λειτουργία το fax[29].

- Οι ***επιχειρησιακές στρατηγικές*** αποσκοπούν στη δημιουργία πλεονεκτήματος έναντι των ανταγωνιστών. Αυτό επιτυγχάνεται με καλύτερη συνεργασία, μείωση λαθών, επίσπευση εργασιών, έγκαιρη πληροφόρηση[30]. Οι παραπάνω πρακτικές είναι εφικτές όταν η πληροφορία ρέει ελεύθερη από και προς όλα τα μέρη μιας επιχείρησης. Αυτό είναι εφικτό όταν όλα τα τμήματα και υπάλληλοι έχουν τη δυνατότητα επικοινωνίας μεταξύ τους. Σ' αυτό διευκολύνονται μέσω των εταιρικών δικτύων ή intranets (intra = έσω και net = δίκτυο). Τα εταιρικά δίκτυα μπορεί να επιτρέπουν μερική, ολική ή και καθόλου πρόσβαση σε ιδιώτες και οργανισμούς εκτός της επιχείρησης. Αυτές οι ενδοεπιχειρησιακές στρατηγικές είναι:
    1. Άμεση ανταπόκριση (quick response): Στοχεύει στην καλύτερη εξυπηρέτηση του πελάτη μέσα από την καλύτερη συνεργασία των τμημάτων (π.χ. εργοστάσιο, αποθήκη και κατάστημα) και των σημείων λιανικής πώλησης. Για παράδειγμα, ο πελάτης δε βρίσκει το προϊόν που επιθυμεί στο κατάστημα του Αμαρουσίου. Για την καλύτερη εξυπηρέτηση του, ο πωλητής μπορεί να ενημερωθεί μέσω του εταιρικού δικτύου για το πότε θα έχει στο κατάστημα το προϊόν ή μπορεί να τον στείλει στο πλησιέστερο κατάστημα της αλυσίδας που έχει το αντίστοιχο προϊόν.
    2. Δικτυακή αγορά: Στοχεύει στην απευθείας επαφή του προμηθευτή με τον πελάτη, ώστε να εξαλειφθούν οι μεσάζοντες, όταν και όπου δεν

[29] Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001

[30] Φωτακοπούλου Δ., Ανάπτυξη Διαδικτυακής Εφαρμογής Ηλεκτρονικού Καταστήματος Παροχέα Ηλεκτρικής Ενέργειας. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2011

προσφέρουν προστιθέμενη αξία στη ροή του προϊόντος από τον παραγωγό στον καταναλωτή.

3. Ευελιξία και προσαρμοστικότητα στις απαιτήσεις της αγοράς: Στόχος εδώ είναι η έγκαιρη προσαρμογή στις απαιτήσεις του πελάτη για αλλαγές στο προϊόν, καθώς και στον τρόπο και την ποσότητα παράδοσης. Ένα απλό παράδειγμα είναι η αλλαγή στον τρόπο λειτουργίας των καταστημάτων ενοικίασης DVD. Ο πελάτης δε χρειάζεται να μεταβεί στο κατάστημα, απλά μπαίνει στην ιστοσελίδα, βρίσκει την ταινία που τον ενδιαφέρει και παίζει τις ημέρες και ώρες αποστολής και επιστροφής από το σπίτι του[31].

- ***Επιχειρησιακές συνεργασίες*** είναι οι συνεργασίες με άλλες επιχειρήσεις. Ουσιαστικά, η επιχείρηση χρησιμοποιεί το διαδίκτυο συναγωνιστικά με άλλες επιχειρήσεις του κλάδου, για πληροφόρηση και μείωση του κόστους οργάνωσης και διαχείρισης[32]. Εδώ δημιουργείται ένα δίκτυο μεταξύ των επιχειρήσεων ώστε η πληροφορία να ρέει ελεύθερη από και προς όλες τις επιχειρήσεις που συνεργάζονται. Το δίκτυο μεταξύ πολλών επιχειρήσεων ονομάζεται extranet από το extra = έξω -εκτός επιχείρησης δηλαδή- και net = δίκτυο. Οι επιχειρησιακές συνεργασίες μπορούν να έχουν τις παρακάτω μορφές:

  i. Just In Time (JIT): Πρωτοεμφανίστηκε στην Ιαπωνία και αποσκοπεί στη μείωση του κόστους αποθεμάτων (πρώτων υλών και αποθηκευτικού χώρου), μέσω της έγκαιρης παραγωγής του προϊόντος, όταν και στην ποσότητα που το ζητήσει ο πελάτης.

  ii. Ιεραρχίες: Είναι η σχέση που έχουν μεγάλες εταιρείες με μικρότερές τους. Για παράδειγμα, μεγάλα νοσοκομεία ή supermarkets επιβάλλουν στους προμηθευτές τους τη χρήση τεχνολογίας η οποία τους επιτρέπει την άμεση πληροφόρηση για επικείμενη έλλειψη κάποιου προϊόντος ή φαρμάκου. Έτσι, οι "μικροί" απολαμβάνουν τη σταθερότητα της εμπορικής συνεργασίας, ενώ οι "μεγάλοι" την καλύτερη εξυπηρέτηση, την οποία και "περνούν" στους δικούς τους πελάτες.

  iii. Διεπιχειρησιακά συστήματα: Δημιουργούνται ώστε να εκμεταλλευτούν κοινούς πόρους, όπως βάσεις δεδομένων (με πελάτες, προμηθευτές, πηγές χρηματοδότησης, συνεργάτες εξωτερικού, δημοσιεύσεις διαγωνισμών), λογισμικό, γνώσεις και εμπειρίες. Στόχος τους είναι η καλύτερη πρόσβαση

[31] Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001

[32] Αποστόλου Κ., και Καρακατσάνη Α., Εμπιστοσύνη του ηλεκτρονικού καταστήματος στις ηλεκτρονικές συναλλαγές, ΑΤΕΙ Κρήτης, πτυχιακή εργασία, 2008

στην αγορά και στον πελάτη ώστε, παρέχοντάς του ολοκληρωμένες υπηρεσίες, να τον διατηρήσουν και να μην τον χάσουν από τον ανταγωνισμό[33].

2.4. Κατηγορίες ηλεκτρονικού εμπορίου

Το Ηλεκτρονικό Εμπόριο προσφέρει τη δυνατότητα εκτέλεσης ενεργειών για την ανταλλαγή προϊόντων ή υπηρεσιών μεταξύ δύο ή περισσότερων μερών με χρήση ηλεκτρονικών υπολογιστών και δικτύων υπολογιστών. Βασίζεται στην ηλεκτρονική επεξεργασία και μετάδοση δεδομένων, ήχου και εικόνων[34]. Οι εφαρμογές ηλεκτρονικού εμπορίου αφορούν τόσο προϊόντα, όπως καταναλωτικά αγαθά όσο και υπηρεσίες, όπως υπηρεσίες πληροφόρησης, χρηματοπιστωτικές και νομικές υπηρεσίες, παραδοσιακές δραστηριότητες, όπως ιατρική περίθαλψη, εκπαίδευση και νέες δραστηριότητες, όπως εικονικά πολυκαταστήματα.

Το Ηλεκτρονικό Εμπόριο καλύπτει κυρίως δύο τύπους δραστηριοτήτων, το Έμμεσο και το Άμεσο Ηλεκτρονικό Εμπόριο. Το πρώτο σχετίζεται με την ηλεκτρονική παραγγελία υλικών αγαθών τα οποία εξακολουθούν να παραδίδονται με παραδοσιακούς τρόπους όπως ταχυδρομικά ή μέσω ιδιωτικών υπηρεσιών διανομής. Σε γενικές γραμμές εξαρτάται από εξωτερικούς παράγοντες, όπως την αποτελεσματικότητα του συστήματος μεταφορών.

Το Άμεσο Ηλεκτρονικό Εμπόριο αφορά την τηλεματική παραγγελία, πληρωμή και παράδοση άυλων αγαθών και υπηρεσιών, όπως λογισμικό υπολογιστών, ψυχαγωγικό περιεχόμενο ή υπηρεσίες πληροφόρησης σε παγκόσμια κλίμακα. Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα. Το άμεσο ηλεκτρονικό εμπόριο παρέχει δυνατότητα πραγματοποίησης απρόσκοπτων ηλεκτρονικών συναλλαγών από άκρη σε άκρη, πέρα από γεωγραφικά σύνορα και με τον τρόπο αυτό, εκμεταλλεύεται όλες τις δυνατότητες των παγκόσμιων ηλεκτρονικών αγορών[35].

[33] Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001
[34] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών, 1998
[35] Συνανιώτη, Α., Φαρσαρώτας, Ι., «Ηλεκτρονική Τραπεζική», Αθήνα- Κομοτηνή: εκδόσεις Αντ. Σακούλας, 2004

Συνήθως οι εταιρείες κάνουν χρήση και των δύο τύπων Δραστηριοτήτων Ηλεκτρονικού Εμπορίου. Ανάλογα με τη φύση των συναλλαγών, το Ηλεκτρονικό Εμπόριο μπορεί να διακριθεί σε τέσσερις κατηγορίες[36]:

- Επιχείρηση προς Επιχείρηση (Business-to-Business – B2B)
- Επιχείρηση προς Καταναλωτή (Business-to-Customer – B2C)
- Επιχείρηση προς Κυβέρνηση (Business-to-Government – B2G)
- Καταναλωτής προς Καταναλωτή (Consumer-to-Consumer – C2C)

Σε αυτές τις κατηγορίες είναι σε θέση πλέον να προστεθεί και το κινητό εμπόριο (mobile commerce – m-commerce).

1. Επιχείρηση προς Επιχείρηση (Business-to-Business – B2B)

Το ηλεκτρονικό εμπόριο αυτής της μορφής αφορά τη διενέργεια ηλεκτρονικών εμπορικών συναλλαγών μεταξύ επιχειρήσεων και σχετίζεται κυρίως με την αγορά προμηθειών. Πρόκειται για τον δυναμικότερο κλάδο του ηλεκτρονικού εμπορίου, διότι οι εφαρμογές B2B περιλαμβάνουν εκατομμύρια συναλλαγές, τεράστιες επενδύσεις, ενώ η ταχύτητα και η ακρίβεια μπορεί να αποτελέσουν σοβαρό ανταγωνιστικό πλεονέκτημα. Μελέτες δείχνουν ότι το μέγεθος της ηλεκτρονικής αγοράς B2B μπορεί να είναι τόσο μικρό όσο 543 δισεκατομμύρια δολάρια ή τόσο μεγάλο όσο 6,8 τρισεκατομμύρια δολάρια. Οι περισσότερες από αυτές τις μελέτες συμφωνούν ότι το μέγεθος της αγοράς θα αυξάνεται κατά περίπου 50 τοις εκατό ανά έτος κατά τα αμέσως επόμενα χρόνια[37].

Οι εφαρμογές B2B έχουν ως στόχο να βελτιώσουν και να απλοποιήσουν τις διάφορες επιχειρησιακές διαδικασίες μέσα σε μια εταιρία, καθώς και να αυξήσουν την αποδοτικότητα των συναλλαγών μεταξύ εταιριών που συνεργάζονται. Οι εταιρίες χρησιμοποιούν το σύστημα B2B για γρηγορότερες συναλλαγές χωρίς σφάλματα, για έλεγχο των αποθεμάτων, αποτελεσματική αναπλήρωση των προϊόντων κ.τ.λ., ενώ επιτυγχάνουν μείωση του κόστους, αύξηση της παραγωγικότητας και αύξηση των ευκαιριών συνεργασίας. Ένα παράδειγμα της κατηγορίας αυτής μπορεί να είναι μια εταιρία, που

[36] A. Kaponen, E-Commerce Electronic Payments, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2006
[37] Πολίτης Δ., Ηλεκτρονικές προμήθειες σχεδιασμός και εφαρμογή, Πανεπιστήμιο Πατρών, διπλωματική εργασία, 2011

χρησιμοποιεί ένα δίκτυο παραγγελίας για τους προμηθευτές της, λαμβάνοντας τιμολόγια και κάνοντας πληρωμές[38].

Υπάρχουν τρεις κύριοι τύποι μοντέλων ηλεκτρονικού εμπορίου B2B: (1) αυτά που ανταλλάσσουν πληροφορίες, (2) αυτά που κάνουν απευθείας πωλήσεις στους επιχειρησιακούς πελάτες, και (3) αυτά που αποτελούν νέους μεσάζοντες.

1. *Ανταλλαγές Πληροφοριών*: Οι επιχειρήσεις χρειάζονται να ανταλλάσσουν πληροφορίες συνεχώς (τιμολόγια, εντολές αγοράς, κ.ο.κ.). Για τον σκοπό αυτό, άρχισαν να χρησιμοποιούν την ηλεκτρονική ανταλλαγή δεδομένων (EDI) μέσω των ιδιωτικών δικτύων.
2. *Εταιρείες Απευθείας Πωλήσεων*: Μερικές από τις πιο επιτυχημένες εταιρείες ηλεκτρονικού εμπορίου B2B (π.χ. Cisco, Dell) χρησιμοποιούν το μοντέλο απευθείας πωλήσεων. Πωλούν τα προϊόντα τους απευθείας σε άλλες επιχειρήσεις. Πολλές επιχειρήσεις ηλεκτρονικού εμπορίου B2B παρέχουν στους πελάτες τους έναν εξατομικευμένο κατάλογο, που προσαρμόζεται ειδικά για κάθε μεμονωμένο πελάτη. Η Dell αναπτύσσει έναν προσαρμοσμένο δικτυακό τόπο, αποκαλούμενο Premier Pages, για τους επιχειρησιακούς πελάτες της. Η τοποθεσία Premier Pages περιέχει περιγραφές και πληροφορίες τιμολόγησης για συστήματα υπολογιστών που διαμορφώνονται με βάση τις προδιαγραφές του πελάτη.
3. *Νέοι Μεσάζοντες*: Οι νέοι μεσάζοντες B2B είναι εικονικές αγορές που εστιάζουν συνήθως σε μια μόνο βιομηχανία ή επιχειρησιακή λειτουργία. Οι αγορές για συγκεκριμένη βιομηχανία ονομάζονται κάθετοι διανομείς, και εκείνοι που εστιάζουν σε μια επιχειρησιακή λειτουργία, όπως το ανθρώπινο δυναμικό ή τις πωλήσεις, ονομάζονται οριζόντιοι διανομείς. Ο οριζόντιος διανομέας βοηθά στην εκτέλεση λειτουργιών, όπως τη διαφήμιση και τη διαχείριση του ανθρώπινου δυναμικού, που απαιτούνται από τις περισσότερες επιχειρήσεις. Οι μεσάζοντες B2B υιοθετούν διάφορες στρατηγικές συνδυασμού για τη σύνδεση αγοραστών και πωλητών. Μερικοί χρησιμοποιούν ένα απλό μοντέλο δημοπρασίας κατά το οποίο οι αγοραστές υποβάλλουν προσφορά σε προϊόντα, και κερδίζει η υψηλότερη προσφορά. Άλλοι επιτρέπουν στους αγοραστές να δημιουργούν εξατομικευμένους καταλόγους που συλλέγουν περιγραφές και τιμές προϊόντων από διάφορους πωλητές. Υπάρχει επίσης μια προσέγγιση χρηματιστηρίου αξιών. Σε αυτό το

[38] Ταχαρίδου Βαρβάρα, Πανεπιστήμιο Μακεδονίας, Μεταπτυχιακό Πρόγραμμα στα Πληροφοριακά Συστήματα, 2004

μοντέλο οι αιτήσεις προσφοράς και πώλησης αντιστοιχούν σε πραγματικό χρόνο. Ο δικτυακός τόπος μπορεί επίσης να παρέχει μηχανισμούς διακανονισμών και εκκαθάρισης, οι οποίοι επιτρέπουν στις επιχειρήσεις που πραγματοποιούν μια συναλλαγή να ανταλλάσσουν αγαθά με χρήματα κατά τρόπο ασφαλή.

Οι συναλλαγές αυτές μπορεί να πραγματοποιούνται άμεσα (πωλητής προς αγοραστή απ' ευθείας), είτε μέσω ενδιάμεσων (τρίτων) φορέων. Τότε αναφερόμαστε σε μια άλλη μορφή που λαμβάνει το B2B, αυτή της Ηλεκτρονικής ή Δικτυακής Αγοράς (e-Marketplace).

2. Επιχείρηση προς Καταναλωτή (Business-to-Consumer – B2C)

Η κατηγορία Επιχείρηση προς Καταναλωτή αντιστοιχεί σε ένα μεγάλο βαθμό στο ηλεκτρονικό λιανικό εμπόριο. Είναι η κατηγορία στην οποία ανήκουν όλες οι εφαρμογές ηλεκτρονικού εμπορίου, οι οποίες αναπτύσσονται με στόχο την πώληση προϊόντων απευθείας στους τελικούς καταναλωτές. Η κατηγορία αυτή εξαπλώθηκε γρήγορα με την ανάπτυξη του παγκόσμιου ιστού (World Wide Web) και των τεχνολογιών πληρωμής μέσω Internet. Τώρα υπάρχουν εμπορικά κέντρα σε όλο το διαδίκτυο που προσφέρουν κάθε είδους καταναλωτικό αγαθό. Ειδικά, οι εταιρίες πληροφορικής, που ήταν οι πρώτες που εισέβαλλαν σ' αυτό το χώρο του ηλεκτρονικού εμπορίου, ίδρυσαν μια καινούργια αγορά μέσου του Internet και προσφέρουν on-line κάθε είδος προϊόν λογισμικού, όπως επίσης και υπηρεσίες, αναβαθμίσεις και τεχνική υποστήριξη στους πελάτες τους[39].

Περιλαμβάνει όλες τις συναλλαγές μεταξύ επιχειρήσεων και καταναλωτών, όπως είναι οι λιανικές πωλήσεις προϊόντων ή η παροχή υπηρεσιών. Πιο συγκεκριμένα, το ηλεκτρονικό εμπόριο B2C περιλαμβάνει μια σειρά από δραστηριότητες[40], οι οποίες είναι:

- ✓ Ηλεκτρονική διαφήμιση και προώθηση
- ✓ Ηλεκτρονική υποστήριξη πωλήσεων
- ✓ Ηλεκτρονική πώληση πληροφοριών - Ηλεκτρονική διανομή προϊόντων
- ✓ Ηλεκτρονική πώληση προϊόντων - Ηλεκτρονικά καταστήματα
- ✓ Ηλεκτρονική αγορά υπηρεσιών
- ✓ Ηλεκτρονική ενημέρωση και ψυχαγωγία - Ηλεκτρονική δημοσιογραφία
- ✓ Ηλεκτρονική τραπεζική

[39] Πάτσα, Χ., Αβαραμούδης, Β., Γκίκα, Σ., Πέτρου, Γ., (2005) ((Ηλεκτρονικό Επιχειρείν - Ηλεκτρονικό Εμπόριο>>, Equal Ανδρομέδα

[40] Χάλαρης Χρήστος, Οικονομία της κοινωνίας και της πληροφορίας , σελ. 14 http://thalis.cs.unipi.gr/dpolemi/e-commerce/index.htm

Ένα παράδειγμα από τον B2C τομέα είναι το Amazon.com το οποίο θα μπορούσε να χαρακτηριστεί σαν ένα εμπορικό κέντρο στο διαδίκτυο και βασίζεται στη μεγάλη ποικιλία προϊόντων. Στην περιοχή του B2C υπάρχουν τομείς που σημειώνουν επιτυχία, όπως είναι τα κτηματομεσιτικά, τα ταξίδια, οι δημοπρασίες, οι τραπεζικές συναλλαγές.

3. Επιχείρηση προς Κυβέρνηση (Business-to-Government – B2G)

Η μορφή ηλεκτρονικού εμπορίου από επιχείρηση σε κυβέρνηση αναφέρεται σε συναλλαγές μεταξύ των επιχειρήσεων και του δημόσιου τομέα. Καλύπτει κάθε μορφή ηλεκτρονικής επικοινωνίας μεταξύ επιχειρήσεων και κρατικών φορέων, τόσο για διεκπεραίωση φορολογικών ή άλλων υποχρεώσεων (π.χ. taxisnet), όσο και για την αυτοματοποίηση της διαδικασίας των δημοσίων προμηθειών. Αφορά δραστηριότητες όπως ηλεκτρονική παροχή πληροφοριών, ηλεκτρονική υποβολή αιτήσεων, ηλεκτρονική έκδοση πιστοποιητικών, προμήθειες δημοσίου, διευκόλυνση και αυτοματοποίηση των συναλλαγών, ηλεκτρονική πιστοποίηση της επιχείρησης, δυνατότητα ηλεκτρονικής πληρωμής, κ.ά.

Σε προηγμένες χώρες η πρότυπη και μεθοδική λειτουργία του ηλεκτρονικού εμπορίου σε αυτή τη μορφή έχει ως αποτέλεσμα τη μείωση των λειτουργικών εξόδων, την παροχή καλύτερων υπηρεσιών και τον αποτελεσματικότερο έλεγχο εσόδων και διαφάνειας.

Η Ελληνική Κυβέρνηση διαθέτει τους επίσημους δικτυακούς τόπους, με διάφορες πληροφορίες που αφορούν τον Έλληνα πολίτη. Επίσης, τα Υπουργεία της Ελληνικής Κυβέρνησης διαθέτουν πλέον δικτυακό τόπο μέσα από τον οποίο προσφέρουν μία σειρά από πληροφορίες και υπηρεσίες. Η έννοια της ηλεκτρονικής κυβέρνησης αφορά κυρίως την Κεντρική και Περιφερειακή Διοίκηση. Η προσπάθεια για την καθολικότητα των ηλεκτρονικών υπηρεσιών αφορά και όλους αυτούς τους φορείς. Έτσι, οι περισσότεροι φορείς του ευρύτερου δημόσιου τομέα διαθέτουν σήμερα δικτυακό τόπο, μέσα από τον οποίο προσφέρουν μία σειρά από πληροφορίες και υπηρεσίες. Τα τελευταία χρόνια στην Ελλάδα λειτουργεί το πρόγραμμα TAXIS μέσω του οποίου μπορεί να γίνει υποβολή φορολογικών δηλώσεων, κλπ[41]. Αυτή η κατηγορία αφορά και την επικοινωνία του κράτους με τον πολίτη (Consumer to Government - C2G) και περιλαμβάνει την ενημέρωση των πολιτών για τις υπηρεσίες που παρέχει το κράτος με ηλεκτρονικό τρόπο.

[41] Δουκίδης Γ- Θεμιστικλέους Μ- Δράκος Β- Παπαζαφιροπούλου Ν., Ηλεκτονικό Εμπόριο, Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 1998

4. Καταναλωτής προς καταναλωτή (Consumer-to-Consumer – C2C)

Το C2C (Consumer-to-Consumer) εμφανίζεται μεταξύ ιδιωτών ή καταναλωτών. Πρόκειται για μια διαδικτυακή τοποθεσία που επιτρέπει στους καταναλωτές να αγοράζουν και να πωλούν προϊόντα άμεσα με άλλους καταναλωτές. Παραδείγματα C2C ηλεκτρονικού εμπορίου αποτελούν (α) οι πύλες δημοπρασιών, όπως το e-Bay, το οποίο επιτρέπει σε πραγματικό χρόνο υποβολή προσφορών για τα είδη που πωλούνται στο διαδίκτυο, (β) τα συστήματα ομότιμων κόμβων (peer-to-peer) όπου τα αρχεία που περιέχουν διαφορετικό είδος δεδομένων διαμοιράζονται από έναν χρήστη προς άλλους χρήστες, (γ) οι πύλες διαφήμισης όπου οι χρήστες μπορούν να πωλούν ή να αγοράζουν μεταξύ τους διάφορα προϊόντα και (δ) οι μικρές αγγελίες σε ιστοσελίδες, ένα διαδραστικό περιβάλλον άμεσα συνδεδεμένων αγορών όπου οι αγοραστές και οι πωλητές μπορούν να διαπραγματεύονται την αγορά και πώληση αγαθών.

Ο μηχανισμός πωλήσεων είναι μια δημοπρασία, στην οποία ένας πωλητής καταγράφει ένα προϊόν και οι καταναλωτές κάνουν όλο και πιο υψηλές προσφορές μέχρις ότου λήξει ο χρόνος της δημοπρασίας. Αυτός που έχει δώσει την υψηλότερη προσφορά κερδίζει την δημοπρασία και πληρώνει το προϊόν. Μόλις πραγματοποιηθεί η πληρωμή, ο πωλητής αποστέλλει το προϊόν άμεσα σε αυτόν που το έχει κερδίσει. Η τοποθεσία δημοπρασίας έχει κέρδος χρεώνοντας τους πωλητές με ένα μικρό ποσό για την παράθεση των προϊόντων και με τη λήψη ενός ποσοστού της προσφοράς που έχει κερδίσει.

5. Κινητό εμπόριο (mobile commerce - m-commerce)

Το κινητό εμπόριο ορίζεται ως η διαδικασία αγοράς και πώλησης προϊόντων ή υπηρεσιών μέσω ασύρματης τεχνολογίας. Στο επίκεντρο του κινητού εμπορίου, οι πληρωμές μέσω κινητού τηλεφώνου αποτελούν σήμερα γεγονός. Η καινοτομία σε αυτόν τον τομέα αποτελεί ουσιαστικό αντικείμενο επένδυσης στη βιομηχανία των έξυπνων-κινητών (smartphones) και δημιουργίας νέων οικοσυστημάτων στην αγορά ηλεκτρονικών καρτών, κινητής τηλεφωνίας, λιανοπωλητών, προμήθειας συσκευών και ολοκληρωμένων υπηρεσιών[42].

Ο ρυθμός των αλλαγών σε αυτόν τον τομέα αποδεικνύεται ήδη από ανακοινώσεις του έτους 2012. Μια ομάδα μεγάλων λιανοπωλητών των ΗΠΑ, συμπεριλαμβανομένων των Wal-Mart, Target, Sears και Best Buy ανακοίνωσαν τον όρο MCX (the Merchant

[42] http://dx.doi.org/10.1016/j.clsr.2013.01.009

Customer Exchange) ως «ολοκληρωμένη επιλογή πληρωμών» στα μέσα Αυγούστου, ορίστηκε το «Έργο Όσκαρ» (Project Oscar) - το B2B Κινητό πορτοφόλι της Αγγλίας, γνωστοποιήθηκε η κοινοπραξία στον τομέα του μάρκετινγκ και των analytics μεταξύ των επιχειρήσεων Everything Everywhere, O2 και Vodafone.

Το κινητό εμπόριο φέρνει πιο κοντά την προσφορά στο σημείο δημιουργίας της ζήτησης μέσω των μοναδικών χαρακτηριστικών που διαθέτει η χρήση του κινητού τηλεφώνου, όπως είναι οι υπηρεσίες με βάση την τοποθεσία (LBS- Location Based Services), ο έλεγχος φωνής, η φωτογραφική μηχανή, η πλήρης διαθεσιμότητα, η σταθερή σύνδεση στο διαδίκτυο και η γρήγορη απόκριση. Το m-commerce έχει καταστήσει το smartphone να εκπληρώνει τις ανάγκες έξω / εκτός από τον χώρο του σπιτιού, τον χώρο εργασίας και το κατάστημα.

Τα εργαλεία που χρησιμοποιεί το κινητό εμπόριο για να προωθήσει προϊόντα, υπηρεσίες και ιδέες για να πετύχει τους στόχους του είναι:

- υπηρεσίες με βάση τη γεωγραφική θέση του χρήστη,
- διαγωνισμοί οι οποίοι συνήθως ζητούν τη σωστή απάντηση σε μία εύκολη ερώτηση ώστε να προσελκύσουν αρκετούς χρήστες, άρα και χρήματα μέσω των χρεώσεων των μηνυμάτων,
- κληρώσεις όπου ο χρήστης απλά στέλνει συνήθως όσες φορές θέλει το μήνυμα που του ζητά ο διαφημιζόμενος και έτσι αυξάνει τις πιθανότητές του να κληρωθεί για κάποιο έπαθλο,
- κουπόνια τα οποία προσφέρονται από εταιρείες που θέλουν να αυξήσουν τις πωλήσεις τους με προσφορές, και εξαργυρώνονται σε σημεία πώλησης όπως super markets, καταστήματα ηλεκτρικών ειδών, βιβλιοπωλεία,
- ειδοποιήσεις όπου ο χρήστης δίνει τη συγκατάθεσή του να δέχεται μηνύματα ηλεκτρονικά,
- υπηρεσίες σε μορφή ειδοποιήσεων μπορεί να περιλαμβάνουν μηνύματα σχετικά με πληροφόρηση, αποτελέσματα αγώνων, διασκέδαση, προσωπικά στοιχεία,
- banners τα οποία μπορεί να ενεργοποιήσει ο χρήστης και να μεταβεί στην ειδικά διαμορφωμένη για κινητά σελίδα του διαφημιζόμενου,

Οι παγίδες και οι κίνδυνοι τους οποίους μπορεί να κρύβει η προώθηση μέσω κινητών τηλεφώνων είναι υπερβολικές χρεώσεις στον τελικό καταναλωτή, αποστολή μηνυμάτων χωρίς τη συγκατάθεση του χρήστη, αποστολή μεγάλου αριθμού μηνυμάτων μέσα σε μία

χρονική περίοδο, έλλειψη δημιουργικότητας και στερεότυπα μηνύματα, κακή χρονική στιγμή αποστολής μηνυμάτων, προσπάθεια εκμαίευσης δημογραφικών στοιχείων.

6. Διεπιχειρησιακές συναλλαγές

Στην κατηγορία αυτή συμπεριλαμβάνονται όλες οι εσωτερικές δραστηριότητες μίας επιχείρησης, οι οποίες συνήθως διενεργούνται μέσα σε ενδοεταιρικά δίκτυα και αφορούν ανταλλαγή προϊόντων, υπηρεσιών και πληροφοριών. Τέτοιου είδους δραστηριότητες είναι για παράδειγμα η πώληση των προϊόντων μίας εταιρίας στους υπαλλήλους της, τα διάφορα εκπαιδευτικά προγράμματα, και άλλες δραστηριότητες μείωσης του κόστους[43].

2.5. Ιστορική αναδρομή ηλεκτρονικού εμπορίου

Το πρώτο «μηχανογραφημένο» πολυκατάστημα στον κόσμο δημιουργήθηκε το 1970. Πρόκειται για το Telemart στο Σαν Ντιέγκο της Καλιφόρνια. Τότε δεν υπήρχε Ίντερνετ και οι πελάτες χρησιμοποιούσαν το αναλογικό τηλέφωνο, για να επιλέξουν τα προϊόντα που επιθυμούσαν να τους αποσταλούν στο σπίτι. Σήμερα, το ηλεκτρονικό εμπόριο είναι πια διαδεδομένο, γνωστό στους χρήστες του Ίντερνετ.

Τη δεκαετία του ‘70 εμφανίζονται τα συστήματα ηλεκτρονικής μεταφοράς χρηματικών πόρων (EFT) μεταξύ τραπεζών, που χρησιμοποιούν ασφαλή ιδιωτικά δίκτυα. Τα συστήματα EFT αλλάζουν τη μορφή των αγορών. Τη δεκαετία του ’80 οι τεχνολογίες ηλεκτρονικής επικοινωνίας που βασίζονται στην αρχιτεκτονική της ανταλλαγής μηνυμάτων αποκτούν σημαντική διάδοση. Κατά τα τέλη της δεκαετίας του 1980 τα ηλεκτρονικά δίκτυα προσφέρουν μια νέα μορφή κοινωνικής επικοινωνίας, με δυνατότητες όπως ηλεκτρονικό ταχυδρομείο (e-mail), ηλεκτρονική διάσκεψη (conferencing) και ηλεκτρονική συνομιλία (IRC), ομάδες συζήτησης (newsgroups, forums), μεταφορά αρχείων (FTP) κτλ. Η πρόσβαση στο δίκτυο γίνεται φθηνότερη λόγω της διεθνούς απελευθέρωσης της αγοράς τηλεπικοινωνιών.

Τη δεκαετία του ’90 η εμφάνιση του Παγκόσμιου Ιστού (WWW) στο Internet και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών (PC) προσφέρουν μεγάλη ευκολία χρήσης λύνοντας το πρόβλημα της δημοσίευσης και της εύρεσης πληροφοριών στο Διαδίκτυο. Το ηλεκτρονικό εμπόριο γίνεται ένας πολύ φθηνότερος τρόπος για την

[43] Κρητικός Κ., Το ηλεκτρονικό εμπόριο ως εργαλείο ανάπτυξης των τραπεζικών εργασιών. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2008

πραγματοποίηση μεγάλου όγκου συναλλαγών, ενώ συγχρόνως διευκολύνει την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών δραστηριοτήτων, επιτρέποντας σε μικρές επιχειρήσεις να ανταγωνιστούν μεγαλύτερες, με πολύ ευνοϊκότερες προϋποθέσεις. Κατά τα τέλη της δεκαετίας του ’90 η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και εξακρίβωσης της ταυτότητας του αποστολέα ηλεκτρονικών μηνυμάτων, καθώς και η σχετική προσαρμογή της νομοθεσίας στους τομείς των εισαγωγών-εξαγωγών και των επικοινωνιών, καθιστούν δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών[44].

2.6. Το ηλεκτρονικό εμπόριο σήμερα

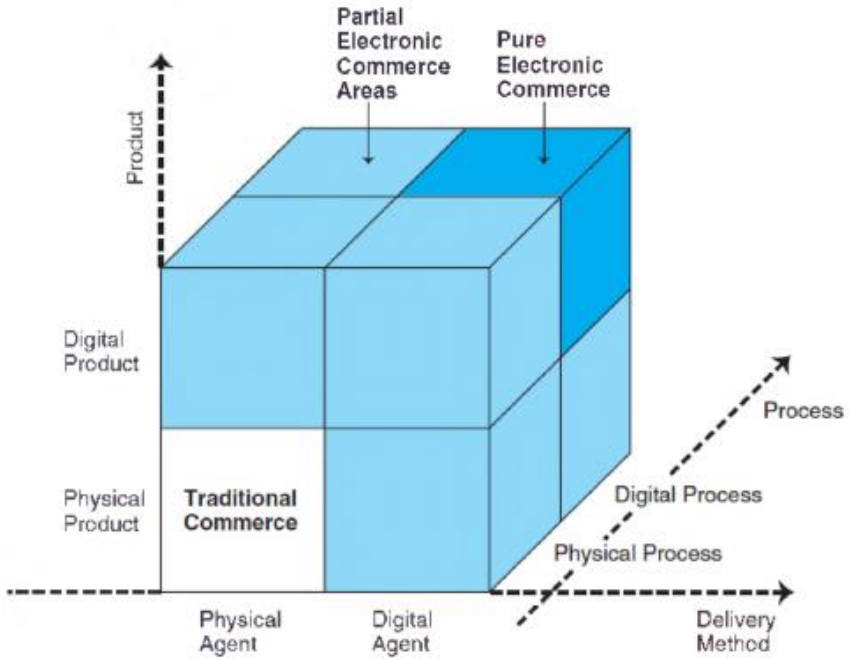
Οι κυριότεροι παράγοντες διάδοσης του ηλεκτρονικού εμπορίου είναι η παγκοσμιοποίηση, ο ταχύς τρόπος ζωής, η οικονομική κρίση και κυρίως η εξάπλωση του Διαδικτύου[45]. Ο πολιτισμός και ο τρόπος ζωής μεταξύ των διαφόρων χωρών δε διαφέρει σχεδόν καθόλου στην εποχή μας, ειδικά στον λεγόμενο δυτικό κόσμο. Οι πολίτες όλων των χωρών έχουν τις ίδιες ανάγκες και ζητούν τα ίδια πράγματα: τάχιστη εξυπηρέτηση και ποιοτικές υπηρεσίες.

Οι επιχειρήσεις έχουν ανάγκη μεγιστοποίησης και διεύρυνσης του καταναλωτικού αγοραστικού κοινού και μείωσης των εξόδων συντήρησης και λειτουργίας της ίδιας της επιχείρησης. Λύσεις στις απαιτήσεις τόσο των καταναλωτών όσο και των προμηθευτών δίνει η εξάπλωση του διαδικτύου. Η εξάπλωση του διαδικτύου αποτελεί τον θεμέλιο λίθο του ηλεκτρονικού εμπορίου μέσω του οποίου ικανοποιούνται οι απαιτήσεις της σύγχρονης εμπορικής δραστηριότητας και φυσικά των σύγχρονων καταναλωτών.

Το επόμενο γράφημα εξηγεί τις πιθανές διαμορφώσεις των τριών διαστάσεων του ηλεκτρονικού εμπορίου. Ένα *προϊόν* μπορεί να είναι φυσικό ή ψηφιακό, η *διαδικασία* μπορεί να είναι φυσική ή ψηφιακή, και η *μέθοδος παράδοσης* μπορεί να είναι φυσική ή ψηφιακή. Αυτές οι εναλλακτικές λύσεις έχουν δημιουργήσει οκτώ κύβους, καθένας εκ των οποίων έχει τρεις διαστάσεις.

[44] Ανδρουλάκη Ε., Κατασκευή ενός πληροφοριακού συστήματος για ηλεκτρονικό εμπόριο εταιρίας. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2009
Βασιλείου Ε. Καζαντζάκη Ε., Recommendation systems. ΤΕΙ Μεσολογγίου Διπλωματική εργασία, 2006
[45] Μπατσίνης Ν., Δέλιας Π., Τσαφαράκης Σ., Ηλεκτρονικό εμπόριο και εικονικές επιχειρήσεις. Εκδόσεις Πολυτεχνείου Κρήτης «Χανιά», 2006

Γράφημα 2.2: Διαστάσεις ηλεκτρονικού εμπορίου



Πηγή: Choi, Soon-Yong, Stahl, Dale, Whinston, Andrew, "The economics of electronic commerce." Indianapolis: McMillan Technical Publishing, 1997*, p.18*

Το παραδοσιακό εμπόριο, όπως απεικονίζεται στον κάτω αριστερά κύβο, είναι αυτό που οι τρεις διαστάσεις του κύβου είναι φυσικοί. Επίσης, το αντίθετο μέρος του κύβου αντικατοπτρίζει το ψηφιακό (online) προϊόν, την παράδοση, την πληρωμή και την κατανάλωση. Οι υπόλοιποι κενοί κύβοι περιλαμβάνουν ένα μείγμα από ψηφιακές και φυσικές διαστάσεις. Παρόλα αυτά, υπάρχει πιθανότητα μερικού και ολικού ηλεκτρονικού εμπορίου τύπος. Για παράδειγμα, η αγορά ενός βιβλίου από την Amazon.com είναι μερική μορφή ηλεκτρονικού εμπορίου, διότι τα εμπορεύματα έχουν φυσική παράδοση. Ωστόσο, η αγορά ενός e-book από το Amazon.com αποτελεί ολική μορφή ηλεκτρονικού εμπορίου, διότι το προϊόν, η πληρωμή και η παράδοση γίνονται όλα ψηφιακά στον αγοραστή[46].

Σύμφωνα με τον Σύνδεσμο Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδας (ΣΕΠΕ), η διείσδυση των υπηρεσιών cloud («νέφος» υπηρεσιών μέσω Διαδικτύου) στις ελληνικές επιχειρήσεις ήταν σε χαμηλά επίπεδα το 2015. Από το σύνολο των εγχώριων εταιρειών που είχαν πρόσβαση στο Διαδίκτυο κατά το 2015 (20.519 επιχειρήσεις) μόνο οι 2.120, που ποσοστιαία αντιστοιχούν στο 10,33%, αγόρασαν υπηρεσίες υπολογιστικού νέφους. Οι υπηρεσίες cloud με τη μεγαλύτερη χρήση από τον επιχειρηματικό κόσμο στην

[46] Choi, Soon-Yong, Stahl, Dale, Whinston, Andrew, "The economics of electronic commerce." Indianapolis: McMillan Technical Publishing, 1997

Ελλάδα είναι τα e-mails με ποσοστό 61,27% και η αποθήκευση αρχείων με 53,40%. Αντίθετα, η μικρότερη είναι στις εφαρμογές διαχείρισης σχέσεων πελατών (CRM), με ποσοστό 25,19%.

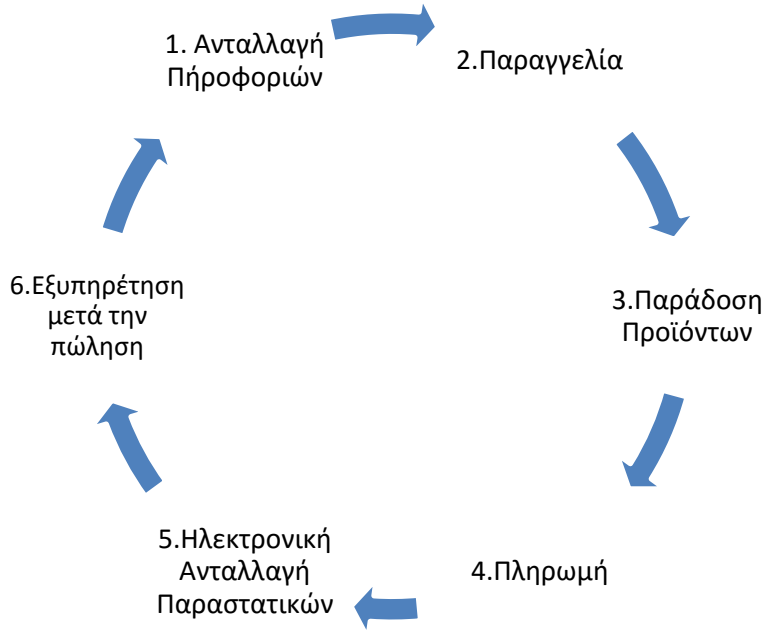
Σύμφωνα με την ετήσια έρευνα χρήσης τεχνολογιών πληροφόρησης, επικοινωνιών και ηλεκτρονικού εμπορίου, που δημοσιοποίησε η Στατιστική Αρχή, από τις 23.225 επιχειρήσεις που ερευνήθηκαν στην Ελλάδα, οι 1.555 απάντησαν ότι έλαβαν παραγγελίες μέσω ιστοσελίδας, ποσοστό 6,70%, και ο τζίρος από αυτές τις παραγγελίες ανήλθε σε ποσοστό 0,84% του συνολικού τζίρου. Επιπλέον, από το σύνολο των επιχειρήσεων που ερευνήθηκαν στο πλαίσιο της έρευνας το 2015, οι 2.597 απάντησαν ότι έκαναν αγορές μέσω ιστοσελίδας, ποσοστό 11,18%, ενώ το αντίστοιχο ποσοστό για το 2014 ήταν 13,66%.

Με βάση τα αποτελέσματα της έρευνας για το 2015, σε σύνολο 23.225 επιχειρήσεων, οι 20.519 χρησιμοποίησαν ηλεκτρονικό υπολογιστή, ήτοι ποσοστό 88,35%, επίδοση υποδεέστερη της περυσινής όταν το αντίστοιχο ποσοστό ήταν 89,86%. Στους ηλεκτρονικούς υπολογιστές συμπεριλαμβάνονται οι προσωπικοί, φορητοί και τα «έξυπνα» κινητά τηλέφωνα. Από τις 20.519 επιχειρήσεις που χρησιμοποίησαν ηλεκτρονικό υπολογιστή, οι 20.240 είχαν πρόσβαση στο Διαδίκτυο, που αντιστοιχεί σε ποσοστό 87,15% σε σχέση με το σύνολο των επιχειρήσεων, και είναι και πάλι μειωμένο έναντι του 2014, οπότε είχε ανέλθει σε 89,09%.

2.7. Ο κύκλος του ηλεκτρονικού εμπορίου - Επιχειρηματικές λειτουργίες του ηλεκτρονικού εμπορίου

Προκειμένου το Ηλεκτρονικό Εμπόριο να φέρει τα επιθυμητά αποτελέσματα πρέπει να περιλαμβάνει έξι βασικά στοιχεία. Αν αυτά τα στοιχεία τοποθετηθούν σε μια σειρά, τότε θα δημιουργηθεί ο γνωστός Κύκλος του Ηλεκτρονικού Εμπορίου, όπως φαίνεται στο παρακάτω γράφημα.

Γράφημα 2.3: Ο Κύκλος του Ηλεκτρονικού Εμπορίου



Πηγή: Μαρκάκη Σ., B2B επιχειρείν. Η συμβολή του ηλεκτρονικού εμπορίου. ΑΤΕΙ Κρήτης, πτυχιακή εργασία, 2010

Το πρώτο στοιχείο αναφέρεται στην *Ανταλλαγή Πληροφοριών*. Έχει να κάνει με την επικοινωνία με τους καταναλωτές και με τις επιχειρήσεις. Αυτή η επικοινωνία μεταξύ αυτών επιτυγχάνεται είτε μέσω του Ηλεκτρονικού Ταχυδρομείου (E-mail) που χρησιμοποιείται κυρίως από τους καταναλωτές είτε μέσω της Ηλεκτρονικής Ανταλλαγής Δεδομένων (EDI - Τιμολόγια, Δελτία Αποστολής). Αποτελεί έναν επίσημο τρόπο ανταλλαγής πληροφοριών μεταξύ των επιχειρήσεων. Κύριος σκοπός της εφαρμογής αυτής είναι η αναζήτηση πληροφοριών-στοιχείων που αφορούν τις προδιαγραφές των προϊόντων και υπηρεσιών που ενδιαφέρουν τους καταναλωτές[47]. Ουσιαστικά, σε επιχειρηματικό επίπεδο λειτουργίας του ηλεκτρονικού εμπορίου μιλάμε για Ηλεκτρονική Διαπραγμάτευση (Electronic Negotiation), η οποία αναφέρεται σε όλες τις μορφές επικοινωνίας μεταξύ δύο επιχειρήσεων οι οποίες έχουν σαν τελική κατάληξη τη σύναψη (ή μη) εμπορικής σχέσης.

Από την πλευρά των επιχειρήσεων με την προβολή των προϊόντων και των υπηρεσιών που παρέχουν μπορούν να μάθουν τις αγοραστικές συνήθειες και προτιμήσεις των υποψήφιων πελατών τους και με τα μηνύματα που στέλνουν οι τελευταίοι μπορούν να βελτιώσουν τα ήδη υπάρχοντα προϊόντα και να δημιουργήσουν νέα και καινοτόμα.

[47] Μαρκάκη Σ., B2B επιχειρείν. Η συμβολή του ηλεκτρονικού εμπορίου. ΑΤΕΙ Κρήτης, πτυχιακή εργασία 2010

Η *Παραγγελία* των προϊόντων από διάφορα ηλεκτρονικά καταστήματα (Product Information Exchange) αποτελεί πλέον σύνηθες φαινόμενο. Μπορεί να πραγματοποιηθεί με Ηλεκτρονική Φόρμα Παραγγελίας και μπορεί να συμπεριλάβει κάθε είδους προϊόντα. Επιπλέον, υπάρχει και η δυνατότητα παραγγελίας μέσω του Ηλεκτρονικού Ταχυδρομείου (E-mail), για τους χρήστες που δεν πραγματοποιούν συχνά ηλεκτρονικές αγορές ή δεν έχουν το κατάλληλο browser για τις συναλλαγές τους[48]. Οι ηλεκτρονικές φόρμες (E-forms) που στην ουσία είναι οι Ηλεκτρονικοί Κατάλογοι (E-cat) και οι εφαρμογές Πολυμέσων (Multimedia) είναι οι πιο αποδοτικοί μέθοδοι προσέλκυσης πελατών.

Η *Παράδοση* του προϊόντος στο Ηλεκτρονικό Εμπόριο (Electronic Product Delivery), εξαρτάται κατά κύριο λόγο από τη φύση αυτών. Τα προϊόντα χαρακτηρίζονται από Υλικά αγαθά και από Άυλα αγαθά. Τα Άυλα αγαθά του Ηλεκτρονικού Εμπορίου είναι αγαθά όπως λογισμικά, e-books, μουσική, φωτογραφίες και άλλα σχέδια που παραδίδονται ηλεκτρονικά. Έτσι, επιτυγχάνεται η μείωση του κόστους παράδοσης, η αποφυγή των μεταφορικών και η άμεση παράδοση του προϊόντος στα χέρια του χρήστη. Τα υλικά αγαθά του Ηλεκτρονικού Εμπορίου είναι τα αγαθά εκείνα που παραδίνονται είτε με τους παραδοσιακούς τρόπους παράδοσης όπως το Ηλεκτρονικό Ταχυδρομείο (E-mail) είτε με υπηρεσίες ιδιωτικής διανομής.

Η *Πληρωμή* για την ηλεκτρονική αγορά προϊόντων γίνεται στις μέρες με ποικίλους τρόπους και φυσικά μέσω του διαδικτύου. Η εφαρμογή αυτή αποτελεί δύσκολο κομμάτι του ΗΕ και αυτό οφείλεται κυρίως[49]:

- Στη μη ύπαρξη κατάλληλης εναρμόνισης σε πολλές εθνικές νομοθεσίες
- Στις αυξημένες απαιτήσεις ασφάλειας που υπάρχουν
- Στην ανυπαρξία ενός παγκόσμιου αποδεκτού προτύπου για τέτοιου είδους πληρωμές

Όπως προαναφέρθηκε παραπάνω, οι ηλεκτρονικές συναλλαγές είναι ιδιαίτερα δύσκολες και επικίνδυνες για τις επιχειρήσεις που ασχολούνται με το λιανικό και το χονδρικό εμπόριο. Για τις Χονδρικές πληρωμές τα πράγματα δεν παρουσιάζουν ιδιαίτερα προβλήματα. Εκεί που δημιουργείται πρόβλημα είναι στις Λιανικές πληρωμές όπου η επαφή πελάτη - εμπόρου είναι σχεδόν ανύπαρκτη και αυτό καθιστά περίπλοκη τη συναλλαγή. Για την καλύτερη διεκπεραίωση των συναλλαγών θα πρέπει να λαμβάνεται υπ'

[48] Πασχόπουλος. Α., Σκαλτσάς, Π., «Ηλεκτρονικό εμπόριο, Επιχειρηματική στρατηγική και marketing στο διαδίκτυο», Αθήνα: εκδόσεις Κλειδάριθμος. 3η έκδοση, 2006

[49] Δουκίδης, Γ., Δράκος, Β., Παπαζαφειροπούλου. Ν., Θεμιστοκλέους, Μ., «Ηλεκτρονικό Εμπόριο >> Αθήνα: Εκδόσεις: Νέων Τεχνολογιών, 1998

όψη η νομιμότητα της ηλεκτρονικής ανταλλαγής εγγράφων και επιπλέον να πραγματοποιείται συστηματική μελέτη στα πιστωτικά όρια διότι είναι δύσκολο να ελεγχθούν με τους παραδοσιακούς τρόπους. Οι τρόποι με τους οποίους μπορεί κάποιος να πραγματοποιήσει ηλεκτρονικές πληρωμές είναι με τη χρήση:

- *Πιστωτικών Καρτών*: Είναι ο πιο συνηθισμένος τρόπος πληρωμής όπου το κύριο στοιχείο αυτής είναι ο αριθμός της κάρτας που αποτελεί και μέρος του συστήματος ασφάλειας. Τη πληρωμή των πιστωτικών καρτών την αναλαμβάνει κυρίως μια Τράπεζα[50]. Ο τρόπος με τον οποίο χρησιμοποιείται γίνεται μέσω του Internet όπου ο πελάτης εφόσον έχει επιλέξει το προϊόν που επιθυμεί να παραγγείλει, μαζί με τη παραγγελία θα δώσει τον αριθμό της πιστωτικής, την ημερομηνία λήξης της και την αρχή έκδοσής της. Τα στοιχεία αυτά προωθούνται στη Τράπεζα ή στο προμηθευτή και στη συνέχεια πραγματοποιείται η αποπληρωμή της παραγγελίας.
- *Finance EDI*: Είναι ένας τρόπος πληρωμής που χαρακτηρίζεται από υψηλό βαθμό ασφαλείας. Εδώ, ο πελάτης στέλνει ένα μήνυμα EDI στη Τράπεζα που συναλλάσσεται δίνοντας την εντολή να μεταφέρει το ποσό που οφείλει στο λογαριασμό του προμηθευτή. Με τη σειρά της η Τράπεζα του πελάτη ενημερώνει την Τράπεζα του προμηθευτή προκειμένου να ολοκληρωθεί η μεταφορά των χρημάτων από το ένα λογαριασμό στον άλλο. Αυτός ο τρόπος πληρωμής έχει δύο μορφές[51]:
  i. Ηλεκτρονικό χρήμα (e-cash) με τη μορφή κάρτας με ιδιότητα χρέωσης και πίστωσης από το πελάτη και εμπεριέχει συγκεκριμένη αγοραστική αξία.[52]
  ii. Ηλεκτρονικό χρήμα με τη μορφή λογισμικού που είναι εγκατεστημένο στον υπολογιστή του χρήστη και το οποίο μεταφέρει σε ψηφιακή μορφή ένα χρηματικό ποσό από τη Τράπεζα του στον υπολογιστή του.

Στη συνέχεια προωθεί το ποσό αυτό από τον υπολογιστή του στον υπολογιστή του προμηθευτή. Ο προμηθευτής καταθέτει τα χρήματα στη Τράπεζα ή τα χρησιμοποιεί για τρέχουσες αγορές[53].

- *Ηλεκτρονικές επιταγές*: ένα σύστημα ηλεκτρονικών πληρωμών το οποίο χρησιμοποιείται τον τελευταίο καιρό σε χώρες με παράδοση χρήσης επιταγών. Μια επιταγή έχει μία σειρά από νούμερα τα οποία καθιστούν την κάθε επιταγή μοναδική. Η

[50] Μαρκάκη Σ., B2B επιχειρείν. Η συμβολή του ηλεκτρονικού εμπορίου. ΑΤΕΙ Κρήτης, πτυχιακή εργασία, 2010
[51] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών, 1998
[52] Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001
[53] Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών 1998

μέθοδος είναι αποτελεσματική αλλά μάλλον ακατάλληλη για την Ελλάδα, δεδομένης της ανυπαρξίας λιανικών συναλλαγών με επιταγή[54].

Αξίζει να αναφερθεί σε αυτό εδώ το σημείο ο όρος ηλεκτρονική διαφήμιση *(Electronic Advertising).* Το Internet δημιούργησε νέα επιστημονική περιοχή στο χώρο του Marketing που ασχολείται με την ηλεκτρονική διαφήμιση και προώθηση προϊόντος. Το Internet, λόγω του γραφικού περιβάλλοντος που παρέχει μέσα από το World Wide Web, της εύκολης πρόσβασης του και του οικονομικού τρόπου παγκόσμιας παρουσίας επιτρέπει τη διείσδυση των επιχειρήσεων στις παγκόσμιες και τοπικές αγορές[55].

Η *Εξυπηρέτηση του πελάτη μετά την πώληση* αποτελεί μια εξαιρετικά σημαντική δραστηριότητα για μια επιχείρηση. Κάθε επιχείρηση οφείλει να ενημερώνεται μέσω της τεχνολογίας για την αρτιότητα του προϊόντος που αγοράστηκε από τον πελάτη, το βαθμό ικανοποίησής του ή της δυσαρέσκειάς του από το αγαθό ή την επιχείρηση που εξυπηρετήθηκε καθώς και τη συχνότητα χρήσης αυτού. Αυτό μπορεί να επιτευχθεί μέσω Ηλεκτρονικών Μηνυμάτων (E-mail) ή με Fax.

[54] Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001
[55] Διαμαντάκης Π., Η χρήση του διαδικτύου από τις επιχειρήσεις. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2011

Κεφάλαιο 3: Ηλεκτρονικές Συναλλαγές

Η ραγδαία εξάπλωση του Διαδικτύου οδήγησε στην έννοια και την πρακτική του ηλεκτρονικού εμπορίου (e-commerce), το οποίο έχει γίνει πλέον ένα κοινό φαινόμενο στον κόσμο. Τα τελευταία χρόνια, οι παραδοσιακές συναλλαγές έχουν αντικατασταθεί από ηλεκτρονικές συναλλαγές. Για την προστασία και την ασφάλεια των ηλεκτρονικών συναλλαγών, έχουν προταθεί διάφοροι μηχανισμοί ηλεκτρονικών πληρωμών (e-πληρωμή). Η νέα επιχειρηματική πραγματικότητα πλέον βασίζεται στις οικονομικές δομές του διαδικτύου καθώς και σε οργανώσεις και άτομα που απολαμβάνουν την ευκολία αγοράς εμπορευμάτων και υπηρεσιών από όλα τα σημεία του κόσμου[56].

3.1. Ηλεκτρονικές συναλλαγές

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, το ηλεκτρονικό εμπόριο αποτελεί την ηλεκτρονική διαδικασία με την οποία τα άτομα ή οι οργανώσεις πραγματοποιούν μια συναλλαγή, όπως η αγορά, η πώληση ή η μεταβίβαση προϊόντων συναλλάγματος ή υπηρεσιών ή/και πληροφοριών[57]. Με λίγα λόγια, το e-commerce μειώνει αποτελεσματικά την αναγκαιότητα τεράστιων επενδύσεων ή δαπανών σε υλική υποδομή για την ανάπτυξη μιας παγκόσμιας παρουσίας, η οποία έχει οδηγήσει σε επανάσταση του τρόπου που μια επιχείρηση διεξάγει συναλλαγές σε όλο τον κόσμο.

Οι ηλεκτρονικές μεταφορές κεφαλαίων προϋπάρχουν στην ουσία από το 1866 όταν η Western Union μετέδιδε πληροφορίες για τιμές μετοχών μέσω τηλέγραφου. Η Federal Reserve χρησιμοποιεί το Fedwire από το 1972, ένα σύστημα EFT για τη μεταβίβαση χρήματος μεταξύ των τραπεζών της[58]. Από τις αρχές του '70 υπάρχει μια μορφή τραπεζικής όπου οι πελάτες μπορούν να έχουν πρόσβαση σε πληροφορίες του λογαριασμού τους μέσω της χρήσης του τηλεφώνου. Την ίδια περίοδο πραγματοποίησαν την εμφάνισή τους οι αυτόματες μηχανές συναλλαγής (ΑΣΜ). Χρειάστηκαν όμως γύρω στα 15 χρόνια για την αποδοχή και τη χρήση αυτών.

Εκατομμύρια άνθρωποι χρησιμοποιούν χρεωστικές κάρτες στα τερματικά σε σημεία πωλήσεως (point-of-sales terminals, POS). Όλη η ηλεκτρονική οικονομική δραστηριότητα

[56] International Conference on Communication, Management and Information Technology (ICCMIT 2015)
[57] Turban, Efraim, Ephraim McLean and James Wetherbe. Information Technology for Management: Transforming Organizations in the Digital Economy. New York: Wiley & Sons, 2004.
[58] Πολίτης Δ., Ηλεκτρονικές προμήθειες σχεδιασμός και εφαρμογή. Πανεπιστήμιο Πατρών, διπλωματική εργασία, 2011

που αναπτύχθηκε έχει σημάνει την ανάγκη αποστολής πληροφοριών μέσω του διαδικτύου με ασφάλεια. Πρέπει οι διακομιστές που αποθηκεύουν αυτές τις πληροφορίες να είναι ασφαλείς. Παρότι πολλές εταιρείες μπορούν να λάβουν μέτρα για την αποτροπή προβλημάτων ασφαλείας, καμία δεν είναι τέλεια κι άρα η ασφάλεια παραμένει ένα ουσιαστικό ζήτημα[59].

3.2. Μηχανισμοί Ηλεκτρονικών Πληρωμών

Τα τελευταία χρόνια, οι παραδοσιακές συναλλαγές έχουν αντικατασταθεί από ηλεκτρονικές συναλλαγές. Για την προστασία και την ασφάλεια των ηλεκτρονικών συναλλαγών, έχουν προταθεί διάφοροι μηχανισμοί ηλεκτρονικών πληρωμών (e-πληρωμή).

Ένα σύστημα πληρωμής χαρακτηρίζεται από τις αλληλεπιδράσεις μεταξύ των διαφόρων θεμάτων και είναι κατασκευασμένο από έναν αριθμό στοιχείων που περιλαμβάνουν τους συμμετέχοντες του συστήματος, τις υποδομές τους και τα μέσα που επιτρέπουν τη μεταφορά της νομισματικής αξίας μεταξύ των οικονομικών παραγόντων. Έτσι, η εποπτεία και οι εποπτικές λειτουργίες του συστήματος πληρωμών έχουν ως στόχο την ομαλή λειτουργία του ίδιου του συστήματος όσον αφορά την ασφάλεια και την αποδοτικότητα σε σχέση με όλα τα στοιχεία (τα μέρη, τα κανάλια και τα μέσα) απ' τα οποία είναι κατασκευασμένο.

Σε αυτό το πλαίσιο, η ασφάλεια περιλαμβάνει επίσης την ακεραιότητα, που έχει να κάνει με τη νόμιμη χρήση και τη χρήση με νόμιμους σκοπούς. Ο κοινός στόχος των αρχών που ασχολούνται με αυτό το θέμα είναι η προστασία του συστήματος από την κατάχρηση, κακή χρήση και την παράνομη πρόσβαση, όπως συμβαίνει με τις τραπεζικές και χρηματοπιστωτικές επιβλέψεις. Ο τελικός στόχος της εποπτείας του συστήματος πληρωμών είναι να διασφαλίσει τη χρηματοπιστωτική σταθερότητα ολόκληρου του συστήματος.

Σε γενικές γραμμές, η εξέλιξη των μέσων πληρωμής προς μια ισχυρότερη χρήση της νέας τεχνολογικής πληροφορίας και μετάδοσης δεδομένων μπορεί να προσφέρει ενδεχομένως μια σειρά από πλεονεκτήματα. Πρώτα απ' όλα, η καταφυγή σε μέσα πληρωμών που έχουν υψηλή τεχνολογική ένταση συνεπάγεται βελτίωση του επιπέδου και της κατάστασης των παρεχόμενων υπηρεσιών προς τους πελάτες. Στην πραγματικότητα τα καινοτόμα μέσα πληρωμών σε σύγκριση με τα μετρητά και άλλα μέσα σε χαρτί είναι

[59] Πολίτης Δ., Ηλεκτρονικές προμήθειες σχεδιασμός και εφαρμογή. Πανεπιστήμιο Πατρών, διπλωματική εργασία, 2011

λιγότερο εκτεθειμένα σε κινδύνους κλοπής, απώλειας και πλαστογραφίας και η διάδοσή τους προκαλεί μια μείωση του κόστους των συναλλαγών.

Εκτός αυτού, η διαθεσιμότητα των μέσων μεταφοράς κεφαλαίων εγγενώς σχεδιασμένα για την κάλυψη απόστασης, των on-line και σε πραγματικό χρόνο συναλλαγών (e-banking, e-commerce και e-finance) έχει ένα διπλό πλεονέκτημα: από τη μία πλευρά, επιτρέπει στους πελάτες να πληροφορηθούν για επιχειρήσεις που παράγουν αποτελέσματα πέραν από τα εθνικά σύνορα. Από την άλλη πλευρά, ουσιαστικά μειώνει το απόθεμα των χρημάτων που οι άνθρωποι αποταμιεύουν για σκοπούς συναλλαγών και ως εκ τούτου, το κόστος απόκτησης και χρήσης μετρητών, ειδικά όταν το ποσό της συναλλαγής υπερβαίνει ένα συγκεκριμένο όριο διαστάσεων.

Με την ίδια λογική, καινοτόμα μέσα επιτρέπουν στις επιχειρήσεις καθώς και στις εποπτικές αρχές, τη μείωση και την πρόληψη της ακατάλληλης χρήσης του συστήματος και τη μείωση του λειτουργικού κόστους καθορισμένα από τη διοίκηση των μέσων με βάση το χαρτί (συνήθως, μετρητά και επιταγές).

Δυστυχώς, μερικές φορές τα ίδια χαρακτηριστικά μπορεί να κάνουν ένα μέσο πιο επιθυμητό, αποδοτικό και αποτελεσματικό, αλλά και πιο ευάλωτο στην κατάχρηση και την κακή χρήση. Αυτά τα χαρακτηριστικά περιλαμβάνουν την ευκολία της πρόσβασης στο σύστημα, τη συντόμευση του χρόνου εκτέλεσης, τη δυνατότητα διενέργειας συναλλαγών χωρίς άμεση επαφή με τον ομόλογό του, την ύπαρξη ενός καθεστώτος ανωνυμίας και την επακόλουθη απόκρυψη της πραγματικής ταυτότητας των οικονομικών φορέων ότι έχουν πραγματοποιήσει τη συναλλαγή.

Μέχρι σήμερα έχουν αναπτυχθεί διάφορες υπηρεσίες μεταφοράς χρήματος που επιτρέπουν στους χρήστες του διαδικτύου να στέλνουν χρήματα σε άλλους χρήστες, και ιδιώτες και επιχειρήσεις. Αυτές διαχειρίζονται τη μεταφορά χρήματος, και με αυτόν τον τρόπο, ο χρήστης αντί να δίνει τον αριθμό της πιστωτικής του κάρτας σε πολλούς δικτυακούς τόπους, στέλνει τον αριθμό αυτόν μόνο σε μια τοποθεσία. Η πιο γνωστή υπηρεσία μεταφοράς χρήματος είναι η PayPal. Βασικά ο χρήστης καταχωρεί την πιστωτική ή τη χρεωστική κάρτα ή τον τρεχούμενο λογαριασμό στην PayPal. Όταν επιθυμεί την αποστολή χρημάτων μέσω Web, το μόνο που χρειάζεται να κάνει είναι να εισάγει τη διεύθυνση του ηλεκτρονικού ταχυδρομείου του παραλήπτη και το ακριβές ποσό που αποστέλλει. Ο παραλήπτης το λαμβάνει ενημερώνεται ότι η πληρωμή είναι διαθέσιμη. Εν συνεχεία, ο παραλήπτης εγγράφεται στην PayPal κι έτσι πιστώνεται ο λογαριασμός του. Η PayPal εξαγοράστηκε απ’ την εταιρεία e-Bay το 2002.

Πολλοί δικτυακοί τόποι αποδέχονται ως μορφή πληρωμής τις προσωπικές επιταγές[60]. Ο πελάτης εισάγει τον πολυψήφιο αριθμό που βρίσκεται στο κάτω μέρος μιας επιταγής, το ποσό και τον αριθμό επιταγής. Η τράπεζα επεξεργάζεται ηλεκτρονικά την επιταγή ή αυτή τυπώνεται και αποστέλλεται στον πωλητή. Λόγω του γεγονότος ότι μια επιταγή χρησιμοποιείται μόνο μία φορά, δεν ελκύει τόσο τους εγκληματίες.

Ορισμένοι επιθυμούν τη διατήρηση της ανωνυμίας τους όταν ψωνίζουν online. Αυτόν τον σκοπό μπορεί να εξυπηρετήσει ένα ψηφιακό πορτοφόλι (digital wallet) ή μια έξυπνη κάρτα (smart card). Το πρώτο αποτελεί μια εφαρμογή που αποθηκεύει το ηλεκτρονικό νόμισμα και εξασφαλίζει την αξιοπιστία και την ασφάλειά του. Οι χρηματοοικονομικοί οργανισμοί εκδίδουν ηλεκτρονικά μετρητά (e-cash) αντί φυσικών μετρητών. Στην ουσία αποτελούν ψηφιακά δεδομένα που δείχνουν το ίδρυμα έκδοσης και το ποσό. Ασφαλίζονται με τη κρυπτογράφηση. Η έξυπνη κάρτα εφευρέθηκε τη δεκαετία του ’70 στην Ευρώπη και την Ιαπωνία[61], είναι πλαστική, έχει το μέγεθος μιας πιστωτικής κάρτας με ενσωματωμένο τσιπ ολοκληρωμένου κυκλώματος (ICC), που έχει τη δυνατότητα αποθήκευσης μόνο μια μικρής ποσότητα δεδομένων. Οι κανονικές κάρτες μαγνητικής ταινίας διαφέρουν απ’ τις έξυπνες κάρτες στο ότι οι δεύτερες μπορούν να αποθηκεύουν μεγαλύτερες ποσότητες δεδομένων και είναι ασφαλέστερες από τις πρώτες. Επίσης, οι κάρτες μαγνητικής ταινίας αποθηκεύουν μόνο βασικά στοιχεία, ενώ μια έξυπνη κάρτα μπορεί να αποθηκεύσει πιο εκτενείς πληροφορίες.

Σε άρθρο των Yang και Lin, παρατηρείται ότι σε παλαιότερους[62] μηχανισμούς e-πληρωμής ένας κακόβουλος πελάτης μπορεί εύκολα να αρνηθεί μια συναλλαγή και ο έμπορος να μην πληρωθεί. Επιπλέον, εκείνοι οι μηχανισμοί έχουν μεγάλα έξοδα υπολογισμού και επικοινωνίας, ώστε να μην μπορούν να εφαρμοστούν στην κινητή πληρωμή για cloud computing. Για την επίλυση των παραπάνω προβλημάτων, έχει ξεκινήσει να προτείνεται ένας νέος μηχανισμός πληρωμών μέσω κινητού με την ανωνυμία για το cloud computing κι εξακολουθούν να πραγματοποιούνται σχετικές έρευνες.

[60] Πολίτης Δ., Ηλεκτρονικές προμήθειες σχεδιασμός και εφαρμογή. Πανεπιστήμιο Πατρών, διπλωματική εργασία, 2011
[61] Πολίτης Δ., Ηλεκτρονικές προμήθειες σχεδιασμός και εφαρμογή. Πανεπιστήμιο Πατρών, διπλωματική εργασία, 2011
[62] J.-H. Yang, P.-Y. Lin, A mobile payment mechanism with anonymity for cloud computing, The Journal of Systems and Software (2015), http://dx.doi.org/10.1016/j.jss.2015.07.023

3.3. Τρόποι συναλλαγών στα ηλεκτρονικά καταστήματα

Τα συστήματα πληρωμών που υιοθετούνται και συνεχώς εξελίσσονται για τις πληρωμές στο κυβερνοχώρο περιλαμβάνουν συστήματα και τεχνολογίες όπως τις πιστωτικές κάρτες, τις ηλεκτρονικές επιταγές, το ψηφιακό χρήμα, τις έξυπνες κάρτες, τα ηλεκτρονικά πορτοφόλια, την ηλεκτρονική μεταφορά κεφαλαίων (EFT), τις χρεωστικές κάρτες, τις προπληρωμένες κάρτες και τις τρίτες υπηρεσίες πληρωμής. Ένα πολυσυζητημένο θέμα στη συγκεκριμένη περίπτωση αποτελεί και το ψηφιακό νόμισμα Bitcoin, όπου κι αναλύεται ακολούθως.

3.3.1. Συναλλαγή με πιστωτική κάρτα

Σε γενικές γραμμές, το πιο σημαντικό χαρακτηριστικό μιας συναλλαγής πιστωτικών καρτών είναι να μετατρέψει τη σχέση για το εμπόριο από ''πωλητή σε αγοραστή'' σε μια σειρά από συμβατικές σχέσεις. Λόγω της μη ύπαρξης πρόσωπο με πρόσωπο αγοράς, η άδεια και η ασφάλεια θα είναι οι δύο πιο σημαντικές ανησυχίες. Σε μια τέτοια συναλλαγή, μετά από επιβεβαίωση της ταυτότητας του αγοραστή, ο πωλητής λαμβάνει εγγυημένη πληρωμή από την τράπεζα και η αποδέκτρια τράπεζα λαμβάνει επίσης εγγυημένη πληρωμή από τους διεθνείς οργανισμούς. Η τράπεζα έκδοσης κάρτας στη συνέχεια κρίνει την έγκριση της πληρωμής με βάση την ημερομηνία πίστωσης και υπόσχεται να εκπληρώσει την καταβολή στους διεθνείς οργανισμούς. Τέλος, ο κάτοχος της πιστωτικής κάρτας (αγοραστής) είναι υποχρεωμένος να διευθετήσει τα χρήματα με την τράπεζα έκδοσης της κάρτας σύμφωνα με τη σύμβαση της πιστωτικής κάρτας. Αυτή η φαινομενικά περίπλοκη διαδικασία, στην πραγματικότητα σε μεγάλο βαθμό απλοποιεί τις εμπορικές σχέσεις μεταξύ των αγοραστών και των πωλητών, επειδή η χρονική διαφορά μεταξύ του συστήματος πληρωμών και διακανονισμού δεν αποτελεί πλέον πρόβλημα και η ροή των πληροφοριών και των μετρητών χωρίζονται όταν η τράπεζα και η νέα συμβατική σχέση παρέμβουν[63]. Επίσης, η αντίστοιχη ροή πληροφορίας μπορεί να αναγνωριστεί από τον έμπορο αμέσως για να εγκρίνει τη συναλλαγή. Παρά το γεγονός ότι ζητείται από τον πωλητή να πληρώσει γύρω στο 3% των συνολικών συναλλαγών, αυτός ο μηχανισμός μπορεί να αυξήσει σημαντικά τις ευκαιρίες πώλησης.

Εν τω μεταξύ, ο έμπορος έχει αδειοδοτηθεί με ένα μήνυμα για να επιβεβαιώσει αν η συναλλαγή ολοκληρώθηκε και η αδειοδότηση αποτελεί αμεσότητα της ροής πληροφοριών.

[63] CreditCards.com, http://www.creditcards.com/

Όσον αφορά τη ροή μετρητών, για κάθε ημέρα, όλες οι συναλλαγές του δικτύου από διαφορετικές συμμετέχουσες τράπεζες-μέλη υπολογίζονται αργότερα από τις διεθνείς οργανώσεις. Αφού οι τράπεζες που είναι μέλη αναγνωρίζονται κατά την ημερομηνία του εμπορικού δικτύου, θα χρησιμοποιήσουν το ''ακαθάριστο σύστημα διακανονισμού σε πραγματικό χρόνο'' για να μεταφέρουν τα κεφάλαια στους διεθνείς οργανισμούς και οι διεθνείς οργανισμοί μεταφέρουν κεφάλαια προς την τράπεζα έκδοσης της κάρτας. Από αυτή τη στιγμή, μπορεί να ειπωθεί ότι η σημασία του ρόλου της τράπεζας στη διαδικασία αυτή είναι χαμηλότερη, αφού η ροή μετρητών εκτελείται στην πραγματικότητα, μερικές φορές αργότερα, μετά τη ροή των πληροφοριών και η αγορά ολοκληρώνεται μετά την ολοκλήρωση της ροής των πληροφοριών. Αξίζει να σημειωθεί σε αυτό το σημείο ότι η VISA έχει αποδείξει ότι «η πληροφορία του χρήματος μερικές φορές είναι πιο σημαντική από ό,τι το ίδιο το χρήμα!».

3.3.2. Πιστωτικές κάρτες

Οι πιστωτικές κάρτες αποτελούν τον πιο δημοφιλή τρόπο πληρωμής κι απαλλάσσουν τους καταναλωτές από το να έχουν χρήματα πάνω τους. Οι πιστωτικές κάρτες είναι εξαιρετικά πολύπλοκες πράξεις οικονομικών καταστάσεων. Τα εμπλεκόμενα μέρη είναι ο κάτοχος της πιστωτικής κάρτας – καταναλωτής, ο έμπορος, ο εκδότης της κάρτας, ο αποδέκτης, ο φορέας του τίτλου μιας κάρτας (π.χ. MasterCard). Η χρήση τους αντικατοπτρίζει ένα μεγάλο αριθμό από διαφορετικά χαρακτηριστικά και κίνητρα (συναλλαγές, πλεονεκτήματα καταναλωτών, κ.λπ.), περιλαμβάνει μεγάλο εύρος τιμών (επιτόκια, ετήσια τέλη κ.λπ.) και ποσοτικούς περιορισμούς (πιστωτικά όρια, τις ελάχιστες πληρωμές). Αυτά τα χαρακτηριστικά[64] και οι συναφείς υπηρεσίες τους παρέχονται από μια μεγάλη ποικιλία από διάφορους παρόχους καρτών (τράπεζες, μη-τράπεζες, κλπ.). Επιπλέον, επειδή οι αγορές με πιστωτική κάρτα περιλαμβάνουν αποφάσεις από τους καταναλωτές (και όχι από επιχειρήσεις ή αγορές), θέματα της συμπεριφοράς των καταναλωτών και του ορθολογισμού τους παίζουν πολύ πιο σημαντικό ρόλο σε αυτή την αγορά σε σχέση με άλλες αγορές οικονομικών καταστάσεων[65].

Ο χειρισμός των πιστωτικών καρτών μπορεί να γίνει on-line με δυο τρόπους. Ο πρώτος αφορά την αποστολή μη κρυπτογραφημένου αριθμού πιστωτικών καρτών στο

[64] Berlin, M., Mester, L.J., Credit card rates and consumer search. Review of Financial Economics 13, 179–198, 2004

[65] Barry Scholnick, Nadia Massoud, Anthony Saunders, Santiago Carbo-Valverde, Francisco Rodrıguez-Fernandez, The economics of credit cards, debit cards and ATMs: A survey and some new evidence, Journal of Banking & Finance 32 (2008) 1468–1483

Διαδίκτυο, κι ο δεύτερος αφορά την κρυπτογράφηση των στοιχείων της κάρτας πριν την πραγματοποίηση της συναλλαγής. Χωρίς τη χρήση της κρυπτογραφίας είναι πολύ πιθανό το ενδεχόμενο της παρακολούθησης της δικτυακής κυκλοφορίας και η υποκλοπή των στοιχείων του αγοραστή. Για τις ασφαλείς επικοινωνίες στο δίκτυο έχουν αναπτυχθεί διάφορες μέθοδοι, πρότυπα και πρωτόκολλα, εξασφαλίζοντας τόσο την εγκυρότητα όσο και την ασφάλεια των στοιχείων της κάρτας τα οποία θα αναλυθούν πιο κάτω.

3.3.3. Ηλεκτρονικές επιταγές

Το σύστημα των ηλεκτρονικών επιταγών[66] αποτελεί στην ουσία την ηλεκτρονική εφαρμογή του συστήματος των έντυπων επιταγών. Τρία μέρη λαμβάνουν μέρος στην όλη συναλλαγή ενός τυπικού ηλεκτρονικού συστήματος επιταγών, μια τράπεζα, πληρωτές και μια ομάδα δικαιούχων. Αν ένας πληρωτής θέλει να χρησιμοποιήσει ηλεκτρονική επιταγή, πρέπει να εγγράψει τους δικαιούχους στην τράπεζα εκ των προτέρων. Όταν ο πληρωτής αποφασίσει να πληρώσει ένα δικαιούχο για ένα προϊόν, πρέπει να πληρώσει την ηλεκτρονική επιταγή του με την καθορισμένη ονομαστική αξία και στις αναγνωριστικές πληροφορίες του δικαιούχου μέσω του δικτύου. Η έννοια της ηλεκτρονικής επιταγής πρώτο εισήχθηκε από τον Chaum το 1988[67].

Η ηλεκτρονική επιταγή, από άποψη ασφάλειας θεωρείται καλύτερη από την έντυπη επειδή ο αριθμός του λογαριασμού του αποστολέα κωδικοποιείται με το δημόσιο κλειδί της τράπεζας, χωρίς να αποκαλύπτεται στον έμπορο[68]. Τα συστήματα ηλεκτρονικών επιταγών έχουν ως χαρακτηριστικά ασφάλειας την κρυπτογράφηση, την ψηφιακή υπογραφή και τα πιστοποιητικά. Απαιτείται ένα άκρως ασφαλές σύστημα πληρωμής ειδικά για πληρωμές μεγάλων ποσών. Για αυτό, το ηλεκτρονικό καρνέ επιταγών θα πρέπει να είναι ενσωματωμένο στο λογιστικό πληροφοριακό σύστημα των αγοραστών και τον server των πωλητών[69].

[66] Wei-Kuei Chen, Efficient on-line electronic checks, Appl. Math. Comput. 162/ 1259–1263, 2005
[67] D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, in: Advances in Cryptology— CRYPTO'88, LNCS, vol. 403, Springer-Verlag, pp. 319–327, 1990
[68] D. Chaum, B. den Boer, E. van Heyst, S. Mjolsnes, A. Steenbeek, Efficient offline electronic check, in: Advances in Eurocrypt'89, LNCS, vol. 434, Springer-Verlag, pp. 294–301, 1989
[69] EfraimT., JaeL., KingD., ChungM., σ. 295

3.3.4. Ψηφιακό χρήμα (e-cash)

Με τον όρο ψηφιακό χρήμα (e-cash), αναφέρεται κάθε μορφή μεταφοράς χρήματος μεταξύ δύο ή περισσοτέρων μερών που γίνεται χωρίς τη μεσολάβηση κάποιου υλικού μέσου και με ψηφιακό τρόπο. Ένα τυπικό σύστημα ηλεκτρονικών μετρητών (e-cash) περιλαμβάνει τρία μέρη, δηλαδή μια τράπεζα, τους καταναλωτές και τους εμπόρους. Η τράπεζα εκδίδει ‘‘νόμισμα’’, δηλαδή ηλεκτρονικές εγγραφές σε υπολογιστές, που είναι γνωστά ως tokens. Αρχικά, ένας καταναλωτής δημιουργεί ένα λογαριασμό στην τράπεζα. Δεύτερον, ο καταναλωτής υπαναχωρεί το νόμισμα από την τράπεζα. Τρίτον, ο καταναλωτής ξοδεύει το νόμισμά του σε έναν έμπορο με αντάλλαγμα ορισμένα αγαθά και υπηρεσίες. Τέλος, ο έμπορος καταθέτει το νόμισμα στην τράπεζα. Εν ολίγοις, οι αγοραπωλησίες γίνονται με ανταλλαγή των tokens.

Ένα σύστημα e-cash θα πρέπει να ικανοποιεί την ανωνυμία, δηλαδή, ούτε ο έμπορος ούτε η τράπεζα πρέπει να μπορούν να αναγνωρίσουν ή να εντοπίσουν τον καταναλωτή από το e-cash. Κεντρικός πυρήνας αυτής της τεχνολογίας είναι η κρυπτογραφία ασύμμετρου κλειδιού. Τα tokens δηλαδή αποτελούν ένα είδος λογιστικών εγγραφών που επιβεβαιώνονται από την ‘‘εκδοτική αρχή’’ μέσω της κρυπτογραφικής αυτής μεθόδου. Η τράπεζα συνεπώς επικυρώνει το κάθε token με την ψηφιακή της σφραγίδα πριν απ’ τη μετάδοση στον υπολογιστή του καταναλωτή[70]. Άρα η συναλλαγή με ψηφιακά μετρητά, ισοδυναμεί με την ανταλλαγή του κατάλληλου ποσού tokens στον έμπορο, ο οποίος στη συνέχεια τα αναμεταδίδει στην τράπεζα για επικύρωση κι εξαργύρωση.

Ένα σύστημα e-cash μπορεί να υλοποιηθεί με τυφλή υπογραφή[71]. Η τυφλή υπογραφή επιτρέπει σε ένα χρήστη να λάβει υπογραφές από έναν υπογράφοντα σε οποιοδήποτε μήνυμα με τέτοιο τρόπο ώστε ο υπογράφων να μην μαθαίνει τίποτα σχετικά με το μήνυμα το οποίο υπογράφεται. Η τυφλή υπογραφή ικανοποιεί την απαίτηση ανωνυμίας των συστημάτων e-cash. Ωστόσο, υπάρχουν κάποιες ελλείψεις στον πραγματικό κόσμο, αν η τράπεζα εκδίδει το νόμισμα με τη χρήση τυφλής υπογραφής. Από τη μία πλευρά, η τράπεζα πρέπει να χρησιμοποιήσει διαφορετικά δημόσια κλειδιά για διαφορετικές αξίες νομισμάτων των e-cash, δεδομένου ότι η τράπεζα δεν μπορεί να ρυθμίσει την αξία σε κάθε τυφλά εκδιδόμενο νόμισμα. Σαν αποτέλεσμα, οι έμποροι και οι πελάτες πρέπει να φέρουν μια λίστα των δημόσιων κλειδιών στο ηλεκτρονικό τους πορτοφόλι, η οποία είναι συνήθως μια έξυπνη κάρτα της οποίας η μνήμη είναι πολύ

[70] Πασχόπουλος Α. & Σκάλτσας Π. , Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001

[71] D. Chaum, Blind signatures for untraceable payments, in: Advances in Cryptology—CRYPTO’82, Plenum, New York, pp. 199–203, 1983

περιορισμένη. Από την άλλη πλευρά, για την αποφυγή των διπλών δαπανών, η τράπεζα θα πρέπει να κρατήσει μια βάση δεδομένων για την αποθήκευση πληροφοριών προηγουμένων νομισμάτων. Ως αποτέλεσμα, η κλίμακα της βάσης δεδομένων θα αυξηθεί απείρως με την πάροδο του χρόνου. Για να ξεπεραστούν οι ελλείψεις των απλών τυφλών υπογραφών, οι Abe και Fujisaki πρότειναν[72] μια νέα έννοια που ονομάζεται μερικώς τυφλή υπογραφή (PBS). Σε αυτό το σύστημα PBS, ένας υπογράφων μπορεί να περιλαμβάνει ρητά ένα κομμάτι των κοινών πληροφοριών σε μια τυφλή υπογραφή κάτω από κάποια συμφωνία με ένα δέκτη. Αυτή η έννοια είναι μια γενίκευση της τυφλής υπογραφής εφόσον η συνηθισμένη τυφλή υπογραφή είναι μια ειδική περίπτωση του PBS όπου η κοινή πληροφορία είναι μια κενή συμβολοσειρά[73].

Τα ψηφιακό χρήμα στην ουσία παρουσιάζει πλήθος προβλημάτων και επειδή είναι η προβληματικότερη μορφή πληρωμών στο διαδίκτυο γίνονται συνεχώς έρευνες και προτάσεις για αυτού του είδους το σύστημα πληρωμής.

3.3.5. Έξυπνες κάρτες

Οι πρώτες έξυπνες κάρτες (smart cards) προτάθηκαν τη δεκαετία του 1970. Οι πλαστικές κάρτες με μαγνητικές γραμμές χρησιμοποιούνται για την αποθήκευση δεδομένων. Η σημερινή γενιά αυτού του είδους των καρτών περιλαμβάνει μικροτσίπ προσωπικής ταυτότητας με δυνατότητες προγραμματιζόμενων λειτουργιών. Βασικά αποτελούν μικροσκοπικούς υπολογιστές, μεγέθους και φόρμας πιστωτικής κάρτας, όπου είναι ενσωματωμένο ένα ολόκληρο κύκλωμα (chip), στην αριστερή εμπρόσθια πλευρά. Αυτές οι κάρτες μπορούν να χρησιμοποιηθούν για αγορά αγαθών, αποθήκευση πληροφοριών, έλεγχο πρόσβασης σε τραπεζικούς λογαριασμούς, κλπ. Κύριο γνώρισμά τους αποτελεί η αποθήκευση κι επεξεργασία πληροφοριών με ασφαλή τρόπο[74].

Διαθέτουν μικροεπεξεργαστές, μνήμες ROM και RAM κι έχουν μεγαλύτερη μνήμη από τις μαγνητικές κάρτες. Βασίζονται σε αλγορίθμους συμμετρικής κρυπτογράφησης. Αποτελούν εξαιρετικά εργαλεία για πολλά είδη συναλλαγών. Βασικά λειτουργούν ως ηλεκτρονικό πορτοφόλι. Η τεχνολογία των έξυπνων καρτών έχει την ικανότητα να έχει

[72] M. Abe, E. Fujisaki, Howto date blind signatures, in: Advances in Cryptology—ASIACRYPT 1996, in: LNCS, vol. 1163, Springer-Verlag, 1996, pp 244–251

[73] Fagen Li, Mingwu Zhang, Tsuyoshi Takagi, Identity-based partially blind signature in the standard model for electronic cash - Mathematical and Computer Modelling 58 (2013) 196–203, 2012 Elsevier Ltd.

[74] Παπαδοπετράκης Γ., Το ηλεκτρονικό εμπόριο και η εφαρμογή του στις χρηματιστηριακές συναλλαγές. ΑΤΕΙ Κρήτης Πτυχιακή εργασία, 2008

πολλαπλές εφαρμογές οι οποίες συνυπάρχουν σε ένα ενιαίο τσιπ έξυπνων καρτών με ασφαλές κι αξιόπιστο τρόπο[75]. Οι κάρτες με αυτή την ικανότητα περιγράφονται γενικά ως πολλαπλών εφαρμογών έξυπνες κάρτες. Οι προτάσεις για πολλαπλών εφαρμογών έξυπνες κάρτες έγιναν γύρω στο δεύτερο ήμισυ της δεκαετίας του 1990. Η πλειοψηφία των ανεπτυγμένων πλατφορμών των έξυπνων καρτών, όπως το Java Card[76] και το Multos[77] υποστηρίζουν πολλαπλές εφαρμογές. Ωστόσο, ένας μεγάλος αριθμός καρτών που έχει αναπτυχθεί προσφέρουν μόνο μια ενιαία εφαρμογή[78] (π.χ. τραπεζικές υπηρεσίες, τηλεπικοινωνίες, μεταφορές).

Οι πολλαπλών εφαρμογών έξυπνες κάρτες επιτρέπουν σε ένα χρήστη ενδεχομένως να έχει ένα ευρύ σύνολο εφαρμογών στην έξυπνη κάρτα. Η αυξανόμενη τάση σύγκλισης των υπηρεσιών που τροφοδοτείται από την Near Field Communication και τα έξυπνα κινητά (smart phones) έχουν κάνει τις πολλαπλών εφαρμογών έξυπνες κάρτες μια απτή πραγματικότητα. Σε ένα τέτοιο περιβάλλον, πλέον οι κάτοχοι καρτών μπορούν να έχουν μια σειρά από εφαρμογές για τις έξυπνες κάρτες τους και αν μια κάρτα χαθεί, τότε και όλες οι εφαρμογές θα χάνονταν με αυτό. Επιπλέον, οι καταναλωτές μπορεί να θέλουν να αναβαθμίσουν τις έξυπνες κάρτες τους που μπορεί να απαιτούν απρόσκοπτη και ασφαλή μετακίνηση δεδομένων από την παλιά έξυπνη κάρτα στη νέα. Επί του παρόντος, η ανάκτηση μιας έξυπνης κάρτας υπηρεσίας μπορεί να διαρκέσει από μία ημέρα έως μία εβδομάδα στην καλύτερη περίπτωση. Κάθε κάρτα που χάνεται μπορεί να αντικαθίστανται μόνο από τον αντίστοιχο εκδότη της κάρτας, κατά τη διάρκεια της οποίας ο εκδότης μπορεί να μην κάνει αυτή τη δουλειά καθώς δεν είναι σε θέση να έχει πρόσβαση σε κάποιες υπηρεσίες. Ομοίως, δεν υπάρχει προς το παρόν κανένας μηχανισμός μετακίνησης υπηρεσιών που να προτείνεται για τις εφαρμογές της έξυπνης κάρτας. Σε αυτό το θέμα υπάρχουν προτεινόμενα πλαίσια που επιτρέπουν στο χρήστη να αποκτήσει μια νέα έξυπνη κάρτα όπως την επιθυμεί και στη συνέχεια να μετακινεί/ επαναφέρει όλες τις εφαρμογές του σε αυτό, επιτρέποντας έτσι την ανάκτηση από την απώλεια ψηφιακού χαρτοφυλακίου του με ασφάλεια.

[75] K. Mayes, K. Markantonakis (Eds.), Smart Cards, Tokens, Security and Applications, Springer, 2008.
[76] Java Card Platform Specification: Classic Edition; Application Programming Interface, Runtime Environment Specification, Virtual Machine Specification, Connected Edition; Runtime Environment Specification, Java Servlet Specification, Application Programming Interface, Virtual Machine Specification, Sample Structure of Application Modules, May 2009. URL: http://java.sun.com/javacard/3.0.1/specs.jsp.
[77] Multos: The Multos Specification, Online. URL: http://www.multos.com/
[78] R.N. Akram, K. Markantonakis, Smart cards: State-of-the-art to future directions, invited paper, in: C. Douligeris, D. Serpanos (Eds.), IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2013, IEEE Computer Science, Athens, Greece, 2013

3.3.6. Ηλεκτρονική μεταφορά κεφαλαίων (EFT)

Η ηλεκτρονική μεταφορά κεφαλαίων (EFT) έκανε την εμφάνισή της τη δεκαετία του 1970 κι αφορά στην επικοινωνία μεταξύ δυο τραπεζών για τη διεκπεραίωση των δοσοληψιών αναμεταξύ τους. Η επικοινωνία αυτή μπορεί να γίνεται μέσω EDI (ηλεκτρονικής ανταλλαγής δεδομένων) ή άλλων τεχνολογιών. Αποτελεί μια πολύ διαδεδομένη εφαρμογή του ηλεκτρονικού εμπορίου. Κάποιος μπορεί να μεταφέρει ένα χρηματικό ποσό από έναν τραπεζικό λογαριασμό σ' έναν άλλο. Επίσης, δυνατή είναι και η ηλεκτρονική κι αυτόματη κατάθεση χρημάτων σε προσωπικό λογαριασμό. Η σύνδεση ανάμεσα σε κυβερνοτράπεζες με ασφάλεια κατά τη διάρκεια της μεταφοράς είναι υποχρεωτική[79]. Η προστασία επιτυγχάνεται με μεθόδους κρυπτογράφησης. Η χρήση της ηλεκτρονικής μεταφοράς κεφαλαίων προσφέρει ταχύτητα, μειώνει το κόστος συναλλαγής, διευκολύνει τους καταθέτες, προσφέρει 24ωρη εξυπηρέτηση, συμβάλει στην αποφυγή γραφειοκρατίας και στην άμεση παρακολούθηση συναλλαγών.

3.3.7. Χρεωστικές κάρτες

Οι χρεωστικές κάρτες εκδίδονται από τις τράπεζες και λειτουργούν μέσω χρέωσης. Πρόκειται για μια κάρτα που εξουσιοδοτεί την ηλεκτρονική μεταφορά κεφαλαίων on-line. Αποτελεί τρόπο άμεσης πληρωμής, χρησιμοποιώντας τη, το ποσό της αντίστοιχης συναλλαγής αφαιρείται από το τραπεζικό λογαριασμό όψεως ή το ταμιευτήριο του χρήστη αυτομάτως και δε μπορεί να υπερβεί το όριο των διαθέσιμων κεφαλαίων του ανάλογου λογαριασμού.

Το πλεονέκτημα της χρεωστικής κάρτας είναι πως σε περίπτωση κλοπής των στοιχείων της κάρτας το ποσό που δύναται να αφαιρεθεί στην ουσία είναι το ενυπάρχον στο λογαριασμό του πελάτη. Για αυτόν το λόγο συνιστάται τα υπόλοιπα να μην είναι σημαντικά υψηλά. Επιπλέον, είναι εύκολη η απόκτησή τους και η επίδειξη αστυνομικής ταυτότητας δε χρειάζεται, είναι αποδεκτά απ' τους εμπόρους κι ο χρήστης της δε χρειάζεται να έχει πάνω του μετρητά ή επιταγές[80].

[79] Παπαδοπετράκης Γ., Το ηλεκτρονικό εμπόριο και η εφαρμογή του στις χρηματιστηριακές συναλλαγές. ΑΤΕΙ Κρήτης Πτυχιακή εργασία, 2008

[80] Παπαδοπετράκης Γ., (2008), το ηλεκτρονικό εμπόριο και η εφαρμογή του στις χρηματιστηριακές συναλλαγές. ΑΤΕΙ Κρήτης Πτυχιακή εργασία, 2008

3.3.8. Προπληρωμένες κάρτες

Οι προπληρωμένες κάρτες ξεκίνησαν στα μέσα της δεκαετίας του 1990 στις ΗΠΑ και στην Ευρώπη εμφανίστηκαν το 1999. Αρχικά εισήχθησαν ως μια πιο αποδοτική αντικατάσταση των δωροεπιταγών σε χαρτί. Οι προπληρωμένες κάρτες αποτελούν πλέον μια ευρεία κατηγορία πληρωμής που καλύπτει ευρύ φάσμα εφαρμογών[81].

Οι προπληρωμένες κάρτες είναι «πληρωμή εκ των προτέρων» ή «pay as you go» κάρτες, που αποθηκεύουν τα χρήματα, αλλά δε συνδέονται με ένα τραπεζικό λογαριασμό. Σε αυτού του είδους τις κάρτες είναι προεγκατεστημένα τα χρήματα από τον κάτοχο της κάρτας ή η χρηματοδότηση πραγματοποιείται πριν από τη χρήση της κάρτας. Υπάρχουν δύο τύποι προπληρωμένων καρτών: (α) κάρτες ανοικτού βρόχου και (β) κάρτες κλειστού βρόχου. Οι κάρτες κλειστού βρόχου περιορίζονται σε συγκεκριμένους εμπόρους ενώ οι κάρτες ανοικτού βρόχου φέρουν την επωνυμία είτε της VISA, της MasterCard ή της American Express και γίνονται δεκτές σε όλες τις τοποθεσίες, όπως σε καταστήματα λιανικής πώλησης ή ATM εμφανίζοντας το λογότυπο της κάρτας. Μπορεί να συσταθεί για μια ή για εκ νέου χρήση. Οι κλειστού βρόχου κάρτες φέρουν το μεγαλύτερο όγκο των προπληρωμένων καρτών λόγω της έκδοσης μεγάλου αριθμού δωροεπιταγών που χρησιμοποιούνται σε όλο τον κόσμο. Ωστόσο, εφόσον μπορούν να χρησιμοποιηθούν μόνο σε περιορισμένες περιοχές και γενικά εκδίδονται από τα καταστήματα ή τους λιανοπωλητές ως μέρος του μάρκετινγκ τους, οι κάρτες κλειστού βρόχου είναι περιορισμένες όσον αφορά την ευελιξία. Οι κάρτες ανοικτού βρόχου μπορούν να χρησιμοποιηθούν οπουδήποτε και να προσφέρουν πραγματική προστιθέμενη αξία τόσο στον κάτοχο της κάρτας όσο και στον εκδότη.

3.3.9. Άλλες υπηρεσίες πληρωμής

Υπάρχουν υπηρεσίες που λειτουργούν ως εικονικές τράπεζες, δηλαδή ως διαμεσολαβητής ανάμεσα στον αγοραστή και τον πωλητή, διευκολύνοντας τη διεκπεραίωση της συναλλαγής, με ασφάλεια και γνωστοποιώντας μόνο τα απαραίτητα στοιχεία στα αντισυμβαλλόμενα μέρη, ώστε ο πελάτης να μη χρειαστεί να δώσει τα στοιχεία της κάρτας του απ' ευθείας στον πωλητή. Το PayPal αποτελεί έναν εισπρακτικό μηχανισμό που αποστέλλει τα χρήματα μιας συναλλαγής στον πωλητή. Θεωρείται από τα ασφαλέστερα είδη συναλλαγών καθώς η υποκλοπή των στοιχείων της κάρτας είναι

[81] Antoine Laronze Groine, Card Technology Today - Article, June 2009

δύσκολη. Η χρήση της υπηρεσίας PayPal απαιτεί άνοιγμα λογαριασμού, είναι δωρεάν για τον αγοραστή κι έχει μικρό κόστος για τον πωλητή.

Από τα μέσα του 2015 υπάρχει η δυνατότητα αποστολής και λήψης χρημάτων μέσω της εφαρμογής του facebook για συνομιλία, δηλαδή του Messenger. Για τη χρήση αυτής της δυνατότητας, πρέπει να προστεθεί στο λογαριασμό των χρηστών μια χρεωστική κάρτα που πρέπει να έχει εκδοθεί από αμερικανική τράπεζα και να εγκαταστήσουν την πιο πρόσφατη έκδοση της εφαρμογής Messenger. Αφού προστεθεί η χρεωστική κάρτα, μπορεί να οριστεί ένας κωδικός PIN για επιπρόσθετη ασφάλεια κατά την επόμενη αποστολή χρημάτων.

Η εφαρμογή για *αποστολή* χρημάτων είναι πολύ εύκολη. Αποστέλλεται αρχικά μήνυμα στον φίλο, υπάρχει ειδικό εικονίδιο με το σήμα του δολαρίου που το πατάει ο αποστολέας, πληκτρολογεί το ποσό που θέλει και τέλος πατάει πληρωμή και προσθέτει τη χρεωστική κάρτα που θα χρησιμοποιηθεί για την αποστολή των χρημάτων. Για τη *λήψη* χρημάτων ο λήπτης απλά ανοίγει το μήνυμα, πατάει προσθήκη κάρτας στη συζήτηση και προσθέτει τη χρεωστική κάρτα που θα χρησιμοποιηθεί για τη λήψη των χρημάτων.

Με βάση το Facebook, οι οικονομικές απάτες αποτελούν σπάνιο φαινόμενο. Γίνονται μέσω δημιουργίας πλαστών λογαριασμών ή μέσω παραβίασης λογαριασμών. Μέσω των πλαστών ή παραβιασμένων λογαριασμών, οι απατεώνες του διαδικτύου προσπαθούν να πείσουν τους χρήστες να τους στείλουν χρήματα αποστέλλοντάς τους εξατομικευμένα μηνύματα στο Messenger. Για την προστασία των χρηστών είναι δυνατή η υποβολή αναφοράς. Οι πιο συνηθισμένες περιπτώσεις οικονομικής απάτης μέσω του Messenger είναι απάτες μέσω ρομαντικών μηνυμάτων, μέσω λοταρίας, μέσω δωρεάς, μέσω κληρονομιάς, μέσω δανείου[82].

3.3.10. Bitcoin και εικονικά νομίσματα

Τι είναι το Bitcoin

Με βάση τον Simser J.[83] σε αντίθεση με τις συναλλαγές μέσω πιστωτικών καρτών, οι οποίες αφήνουν ένα ψηφιακό ίχνος, οι συναλλαγές Bitcoin[84] έχουν σχεδιαστεί για να είναι

[82] https://www.facebook.com/help/messenger-app/750020781733477/

[83] Jeffrey Simser , "Bitcoin and modern alchemy: in code we trust", Journal of Financial Crime, Vol. 22 Iss 2 pp. 156 – 169, 2015 Permanent link to this document: http://dx.doi.org/10.1108/JFC-11-2013-0067

[84] **Bitcoin**: το λογισμικό ανοιχτού κώδικα που αποτελεί τη βάση του δικτύου
bitcoins: οι μονάδες συναλλαγής πληροφοριών του λογισμικού
Block: Ομάδα συναλλαγών που έχουν υποβληθεί στο δίκτυο για επιβεβαίωση εγκυρότητας
Blockchain: Η αλυσίδα των επιβεβαιωμένων ομάδων συναλλαγών που ξεκινά από την πρώτη, έως την πιο πρόσφατη έγκυρη ομάδα.

ανώνυμη η συναλλαγή και δύσκολη ως προς τον εντοπισμό. Όταν μεταφέρονται Bitcoins σε κάποιον άλλο, είναι σαν να παραδίδεται μία χάρτινη σακούλα γεμάτη με $100 λογαριασμούς σε ένα σκοτεινό σοκάκι. Σίγουρα η κύρια χρήση του Bitcoin μέχρι στιγμής, πλην ως στόχο την κερδοσκοπία (των αγορών), έχει και την πραγματοποίηση ανταλλαγών σε απευθείας σύνδεση αυτών σε σκοτεινό σοκάκι, με τα Bitcoins να χρησιμοποιούνται ιδίως για διαπραγματεύσεις για αγορά ναρκωτικών κι άλλων παράνομων αντικειμένων[85].

Το Bitcoin είναι ένα είδος εικονικού νομίσματος ή αλλιώς αποτελεί ένα ψηφιακό περιουσιακό στοιχείο που βασίζεται σε ένα δίκτυο πληρωμής μεταξύ ομότιμων (peer-to-peer) κι ένα αποκεντρωμένο πρωτόκολλο, προκύπτει από υπολογιστή, είναι βασισμένο στα μαθηματικά κι αποτελεί και κρυπτογραφικό πρωτόκολλο. Είναι ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα. Τα bitcoins μπορούν μεταξύ άλλων να χρησιμοποιηθούν για να αγοράζουν και να πωλούν αγαθά ή υπηρεσίες, ή ως λογιστική μονάδα. Τα Bitcoins μπορούν να μετατραπούν σε εξουσιοδοτημένο νόμισμα, όπως δολάρια ΗΠΑ ή άλλα εθνικά νομίσματα με βάση τις τρέχουσες συναλλαγματικές ισοτιμίες[86]. Από τη σκοπιά του χρήστη, το Bitcoin είναι σαν τα μετρητά χρήματα του Διαδικτύου. Ουσιαστικά χρησιμοποιεί μεθόδους κρυπτογραφίας για τη δημιουργία και διαχείριση των χρημάτων και για την επιβεβαίωση εγκυρότητας συναλλαγών.

Τα μέρη έχουν ένα "κοινό" κλειδί στο σύστημα για την πρόσβαση στο Bitcoin και μπορούν να χρησιμοποιήσουν οποιοδήποτε συνδυασμό για να περιγράψουν δημοσίως τον εαυτό τους. Η τυχαιότητα του δημόσιου κλειδιού μπορεί να προσφέρει ανωνυμία. Οι υποστηρικτές περιγράφουν το Bitcoin ως ένα ζωντανό και εξελισσόμενο σύστημα πληρωμών διαθέτοντας τα μέσα για να διακόψει τα συμβατικά συστήματα. Οι επενδυτές έχουν στρέψει το ενδιαφέρον τους ως προς τις δυνατότητες επένδυσης που διαθέτει[87]. Οι νομοθέτες και οι υπεύθυνοι της ασφάλειας έχουν εγείρει συναγερμούς για το Bitcoin ως το κρυπτο-νόμισμα επιλογής σε βαθιά ιστοσελίδα όπως είναι το Silk Road (μια μαύρη αγορά για τα ναρκωτικά) και η Μαύρη Αγορά (Black Market Reloaded) που προσφέρουν τα πάντα, από παράνομα όπλα σε υπηρεσίες ως και προσφορά αυτών ως προϊόν στους χρήστες[88] τους.

Το πρωτόκολλο και το δίκτυο υπολογιστών που βρίσκονται πίσω από το Bitcoin (το Δίκτυο Bitcoin) δεν παρέχουν στους χρήστες πλήρη ανωνυμία, στην ουσία όλες οι

[85] Krugman, P., "The antisocial network", New York Times, 14 April, 2013
[86] Katten Muchin Rosenman LLP, "Bitcoin: Current US Regulatory Developments," November 26, 2013
[87] Murck, P., "*Bitcoin* a webinar", in *Association of Financial Crime Specialists*, Murck is general counsel to the Bitcoin Foundation, 2013
[88] Cottle, M., *The Government's Perilous Bitcoin Chase*, The Daily Beast, 2013

συναλλαγές με Bitcoin καταγράφονται σε δημόσιους λογαριασμούς του δικτύου Bitcoin (γνωστά ως Blockchain), τα οποία είναι πλήρως διαφανή. Οι χρήστες Bitcoin αναγνωρίζονται στο Blockchain από ένα ή περισσότερα ψευδώνυμα με τη μορφή των «ψηφιακών διευθύνσεων», εκ των οποίων ένας χρήστης μπορεί να έχει πολλές. Χρησιμοποιώντας την υπάρχουσα τεχνολογία και τη στατιστική ανάλυση του Blockchain, είναι δυνατό να παρακολουθείται η δραστηριότητα του δικτύου Bitcoin, περιορίζοντας έτσι την ανωνυμία των χρηστών Bitcoin.

Μέχρι σήμερα, το Bitcoin είναι το πιο σημαντικό εικονικό νόμισμα με τη μεγαλύτερη βάση χρηστών και εμπόρων και την κεφαλαιοποίηση της αγοράς. Τα τεχνικά χαρακτηριστικά του Bitcoin που συνέβαλαν στην σχετικά ταχεία έγκριση περιλαμβάνουν τον ανοιχτό κώδικα του δικτύου Bitcoin, τον αποκεντρωμένο χαρακτήρα και την ικανότητα για γρήγορη επιδιόρθωση τρωτών σημείων ή ελαττωμάτων στο πρωτόκολλο του δικτύου Bitcoin μέσω ενημερώσεων του λογισμικού. Επίσης, κρυπτογραφικά ιδρύθηκε το σύστημα του δικτύου Bitcoin ως απόδειξη επί τω έργο που περικλείει την ασφάλεια και την πιστοποίηση της συναλλαγής για την εξάλειψη της παραποίησης και αποτρέπει τους χρήστες από την προσπάθεια να χρησιμοποιήσουν κατ' επανάληψη πάλι τα ίδια bitcoins κι επιπλέον, η ικανότητα των Bitcoin να διευκολύνουν τις εγχώριες και τις διεθνείς συναλλαγές οποιουδήποτε ποσού με ελάχιστα (ή μηδενικά) παράβολα συναλλαγής και σχεδόν σε πραγματικό χρόνο συναλλαγής συμπεριλαμβάνεται στα παραπάνω χαρακτηριστικά[89].

Υπάρχουν περισσότερα από 600 εικονικά νομίσματα που χρησιμοποιούνται σήμερα, πολλά από τα οποία είναι βασισμένα σε παρόμοια πρωτόκολλα με ή προέρχονται ουσιαστικά από το Bitcoin. Ωστόσο, αυτά τα εναλλακτικά νομίσματα έχουν επιτύχει μόνο ένα κλάσμα της κεφαλαιοποίησης του Bitcoin λόγω της κατάστασης του Bitcoin ως πρωτοπόρου στο χώρο του εικονικού νομίσματος και την ταχεία, ευρεία υιοθέτησή του εξαιτίας της τεχνολογικής φύσης του και του ελάχιστου αρχικού κόστους. Μόνο τα 20 περίπου εναλλακτικά νομίσματα επιτυγχάνουν ημερήσιο όγκο συναλλαγών τουλάχιστον 0,1 τοις εκατό που βιώνουν τα Bitcoin σχετικά με την εικονική αγορά συναλλάγματος, και μόνο περίπου τα 14 έχουν τουλάχιστον 0,1 τοις εκατό της αγοράς κεφαλαιοποίηση του Bitcoin[90].

[89] Katten Muchin Rosenman LLP, "Bitcoin: Current US Regulatory Developments,", 2013
[90] www.Coinmarketcap.com

Το όνειρο του εικονικού νομίσματος

Η ιδέα του ψηφιακού νομίσματος δεν είναι νέα. Το 1982, προτάθηκε ένα σχέδιο για ανώνυμα ηλεκτρονικά μετρητά και στη συνέχεια δημοσιεύτηκαν εκατοντάδες έγγραφα, ιδίως στην κοινότητα της κρυπτογραφίας όπου το Bitcoin έκανε την εμφάνισή του ως όρος για πρώτη φορά[91]. Οι ιδεατές της ελευθερίας έλκονται από την ιδέα ενός ανώνυμου νομίσματος που μπορεί να λειτουργεί εκτός των κλασσικών νομισμάτων. Για παράδειγμα, το e-Gold προσέφερε ένα νόμισμα σε απευθείας σύνδεση που οι υποστηρικτές του πίστευαν ότι ήταν σε μη χρήση λόγω των κοιτασμάτων χρυσού που βρίσκονταν στο Σεντ Κιτς και Νέβις. Όπως και με το Bitcoin, έτσι και οι μεταφορές e-Gold ήταν ανώνυμες και αμετάκλητες. Δυστυχώς για την επιχείρηση, το e-Gold έγινε ένα ελκυστικό όχημα για απατεώνες και φορείς Ponzi[92]. Όταν αυτό το πρόβλημα επισημάνθηκε στην εταιρεία με την επιβολή του νόμου, το e-Gold συνεργάστηκε για την παροχή πληροφοριών σχετικά με τους πιθανούς καταχραστές του συστήματος, όταν εξαργύρωναν τις εκμεταλλεύσεις τους για την απόκτηση πραγματικού νομίσματος. Η συνεργασία αυτή δεν εμπόδισε τις αρχές από τη φόρτωση στην εταιρεία μιας σειράς από αδικήματα ξεπλύματος βρώμικου χρήματος, η οποία είχε ως αποτέλεσμα την ενοχή[93] τους. Ο κρυπτογράφος David Chaum δημιούργησε το E-Cash, αλλά κι αυτό δεν άνθισε λόγω του ότι στηριζόταν στην υπάρχουσα υποδομή της κυβέρνησης και των οικονομικών μεσαζόντων.

Άλλα εικονικά νομίσματα

Από ρυθμιστικής απόψεως, ο καλύτερος τρόπος για τον αναλογισμό της έννοιας του εικονικού χρήματος είναι η εξέταση της σχέσης του με το σταθερό νόμισμα. Για παράδειγμα, το World of Warcraft Gold είναι ένα εικονικό νόμισμα που χρησιμοποιείται σε ένα παιχνίδι στον υπολογιστή. Οι παίκτες μπορούν να αποκτήσουν το "χρυσό" όταν δημιουργούν ένα λογαριασμό ή μπορούν να κερδίσουν το χρυσό κατά τη διάρκεια του παιχνιδιού. Το νόμισμα είναι απαραίτητο να εξελίσσεται μέσα στα διάφορα επίπεδα του παιχνιδιού. Τούτου λεχθέντος, η διαπραγμάτευση του χρυσού στο πραγματικό κόσμο απαγορεύεται αυστηρά σύμφωνα με τους όρους και τις προϋποθέσεις του παιχνιδιού. Το νόμισμα λειτουργεί σε ένα κλειστό σύστημα. Οι πιστώσεις Facebook (Facebook credits) θα

[91] Barber, S., Boyen, X., Shi, E. and Uzun, E. , "Bitter to better – How to make bitcoin a better currency", 2012 available at: http://crypto.standford.edu/ xb/fc12/bitcoin.pdf
[92] Simser, J. , "Recovering the stolen sweets of fraud and corruption", Working Paper Observatario de Economica a Gestao de Fraud, University of Porto, 2013
[93] Condon, S., "Judge spares E-Gold directors jail time posted", 2013 available at: http://news.cnet.com/8301-13578_3-10104677-38.html

μπορούσαν να θεωρηθούν μια άλλη μορφή εικονικού νομίσματος. Οι χρήστες μπορούν να αγοράσουν τις πιστώσεις και με τη σειρά τους να αγοράσουν εικονικά αγαθά με εφαρμογές στην πλατφόρμα του Facebook. Τέλος, το Second Life είναι ένα online παιχνίδι όπου οι παίκτες δημιουργούν είδωλα μέσα σε μια εικονική κοινότητα. Οι παίκτες, μέσω των ειδώλων τους, μπορούν να "ζήσουν" μια ζωή που είναι εντελώς διαφορετική από το πραγματικό κόσμο. Υπάρχει μια αυτοδύναμη οικονομία με το Second Life που χρησιμοποιεί δολάρια Linden ως εικονικό νόμισμα. Τα δολάρια Linden μπορούν να μετατραπούν σε σταθερό νόμισμα, φέροντας ουσιαστικά στην επιφάνεια ζητήματα παρόμοια με εκείνα που τίθενται από το Bitcoin[94].

Η δημιουργία του Bitcoin

Το Bitcoin προτάθηκε για πρώτη φορά στις αρχές του 2009, μέσα από μια ερευνητική εργασία που γράφτηκε από τον «Satoshi Nakamoto» και δημοσιεύτηκε σε κρυπτογραφία[95] listserv[96]. Για τον Nakamoto λίγα πράγματα είναι γνωστά. Το σε απευθείας σύνδεση προφίλ του υποδεικνύει σαν τοποθεσία κατοικίας την Ιαπωνία. Η διεύθυνση του e-mail του όμως ήταν στα γερμανικά. Το όνομα Nakamoto φαίνεται να είναι ψευδώνυμο. Οι δημοσιεύσεις του Nakamoto αφορούσαν σε μεγάλο βαθμό συζητήσεις γύρω από το πηγαίο κώδικα. Οι δεξιότητες της αγγλικής γλώσσας του ήταν άψογες. Στην τελευταία του δημοσίευση, τον Δεκέμβριο του 2010, αποθάρρυνε το WikiLeaks από τη χρήση των Bitcoins για δωρεές, φοβούμενος/η ότι η μικρή «beta κοινότητα» που είχε φτιάξει ήταν «στα σπάργανα» και η «ένταση» που θα ασκούνταν από τις δωρεές θα κατέστρεφε το νόμισμα. Ένας πρώιμος προγραμματιστής Bitcoin παρατήρησε ότι το σύστημα ήταν «πολύ καλά σχεδιασμένο για ένα άτομο ώστε να ξεκινήσει από έναν» και σκέφτηκε ότι ο Nakamoto στην πραγματικότητα ίσως αποτελεί μια κοινοπραξία από προγραμματιστές[97].

Αλχημεία Bitcoin

Το Bitcoin είναι ένα πρωτόκολλο πληρωμών στο Διαδίκτυο που λειτουργεί σαν ένα εικονικό νόμισμα. Το Bitcoin στερείται της φυσικής μορφής και δεν απαιτεί τη διαμεσολάβηση της κυβέρνησης ή ενός ιδιωτικού τρίτου μέρους για το διακανονισμό των

[94] European Central Bank (2012), Virtual Currency Schemes, ECB, Frankfurt.
[95] Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009 available at: http://bitcoin.org/bitcoin.pdf
[96] μια εφαρμογή που διανέμει μηνύματα στους συνδρομητές σε ένα ηλεκτρονικό κατάλογο αλληλογραφίας
[97] Wallace, B., "The rise and fall of bitcoin wired magazine", 2011 available at: www.wired.com/magazine/2011/11/mf_bitcoin/

συναλλαγών. Σε ένα βασικό επίπεδο, ένα Bitcoin είναι απλά ένα ηλεκτρονικό αρχείο, παρόμοιο με ένα τραγούδι ή ένα κομμάτι του κειμένου, το οποίο μπορεί να αποθηκευτεί σε έναν υπολογιστή. Το εικονικό νόμισμα μπορεί να δαπανηθεί με τρόπο παρόμοιο με την αποστολή ενός e-mail σε απευθείας σύνδεση. Οι χρήστες κατεβάζουν ένα λογισμικό ανοιχτού κώδικα και αποθηκεύουν τα Bitcoins, εφόσον αποκτηθούν, σε ένα ψηφιακό πορτοφόλι στον υπολογιστή τους ή στο έξυπνο τηλέφωνό τους. Η λειτουργία του νομίσματος, από τεχνικής απόψεως είναι εξαιρετικά πολύπλοκη.

Το Bitcoin βασίζεται σε ένα καθολικό συναλλαγών ψηφιακής ψευδωνυμίας σε πραγματικό χρόνο που ονομάζεται «Αλυσίδα μπλοκ – block chain», το οποίο διατηρείται δημόσια και συλλογικά από τους χρήστες οι οποίοι ρυθμίζουν και επαληθεύουν μέσω ενός μηχανισμού απόδειξης επί τω έργο και είναι γνωστή ως εξόρυξη. Κάθε ιδιοκτήτης κατέχει δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Για την αγορά ενός Bitcoin, ο αγοραστής στέλνει στον πωλητή το δημόσιο κλειδί του. Ο πωλητής προσθέτει το ιδιωτικό κλειδί του και τα Bitcoins στη συνέχεια μεταφέρονται ηλεκτρονικά μέσω ενός κατακερματισμού των τωρινών και των προηγούμενων συναλλαγών. Το καθολικό του λογαριασμού για Bitcoin είναι κοινό και διανέμεται, περιέχοντας μια ηλεκτρονική ιστορία όλων των συναλλαγών. Μόλις λάβει χώρα η συναλλαγή, αποστέλλεται στο δίκτυο peer-to-peer. Ο δημιουργός του Bitcoin προσδιόρισε την πρόληψη από τη «διπλή δαπάνη» ως το βασικό χαρακτηριστικό του συστήματος. Αν κάποιος μπορούσε να αποκόψει και να επικολλήσει πολλαπλές εκδοχές του ίδιου νομίσματος, τότε σύντομα τα Bitcoins δε θα είχαν καμία αξία.

Η λύση έχει ως ακολούθως. Όταν η συναλλαγή καταχωρείται δημόσια, θα πρέπει να επαληθευτεί. Οι εθελοντές εντός του δικτύου peer-to-peer ελέγχουν τις συναλλαγές και δημιουργούν μια χρονική σήμανση από τον κατακερματισμό τους σε μια συνεχή αλυσίδα κατακερματισμών που βασίζεται στην απόδειξη επί τω έργο, σχηματίζοντας ένα αρχείο που δεν μπορεί να αλλάξει χωρίς την επανάληψη της απόδειξης επί τω έργο[98]. Η χρονική σήμανση γίνεται μέρος της κωδικοποίησης του συγκεκριμένου Bitcoin, που σημαίνει ότι δεν μπορεί να αντιγραφεί ή να περαστεί πάνω από μία φορές.

Η εξόρυξη των Bitcoins

Δεν υπάρχει κάποια κεντρική αρχή εγκατάστασης ή κατάργησης μιας συναλλαγής Bitcoin. Αντίθετα, η καταβολή δικτύου peer-to-peer βασίζεται σε εθελοντές για την

[98] Nakamoto, S. (2009), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: http://bitcoin.org/bitcoin.pd

επαλήθευση της συναλλαγής, μια υπολογιστική διαδικασία που ονομάζεται λεπτομερής εξέταση που απαιτεί χρόνο και υπολογιστική ισχύ. Οι εθελοντές ανταμείβονται για την εξόρυξη τους με Bitcoins κάθε φορά που το σύστημά τους περιηγείται σε πολύπλοκους μαθηματικούς υπολογισμούς που απαιτούνται για την επαλήθευση (τα ποσά που διατίθενται μειώνονται κατά το ήμισυ κάθε τέσσερα χρόνια). Μόλις γίνει η επαλήθευση, η συναλλαγή είναι αμετάκλητη. Η αρχιτεκτονική του συστήματος είναι ευρέως διαδεδομένη, γεγονός που το καθιστά λιγότερο ευάλωτο σε επιθέσεις. Τα λαμβανόμενα μέρη έχουν ως κίνητρο μέσω της εξόρυξης να διατηρούν την ακεραιότητά τους.

Η δύναμη της CPU είναι αφιερωμένη στην επίλυση «μη αναστρέψιμου παζλ κρυπτογράφησης που περιέχει στοιχεία από διάφορες συναλλαγές[99]». Μόλις το παζλ λυθεί, ένα «κλειδί» δημιουργείται μέσω υπολογιστή, μεταδίδεται στο υπόλοιπο δίκτυο και η εν λόγω πράξη μπορεί να πραγματοποιηθεί. Μόλις εκκαθαριστεί η συναλλαγή τότε τίθεται μη αναστρέψιμη. Για την επικύρωση της συναλλαγής γενικά απαιτείται διάρκεια μεταξύ 10 και 60 λεπτών. Για την κινητοποίηση του συστήματος, οι εξορύκτες (miners) λαμβάνουν νομίσματα Bitcoin κι ανταγωνίζονται για να λύσουν το γρίφο. Ο νικητής λαμβάνει Bitcoins. Καθώς ο αριθμός των miners αυξάνεται, το ίδιο γίνεται και με το βαθμό δυσκολίας του κάθε παζλ. Περαιτέρω, η γενναιοδωρία για έναν επιτυχή Miner μειώνεται σταδιακά, έτσι ώστε, θεωρητικά, το προαποφασισμένο όριο των 21 εκατομμυρίων Bitcoins να φτάσει στο 2140 (υποθέτοντας ότι το νόμισμα δεν θα εξαφανιστεί πριν από τότε). Κάθε Bitcoin διαιρείται με έως και οκτώ δεκαδικά ψηφία, έτσι ώστε η διαθέσιμη δυναμική κβαντική πραγματικότητα να είναι αρκετά μεγάλη. Ο Nakamoto εξόρυξε ο ίδιος τα πρώτα 50 Bitcoins στις 3 Ιανουαρίου του 2009, με συνεπαγωγή τη γένεση του μπλοκ.

Αποθήκευση των Bitcoins

Υπάρχουν δύο τρόποι για να κρατήσει κάποιος τα Bitcoins. Μπορούν να αποθηκευτούν σα νόμισμα στο σκληρό δίσκο του υπολογιστή (ή το τηλέφωνο) μέσω e-wallet ή υπάρχει η δυνατότητα εμπιστοσύνης αυτών σε έναν τρίτο πάροχο, όπως το Coinbase, για την αποθήκευση των Bitcoins. Η αποθήκευση των Bitcoins επί προσωπικού υπολογιστή αφήνει ευάλωτο οποιονδήποτε σχετικά με επιθέσεις από hackers, σφάλματα από τον ίδιο το χρήστη και αποτυχίες λειτουργίας σκληρού δίσκου. Οι online υπηρεσίες πορτοφολιού είναι «επιρρεπείς στην ίδια ασφάλεια και σε παγίδες αξιοπιστίας όπως στο

[99] Wallace, B. (2011), "The rise and fall of bitcoin wired magazine", available at: www.wired.com/magazine/2011/11/mf_bitcoin/

ιδιωτικό κομμάτι», αν και ελπίζει κανείς ότι τα πρωτόκολλα κρυπτογράφησης τους καθώς και υποστήριξης αυτών είναι ισχυρότερα[100].

Είναι τα Bitcoin βιώσιμα ως νόμισμα;

Τα χρήματα λειτουργούν ως μέσο ανταλλαγής γιατί οι χρήστες γνωρίζουν, με κάποιο μέτρο αξιοπιστίας, τι μπορεί να κάνει το νόμισμά τους. Ένας αγοραστής στο Παρίσι ξέρει περίπου πόσα ευρώ θα χρειαστεί να δαπανήσει για την αγορά ενός προϊόντος. Πόσα Bitcoins θα πρέπει να διαθέσει όμως για να αγοράσει αυτό το προϊόν; Το νόμισμα Bitcoin διαπραγματευόταν στο Mt. Gox, έναν ιστότοπο που εξελίχθηκε στο αγαπημένο γραφείο συμψηφισμού για τα Bitcoins. Υπήρξε μια ταλάντευση το 2011, όταν η αξία του νομίσματος αυξήθηκε κατακόρυφα, αλλά γενικά τα Bitcoins εξελίχθηκαν σε μια ζώνη συναλλαγών αξίας περίπου US $10. Στη συνέχεια, την άνοιξη του 2013, η αξία του Bitcoin έπεσε απότομα από τα γεγονότα που συνέβησαν στην Κύπρο. Οι καταθέτες τότε έχασαν τμήματα των τραπεζικών λογαριασμών τους για να αποτρέψουν μια μεγαλύτερη κατάρρευση του χρηματοπιστωτικού συστήματός τους. Η αγορά φαινόταν να υποστηρίζει για το Bitcoin ότι αυτό το εικονικό νόμισμα με κάποιο τρόπο ήταν πιο ασφαλές από ότι οι τραπεζικοί λογαριασμοί που αποδείχτηκαν λιγότερο ασφαλείς. Αλλά τον Απρίλιο του 2013, οι τιμές μειώθηκαν από $266 στα $105 την επόμενη μέρα, ανακάμπτοντας στα $180 και έπειτα η αξία έπεσε στα $120. Όπως σημείωσε ένας σχολιαστής, τα χρήματα πρέπει να είναι εύλογα σταθερά σε γενικές γραμμές για να γίνουν αποδεκτά ως μέσο συναλλαγής. Το Bitcoin σημείωσε επίσης ότι δεν ενεργεί ως νόμισμα, αλλά ως ένα απόθεμα dot-com στην ουσία. Όταν αυξάνεται απότομα σε αξία, οι άνθρωποι συσσωρεύουν Bitcoins, όταν όμως πέφτει η αξία αυτών τότε κανείς δεν τα θέλει. Η απουσία μιας κεντρικής τράπεζας να ταιριάζει την προμήθεια των Bitcoins με τη ζήτηση σημαίνει ότι το Bitcoin αποτελεί περισσότερο μια επιχείρηση dot-com από ότι ένα νόμισμα[101]. Το Bitcoin δηλαδή είναι μια νέα ιδέα. Η αυξημένη χρήση των συμβατικών τεχνικών της αγοράς που χρησιμοποιούνται για την σταθεροποίηση των τιμών συναλλάγματος και των τιμών των βασικών εμπορευμάτων, θα μπορούσε να φέρει κάποια σταθερότητα σε μια αγορά η οποία, αυτή τη στιγμή, είναι εξαιρετικά χαμηλής ρευστότητας και ασταθής.

[100] Lee T., "Four reasons you shouldn't buy bitcoins forbes", 2013 available at: www.forbes.com
[101] O'Brien, M., Op Cit note 11, The US Attorneys Office, Southern District of NewYork, Indictments and Supporting Materials in *US v. Liberty Reserve S.A*. et al filed, 2013 and available at www.justice.gov/usao/nys/pressreleases/may13/libertyreserveetaldocuments.php

Bitcoin: αδυναμίες και τρωτά σημεία

Οι ιστότοποι Black Market Reloaded και Silk Road λειτουργούν ως «βαθύς ιστότοποι» ("deep web") γνωστοί ως Tor. Το Tor ήταν αρχικά ένα αρκτικόλεξο για το The Onion Router, ένα open-source λογισμικό που έχει σχεδιαστεί για να επιτρέψει την ανωνυμία σε απευθείας σύνδεση (οι διασυνδέσεις έχουν αλλάξει και το Tor δε χρησιμοποιείται πλέον ως αρκτικόλεξο). Η κίνηση στο Διαδίκτυο δρομολογείται μέσω ενός δωρεάν σε όλο τον κόσμο δικτύου που κρύβει την τοποθεσία του χρήστη από οποιονδήποτε διεξάγει επιτήρηση του δικτύου ή ανάλυση δεδομένων κυκλοφορίας. Καθώς τα δεδομένα διακινούνται μέσω του συστήματος, είναι «δρομολογούμενα σα κρεμμύδι», όπου τα στρώματα της κρυπτογράφησης ουσιαστικά προστίθενται κάθε φορά που κινείται μέσω των διαφόρων αναμεταδόσεων[102].

Το βαθύ διαδίκτυο επιτρέπει σε άτομα, όπως πληροφοριοδότες και πολιτικά αντιφρονούντες, να επικοινωνούν με κάποιο μέτρο ανωνυμίας, αν και η προστασία της ιδιωτικής ζωής του συστήματος δεν είναι άτρωτη. Διαδικτυακές τοποθεσίες, όπως οι Silk Road και Black Market Reloaded, έχουν δημιουργήσει ανώνυμες αγορές, όπου κάθε λογής πράγματα μπορούν να αγοράζονται και να πωλούνται. Μπορεί κανείς να αγοράσει παράνομα ναρκωτικές ουσίες και να πραγματοποιήσει σύμβαση με χάκερς. Το νόμισμα σε αυτήν την σφαίρα είναι το Bitcoin. Τα Bitcoin, όπως και τα μετρητά είναι αμετάκλητα, αν πραγματοποιηθεί μια φορά μια συναλλαγή με Bitcoin κι αυτή επαληθευτεί τότε δεν υπάρχει επιστροφή[103].

Έγκλημα - κλοπή των Bitcoins

Ένα κακόβουλο λογισμικό, δηλαδή ένα λογισμικό υπολογιστών που έχει σχεδιαστεί για να κλέψει το ιδιωτικό κλειδί του ιδιοκτήτη του Bitcoin, έχει χρησιμοποιηθεί για να κλαπεί το νόμισμα. Ερευνητές στην Καλιφόρνια έχουν σημειώσει ότι το κατώτατο όριο αντίμετρου κρυπτογραφίας, όπως ο διαχωρισμός των ιδιωτικών κλειδιών σε τυχαίες μετοχές, και διασπασμένα "υπερ-πορτοφόλια" σε πολλές υπολογιστικές συσκευές μπορούν

[102] π.χ. www.torproject.org
[103] Greenberg, A., *Founder of Drug Site Silk Road Says Boom and Bust won't Kill His Black Market*, Forbes, 2013, available at: www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/

να αντιμετωπίσουν τον κίνδυνο αυτό[104]. Ο κίνδυνος της κλοπής είναι πιθανό να αυξηθεί ανάλογα με την έκταση που το Bitcoin γίνεται πιο διαδεδομένο.

Περιπέτειες - απώλεια Bitcoins

Τα Bitcoins πράγματι αποτελούνται από ένα αρχείο υπολογιστή. Ένας ιδιοκτήτης Bitcoin, ο Stefan Thomas, κατά λάθος διέγραψε δύο αντίγραφα του ηλεκτρονικού πορτοφολιού του και έχασε τον κωδικό πρόσβασης στο τρίτο αντίγραφο που είχε. Σε ένα πολύ σύντομο χρονικό διάστημα, έχασε περίπου 7.000 Bitcoins (αξίας $140.000 το 2011, αξίζοντας πολύ περισσότερο σήμερα[105]. Τα Bitcoins είναι τόσο καλά όσο είναι και ο χρήστης του υπολογιστή σε αυτό. Περαιτέρω, οι υπολογιστές είναι μηχανές που είναι επιρρεπείς στο να αλλάζουν σα συσκευασία κάθε λίγα χρόνια. Υπάρχουν τρίτοι πάροχοι, λίγο περισσότερο αξιόπιστοι από άλλους, οι οποίοι θα βάλουν τα Bitcoin άλλων σε "τράπεζα" για προστασία. Όπως σημειώθηκε παραπάνω, υπάρχουν απατεώνες και hackers οι οποίοι θα κλέψουν με μεγάλη επιθυμία Bitcoin.

Προστασία Προσωπικών Δεδομένων - αποτελεί μια ανώνυμη συναλλαγή;

Μια περιστασιακή σάρωση των blogs και των άρθρων αφήνουν την εντύπωση ότι οι Bitcoin συναλλαγές είναι όλες εντελώς ανώνυμες. Αυτό όμως δεν ισχύει. Κάθε Bitcoin συναλλαγή δημοσιεύεται στο διαδίκτυο, αν και αυτό δεν κάνει δημόσια τη συναλλαγή. Οι χρήστες προσδιορίζονται από μια «ψευδοτυχαία παραγόμενη Bitcoin διεύθυνση» και το επίπεδο της ανωνυμίας εξαρτάται από το χρήστη. Τα Πρωτόκολλα Διαδικτύου (IP) σχετίζονται με κάθε συναλλαγή. Ένας χρήστης μπορεί να επιλέξει μια ανώνυμη διεύθυνση IP, εάν δεν θέλουν η φυσική τους τοποθεσία να εντοπιστεί. Οι χρήστες μπορούν να ενισχύσουν την ανωνυμία μέσα από μια σειρά τεχνικών όπως τη δημιουργία μιας νέας Bitcoin διεύθυνσης για κάθε πληρωμή, και χρησιμοποιώντας τις υπηρεσίες e-wallet τρίτων για την εδραίωση διευθύνσεων.

---

[104] FBI Directorate of Intelligence, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Unlawful Activity*, Wired Magazine, 2012
Barber, S., Boyen, X., Shi, E. and Uzun, E., "Bitter to better – How to make bitcoin a better currency", 2012 available at: http://crypto.standford.edu/_xb/fc12/bitcoin.pdf

[105] Wallace, B. (2011), "The rise and fall of bitcoin wired magazine", available at: www.wired.com/magazine/2011/11/mf_bitcoin/

Ερευνητές στη Γερμανία και την Ελβετία σημείωσαν ότι παρά τη χρήση ψευδώνυμων, υπήρχαν «σοβαρές ανησυχίες όσον αφορά την προστασία της ιδιωτικής ζωής των χρηστών»[106]. Η έρευνα επικεντρώθηκε στη χρήση των Bitcoins για τη στήριξη καθημερινών συναλλαγών σε ένα πανεπιστημιακό περιβάλλον. Οι ερευνητές διαπίστωσαν ότι η γνώση για τους χρήστες Bitcoin μπορεί να συγκεντρωθεί με την αξιοποίηση των ιδιοτήτων του συστήματος και εφαρμόζοντας τεχνικές ομαδοποίησης της συμπεριφοράς αυτών.

Όπως φανερώνει η υπόθεση Liberty Reserve, οι εγκληματίες είναι ανήσυχοι ως προς την ιδιωτική ζωή άλλων. Υπάρχουν προσπάθειες για βελτίωση της ανωνυμίας του συστήματος Bitcoin μέσω της "zerocoin" διαδικασίας[107]. Ένα από τα διαρκή πλεονεκτήματα του συστήματος Bitcoin είναι η προθυμία χρηστών και της κοινότητας προγραμματισμού να βελτιώσουν τον ανοιχτού τύπου κώδικα.

Bitcoin-επονομαζόμενη απάτη

Τον Ιούλιο του 2013, η Επιτροπή Κεφαλαιαγοράς (SEC) χρέωσε ευθύνη απάτης σε έναν άνθρωπο από το Τέξας. Η εταιρεία του έτρεξε ένα σύστημα Ponzi. Ένα σύστημα Ponzi φιλοδοξεί να ανταμείψει τους επενδυτές με υψηλές αποδόσεις, αλλά στην πραγματικότητα χρησιμοποιεί τις "επενδύσεις" των κεφαλαίων που κατέθεταν τα νέα θύματα για να πληρώνουν έγκαιρα τα υπόλοιπα θύματα. Με άλλα λόγια, δεν υπάρχει καμία είδους επένδυση στην πραγματικότητα, με κάθε θύμα να είναι αυτό που καταβάλλει τις αποδόσεις είτε με δικά του χρήματα ή με αυτά των άλλων θυμάτων[108]. Αυτή η περίπτωση της SEC ήταν μια τυπική απάτη. Είχε διατυπωθεί στους επενδυτές ότι θα μπορούσαν να κερδίζουν επτά τοις εκατό την εβδομάδα μέσω της δραστηριότητας Bitcoin αρμπιτράζ και θα μπορούσαν να διεξάγουν συναλλαγές που θα αφορούν το εικονικό νόμισμα. Προωθημένα σε ιστοσελίδες συζήτησης περί Bitcoin ο απατεώνας υποσχόταν φανταστικές αποδόσεις με κίνδυνο που ήταν σχεδόν μηδενικός. Η απάτη απέδωσε 700.000 Bitcoins (αξίας 4.500.000$ βασισμένο σε μέσες τιμές συναλλαγών κι όπου κατά τον χρόνο των επιβαρύνσεων η

[106] Androulaki, E., Karame, G., Roeschlin, M., Scherer, T. and Capkun, S., "Evaluating user privacy in Bitcoin", 2012 available at: http://eprint.iarc.org/2012/596.pdf
[107] Miers, I., Garman, C., Green, M. and Rubin, A., *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, IEEE Symposium on Security and Privacy, 2013 http://zerocoin.org/
[108] Simser, J., "Recovering the stolen sweets of fraud and corruption", Working Paper Observatario de Economica a Gestao de Fraud, University of Porto, 2013

φούσκα σε Bitcoin σήμαινε ότι η αξία υπερέβη τα $60 εκατομμύρια). Το δικαστήριο, κατά την εξέταση των τεχνικών άμυνας, αποφάνθηκε ότι το Bitcoin αποτελεί ένα νόμισμα[109].

Bitcoin - Μηχανισμός Πληρωμής ή Εργαλείο Πρόληψης Απατών

Δεν είναι μυστικό ότι το ηλεκτρονικό εμπόριο είναι ο ταχύτερα αναπτυσσόμενος τομέας λιανικού εμπορίου στην Ευρώπη. Το Κέντρο Retail Research προέβλεψε ότι οι online πωλήσεις στο Ηνωμένο Βασίλειο, τη Γερμανία, τη Γαλλία, τη Σουηδία, την Ολλανδία, την Ιταλία, την Πολωνία και την Ισπανία αναμένεται να αυξηθούν από £ 132.05 δις του 2014 σε £156.67 δις το 2015, φθάνοντας τα αναμενόμενα £ 185.44 δις από το 2016[110].

Δυστυχώς, με την ολοένα και πιο διαδεδομένη αποδοχή των καταναλωτών της αγοράς αγαθών σε απευθείας σύνδεση με τις παραδοσιακές πιστωτικές και χρεωστικές κάρτες, οι απάτες αυξάνονται επίσης με ανησυχητικό ρυθμό. Στην Αγγλία για παράδειγμα, το 85% των online εμπόρων αναμένουν η απάτη είτε να παραμείνει στάσιμη ή να αυξηθεί μέσα στους επόμενους 12 μήνες[111].

Δεν είναι μόνο οι καταναλωτές που υποφέρουν από τη μάστιγα της απάτης. Οι έμποροι είναι κι αυτοί που υποφέρουν λόγω της δυσκολίας της διατήρησης μιας πλήρους διαδρομής ελέγχου για αγαθά ή υπηρεσίες που αγοράστηκαν σε απευθείας σύνδεση. Η χρέωση απάτης (chargeback), επίσης γνωστή ως φιλική απάτη συμβαίνει όταν ένας καταναλωτής πραγματοποιεί μια online αγορά με τη δική τους πιστωτική κάρτα, και στη συνέχεια ζητά χρέωση (chargeback) από την εκδότρια τράπεζα μετά την παραλαβή των αγαθών που αγοράζουν ή των υπηρεσίες που λαμβάνουν. Μόλις εγκριθεί, η χρέωση ακυρώνει την οικονομική συναλλαγή και ο καταναλωτής λαμβάνει την επιστροφή των χρημάτων που δαπανώνται. Όταν συμβεί μια χρέωση, ο έμπορος είναι υπόλογος, ανεξάρτητα από όλα τα μέτρα που μπορεί να έχει λάβει για την επαλήθευση της συναλλαγής.

Η εταιρεία LexisNexis ανέφερε ότι οι έμποροι πληρώνουν μέχρι και $ 2.79 για κάθε $ 1 που χάνεται σε δόλια συναλλαγή[112]. Το πρόβλημα με την απάτη έχει επεκταθεί από το

[109] Securities and Exchange Commission *SEC Charges Texas Man with Running Bitcoin Denominated Ponzi Scheme,* Washington: SEC, 2013
[110] 'Online Retailing: Britain, Europe, US and Canada 2015'. Centre for Retail Research. www.retailresearch.org/onlineretailing.php
[111] 'UK eCommerce Fraud Report'. CyberSource. www.cybersource.com/en-EMEA/products/fraud_management/ukfraudreport2013/
[112] 'LexisNexis True Cost of Fraud Study Says Merchants Are Incurring a $279 Loss For Every $100 of Fraud Losses'. LexisNexis, 2013. www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1379105834100604

γεγονός ότι τα τρέχοντα συστήματα ανίχνευσης της απάτης απέχουν πολύ από το άριστο. Στην πραγματικότητα, η 41η έρευνα της «Παράμετρος» ισχυρίζεται ότι γύρω στα $40 δισεκατομμύρια των πωλήσεων χάνονται ετησίως λόγω ψευδών στοιχείων από τα συστήματα ανίχνευσης απάτης[113] των τρεχόντων εκδοτών.

Πίσω στο 2009 από τον/ την ανώνυμο/η Satoshi Nakamoto, το Bitcoin έχει δει την αξία του να κυμαίνεται εξωφρενικά σε διάφορες αξίες. Ωστόσο, με το Bitcoin να έχει ήδη γίνει αποδεκτό από 60.000 εμπόρους σε παγκόσμιο επίπεδο είναι πιθανώς ασφαλής η υπόθεση ότι το Bitcoin είναι εδώ για να παραμείνει. Οι πληρωμές μέσω Bitcoin πλέον πλήττουν τακτικά 100.000 συναλλαγές ανά ημέρα και δεν παρουσιάζουν κανένα σημάδι επιβράδυνσης[114]. Την Μαύρη Παρασκευή[115] του 2013, οι συνολικές συναλλαγές με Bitcoin υπερέβησαν τα $487 εκατομμύρια, τοποθετώντας το Bitcoin ως το πέμπτο μεγαλύτερο δίκτυο πληρωμών εκείνη την ημέρα, τερματίζοντας μπροστά από το PayPal και ακριβώς πίσω από Visa, MasterCard, Amex και την UnionPay της Κίνας.

Σε έναν κόσμο με τα αντίτιμα (fees) της συναλλαγής μέσω πιστωτικών καρτών να χτυπούν τους εμπόρους κάτω απ' το όριο και οι διασυνοριακές προμήθειες να δημιουργούν φραγμούς στο εμπόριο, το Bitcoin[116] φαίνεται να ξεπερνά τα εμπόδια των συναλλαγών του ψηφιακού νομίσματος και έχει τη δυνατότητα να αλλάξει τον τρόπο που γίνονται οι πληρωμές για τα αγαθά και τις υπηρεσίες σε όλο τον κόσμο. Λαμβάνοντας μια πληρωμή με Bitcoin είναι φθηνότερη για τον πωλητή από την αποδοχή μιας παραδοσιακής μεθόδου κάρτας πληρωμής και δεν υπάρχει κανένας κίνδυνος χρέωσης.

Χάρη σε ένα δημόσιο καθολικό στο οποίο λειτουργεί το Bitcoin, που ονομάζεται blockchain, για πρώτη φορά στην ιστορία, το κοινό/ δημόσιο καθολικό είναι αποτελεσματικά μόνιμο, άφθαρτο και μη αναστρέψιμο, μαζικό εξαντλώντας τις δυνατότητες για απάτη. Το blockchain ελέγχεται με τη συναίνεση της ομάδας, είναι έξυπνα σχεδιασμένο για να ελέγχει την εγκυρότητα των συναλλαγών και να παρέχει μια αδιαμφισβήτητη καταγραφή των γεγονότων.

Το σύστημα είναι στην ουσία, μια συναλλαγή κοινόχρηστης βάσης δεδομένων με όλους τους κόμβους που συμμετέχουν σε ένα σύστημα που βασίζεται στο πρωτόκολλο

[113] Digital Consumers Are Frustrated: TrustInsight Study Reveals 17% of Online Shoppers Have Experienced Credit Card Declines'. 41st Parameter. www.the41.com/buzz/announcements/digital-consumers-are-frustratedtrustinsight-study-reveals-17-percentonline
[114] Number of Transactions Per Day'. https://blockchain.info/charts/ntransactions
[115] Black Friday - Μαύρη Παρασκευή ή Παρασκευή μετά την Ημέρα των Ευχαριστιών στις ΗΠΑ (την τέταρτη Πέμπτη του Νοεμβρίου). Από τις αρχές της δεκαετίας του 2000, έχει θεωρηθεί ως η αρχή της σεζόν για ψώνια των Χριστουγέννων στις ΗΠΑ, και οι περισσότερες μεγάλες επιχειρήσεις λιανικού εμπορίου ανοίγουν πολύ νωρίς και προσφέρουν προώθηση των πωλήσεων.
[116] https://blockchain.info/charts

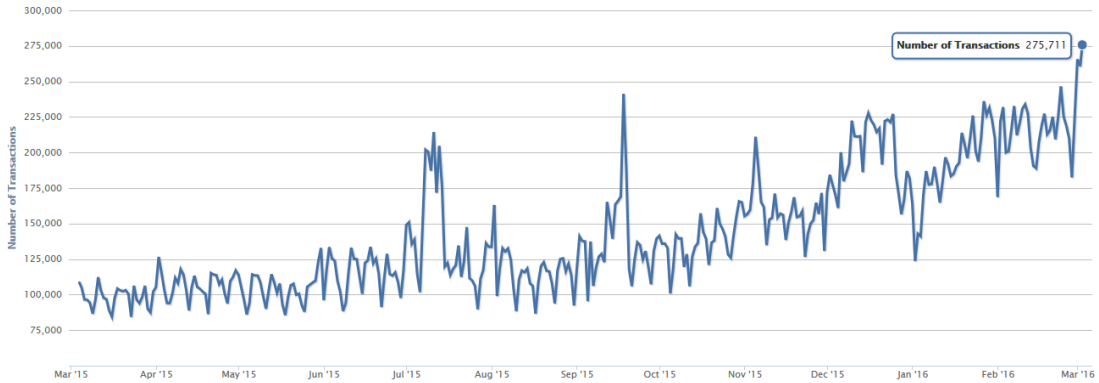
Bitcoin. Ένα πλήρες αντίγραφο του blockchain ενός νομίσματος περιέχει μια διαδρομή ελέγχου κάθε συναλλαγής που εκτελέστηκε ποτέ σε κάθε νόμισμα. Με αυτές τις πληροφορίες, μπορεί κανείς να μάθει πόση αξία ανήκε σε κάθε διεύθυνση (χρήστη) σε οποιοδήποτε σημείο στην ιστορία.

«Έχοντας μικρότερη έκθεση απάτης μπορεί επίσης να επιτρέψει τους εμπόρους να δέχονται τις επιχειρήσεις που μπορεί να έχουν απορριφθεί στο παρελθόν». Το blockchain Bitcoin είναι απλά ένα συγχρονισμένο καθολικό που είναι αποθηκευμένο σε υπολογιστές που συμμετέχουν σε όλο τον κόσμο. Το καθολικό αυτό είναι:

- Προσβάσιμο σε όλους. Καθένας στον κόσμο είναι ελεύθερος να κάνει εγγραφές σε αυτό.
- Κατανεμημένο - αντί συγκεντρωτικό και ελέγχεται δημόσια και όχι από «αξιόπιστους» τρίτους.
- Ασφαλές - όλες οι συναλλαγές που έχουν εισαχθεί στο βιβλίο / καθολικό είναι ουσιαστικά μόνιμες, άφθαρτες και μη αναστρέψιμες.

Κάθε μπλοκ περιέχει ένα hash του προηγούμενου μπλοκ. Αυτό έχει ως αποτέλεσμα τη δημιουργία μιας αλυσίδας των μπλοκ από τη γένεσή του ως το τρέχον μπλοκ. Κάθε μπλοκ είναι εγγυημένα ερχόμενο μετά το προηγούμενο μπλοκ χρονολογικά, διότι το προηγούμενο hash του μπλοκ δε θα μπορούσε διαφορετικά να είναι γνωστό. Κάθε μπλοκ δεν μπορεί να αποτελεί απάτη καθώς δεν μπορεί να τροποποιηθεί μιας και κάποτε υπήρξε στην αλυσίδα, όπως και κάθε επόμενο μπλοκ θα πρέπει επίσης να αναγεννηθεί. Ως εκ τούτου, η αλυσίδα είναι έγκυρη μόνο εάν όλα τα τμήματα και οι συναλλαγές μέσα σε αυτό είναι έγκυρες, και μόνο αν ξεκινά με τη γένεση του μπλοκ.

Γράφημα 3.1: Ημερήσιες Συναλλαγές Bitcoin



Πηγή: https://blockchain.info/charts/n-transactions

Το τέλος της απάτης όπως τη γνωρίζουμε

Οι σε απευθείας σύνδεση επιχειρήσεις που ασχολούνται με τις ολοένα και πιο υψηλές σε όγκο συναλλαγές πληρωμών χρειάζονται μια πλατφόρμα πληρωμών την οποία να μπορούν να εμπιστευθούν και να εξαρτώνται σε αυτό. Το Bitcoin δεν αποτελεί μόνο το ηγετικό ψηφιακό νόμισμα στον κόσμο, αλλά το πρωτόκολλο τεχνολογίας πίσω απ' το Bitcoin λύνει τα προβλήματα που υπάρχουν στο σημερινό οικοσύστημα πληρωμής. Το καθολικό είναι επίσης τόσο ανοικτό δημοσίως και αποδεδειγμένα ασφαλές, εξαλείφοντας σχεδόν την πιθανότητα απάτης. Και η τεχνολογία έχει αμέτρητες πιθανές χρήσεις (από τα οποία μόνο μερικά είναι οικονομικής φύσεως). Για παράδειγμα, οι άμεσα ενδιαφερόμενοι με την καινοτομία εξερευνούν το blockchain ως υπηρεσία μεταβιβάσεων για την ανταλλαγή στοιχείων μεγάλης αξίας, π.χ. μέσω σχεδιαγραμμάτων. Με έναν πελάτη να πληρώνει με bitcoins, ένας έμπορος έχει την εμπιστοσύνη ότι η συναλλαγή θα πραγματοποιηθεί και δε θα υπάρχει κανένας κίνδυνος απάτης - χρέωσης.

Τα Bitcoin σήμερα

Πρόσφατα το Bitstamp, ένα από τα μεγαλύτερα ανταλλακτήρια Bitcoin, ανακοίνωσε ότι θα οι χρήστες θα μπορούν να αγοράζουν Bitcoin με τη χρήση πιστωτικών και χρεωστικών καρτών MasterCard ή Visa. Αρχικά αυτή τη δυνατότητα την είχαν οι κάτοικοι της Σλοβενίας και της Αγγλίας, ενώ τον Ιανουάριο του 2016 ανακοινώθηκε πως και η Ιταλία και η Γερμανία θα εισάγουν αυτό τον τρόπο συναλλαγής[117]. Αυτό το είδος της νέας συναλλαγής, γίνεται κάτω από την επίβλεψη της Καναδέζικης εταιρείας συναλλαγών Vogogo[118]. Οι κάτοχοι MasterCard και Visa των παραπάνω χωρών θα μπορούν να αγοράζουν ημερησίως Bitcoin μόνο αξίας έως 300$ ενώ το εβδομαδιαίο όριο κυμαίνεται στα 1500$.

Επιπλέον, ο μεγαλύτερος επεξεργαστής πληρωμών στη Γαλλία - Lyra Network που επεξεργάζεται πληρωμές ύψους 5,5 δις ευρώ ετησίως κι έχοντας παρουσία σε επτά χώρες ανακοίνωσε πως θα φέρει το Bitcoin σε 35.000 εμπόρους. Ενδέχεται να ακολουθήσει υποστήριξη και για άλλα ψηφιακά νομίσματα. Το Bitcoin είναι ενσωματωμένο σε μια online πλατφόρμα πληρωμών, στην PayZen που τη διαχειρίζεται η εταιρεία. Η κίνηση υποστηρίζεται από μια κορυφαία ευρωπαϊκή υπηρεσία ανταλλαγής Bitcoin, την Paymium,

[117] http://bitcoinx.gr/bitstamp-%CE%B1%CE%B3%CE%BF%CF%81%CE%AC-bitcoin-%CE%BC%CE%B5-%CE%BA%CE%AC%CF%81%CF%84%CE%B5%CF%82/
[118] https://www.vogogo.com/

γαλλική Bitcoin start-up. Επιτρέπει στους πελάτες της να επιλέξουν εάν επιθυμούν να λαμβάνουν απευθείας bitcoins ή να μετατρέψουν αυτομάτως τις πληρωμές με Bitcoin, ολικώς ή μερικώς σε ευρώ.

Το Bitcoin φαίνεται να μην μπορεί να προσεγγίσει όλα τα στρώματα των τάξεων και στην Ελλάδα δεν έχει εφαρμογή σε μεγάλο βαθμό, λόγω, κυρίως της μη ύπαρξης ρευστότητας στις τράπεζες. Επίσης, ένας απλός αστός δεν έχει την δυνατότητα να πληροφορηθεί τόσο καλά για την ψηφιακή εποχή, μιας και αυτό απαιτεί γνώσεις υπολογιστή ή σύνδεσή στο διαδίκτυο, κάτι που δυστυχώς είναι δύσκολο μιας και οι περισσότεροι άνθρωποι πλέον προσπαθούν απλά να επιβιώσουν σε μια εποχή που η κρίση και το θέμα του προσφυγικού βρίσκονται στην επιφάνεια. Επιπροσθέτως, κεφάλαιο επένδυσης επί οποιουδήποτε κρυπτογραφικού νομίσματος είναι ανύπαρκτο. Περαιτέρω, η τιμή των εικονικών νομισμάτων έχει αυξηθεί σημαντικά σε παγκόσμια κλίμακα κι ο κίνδυνος είναι μεγάλος. Αν η απήχηση κάποιου εικονικού νομίσματος μειωθεί είναι πολύ πιθανό η αξία του να μειωθεί σημαντικά και μόνιμα. Εν κατακλείδι, στην χώρα μας φαντάζει απίθανο με τις παρούσες συνθήκες η εξέλιξη αυτού του είδους του νομίσματος.

3.4. Η εξέλιξη της τεχνολογίας της κινητής πληρωμής

Τα τελευταία είκοσι χρόνια αποτελούν ένα διάστημα από πολλές νέες τεχνολογικές εξελίξεις, μεταβαλλόμενες επιχειρηματικές πρακτικές κι ενδιαφέρουσες καινοτομίες στα χρηματοοικονομικά πληροφοριακά συστήματα. Έχουν οδηγήσει στην αυξανόμενη χρήση προηγμένων καινοτομιών που έχουν υποστηρίξει το ηλεκτρονικό εμπόριο και που τώρα τίθενται σε χρηματοπιστωτικές υπηρεσίες για να υποστηρίξουν διαφορετικά είδη βελτιώσεων σε βασικές επιχειρηματικές διεργασίες. Αυτή η έρευνα εξετάζει τις πρόσφατες αλλαγές στον τομέα των πληρωμών, στις χρηματοπιστωτικές υπηρεσίες, που σχετίζονται με τις πληρωμές μέσω κινητού τηλεφώνου (m-payments) που επιτρέπουν την ανάπτυξη νέων διαύλων για τις πληρωμές των καταναλωτών για αγορά προϊόντων και υπηρεσιών, καθώς και άλλες μορφές οικονομικής ανταλλαγής.

Από τη δεκαετία του 1950 και του 1960, οι τράπεζες έχουν καταπιαστεί με σημαντικά προβλήματα που δημιουργούνται από την ταχεία οικονομική ανάπτυξη, η οποία οδήγησε σε αύξηση των δραστηριοτήτων διαμεσολάβησης. Αυτό έχει προκαλέσει υψηλή ζήτηση για τη διαδικασία των πληρωμών και το χειρισμό άλλων χρηματοπιστωτικών μέσων. Στη δεκαετία του 1960 και του 1970, η αυτοματοποίηση των τραπεζικών προϊόντων και διαδικασιών από τους υπολογιστές και τα δίκτυα είχαν μόλις αρχίσει, και

από τότε οι ηλεκτρονικές πληρωμές που πραγματοποιούνται μέσω δικτυακών καρτών πληρωμών και τα συστημάτων ACH[119] έχουν γίνει το επίκεντρο των επιχειρήσεων αυτού του κλάδου. Η αυτοματοποιημένη επεξεργασία των πληρωμών έχει οδηγήσει πολλά κύματα των καινοτομιών προς στον τραπεζικό τομέα και τον τομέα των πληρωμών, οδηγώντας σε βελτιώσεις ως προς την αποδοτικότητα και την αποτελεσματικότητα των συστημάτων πληρωμών. Η εμφάνιση των κινητών πληρωμών (m-payments) έχει προκύψει από την ενσωμάτωση των προκαταβολών σε ανέπαφες πληρωμές, από την ύπαρξη της σε απευθείας σύνδεση (online) και των κινητών (mobile) τραπεζικών συναλλαγών, την εμφάνιση κινητών και έξυπνων τηλεφώνων, από εφαρμογές που βασίζονται στην κινητή τηλεφωνία, και απ' την ψηφιακή σύγκλιση του ηλεκτρονικού εμπορίου με το κινητό εμπόριο[120].

Από την εμφάνιση του πρώτου κινητού εμπορίου και των πρωτοβουλιών της τραπεζικής κινητής συναλλαγής μέσω SMS ξεκίνησαν στη Φινλανδία στα τέλη της δεκαετίας του 1990, έχουν προταθεί πολλές νέες δυνατότητες που επιτρέπουν στους πελάτες τραπεζών να χρησιμοποιούν τα κινητά τους τηλέφωνα για να εκτελέσουν πολλές νέες χρηματοπιστωτικές λειτουργίες (Βλ. Γράφημα). Επίσης, εκείνη την εποχή, οι επιχειρηματίες που βρίσκονταν σε σύνδεση με το Πανεπιστήμιο του Στάνφορντ, συν- ίδρυσαν το Fieldlink, το οποίο υποστήριξε την ψηφιακή κρυπτογράφηση των πληροφοριών σε χειροκίνητες/ κινητές υπολογιστικές συσκευές και δημιούργησαν το Confinity[121]. Αυτές οι νεοφυείς επιχειρήσεις επιδίωξαν να υποστηρίξουν τις μεταφορές χρημάτων σε συσκευές όπως το Palm Pilots, το οποίο οδήγησε στην επέκταση των PayPal και των ψηφιακών πορτοφολιών[122]. Η απόκτηση του PayPal το 2002 ενεργοποίησε περαιτέρω το eBay για να τελειοποιήσει συντομότερα τη διαδικτυακή πλατφόρμα δημοπρασιών του με την υποστήριξη της ψηφιακής ανταλλαγής ηλεκτρονικών πληρωμών. Εν τω μεταξύ, η ανάπτυξη του Alipay στην Κίνα εκτινάχθηκε στα ύψη κατά τη διάρκεια αυτών των ετών,

[119] https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network
Automated Clearing House Network - Το Δίκτυο ACH βρίσκεται στο κέντρο του εμπορίου στις ΗΠΑ, μεταφέροντας χρήματα και πληροφορίες από έναν τραπεζικό λογαριασμό σε άλλο μέσω Απευθείας Καταθέσεων και Άμεσης πληρωμής μέσω των συναλλαγών ACH, συμπεριλαμβανομένων των ACH πιστωτικών και χρεωστικών συναλλαγών, επαναλαμβανόμενων και εφάπαξ πληρωμών, κυβέρνησης, καταναλωτικών και B2B συναλλαγών, διεθνών πληρωμών, καθώς και πληροφοριών που σχετίζονται με πληρωμές. Κάθε χρόνο, διακινεί περισσότερα από $40 τρισεκατομμύρια και σχεδόν 23 δισεκατομμύρια ηλεκτρονικές χρηματοοικονομικές συναλλαγές, και υποστηρίζει σήμερα πάνω από το 90 τοις εκατό της συνολικής αξίας όλων των ηλεκτρονικών πληρωμών στις ΗΠΑ. Ως εκ τούτου, το δίκτυο ACH είναι σήμερα μία από τις μεγαλύτερες, πιο ασφαλή και από τα πιο αξιόπιστα συστήματα πληρωμών στον κόσμο, δημιουργώντας αξία και επιτρέποντας την καινοτομία για όλους τους συμμετέχοντες.
[120] Montgomery, K.C., Testimony on developing the framework for safe and efficient mobile payments. U.S. Senate Hearing, Washington, DC, 2012.
[121] Fried, I., 2002. A building blessed with tech success, Plotkin, H., 1999. Beam me up some cash. HalPlotkin.com
[122] Lillington, K., 1999. PayPal puts dough in your palm. Wired.com, Reuters, 2002. PayPal execs enjoy deja woo-hoo. Wired.com

εξυπηρετώντας τους καταναλωτές μέσω διαδικτυακών τραπεζικών υπηρεσιών και μέσω του ηλεκτρονικού εμπορίου[123].

Οι εξελίξεις στο ηλεκτρονικό χρήμα και η πρώτη γενιά λύσεων ηλεκτρονικού χρήματος θέτουν το στάδιο για ανέπαφες πληρωμές που σήμερα χρησιμοποιούνται ευρέως στην είσπραξη των εισιτηρίων για συστήματα δημόσιων μεταφορών. Οι επιτυχείς εφαρμογές περιλαμβάνουν το σύστημα της κάρτας «Χταπόδι» στο Χονγκ Κονγκ, το ηλεκτρονικό σύστημα έκδοσης εισιτηρίων Oyster στο Λονδίνο, και άλλες καινοτομίες στο ταχέως μεταβαλλόμενο οικοσύστημα πληρωμής στην Ολλανδία. Οι περισσότεροι από αυτούς χρησιμοποιούν την έξυπνη κάρτα FeliCa της Sony στην Ιαπωνία, η οποία όρισε το πρότυπο για το ηλεκτρονικό χρήμα και πληρωμές μέσω κινητού τηλεφώνου. Αργότερα, το PayPass της MasterCard και το PayWave της VISA τυποποίησαν περαιτέρω τις ανέπαφες πληρωμές στα δίκτυα του σημείου πώλησης[124] (POS).

Παρ' όλα αυτά, οι περισσότερες προσφορές χρηματοπιστωτικών υπηρεσιών των αρχών της δεκαετίας του 2000 απέτυχαν να ανταποκριθούν στις προσδοκίες των καταναλωτών και της αγοράς λόγω της περιορισμένης ικανότητάς τους για το χειρισμό των δεδομένων μέσω των δικτύων κινητής τηλεφωνίας[125]. Ο ρυθμός υιοθέτησης τους ήταν χαμηλότερος από ό, τι οι προβλέψεις αντίστοιχων φορέων. Μέχρι το 2006 όμως, οι κατασκευαστές κινητών τηλεφώνων εισήγαγαν τα έξυπνα κινητά τηλέφωνα (smartphones) τα οποία προσφέρουν περιήγηση στο διαδίκτυο και δυνατότητα μεταφοράς δεδομένων. Τα Smartphones διέφεραν ως προς τα χαρακτηριστικά τους από τα παραδοσιακά τηλέφωνα λόγω της καλύτερης χρηστικότητάς τους, τη βελτιωμένη ασφάλεια πληροφοριών, καθώς επίσης και της δυνατότητας αξιοποίησης του κινητού οικοσυστήματος των εφαρμογών. Οι δυνατότητές τους συμπληρώθηκαν από την άφιξη των δικτύων της τρίτης (3G) και της τέταρτης γενιάς (4G) τεχνολογιών τηλεπικοινωνίας και της δυνατότητας πραγματοποίησης αποφάσεων τραπεζικών συναλλαγών (Internet Banking). Όλα αυτά έχουν οδηγήσει τη ζήτηση της αγοράς για πιο προηγμένες υπηρεσίες κινητών πληρωμών.

Το 2007, η υπηρεσία μεταφοράς χρημάτων M-Pesa πρωτο-ξεκίνησε έξω στην Κένυα και σε άλλες αφρικανικές χώρες[126]. Μετά το 2011, προέκυψε ένας αριθμός νέων τεχνολογικών λύσεων για πληρωμές μέσω κινητών. Επί του παρόντος, η υποδομή για

[123] Heggestuen, J., Alipay overtakes PayPal as the largest mobile payments platform in the world. Business Insider, 2014
[124] BusinessWire, New VISA PayWave issuers and merchants sign up for faster, more convenient payments, 2007 - Stevens, S., PayPass and PayWave pave the way for Apple Pay on your smartphone, 2014
[125] Montgomery, K.C., Testimony on developing the framework for safe and efficient mobile payments. U.S. Senate Hearing, Washington, DC, 2012
[126] Graebner, C., Ten days in Kenya with no cash, only a phone. Bloomberg Businessweek, 2014

ασφαλή και αποδοτικά συστήματα κινητών πληρωμών βασίζεται σε μεγάλο βαθμό στην ανέπαφη τεχνολογία[127] NFC. Αυτό περιλαμβάνεται πλέον στα smartphones και τα τερματικά των εμπόρων και έχει γίνει διαθέσιμο από το Softcard Πορτοφόλι της Google και το Apple Pay[128]. Οι πληρωμές μέσω κινητών λόγω Cloud αποτελούν μια άλλη τεχνολογική λύση, με τις πιστοποιήσεις πληρωμών να αποθηκεύονται σε έναν ασφαλές σύννεφο διακομιστή (cloud server). Λύσεις όπως το PayPal App και το Alipay Mobile App είναι καλές στη μείωση ανησυχιών για την ασφάλεια των πελατών, και εκμεταλλεύονται την υφιστάμενη online πλατφόρμα πληρωμών για την επίτευξη αποτελεσματικότερου δικτύου και για διαλειτουργικότητα[129]. Υπάρχουν και άλλα καινοτόμα συστήματα που χρησιμοποιούν εφαρμογές τρίτων για διάφορες πλατφόρμες smartphone ή γρήγορη ανταπόκριση (QR-codes) για να κάνουν το ρόλο που παίζουν οι τράπεζες στις πληρωμές με κάρτα πιο κεντρικό[130]. Ουσιαστικά ωθούνται έτσι και οι μικροί έμποροι να δημιουργήσουν «τραπεζικό λογαριασμό» για την επεξεργασία πληρωμών μέσω κάρτας που σε διαφορετική περίπτωση δεν θα είχαν κάνει τέτοια ενέργεια[131].

[127] Eldridge, A., Is NFC the future of safe credit card processing? Business 2 Community, 2014
[128] Kharif, O., 2011. AT&T-Verizon-T Mobile sets $100 million for Google fight: tech. Businessweek. August 29 - Warren, C., 2011. Google reveals mobile payment system: Google Wallet. Mashable,
May 26 - Turner, A., 2014. Apple Pay gives tap-and-go a much-needed shove. Sydney Morning Herald, September 10.
[129] Jesdanun A., Apple Pay, Google Wallet, PayPal: pros and cons of mobile payment system, 2014
[130] Lunden, I., Ahead of PayPal and Square, Intuit rolls out mobile payments in Europe, starting first in the UK. Techcrunch, 2013
[131] Wilhelm A., Putting Square's $5B valuation into context. TechCrunch, 2014

Γράφημα 3.2: Οπτικό χρονοδιάγραμμα της εξέλιξης της τεχνολογίας πληρωμής μέσω κινητών και σχετικές τεχνολογικές καινοτομίες.

Πηγή: Jun Liu, Robert J. Kauffman, Dan Ma, Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem, Electronic Commerce Research and Applications 14 (2015) 372–391

Κεφάλαιο 4: Ασφάλεια στο Ηλεκτρονικό Εμπόριο

Η τέχνη του πολέμου μας διδάσκει να μη βασιζόμαστε στην πιθανότητα να μην έρθει ο εχθρός αλλά στη δική μας ετοιμότητα να τον υποδεχτούμε. Όχι στην πιθανότητα να μην επιτεθεί, αλλά καλύτερα στο γεγονός ότι έχουμε κάνει τη θέση μας απρόσβλητη.

- Η τέχνη του πολέμου, Sun Tzu

Ο αγγλικός όρος "security", είναι λατινικής προέλευσης και προέρχεται από τις λέξεις "se" και "cura" που σημαίνουν "χωρίς" και "φροντίδα" αντίστοιχα. Η ερμηνεία δηλαδή της ασφάλειας έχει να κάνει με μία επιθυμητή ιδιότητα ενός συστήματος, κατά την οποία οι χρήστες του απαλλάσσονται κάθε έγνοιας σχετικά με τη σωστή λειτουργία αυτού. Η ανάπτυξη του διαδικτύου κι εν συνεχεία του ηλεκτρονικού εμπορίου και των συναλλαγών μέσω δικτύων κάνουν την ανάγκη ασφάλειας περί συναλλαγών επιτακτική. Στην παρούσα εργασία αναφέρονται οι κίνδυνοι που πηγάζουν απ' την απρόσωπη διεξαγωγή συναλλαγών ηλεκτρονικού εμπορίου[132].

Επιπλέον, αναφέρονται οι τρόποι με τους οποίους κάποιος μπορεί να προφυλαχθεί από αυτές τις απειλές, όπως είναι η κρυπτογράφηση, οι ψηφιακές υπογραφές, τα ψηφιακά πιστοποιητικά και η χρήση πρωτοκόλλων όπως το SSL και το SET. Τα τελευταία ειδικά είναι ιδιαίτερα χρήσιμα στην πραγματοποίηση ηλεκτρονικών πληρωμών. Για να ενισχυθεί η ασφάλεια των online αγορών έχουν γίνει κι άλλες προτάσεις, όπως αυτή της δημιουργίας ασφαλούς συστήματος κινητού εμπορίου. Τέλος, γίνεται μία αναφορά στα Firewalls. Σκοπός του κεφαλαίου είναι να προσφέρει μια συνοπτική εικόνα σχετικά με την Ασφάλεια στο Ηλεκτρονικό Εμπόριο.

Οι ανησυχίες που προκαλεί η ασφάλεια στο ηλεκτρονικό εμπόριο μπορούν να καταταχθούν σε δυο κατηγορίες που αφορούν προβληματισμούς αναφορικά με: (α) την εξουσιοδότηση του χρήστη και (β) την ασφάλεια των στοιχείων και της διαδικασίας της συναλλαγής. Για την εξασφάλιση αυτών θα πρέπει να λαμβάνονται μέτρα που θα διασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα των δεδομένων καθώς και την αδιάλειπτη λειτουργία του υπολογιστικού συστήματος[133].

[132] Ανδρέου Πέτρος, Πέππα Ηλέκτρα, Παπακωνσταντίνου Κωνσταντίνα, "Ηλεκτρονικό Εμπόριο (e-commerce)", Πανεπιστήμιο Αιγαίου, 2002.
[133] Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.16)

Για την ύπαρξη ασφάλειας στις συναλλαγές υποχρεωτική είναι η παρουσία ενός ασφαλούς web server. Αυτός χρησιμοποιείται για την απόκρυψη δεδομένων μεταξύ server και browser. Τα δεδομένα κρυπτογραφούνται ως προς και τις δύο κατευθύνσεις, για να μην μπορέσει να υπάρξει παρακολούθηση κατά τη μεταφορά τους στο διαδίκτυο[134].

Λόγω της κρυπτογράφησης κι αποκρυπτογράφησης που απαιτείται να γίνει στα δεδομένα, η πρόσβαση μέσω ενός ασφαλούς server είναι αρκετά πιο αργή σε σχέση με τη σύνδεση από έναν κοινό server. Αυτή είναι και η αιτία που η επιλογή της χρήσης ασφαλούς web server πρέπει να γίνεται όταν πρόκειται για την προστασία ευαίσθητων δεδομένων.

4.1. Στόχοι Ασφάλειας στο Ηλεκτρονικό Εμπόριο

Οι κύριες υπηρεσίες που συνθέτουν ένα ασφαλές πλαίσιο εργασίας χωρίζονται στα παρακάτω θέματα[135]:

- *Έλεγχος αυθεντικότητας (authentication)*: Αποτελεί μια διαδικασία που αποσκοπεί στην εξακρίβωση της ταυτότητας του χρήστη με κωδικούς πρόσβασης (passwords) ή με προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers - PIN's) και διάφορα άλλα. Ο έλεγχος του χρήστη πραγματοποιείται πριν την έναρξη οποιασδήποτε συναλλαγής κι υλοποιείται με τη χρήση των παραπάνω καθώς κι άλλων τεχνολογιών όπως είναι οι ψηφιακές υπογραφές και τα πιστοποιητικά[136].
- *Εξουσιοδότηση (authorization):* Αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στο χρήστη. Ουσιαστικά περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες κι υπηρεσίες όταν έχει εξακριβωθεί η ταυτότητα του χρήστη. Αποτελείται από μηχανισμούς ελέγχου πρόσβασης, δικτυακούς πόρους και δικαιώματα πρόσβασης.
- *Εμπιστευτικότητα (confidentiality):* Είναι σχετική με τη διασφάλιση της προσπελασιμότητας της πληροφορίας μόνο από όσους έχουν τα απαραίτητα δικαιώματα, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Άλλες εκφάνσεις της εμπιστευτικότητας είναι η ιδιωτικότητα (privacy) που έχει να κάνει

[134] N. Kolokotronis C. Margaritis P. Papadopoulou P. Kanellis D. Martakos, "An integrated approach for securing electronic transactions over the Web", Benchmarking: An International Journal, 2002, Vol. 9 Iss 2 pp. 166- 181 Permanent link to this document: http://dx.doi.org/10.1108/14635770210421836

[135] Δουκίδης Γ. και Φραιδάκη Κ, Καταγραφή του Ηλεκτρονικού Εμπορίου Β-C στην Ελλάδα: Αντιλήψεις και συμπεριφορά των online καταναλωτών, Εργαστήριο Ηλεκτρονικού Εμπορίου (ELTRUN), 2010

[136] Τσακαλίδης Α, Δρ Συρμακέσης Σ, Δρ.Τσώλης, Παν. Πατρών, Τμ Μηχ. Η/Υ e-εμπόριο e-επιχειρήν, http://www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf http://nemis.cti.gr/ebusiness/distance_course.htm

με την προστασία δεδομένων που αφορούν συγκεκριμένα πρόσωπα και η μυστικότητα (secrecy) μέσω της ποίας υπονοείται προστασία δεδομένων που ανήκουν σε έναν οργανισμό.

- *Ακεραιότητα (integrity):* Αφορά τη διαφύλαξη της ακρίβειας και πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας της. Στην ουσία εξασφαλίζει ότι δε θα υπάρξει αλλοίωση κατά την μεταφορά των δεδομένων ή στην περίπτωση που αλλοιωθούν, αυτό θα γίνει αντιληπτό από τις συναλλασσόμενες πλευρές και θα προβούν στις απαιτούμενες ενέργειες. Είναι ανεξάρτητη όλων των άλλων παραμέτρων ασφαλείας. Με δυο λόγια σημαίνει πως η μετατροπή, διαγραφή, δημιουργία δεδομένων γίνεται μόνο από μέρη εξουσιοδοτημένα.
- *Διαθεσιμότητα (availability):* Έχει να κάνει με την ιδιότητα της προσπελασιμότητας και τη χωρίς αδικαιολόγητη καθυστέρηση παροχής υπηρεσιών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Επομένως, οι χρήστες που είναι εξουσιοδοτημένοι για πρόσβαση, δεν πρέπει να έχουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν θέλουν να προσπελάσουν τους πόρους του συστήματος.
- *Μη αποποίηση της ευθύνης (non – repudiation):* Έχει να κάνει με την ολοκλήρωση της συναλλαγής, όπου κανένα από τα συναλλασσόμενα μέρη δε μπορεί να ισχυρισθεί ότι δεν συμμετείχε σε αυτήν[137].

Ο παγκόσμιος ιστός φέρει πολλούς κινδύνους. Ο φυλλομετρητής ιστοσελίδων (browser) είναι το κατάλληλο μέσο για την αυτόματη εκτέλεση προγραμμάτων δίχως τη γνώση του χρήστη, δηλαδή επιθέσεις Δούρειου Ίππου (Trojan Horse attack). Οι πιο τυπικές απειλές ασφάλειας στο διαδίκτυο περιλαμβάνουν, πρώτον *βλάβες συστατικών μερών* οι οποίες αναφέρονται σε ελαττωματικά μέρη λογισμικού που προκαλούν συνήθως δυσλειτουργία στο σύστημα κι οδηγούν σε άρνηση εξυπηρέτησης ή άλλες παρόμοιες καταστάσεις. Άλλη απειλή αφορά σε *αποκάλυψη ευαίσθητων πληροφοριών* σε χρήστες μη εξουσιοδοτημένους οι οποίοι επιχειρούν προσπέλαση σε πληροφορίες των νόμιμων χρηστών οδηγώντας έτσι στην απώλεια εμπιστευτικότητας. Τρίτον, *η μη εξουσιοδοτημένη διαγραφή, μεταβολή ή εισαγωγή πληροφοριών* προκαλώντας ζημία στα πληροφοριακά συστήματα μπορεί να οδηγήσει σε απώλεια ακεραιότητας. Επιπλέον, μπορεί να υπάρξει *κατάχρηση*, δηλαδή η χρήση πόρων για διαφορετικούς σκοπούς από αυτούς που έχουν προκαθοριστεί προκαλώντας πάλι διαφόρων ειδών ζημίες, όπως αύξηση κόστους λειτουργίας, άρνηση εξυπηρέτησης και δυσφήμιση των οργανισμών. Πέμπτον, η *διείσδυση*

[137] Τσακαλίδης Α, Δρ Συρμακέσης Σ, Δρ.Τσώλης, Παν. Πατρών, Τμ Μηχ. Η/Υ e-εμπόριο e-επιχειρήν, http://www.aegean.gr/culturaltec/dgavalas/ECommerce/slides/E-C_2005_04.pdf
http://www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf

που αφορά στην πρόκληση άρνησης εξυπηρέτησης και στην απαίτηση σημαντικών χρηματικών ποσών από εισβολείς για την αντιμετώπιση των παρενοχλήσεων ανήκει στις απειλές ασφάλειας. Τέλος, η *διαστρέβλωση* αποτελεί άλλη μια είδους απειλή που σχετίζεται με τις προσπάθειες χρηστών που παρανομούν, να μεταμφιέζονται σε εξουσιοδοτημένους χρήστες και εκμεταλλεύονται πληροφορίες κι υπηρεσίες φέροντας σε δυσχερή θέση πρόσωπα προκαλώντας τους υλικές και μη ζημίες[138].

Διαδικτυακά, η παρέμβαση στην επικοινωνία δυο νόμιμων μερών μπορεί να προκύψει μέσω των εξής τριών τρόπων. Η πρώτη είναι γνωστή ως *υποκλοπή* (eavesdropping) κι έχει να κάνει με πληροφορίες οι οποίες ναι μεν δεν χρησιμοποιούνται, αλλά υπάρχει παραβίαση εμπιστευτικότητας. Δεύτερον, μέσω της *παραποίησης* (tampering), όπου οι πληροφορίες τροποποιούνται ή μεταβάλλονται κατά τη μεταφορά τους και τρίτον, μέσω της *πλαστοπροσωπίας* (impersonation) όπου οι πληροφορίες χρησιμοποιούνται από πρόσωπο το οποίο παριστάνει το νόμιμο εκπρόσωπο. Αυτός ο όρος χρησιμοποιείται κι εναλλακτικά του όρου *προσποίηση* (spoofing) όπου κάποιος επιχειρεί να φανεί σαν κάποιος άλλος σε μια δεδομένη κατάσταση. Όταν η αναφορά γίνεται σε επίπεδο οργανισμού, τότε στη θέση του όρου πλαστοπροσωπία χρησιμοποιείται ο όρος *παραπλάνηση* (misrepresentation).

4.2. Βασικοί χειρισμοί ασφάλειας στο διαδίκτυο

Οι χειρισμοί ασφάλειας (security controls) στο διαδίκτυο, οι οποίες στην ουσία σχετίζονται με διαφόρων ειδών τεχνικές που μπορούν να εφαρμοστούν έτσι ώστε να γίνει επιτυχής η ασφάλεια όσων πληροφοριών μεταδίδονται διαδικτυακά, κινούνται σε τέσσερις κύριες κατευθύνσεις.

Η πρώτη αφορά την *προστασία της εμπιστευτικότητας δεδομένων* (data confidentiality) στην οποία η τεχνολογία της κρυπτογράφησης (encryption/ cryptography) αποτελεί το κλειδί. Η ύπαρξη μηνυμάτων από μόνη της καθιστά αναγκαία την προστασία της διακίνησης δεδομένων στο διαδίκτυο κι άρα η εμπιστευτικότητα ροής δεδομένων είναι απαραίτητη. Η πιθανότητα διαρροής πληροφοριών είναι μεγαλύτερη στην περίπτωση που ένας εισβολέας έχει δημιουργήσει κρυφό κανάλι (covert channel) από όπου απλά με την καταγραφή των bits μπορεί να εξαγάγει συμπεράσματα σχετικά με αυτά που παρακολουθεί. Πιο συγκεκριμένα, οι επιθέσεις αυτές πραγματοποιούνται μέσω ανάλυσης

[138] Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.181)

κίνησης (traffic analysis) κι εξαλείφονται ιδίως με δυο μεθόδους ελέγχου κίνησης δικτύου, τις παρεμβολές στην κίνηση (traffic pad) και τον έλεγχο δρομολόγησης (routing control). Στην πρώτη περίπτωση, ο διαχειριστή ασφάλειας εισάγει πλαστά μηνύματα με σκοπό τη συγκάλυψη πραγματικών πληροφοριών και ποσοτήτων της κυκλοφορίας αυτών. Στην άλλη περίπτωση, ο διαχειριστής επεμβαίνει ενεργά στην κυκλοφορία, καθυστερώντας πακέτα δεδομένων, αλλάζοντας τους ενδιάμεσους κόμβους επίσκεψης ή και σβήνοντας μερικά από αυτά.

Η δεύτερη τεχνική αφορά στην *προστασία μεταξύ των συμμετεχόντων μερών*, δηλαδή την ακεραιότητα (data integrity) των αποστελλόμενων δεδομένων καθώς και την επίλυση της αδυναμίας απάρνησης ενεργειών (non repudiation). Για την προστασία της ακεραιότητας χρησιμοποιούνται και μηχανισμοί δημιουργίας συνοψίσεων μηνυμάτων και ψηφιακών υπογραφών. Για την αδυναμία απάρνησης χρησιμοποιούνται οι προαναφερθέντες μηχανισμοί μαζί με υποδομές υποστήριξης και διακίνησης ψηφιακών πιστοποιητικών (X.509 certificates). Ως τρίτα έμπιστα μέρη (Trusted Third Parties – TTPs), οι Αρχές Πιστοποίησης (Certification Authorities) δημιουργούν βασικά την απαραίτητη εμπιστοσύνη μεταξύ των συμμετεχόντων μερών.

Ο τρίτος χειρισμός ασφάλειας αφορά στον *έλεγχο της ταυτότητας των χρηστών* (identification and authentication), των προγραμμάτων και των εξουσιοδοτήσεων με χρήση συνθηματικών και ψηφιακών πιστοποιητικών. Οι πληροφορίες ουσιαστικά διακινούνται κρυπτογραφημένες κι ο έλεγχος αφορά πρώτον, την *ταυτότητα των χρηστών* (user or entity authentication) που συμβαίνει στην αρχή της τοπικής σύνδεσης και οι μηχανισμοί του ονομάζονται πρωτόκολλα αυθεντικοποίησης και δεύτερον, την *ταυτότητα των συστημάτων ως πηγές προέλευσης μηνυμάτων* [139](origin authentication). Αυτή η λειτουργία στηρίζεται στους μηχανισμούς ψηφιακών υπογραφών – πιστοποιητικών κι αξιοποίησης έμπιστων τρίτων μερών.

Τέλος, γίνεται αναφορά σε κατευθύνσεις ελέγχου προσπέλασης (access control) κι εξουσιοδοτήσεις (authorizations). Χρησιμοποιούνται διάφοροι μηχανισμοί για το περιορισμό στην προσπέλαση των πόρων που υποστηρίζουν πολιτικές ασφάλειας οι οποίες παρέχουν μια πολλαπλών επιπέδων προσπέλαση στους χρήστες ανάλογα με το επίπεδο εμπιστοσύνης που μπορούν να τεκμηριώσουν. Η ασφάλεια του ελέγχου πρόσβασης μπορεί να εφαρμοστεί με διάφορους τρόπους, όπως είναι οι ψηφιακές υπογραφές , τα συνθηματικά, τα firewalls.

[139] Εναλλακτικά ο όρος αυτής είναι γνωστός ως πιστοποίηση κατανεμημένων συστημάτων.

Επιπλέον, καλές παράμετροι για τη διαχείριση ασφάλειας στο διαδίκτυο, αποτελούν οι μηχανισμοί (α) ε*πίβλεψης (auditing) κι υπευθυνότητας (accountability*) που καταγράφουν δηλώσεις ταυτότητας κι ενέργειες χρηστών που αποκτούν πρόσβαση στους πόρους, (β) ε*λέγχου αποδοτικότητας δικτύου (efficiency controls)* που καταγράφουν και παρακολουθούν τη συνολική απόδοση του δικτύου για την *αποτροπή καταστάσεων άρνησης εξυπηρέτησης*, (γ) υ*ποστήριξης συνεργασίας των υπηρεσιών ασφάλειας που προσφέρονται από εφαρμογές (callable security services from applications)* οι οποίες ενδεχομένως διαθέτουν χαρακτηριστικά ασφάλειας που είναι απαραίτητο να λειτουργούν με ενιαίους τρόπους. Αυτή η έννοια προωθείται μέσω των *Generic Security Service AP*I, *Generic Cryptographic Service API* και *Generic Audit Service AP*I τεχνολογιών.

4.3. Κρυπτογράφηση

Η ανάγκη για εμπιστευτικότητα στις ηλεκτρονικές συναλλαγές ικανοποιείται με την κρυπτογράφηση. Η *κρυπτογραφία* (cryptography) αφορά τον επιστημονικό κλάδο που ασχολείται με την μελέτη, χρήση κι ανάπτυξη τεχνικών κρυπτογράφησης κι αποκρυπτογράφησης για την απόκρυψη των περιεχομένων των μηνυμάτων και τη διευκόλυνση της ανίχνευσης κακόβουλων μετατροπών στα μηνύματα[140]. Η *κρυπτογράφηση* (encryption/ encipherment) αποτελεί το σημαντικότερο αυτοματοποιημένο εργαλείο για την ασφάλεια δικτύων κι επικοινωνιών. Αφορά τη διεργασία μετασχηματισμού μηνυμάτων σε ακατανόητη μορφή ώστε να μην είναι αναγνώσιμο από τρίτα μέρη, μέσω της χρήσης κρυπτογραφικού αλγορίθμου. Η ύπαρξή του είναι απαραίτητη για την εξασφάλιση της εμπιστευτικότητας και του απορρήτου των μηνυμάτων και στην περίπτωση που πέσουν σε λάθος χέρια. Η αποκρυπτογράφηση (decryption / decipherment) έχει να κάνει με την ανάκτηση του αρχικού μηνύματος μετά από κρυπτογράφηση κι εκτελείται από εξουσιοδοτημένο μέρος.

Η κρυπτογραφία βασίζεται σε τέσσερα βασικά μέρη:

1. *Καθαρό κείμενο*- το αρχικό (plaintext), πρωτότυπο μήνυμα σε μορφή που μπορεί να αναγνωστεί από τους ανθρώπους.
2. *Κρυπτογραφημένο κείμενο* (ciphertext)- το καθαρό κείμενο αφού υποστεί κρυπτογράφηση, δηλαδή είναι το αποτέλεσμα της εφαρμογής κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

[140] Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.187)

3. *Αλγόριθμος κρυπτογράφησης* (cipher) - αφορά μαθηματικούς τύπους οι οποίοι χρησιμοποιούνται για κρυπτογράφηση του καθαρού κειμένου και μετατροπή του σε κρυπτογραφημένο κείμενο καθώς και το αντίστροφο. Αποτελεί δηλαδή τη μέθοδο μετασχηματισμού των δεδομένων σε μορφή που να μην μπορεί να αναγνωριστεί από μη εξουσιοδοτημένα άτομα.
4. *Κλειδί* (key) - το μυστικό κλειδί που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος. Αφορά τη διατήρηση της μυστικότητας των πληροφοριών. Η ανθεκτικότητα της κρυπτογράφησης βασικά εξαρτάται από το μέγεθος των κλειδιών κι όχι τον αλγόριθμο. Αυτό το μέγεθος μετριέται σε bits.

Η κρυπτογραφία επιτρέπει επιπλέον την κρυπτογράφηση δυαδικών πληροφοριών, όπως βίντεο, ήχου και εκτελέσιμων λειτουργικών μονάδων λογισμικού για ασφαλή μετάδοση μέσω του διαδικτύου. Για κρυπτογράφηση μηνυμάτων μπορούν να χρησιμοποιηθούν διάφοροι αλγόριθμοι. Ένας αλγόριθμος μπορεί να είναι ασφαλής ακόμα κι αν είναι γνωστός, αρκεί το κλειδί να μην είναι γνωστό[141]. Η εύρεση ενός κλειδιού είναι δυνατή με απλές δοκιμές όλων των πιθανοτήτων μέσω ένα υπολογιστή, μέχρι να αποκρυπτογραφηθεί εν τέλει το ζητούμενο μήνυμα. Αυτή είναι η αιτία που το μέγεθος του κλειδιού αποτελεί τον κύριο παράγοντα διασφάλισης ενός μηνύματος[142]. Για παράδειγμα, αν ένα κλειδί έχει μέγεθος 4 bits τότε θα υπάρχουν δεκαέξι πιθανές λύσεις που μπορεί να δοκιμαστούν για να αποκρυπτογραφηθεί κάποιο μήνυμα (2^4 = 16). Στη σημερινή εποχή όμως οι υπολογιστές υψηλής ταχύτητας μπορούν να δοκιμάσουν εκατομμύρια συνδυασμούς μόλις σε ένα δευτερόλεπτο. Το πραγματικό μέγεθος του κλειδιού που χρησιμοποιείται εξαρτάται από διάφορους παράγοντες, όπως είναι η χρήσιμη διάρκεια ζωής των δεδομένων.

Τα κρυπτογραφικά συστήματα χρησιμοποιούνται για να παρέχουν μυστικότητα (secrecy), ακεραιτότητα δεδομένων (data integrity), αυθεντικοποίηση χρηστών (user authentication), αδυναμία απάρνησης (non- repudiation).

Σε γενικές γραμμές υπάρχουν διάφοροι μέθοδοι κρυπτογραφίας, κι ανάλογα με τα *κλειδιά* και τον *τρόπο κρυπτογράφησης* ταξινομούνται σε κατηγορίες. Σύμφωνα με τα κλειδιά χρησιμοποιούνται (α) τα μυστικά ή συμμετρικά κλειδιά (symmetric key) κι έχουν να κάνουν με τη χρήση του ίδιου μυστικού κλειδιού για κρυπτογράφηση κι αποκρυπτογράφηση και (β) τα δημόσια ή ασύμμετρα κλειδιά (public or asymmetric key) τα

[141] http://www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf
[142] http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf

οποία για κρυπτογράφηση κι αποκρυπτογράφηση χρησιμοποιούν διαφορετικά κλειδιά, δηλαδή ένα δημόσιο κι ένα προσωπικό κλειδί παραλήπτη.

Τώρα, με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων υπάρχει η μέθοδος της δέσμης (block ciphers) κι αυτή της ροής (stream ciphers). Σύμφωνα με την πρώτη, μετατρέπεται το αρχικό μήνυμα σε δέσμες τις οποίες κρυπτογραφούν. Σε μια σύνοδο, κρυπτογραφούνται όλες οι ομάδες δεδομένων από το ίδιο αρχείο με το ίδιο κλειδί. Στην ροής, το μήνυμα κρυπτογραφείται ανά byte/ bit κάθε φορά. Η κρυπτογράφηση εδώ γίνεται με ένα σταθερά εναλλασσόμενο κλειδί, επομένως και η ανθεκτικότητα εξαρτάται από την γεννήτρια κλειδιών της ροής.

Συμμετρική Κρυπτογραφία

Για αρκετά χρόνια οι αλγόριθμοι κρυπτογράφησης ήταν συμμετρικοί, δηλαδή χρησιμοποιούνταν το ίδιο κλειδί για κρυπτογράφηση κι αποκρυπτογράφηση ενός μηνύματος. Βασίζεται ουσιαστικά στην ύπαρξη ενός μόνο μυστικού κλειδιού, που γνωρίζουν μόνο τα συναλλασσόμενα μέρη. Αυτού του είδους η κρυπτογράφηση καλείται επίσης κρυπτογράφηση ιδιωτικού κλειδιού[143]. Ο πιο ευρύς χρησιμοποιούμενος συμμετρικός αλγόριθμος κρυπτογράφησης ήταν ο DES (Data Description Standard) - Πρότυπο Κρυπτογράφησης Δεδομένων, ο οποίος υιοθετήθηκε το 1977 από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST). Από τότε όμως έχουν εφευρεθεί κι άλλοι αλγόριθμοι, εξαιτίας της ευαισθησίας του DES σε επιθέσεις μεγάλης δύναμης.

Μια δυσκολία με την κρυπτογράφηση συμμετρικού κλειδιού έχει να κάνει με τη μη εξασφάλιση και μη ταυτοποίηση του αποστολέα και του παραλήπτη[144]. Αν το ιδιωτικό κλειδί ενός server διανεμηθεί σε πολλούς χρήστες, δεν υπάρχει τρόπος το κλειδί να παραμείνει μυστικό για αρκετό χρονικό διάστημα. Για τους λόγους αυτούς, το 1976 επινοήθηκε ένας νέος τύπος αλγορίθμου, από τους Whitfield και Martin Hellmann που καλείται κρυπτογράφηση δημόσιου κλειδιού.

Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογράφηση, επίσης γνωστή ως κρυπτογράφηση δημόσιου κλειδιού, χρησιμοποιεί ζεύγος κλειδιών - ένα δημόσιο και ένα ιδιωτικό (μυστικό). Τα δύο

[143] Efraim Turban, Jae Lee, David King, Michael Chung, Ηλεκτρονικό εμπόριο: Αρχές, Εξελίξεις, Στρατηγική από τη σκοπιά του manager, Έκδοση Μ. Γκιούρδας, Αθήνα 2002
[144] http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf

κλειδιά συνδέονται μεταξύ τους με μαθηματική σχέση, δηλαδή όταν χρησιμοποιηθεί το ένα, τότε πρέπει απαραίτητα να χρησιμοποιηθεί και το άλλο κλειδί για την αποκρυπτογράφηση του μηνύματος. Έτσι, μηνύματα μπορούν να αποστέλλονται χωρίς να υπάρχει συμφωνία εκ των προτέρων για τα κλειδιά[145].

Για την εξασφάλιση της εμπιστευτικότητας του μηνύματος και της αυθεντικότητας του δημιουργού τα δυο κλειδιά μπορούν να χρησιμοποιηθούν με δυο διαφορετικούς τρόπους. Στην μια περίπτωση, ο αποστολέας κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη το μήνυμα και το αποστέλλει. Μετά ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί και το διαβάζει. Στην άλλη περίπτωση χρησιμοποιείται *ψηφιακός φάκελος*, δηλαδή μια συνδυαστική μορφή. Πιο συγκεκριμένα, ο αποστολέας κρυπτογραφεί με το ιδιωτικό του κλειδί τα δεδομένα κι εν συνεχεία με το δημόσιο του παραλήπτη. Ο παραλήπτης αποκωδικοποιεί το μήνυμα αρχικά με το ιδιωτικό του κλειδί κι ακολούθως με το δημόσιο του αποστολέα. Κατά αυτόν τον τρόπο γνωρίζουν και οι δυο πλευρές την ταυτότητα του ενός και του άλλου[146].

Εξαιτίας των παραπάνω υπολογισμών που απαιτούνται, η ασύμμετρη διαδικασία είναι πιο αργή απ' τη συμμετρική, αλλά παρέχει τη δυνατότητα ταυτοποίησης του αποστολέα, η οποία εξασφαλίζεται απ' την κρυπτογράφηση του μυστικού κλειδιού. Για κρυπτογράφηση μηνυμάτων δημοσίου κλειδιού υπάρχουν μόνο δύο αλγόριθμοι[147]: ο RSA και ο DiffieHellman.

Ψηφιακές Υπογραφές

Το πρόβλημα της παραποίησης και προσποίησης στην κρυπτογράφηση κι αποκρυπτογράφηση δεν συναντάται κι αυτό λόγω της χρήσης μιας μαθηματικής συνάρτησης που καλείται μονόδρομος τεμαχισμός (one way hash) ή συνόψιση μηνύματος (message digest). Η εφαρμογή της μονόδρομου τεμαχισμού σε ένα μήνυμα είναι ένας αριθμός που είναι μοναδικός για κάθε μήνυμα και το περιεχόμενό του δεν μπορεί να εξαχθεί από τον αριθμό του τεμαχισμού, γι' αυτό και λέγεται μονόδρομος.

Η χρήση του προσωπικού κλειδιού για κρυπτογράφηση και του δημόσιου για αποκρυπτογράφηση φέρει την έννοια της ψηφιακής υπογραφής σε κάθε μήνυμα που στέλνει ο αποστολέας. Ο μονόδρομος τεμαχισμός που δημιουργείται για το κάθε μήνυμα

[145] http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf
[146] Καλογέρα Ασημίνα, 'Στρατηγική και εφαρμογές e-banking' Πτυχιακή Εργασία ΤΕΙ Καβάλας, 2005
[147] Γιάννης Β. Σαμαράς, Γκιούρδας Μ., (μετάφραση) Efraim Turban, David King, Jae Kyu Lee, Michael Chung, Ηλεκτρονικό εμπόριο - Αθήνα, 2002. - σελ. 398

κρυπτογραφείται με το προσωπικό κλειδί του αποστολέα. Ο κρυπτογραφημένος τεμαχισμός και η πληροφορία γι' αυτόν αποτελούν την ψηφιακή υπογραφή.

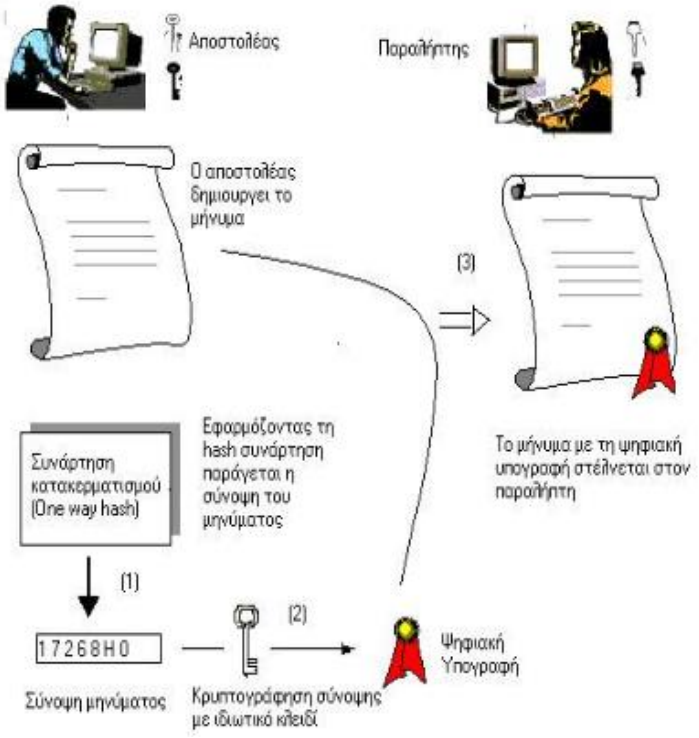
Η ψηφιακή υπογραφή του παραλήπτη αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα. Σύμφωνα με τον αλγόριθμο τεμαχισμού επανυπολογίζεται ο τεμαχισμός του μηνύματος και συγκρίνονται οι δυο τεμαχισμοί δηλώνοντας έτσι πως σε περίπτωση που δεν είναι ίδιοι ή το μήνυμα έχει τροποποιηθεί ή η ψηφιακή υπογραφή δεν αντιστοιχεί στου αποστολέα το δημόσιο κλειδί. Αν πάλι είναι ίδιοι τότε ο παραλήπτης είναι βέβαιος για την αντιστοιχία του δημόσιου κλειδιού με το προσωπικό που χρησιμοποιήθηκε για τη δημιουργία της ψηφιακής υπογραφής[148].

Για τη χρήση της ηλεκτρονικής υπογραφής απαιτούνται δύο διαδικασίες, πρώτον η δημιουργία της υπογραφής και δεύτερον, η επαλήθευσή της. Τα βήματα που ακολουθούνται για τη δημιουργία της ψηφιακής υπογραφής είναι:

1. Ο αποστολέας με τη χρήση του αλγόριθμου κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που επιθυμεί να στείλει. Έτσι, παράγεται μία σειρά ψηφίων συγκεκριμένου μήκους.
2. Ο αποστολέας κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί. Παράγεται ακολούθως η ψηφιακή υπογραφή, δηλαδή μία σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η ψηφιακή υπογραφή - κρυπτογραφημένη σύνοψη - προσαρτάται στο κείμενο και μέσω του δικτύου μεταδίδονται το μήνυμα με τη ψηφιακή υπογραφή.
4. Ο παραλήπτης αποσπά την ψηφιακή υπογραφή με το ιδιωτικό κλειδί του αποστολέα.
5. Ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος εφαρμόζοντας τον ίδιο αλγόριθμο κατακερματισμού που έλαβε.
6. Εν συνεχεία, αποκρυπτογραφεί την
7. κρυπτογραφημένη σύνοψη του μηνύματος με το δημόσιο κλειδί του αποστολέα.
8. Συγκρίνει τις δύο συνόψεις κι εντοπίζει αν το μήνυμα που έλαβε είναι ακέραιο ή όχι.

[148] Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.214)

Γράφημα 4.1: Δημιουργία ψηφιακής υπογραφής



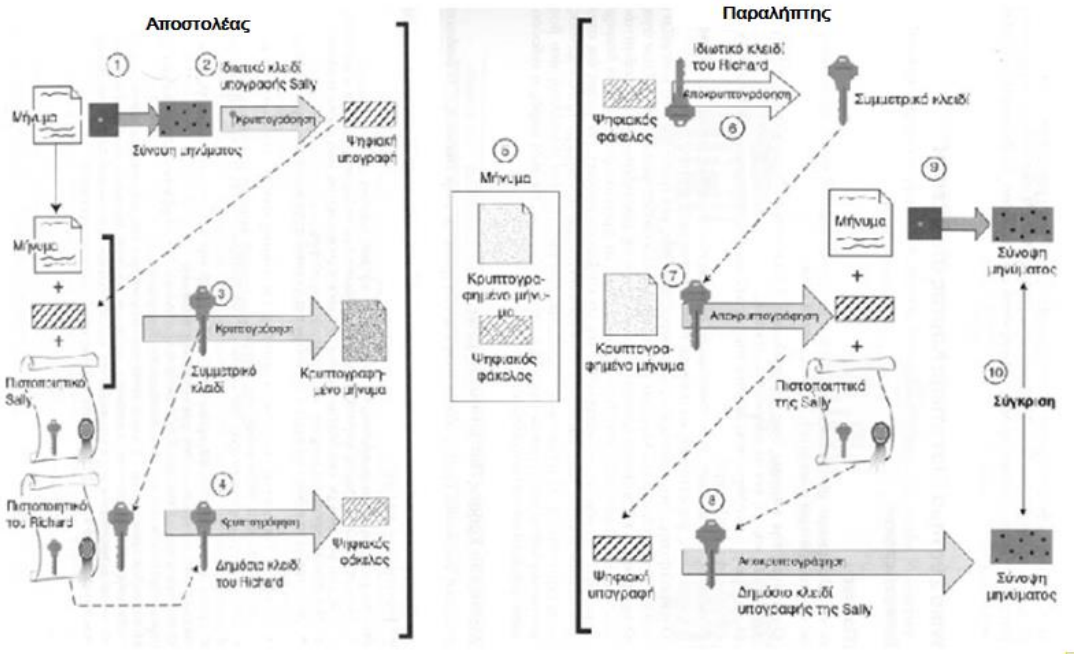
4.4. Συνολική Διαδικασία Κρυπτογράφησης

Για τη μετάδοση ενός μηνύματος από τον αποστολέα στον παραλήπτη, η διαδικασία της κρυπτογράφησης γίνεται με την ακολουθία των εξής βημάτων, τα οποία απεικονίζονται στο παρακάτω γράφημα:

1. Πραγματοποιείται εφαρμογή μονόδρομης συνάρτησης κατακερματισμού από τον αποστολέα στο αρχικό μήνυμα. Παράγεται μια τιμή η οποία αποτελεί τη σύνοψη του μηνύματος και η οποία πρόκειται να χρησιμοποιηθεί για την επιβεβαίωση της ακεραιότητας αυτού κατά την παραλαβή.
2. Γίνεται κρυπτογράφηση της σύνοψης του μηνύματος από τον αποστολέα μέσω της χρήσης του ιδιωτικού του κλειδιού, προκύπτοντας έτσι η ψηφιακή υπογραφή.
3. Δημιουργείται ένα τυχαίο συμμετρικό κλειδί από τον αποστολέα το οποίο χρησιμοποιείται για την κρυπτογράφηση (α) του μηνύματος που πρόκειται να αποσταλεί, (β) της ψηφιακής υπογραφής και (γ) ενός αντίγραφου του ψηφιακού πιστοποιητικού το οποίο περιέχει το δημόσιο κλειδί για υπογραφές. Προκειμένου να γίνει αποκρυπτογράφηση από τον παραλήπτη, είναι απαραίτητη η ύπαρξη ενός αξιόπιστου αντίγραφου του συμμετρικού κλειδιού του αποστολέα.

4. Ο αποστολέας πρέπει να διαθέτει το πιστοποιητικό του παραλήπτη. Αυτό το πιστοποιητικό περιέχει αντίγραφο του δημόσιου κλειδιού, το οποίο κλειδί είναι διαφορετικό από αυτό για υπογραφές, για την κρυπτογράφηση μηνυμάτων. Για να μεταδοθεί με ασφάλεια το συμμετρικό κλειδί, ο αποστολέας πραγματοποιεί κρυπτογράφηση με το δημόσιο κλειδί του παραλήπτη. Το κλειδί που πλέον είναι κρυπτογραφημένο αποτελεί τον ψηφιακό φάκελο κι αποστέλλεται μαζί με το μήνυμα που προέκυψε στο βήμα 3.
5. Στον παραλήπτη αποστέλλεται (α) το συμμετρικό κρυπτογραφημένο μήνυμα με το ψηφιακό πιστοποιητικό του αποστολέα και την ψηφιακή υπογραφή του καθώς και (β) το ασύμμετρα (με το δημόσιο κλειδί του παραλήπτη) κρυπτογραφημένο συμμετρικό κλειδί, δηλαδή ο ψηφιακός φάκελος.
6. Για την απόκτηση του συμμετρικού κλειδιού, ο παραλήπτης αφού λάβει το μήνυμα, αποκρυπτογραφεί τον ψηφιακό φάκελο με το δικό του ιδιωτικό κλειδί.
7. Γίνεται αποκρυπτογράφηση του μηνύματος με το συμμετρικό κλειδί (με την υπογραφή και το πιστοποιητικό του αποστολέα).
8. Ο παραλήπτης αποκρυπτογραφεί με το δημόσιο κλειδί την ψηφιακή υπογραφή το οποίο περιέχεται στο πιστοποιητικό που έλαβε, αποκτώντας έτσι τη συνόψιση του κρυπτογραφημένου μηνύματος.
9. Ο παραλήπτης χρησιμοποιεί την ίδια μονόδρομη συνάρτηση με την αρχική του αποστολέα παράγοντας μια καινούρια συνόψιση για το αποκρυπτογραφημένο μήνυμα.
10. Μέσω της σύγκρισης της συνόψισης του μηνύματος που προέκυψε στον παραλήπτη με αυτήν από την ψηφιακή υπογραφή του αποστολέα γίνεται επιβεβαίωση του περιεχομένου του μηνύματος και ότι κατά τη μετάδοση δεν υπήρξε κάποιου είδους μεταβολή/ παρεμβολή μετά την ψηφιακή υπογραφή.

Γράφημα 4.2: Μετάδοση μηνύματος από τον αποστολέα στον παραλήπτη



Πηγή: Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.218)

4.5. Ψηφιακά Πιστοποιητικά

Ένα σύστημα κρυπτογράφησης από μόνο του χωρίς την ύπαρξη μιας υπεύθυνης αρχής διαχείρισης των δημόσιων κλειδιών δεν είναι τόσο χρήσιμο. Αυτού του είδους η αρχή θα πρέπει να μπορεί να διασφαλίζει ότι ένα δημόσιο κλειδί αντιστοιχεί σε ένα συγκεκριμένο χρήστη. Αυτή η αντιστοίχιση ενός χρήστη σε δημόσιο κλειδί παρέχεται από ένα πιστοποιητικό (certificate) που διανέμει η Αρχή Πιστοποίησης (Certification Authority ή CA), που αποτελεί έναν έμπιστο οργανισμό. Αυτή η Αρχή έχει την ευθύνη της δημιουργίας, της διανομής, της ανάκλησης και γενικής διαχείρισης των πιστοποιητικών. Η Πιστοποίηση δηλαδή είναι η διαδικασία δέσμευσης ενός δημόσιου κλειδιού σε άτομο, οργανισμό ή και οντότητα. Για το σκοπό αυτό χρησιμοποιούνται τα ψηφιακά πιστοποιητικά τα οποία αποτελούν το μέσο μετάδοσης των τιμών των δημόσιων κλειδιών με ασφαλή τρόπο[149]. Η πιστοποίηση αποτελεί βασική λειτουργία των Υποδομών Δημόσιου Κλειδιού (ΥΔΚ).

[149] Ταχαρίδου Βαρβάρα, Πανεπιστήμιο Μακεδονίας, Μεταπτ. Προγρ. στα Πληρ. Συστήματα, σελ. 42, http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf

4.6. Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure, PKI)

Η Υποδομή Δημόσιου Κλειδιού (ΥΔΚ) αποτελεί συνδυασμό λογισμικού, τεχνολογιών ασύμμετρης κρυπτογραφίας και διαδικασιών που πιστοποιεί την εγκυρότητα κάθε εμπλεκόμενου σε μια ψηφιακή συναλλαγή. Οι κυριότεροι μηχανισμοί ασφάλειας που καλύπτει η ΥΔΚ είναι (α) το απόρρητο της επικοινωνίας, όπου τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, (β) η ακεραιότητα, όπου τα δεδομένα προστατεύονται μέσω μηχανισμών κρυπτογράφησης, (γ) η πιστοποίηση, όπου πραγματοποιείται επιβεβαίωση της ταυτότητας του αποστολέα και (δ) μη άρνηση αποδοχής, που συνδυάζει υπηρεσίες Πιστοποίησης και Ακεραιότητας και διασφαλίζει τη μη αμφισβήτηση της πραγματοποιηθείσας συναλλαγής από τα συμβαλλόμενα μέρη.

4.7. Σύστημα Ασφάλειας Εμπορίου μέσω Κινητού

Σήμερα οι απαιτήσεις για ασύρματες αγορές μέσω Διαδικτύου συνεχώς αυξάνονται. Αλλά η απάτη μέσω πιστωτικών καρτών αποτελεί σοβαρό ζήτημα και τα SET και SSL έχουν τα δικά τους προβλήματα. Για να ενισχυθεί η ασφάλεια των online αγορών έχουν γίνει πολλές προτάσεις. Για παράδειγμα, μια από αυτές είναι η δημιουργία ενός ασφαλούς συστήματος εμπορίου μέσω του κινητού (m-commerce), το οποίο ονομάζεται Σύστημα Ασφάλειας Εμπορίου μέσω Κινητού (Secure System M-Commerce - SMCS χάριν συντομίας), με το οποίο οι χρήστες μπορούν να δημιουργήσουν μια πιο ασφαλή συναλλαγή μέσω πιστωτικής κάρτας για αγορές στο διαδίκτυο. Βασικά, το SMCS συντονίζει τη ροή μετρητών ενός συστήματος συναλλαγών και των οντοτήτων των πιστωτικών καρτών ώστε να προστατεύσει αποτελεσματικά τις εκδοθείσες συναλλαγές έναντι διαφόρων επιθέσεων και για την αποφυγή διαρροής πληροφοριών. Το προτεινόμενο σύστημα επίσης απασχολεί ένα πυρήνα σύνδεσης δεδομένων (Data Connection Core - DCC για συντομία) της έκδοσης της κάρτας για τη σύνδεση της τράπεζας με τους καταναλωτές πριν ξεκινήσει η ασύρματη επικοινωνία, έτσι ώστε να βελτιωθεί αισθητά το επίπεδο ασφαλείας του m-commerce περιβάλλοντος. Η θεωρητική ανάλυση[150] των Fang-Yie Leu, Yi-Li Huang και Sheng-Mao Wang δείχνει ότι η SMCS είναι πιο ασφαλές σύστημα από ό, τι τα SET και SSL. Η ανάλυση επίδοσης δείχνει ότι το SMCS αποτελεί πράγματι ένα εφικτό σύστημα m-commerce.

[150] Fang-Yie Leu, Yi-Li Huang, Sheng-Mao Wang, A Secure M-Commerce System based on credit card transaction - Electronic Commerce Research and Applications 14 (2015) 351–360, Elsevier

Πρόσφατα, η άνεση και η ασφάλεια της ασύρματης επικοινωνίας έχουν βελτιωθεί σημαντικά[151]. Πολλοί άνθρωποι απολαμβάνουν τις online αγορές τους με τις πιστωτικές τους κάρτες. Όμως, λόγω της υποδομής ενός ασύρματου συστήματος, οι συναλλαγές που εκδίδονται δημιουργούνται ασύρματα. Από την άλλη πλευρά, οι απάτες πιστωτικών καρτών στις μέρες μας είναι σοβαρές και μειώνουν αισθητά τις online αγορές για μερικούς ανθρώπους[152]. Επίσης, λόγω της έντονης ανάπτυξης των ασύρματων δικτύων, των τρεχόντων συσκευών κινητής τηλεφωνίας, όπως είναι τα έξυπνα κινητά τηλέφωνα, οι υπολογιστές tablet και οι φορητοί υπολογιστές, όλα αυτά έχουν παράσχει στους χρήστες ποικίλα χαρακτηριστικά και υπηρεσίες, τα οποία έχουν αλλάξει την καθημερινή ζωή καθώς και τις αγοραστικές συνήθειες των ανθρώπων. Σε γενικές γραμμές, ένας ασφαλής μηχανισμός πιστωτικής κάρτας για το κινητό εμπόριο θα πρέπει να προστατεύει με ασφάλεια τις αντίστοιχες συναλλαγές και τις προσωπικές πληροφορίες. Προς το παρόν, όταν πραγματοποιούνται ψώνια σε ένα ασύρματο περιβάλλον, όπως για παράδειγμα η πληρωμή μέσω χρήσης Secure Sockets Layer (SSL), πρέπει να αποστέλλονται ο αριθμός της κάρτας, η ημερομηνία λήξης και άλλες πληροφορίες για τον έμπορο. Στην πραγματικότητα, το SSL μπορεί να εξασφαλίσει peer-to-peer παράδοση ασφάλειας, αλλά δεν μπορεί να είναι σίγουρο για τις ταυτότητες των υποκείμενων χρηστών[153].

Για την επίλυση αυτού του προβλήματος, οι οργανώσεις δικτύων Visa και MasterCard παρουσίασαν ένα ηλεκτρονικό σύστημα πληρωμής γνωστό ως Ασφαλείς Ηλεκτρονικές Συναλλαγές[154] (Secure Electronic Transaction - SET). Ωστόσο, αυτό το σύστημα έχει τα δικά του προβλήματα. Παραδείγματος χάρη, ένας καταναλωτής θα χρειαστεί να υποβάλλει αίτηση για παραλαβή βεβαίωσης[155]. Αυτό σημαίνει ότι από την πλευρά του χρήστη, η αντίστοιχη πληροφορία της πιστωτικής κάρτας θα πρέπει να αποθηκεύεται σε ένα σκληρό δίσκο. Επίσης, για να βελτιωθεί το επίπεδο ασφάλειας του, το σύστημα SET παίρνει πολύ χρόνο για τον υπολογισμό πολύπλοκων κλειδιών ασύμμετρης κρυπτογράφησης και αποκρυπτογράφηση[156], παρέχοντας έτσι στους χρήστες μια εμπειρία

[151] Nabi, F., Secure business application logic for e-commerce systems - Computers and Security 24 (3), 208–217, 2005

[152] Mahmoudi, N., Duman, E., Detecting credit card fraud by modified fisher discriminant analysis. Expert Systems with Applications 42 (5), 2510–2516, 2015

Gold, S., 2014. The evolution of payment card fraud. Computer Fraud and Security (3), 12–17, 2014

[153] Oppliger, R., Hauser, R., Basin, D., SSL/TLS session-aware user authentication revisited. Computers and Security 27 (3–4), 64–70, 2008

[154] Lu, S., Smolka, S.A., Model checking the secure electronic transaction (SET) protocol. In 7th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 358–364, 1999

[155] Bella, G., Massacci, F., Paulson, L.C., Verifying the SET registration protocols. IEEE Journal on Selected Areas in Communications 21 (1), 77–87, 2003

[156] Shedid, S.M., Kouta, M., Modified SET protocol for mobile payment: an empirical analysis. In International Conference on Software Technology and Engineering, vol. 1, V1-350–V1-355 , 2010

ενόχλησης μέσω του κινητού εμπορίου. Σήμερα, οι αυξανόμενες απαιτήσεις για το κινητό εμπόριο παρακινούν για την κατασκευή ενός πιο ασφαλούς και βολικού μηχανισμού m-commerce. Ως εκ τούτου, προτείνεται από τους Fang-Yie Leu, Yi-Li Huang και Sheng-Mao Wang ένα ασφαλές σύστημα m-commerce το οποίο ονομάζεται SMC και συντονίζει τη ροή μετρητών από ένα σύστημα συναλλαγών και φορέων πιστωτικής κάρτας για την ανάπτυξη ενός ασφαλούς και άνετου περιβάλλοντος, χωρίς την αύξηση επιπλέον περιοριστικών μέτρων και πόρων σχετικά με την ταμειακή ροή και τις οντότητες πιστωτικών καρτών. Βασικά, παράγεται ένας δυναμικός κωδικός ταυτότητας της πιστωτικής κάρτας για να αντικαταστήσει τις πληροφορίες της πιστωτικής κάρτας έτσι ώστε ο έμπορος διαπραγμάτευσης να μην μπορεί να γνωρίζει τον πιστωτικό αριθμό της κάρτας και τα στοιχεία αυτής. Το σύστημα SMCS απασχολεί επίσης Δεδομένα Σύνδεσης Πυρήνα (Data Connection Core - DCC για συντομία) για τη σύνδεση με την τράπεζα έκδοσης της κάρτας και τους καταναλωτές πριν από την έναρξη της ασύρματης επικοινωνίας τους. Επιπλέον, η τράπεζα έκδοσης της κάρτας πιστοποιεί το δυναμικό κώδικα ταυτότητας της πιστωτικής κάρτας και το δυναμικό κώδικα του εμπόρου απ' ότι να επικυρώνει απευθείας την πιστωτική κάρτα και τις πληροφορίες του εμπόρου. Αυτό μπορεί επαρκώς να βεβαιώσει τη νομιμοποίηση του καταναλωτή και της εμπορίας του έμπορου, έτσι ώστε να αυξηθεί αποτελεσματικά το επίπεδο ασφάλειας του συστήματος SMCS.

4.8. Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)

Το πρωτόκολλο αυτό σχεδιάστηκε προκειμένου να πραγματοποιεί ασφαλή σύνδεση με τον εξυπηρετητή (server). Δηλαδή, παρέχει απόρρητη επικοινωνία μεταξύ εμπόρου και πελάτη σε μια συναλλαγή πληρωμής. Το SSL χρησιμοποιεί "κλειδί" δημόσιας κρυπτογράφησης, με σκοπό να προστατεύει τα δεδομένα καθώς "ταξιδεύουν" μέσα στο Internet. Πιο συγκεκριμένα, παρέχει κρυπτογράφηση της μεταδιδόμενης πληροφορίας (data encryption), υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρετητή (server authentication) και προαιρετική πιστοποίηση της ταυτότητας του πελάτη (client authentication) μέσω έγκυρων πιστοποιητικών εκδιδόμενες από Αρχές Πιστοποίησης (Certificates Authorities).

Το SSL σχεδιάστηκε από τη Netscape κι έχει δύο βασικά χαρακτηριστικά. Το πρώτο είναι η χρήση ενός δημόσιου κλειδιού και ο μηχανισμός του ιδιωτικού κλειδιού για να

Yong, X., Jindi, L., Electronic payment system design based on SET and TTP, International Conference on E-Business and E-Government, 275–278, 2010

συνδέσει τις δύο πλευρές ενός δικτύου σύνδεσης. Με αυτόν το μηχανισμό, μπορούν να ανταλλάξουν με ασφάλεια τα κρυπτογραφημένα μηνύματα το ένα μέρος με το άλλο. Το δεύτερο είναι ότι κάνει χρήση πιστοποίησης ενός τρίτου μέρους για να επιτρέψει στις δύο πλευρές της σύνδεσης την επικύρωση της πληροφορίας του ενός με τον άλλο[157].

Το SSL διασφαλίζει τις λεπτομέρειες των ηλεκτρονικών συναλλαγών με τη χρήση του αριθμού της πιστωτικής κάρτας και της ημερομηνίας λήξης αυτής ή των διαθέσιμων πληροφοριών του κατόχου της κάρτας, και μεταδίδει τα κρυπτογραφημένα μηνύματα στον έμπορο. Ο έμπορος επαναχρησιμοποιεί το κρυπτογραφημένα μηνύματα για να ζητήσει από την τράπεζα έκδοσης της κάρτας την αποπληρωμή. Οι καταναλωτές προτιμούν αυτόν τον τρόπο, επειδή το σύστημα δε ζητάει από τους χρήστες να υποβάλλουν αίτηση για ηλεκτρονικό πορτοφόλι και πιστοποιητικό ασφαλείας στην τράπεζα έκδοσης της κάρτας.

Αλλά το SSL έχει δύο μειονεκτήματα. Το πρώτο είναι ότι οι δύο πλευρές μιας σύνδεσης SSL μπορούν μόνο να καθορίσουν αν επιτρέπεται ή όχι το άλλο μέρος να χρησιμοποιήσει το μηχανισμό SSL. Αυτό σημαίνει ότι ο καταναλωτής δεν γνωρίζει ποιος είναι ο έμπορος, αν είναι πράγματι έννομος έμπορος ή ένας χάκερ. Ούτε ο έμπορος γνωρίζει την ταυτότητα του καταναλωτή, κι επίσης δεν μπορεί να επιβεβαιώσει αν ο αριθμός της πιστωτικής κάρτας του καταναλωτή είναι σωστός ή όχι[158].

Το δεύτερο είναι ότι αν και το SSL είναι βολικό για τους καταναλωτές για να εκτελούν τα ψώνια στο διαδίκτυο μέσω ενός ασύρματου συστήματος, όταν το SSL επικαλείται για την πραγματοποίηση μιας συναλλαγής, ο αριθμός της κάρτας και οι σχετικές πληροφορίες του κατόχου μπορούν να φανούν καθαρά στον έμπορο, έτσι πιθανώς μπορούν να τα χρησιμοποιήσουν κάποια άτομα. Εκτός αυτού, εάν ο αριθμός της κάρτας και οι άλλες σχετικές πληροφορίες που έχουν κλαπεί από τους χάκερ, χρησιμοποιηθούν παράνομα για αγορές μέσω διαδικτύου μπορούν να προκαλέσουν απώλειες όχι μόνο στον κάτοχο της κάρτας, αλλά και στον έμπορο ο οποίος θα έχανε τα πριν από την καταβολή χρημάτων προϊόντα, εάν ο κάτοχος της κάρτας υπέβαλλε σχετικές αποδείξεις για την άρνηση πραγματοποίησης αυτής της συναλλαγής. Όταν το SSL ολοκληρώνει μια συναλλαγή, ο έμπορος δεν μπορεί να καθορίσει αν αυτή η συναλλαγή ολοκληρώνεται πριν από την παραλαβή της σχετικής χρηματοδότησης ή από την τράπεζα.

[157] Bicakci, K., Unal, D., Ascioglu, N., Adalier, O., Mobile authentication secure against man-in-the-middle attacks. Procedia Computer Science 34, 323–329 , 2014
Badra, M., Urien, P., Toward SSL integration in SIM smartcards. IEEE Wireless Communications and Networking Conference 2, 889–893, 2004
[158] Bisel, L.D., The role of SSL in cybersecurity. IT Professional 9 (2), 22–25, 2007

Η διαδικασία SSL για συναλλαγή με πιστωτική κάρτα έχει τέσσερα στάδια[159]. Στο πρώτο στάδιο, ο καταναλωτής ενημερώνει τον έμπορο ποια έκδοση του SSL υποστηρίζει το τερματικό, μια λίστα κρυπτογράφησης-αλγόριθμου και μια λίστα συμπιεσμένου αλγόριθμου που υποστηρίζει η συσκευή. Ο έμπορος επιλέγει τις υψηλότερες εκδόσεις του SSL, έναν κρυπτογραφημένο αλγόριθμο και ένα συμπιεσμένο αλγόριθμο για χρήση. Σε δεύτερο στάδιο, ο έμπορος στέλνει τη δική του βεβαίωση και το δημόσιο κλειδί του πρωτοκόλλου Diffie–Hellman στον καταναλωτή. Στο τρίτο στάδιο, ο καταναλωτής παραδίδει τη δική του βεβαίωση και το δημόσιο κλειδί του πρωτοκόλλου Diffie–Hellman στον έμπορο. Με το δημόσιο κλειδί του εμπόρου (καταναλωτή) και το ιδιωτικό κλειδί του καταναλωτή (εμπόρου), ο καταναλωτής (έμπορος) μπορεί να αντλήσει το κοινό μυστικό κλειδί του πρωτοκόλλου Diffie–Hellman. Στο τέταρτο στάδιο, ένα μήνυμα μεταφέρεται από την αποδέκτρια τράπεζα στον έμπορο για να αποδείξει ότι το κλειδί της διαδικασίας ανταλλαγής και ο έλεγχος ταυτότητας ολοκληρώθηκαν με επιτυχία.

4.9. Ασφαλές Σύστημα Συναλλαγών

Ένα ασφαλές σύστημα συναλλαγών πρέπει να υποστηρίζει τα εξής[160]:

- ισχυρή αυθεντικοποίηση κάθε συμμετέχοντα βασισμένη στη χρήση πιστοποιητικών, ψηφιακών υπογραφών κι έξυπνων καρτών.
- Ιδιωτικότητα συναλλαγών μέσω της χρήσης της κρυπτογραφίας.
- ακεραιότητα μέσω συνόψισης μηνύματος.
- μη απάρνηση για αποφυγή αμφισβητήσεων των συναλλαγών.
- πρωτόκολλα συναλλαγών.

Σε γενικές γραμμές έχει σημειωθεί σημαντική πρόοδος τεχνικά και συνεχίζει να υιοθετείται το διαδίκτυο για την πραγματοποίηση συναλλαγών με χρηματικό αντίκρισμα. Ακολουθεί πίνακας στον οποίο παρουσιάζονται μερικά από τα υπάρχοντα συστήματα ηλεκτρονικών συναλλαγών. Από αυτά τα συστήματα, το SET έχει αποκτήσει την μεγαλύτερη αποδοχή ως αποδοτικό σύστημα.

---

[159] Zhao H., Liu R., A scheme to improve security of SSL. In Pacific-Asia Conference on Circuits, Communications and Systems, 401–404 , 2009
Du, L., Hu, X., Li, Y., Zhao, G., A CSK based SSL handshake protocol. IEEE International Conference on Network Infrastructure and Digital Content, 600–603 , 2009
Petridou, S., Basagiannis, S., Towards energy consumption evaluation of the SSL handshake protocol in mobile communications. Annual Conference on Wireless On-demand Network Systems and Services, 135–138, 2012

[160] Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, ISBN 906-516-018-8 (σελ.230), Θεσσαλονίκη 2002

Πίνακας 4.1: Συστήματα Ηλεκτρονικών Συναλλαγών

Συστήματα Ηλεκτρονικών Συναλλαγών		
Cybercash	Checkfree	Digicash
Netbill Project	Intuit	Electronic Funds Clearinghouse
Netcheque	iPK protocol	Sandia's Ecash system
Net market	Netscape	Netbank
VISA/MC SET	Mondex	IBM electronic commerce
Security 1st Networkbank FSB	GC Tech/ GlodeD	

Πηγή: Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.231)

4.10. Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)

Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το σύστημα συναλλαγής SET αναπτύχθηκε από τις VISA, MasterCard, IBM από κοινού καθώς κι άλλους οργανισμούς[161]. Όπως το SSL έτσι κι αυτό χρησιμοποιεί το δημόσιο και το ιδιωτικό κλειδί ως βάση για την εξασφάλιση της διαδικασίας ανταλλαγής μηνύματος. Ωστόσο, το SET απαιτεί τόσο απ' τους καταναλωτές και τους εμπόρους να κάνουν αίτηση για την απόκτηση πιστοποίησης SET και στη συνέχεια να χρησιμοποιήσουν το λογισμικό για να ολοκληρώσουν μια συναλλαγή σε απευθείας σύνδεση.

Το μεγαλύτερο πλεονέκτημα της SET, σε αντίθεση με αυτό του SSL, είναι ότι και οι δύο πλευρές διαπραγμάτευσης μιας σύνδεσης μπορούν να επιβεβαιώσουν την ταυτότητα του ενός και του άλλου. Επιπλέον, το SET μπορεί να προστατεύσει τα πιστωτικά στοιχεία των καταναλωτών, δεδομένου ότι ο έμπορος απαιτεί μόνο τα διαπιστευτήρια SET του καταναλωτή πριν να μπορέσει να χρεώσει την τράπεζα έκδοσης της κάρτας[162].

[161] Venkataiahgari, A.K., Atwood, J.W., Debbabi, M., Secure e-commerce transactions for multicast services. In IEEE International Conference on and Enterprise E-Commerce Technology, p. 18., 2006

[162] Guan, H.J., The research of SET-based electronic payment system model, International Conference on E-Business and Information System Security, 1–4 , 2009

Li, Y., The design of the secure electronic payment system based on the SET protocol. International Conference on Computer Science and Information Technology, 29–33 , 2008

Sherif, M.H., Serhrouchni, A., Gaid, A.Y., Farazmandnia, F., SET and SSL: electronic payments on the Internet. IEEE Symposium on Computers and Communications, 353–358, 1998

Με το μηχανισμό SET, εάν ένας καταναλωτής θέλει να πραγματοποιήσει συναλλαγή, θα πρέπει να εγκαταστήσει στον υπολογιστή το λογισμικό ηλεκτρονικού πορτοφολιού[163], το οποίο σαν ένα πραγματικό πορτοφόλι, είναι υπεύθυνο για την αποθήκευση των ηλεκτρονικών μετρητών. Πριν από τη συναλλαγή, ο καταναλωτής θα πρέπει πρώτα να αποσύρει κάποιο ποσό μετρητών από την τράπεζα. Η τράπεζα στη συνέχεια πιστοποιεί την ταυτότητα του καταναλωτή, αφαιρεί το ποσό των χρημάτων από το λογαριασμό του καταναλωτή, και καταβάλει το ποσό των ηλεκτρονικών μετρητών στο ηλεκτρονικό πορτοφόλι του καταναλωτή. Μετά από αυτό, ο καταναλωτής μπορεί να αγοράσει αγαθά από τους κατασκευαστές ή τα καταστήματα. Η παραπάνω διαδικασία δεν είναι πολύ φιλική προς τον καταναλωτή δεδομένου ότι δεν είναι μηχανισμός ''αρχική απόλαυση – πληρωμή στη συνέχεια''.

4.11. Υλοποίηση ενός Ολοκληρωμένου Συστήματος Ηλεκτρονικών Συναλλαγών

Για την Υλοποίηση ενός Ολοκληρωμένου Συστήματος Ηλεκτρονικών Συναλλαγών με ασφάλεια είναι απαραίτητη η ύπαρξη διαφόρων μεθόδων πληρωμών και οι πελάτες να έχουν προ-εγκαταστήσει λογισμικό πληρωμών καταναλωτή (customer wallet). Επιπλέον, το να υπάρχει ένας εξυπηρετητής πύλης πληρωμών με μια τράπεζα κάνει επιτρεπτή τη συμπλήρωση περιβάλλοντος ηλεκτρονικού εμπορίου[164].

Το λογισμικό *πληρωμών* καταναλωτή περιλαμβάνει λειτουργίες όπως το:

- Τμήμα καταχώρησης για τοπική καταχώρηση στο λογισμικό πληρωμών καταναλωτή.
- Τμήμα εισόδου για τοπική αυθεντικοποίηση καταναλωτών.
- Τμήμα πιστοποίησης καταχώρησης καταναλωτή και πιστοποίησης τράπεζας καταναλωτή.
- Τμήμα ασφαλών πληρωμών για ασφαλείς συναλλαγές με τον προμηθευτή.
- Τμήμα ερωτήσεων για πληρωμές και παραγγελίες.
- Τμήμα τοπικής διαχείρισης πληροφοριών με τις πιστωτικές κάρτες και σχετικό τμήμα με τις συναλλαγές.

[163] Chaudhary, A., Ahmad, K., Rizvi, M.A., E-commerce security through asymmetric key algorithm. International Conference Communication Systems and Network Technologies, 776–781, 2014
[164] Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.237)

Το λογισμικό *εξυπηρετητή* προμηθευτή επικοινωνεί με τρεις οντότητες του ολοκληρωμένου συστήματος συναλλαγών ασφάλειας, ήτοι (α) καταναλωτές, που τους παρέχεται η δυνατότητα εκτέλεσης συναλλαγών για πληρωμές κι αγορές με ασφαλή τρόπο, (β) πύλες πληρωμών (payment gateways) όπου εκτελούνται συναλλαγές πιστοποίησης κι ασφαλών πληρωμών, και (γ) τράπεζες, όπου εκτελούνται λειτουργίες καταχώρησης και πιστοποίησης.

Συνήθως, το λογισμικό εξυπηρετητή προμηθευτή εκτελεί λειτουργίες (α) διεπαφών κι ασφαλών ηλεκτρονικών συναλλαγών με τους καταναλωτές, (β) καταχώρησης και πιστοποίησης με τράπεζες, (γ) οικονομικών συναλλαγών με πύλες πληρωμών και (δ) διαχειριστικές του εξυπηρετητή.

4.12. Γραμμωτός κώδικας (Barcode)

Η τεχνολογία του γραμμωτού κώδικα αποτελεί τμήμα του γενικότερου τομέα τεχνολογιών αυτόματης αναγνώρισης (Auto ID Technologies). Είναι ένα εργαλείο σύγχρονο, και βοηθά στην ομαλή διακίνηση και διαχείριση προϊόντων και υπηρεσιών. Η ανάπτυξη αυτού του είδους της τεχνολογίας ξεκίνησε στις αρχές της δεκαετίας του 1960, για να εξυπηρετήσει την πληρωμή προϊόντων στα καταστήματα τροφίμων. Οι πρώτες εφαρμογές εμφανίστηκαν στα τέλη της ίδιας δεκαετίας, σε βιομηχανικό περιβάλλον, σε μεγάλες αυτοκινητοβιομηχανίες, με σκοπό τον περιορισμό του κόστους εργασίας που αφορούσε την παραγωγή. Έντονη χρήση του παρουσιάστηκε μετά την ανάπτυξη των πρώτων προτύπων, κυρίως λόγω των πιέσεων που ασκούσαν αρκετοί πλέον χρήστες - προμηθευτές, υποκατασκευαστών μεγάλων βιομηχανιών, στα τέλη του 1970. Κατά το 1980 εντάθηκε η ανάπτυξη του εξοπλισμού και κατ' επέκταση και των τρόπων χρήσης της τεχνολογίας γραμμωτού κώδικα.

4.13. Πυρήνας Σύνδεσης Δεδομένων (DCC)

Από την άποψη της ασφάλειας, σε ένα ασύρματο περιβάλλον επικοινωνίας υπάρχουν δύο βασικά χαρακτηριστικά. Πρώτον, τα μηνύματα που μεταδίδονται ασύρματα είναι ανασφαλή δεδομένου ότι οι χάκερς, τα ασύρματα συστήματα νόμιμης επιτελείας και οι χρήστες μπορούν να λαμβάνουν τα μηνύματα στο ίδιο χρόνο. Δεύτερον, ένα ασύρματο σύστημα πρέπει να πιστοποιεί τις ταυτότητες όσων παρουσιάζονται ανταποκριτές. Αν το σύστημα και ένας από τους χρήστες του δεν έχουν καμία σχέση πριν από την ασύρματη

επικοινωνία τους, τότε οι δύο οντότητες κατά την έναρξη της επικοινωνίας τους, δεν μπορούν να δημιουργήσουν ένα ασφαλές κανάλι για την ανταλλαγή μηνυμάτων. Φυσικά, οι δύο οντότητες επίσης δεν μπορούν αμοιβαία να αναγνωρίσουν ο ένας την ταυτότητα του άλλου από την ανταλλαγή ασφαλών μηνυμάτων. Αυτό θα προκαλέσει σοβαρά προβλήματα, όπως οι απάτες πιστωτικών καρτών ή η διαρροή των δεδομένων επικοινωνίας[165].

Μία από τις μεθόδους για την επίλυση αυτού του προβλήματος είναι η δημιουργία ενός μηχανισμού επαλήθευσης της ταυτότητας μεταξύ των δύο οντοτήτων εκ των προτέρων. Καλείται μηχανισμός ασφαλείας DCC, που χρησιμοποιείται για να προ-συνδέσει το ασύρματο σύστημα και τους χρήστες του. Για διαφορετικά συστήματα ασφαλείας και μηχανισμούς επικοινωνίας, το DCC έχει διαφορετικά περιεχόμενα.

4.14. Firewalls

Η λέξη firewall έχει να κάνει με πυρίμαχους τοίχους που δεν επιτρέπουν την εξάπλωση της φωτιάς από δωμάτιο σε δωμάτιο. Σχετικά με τα υπολογιστικά συστήματα νοούνται ως η αναγκαία λύση προστασίας αυτών ενώ συνδέονται με δίκτυα που είναι κι αυτά συνδεδεμένα στο διαδίκτυο. Πιο συγκεκριμένα, ως firewall μπορεί να οριστεί το λογισμικό ή το υλικό που επιτρέπει σε ορισμένους εξωτερικούς χρήστες με συγκεκριμένα χαρακτηριστικά να έχουν πρόσβαση σε ένα προστατευμένο δίκτυο ή δικτυακό τόπο. Ένα τέτοιο προστατευτικό τείχος επιτρέπει την πλήρη πρόσβαση στους έσω, σε υπηρεσίες έξω από συγκεκριμένο δίκτυο και παράλληλα παραχωρεί άδεια πρόσβασης επιλεκτικά στους έξω. Με δυο λόγια, τα firewalls αποτελούν μέθοδο ασφαλούς διατήρησης δικτύου.

Ένα firewall αποτελείται από τρεις ομάδες συνιστωσών[166]. Πρώτον, φίλτρα για μπλοκάρισμα ή και για παρακολούθηση μετάδοσης συγκεκριμένου είδους μηνύματος, δεύτερον, gateways για προώθηση των αποδεκτών μηνυμάτων από τη μια μεριά του firewall στην άλλη πλευρά και τρίτον, application proxies που εκτελούν έλεγχο ειδικής πρόσβασης σε εφαρμογές, παρακολούθηση και αναφορά.

Ένα σύστημα firewall θα πρέπει να:

- απορρίπτει κάθε πακέτο που ρητά ένας κανόνας δεν επιτρέπει να περάσει,
- κρατά τους εξωτερικούς χρήστες έξω απ' το προστατευμένο δίκτυο,

[165] Wei, W., Li, J., Cao, L., Ou, Y., Chen, J., Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web 16 (4), 449–475, 2013

[166] www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf

- διαθέτει προηγμένα εργαλεία καταγραφής, επίβλεψης και πρόκλησης συναγερμού που θα μπορούν να αναλύουν τις πραγματοποιημένες συναλλαγές για την εξαγωγή συμπερασμάτων αναφορικά με τις επιθέσεις και συνακόλουθα την προσαρμογή σε υφιστάμενη πολιτική ασφάλειας.

Περιληπτικά, ένα τέτοιο σύστημα πρέπει να μπορεί να προσφέρει υπηρεσίες ασφάλειας ελέγχου προσπέλασης συνδυάζοντας μηχανισμούς αυθεντικοποίησης, εξουσιοδότησης, επίβλεψης και κρυπτογράφησης.

Κεφάλαιο 5: Διαχείριση Ασφάλειας Πληροφοριών

Ο επιστημονικός κλάδος της πληροφορικής στην Ελλάδα υποφέρει από έλλειψη γενικής αποδεκτής ορολογίας, ιδίως στο θέμα ασφάλεια πληροφοριών. Οι αγγλικές λέξεις security, safety, insurance στα ελληνικά αποδίδονται ως ασφάλεια. Επομένως, χρειάζεται διαμόρφωση ενός κοινού λεξιλογίου για τα ζητήματα της Ασφάλειας Πληροφοριακών κι Επικοινωνιακών Συστημάτων. Ό,τι έχει αξία για έναν οργανισμό, για τις επιχειρησιακές του λειτουργίες, τη συνέχιση ύπαρξής του, ονομάζεται αγαθό (asset), συμπεριλαμβανομένων των πληροφοριακών πόρων. Τα αγαθά διακρίνονται σε φυσικά, πληροφορίες, λογισμικό, ανθρώπους κι άυλα. Λόγω της αξίας (value) που έχουν αυτά τα αγαθά, χρηματική ή μη, η προστασία τους θεωρείται απαραίτητη. Με την ύπαρξη κάποιας ζημίας (harm), η αξία αυτή θα μπορούσε να μειωθεί.

Μια δυνητική αιτία πρόκλησης παραβίασης της ασφάλειας που μπορεί να επιφέρει ζημία, καλείται απειλή (threat). Οι απειλές μπορεί να είναι φυσικές, τεχνικής φύσεως ή ανθρώπινες. Οι τελευταίες κατηγοριοποιούνται σε σκόπιμες και τυχαίες. Απειλές πραγματοποιούνται στην περίπτωση που το αγαθό έχει ευπάθειες. Με τον όρο ευπάθεια (vulnerability) νοείται η αδυναμία εκμετάλλευσης των απειλών απ' τα αγαθά. Οι ευπάθειες διακρίνονται σε υλικού, λογισμικού, δικτύου, προσωπικού, διαχειριστικής φύσεως, κτηρίου. Επίσης, η ύπαρξη ευπαθειών είναι δυνατή χωρίς να έχουν εντοπιστεί απειλές. Αν μια απειλή εκμεταλλευτεί μια ευπάθεια τότε προκύπτει παραβίαση ασφάλειας κι άρα υπόκεινται επιπτώσεις.

Η δυσμενής αλλαγή στο επίπεδο επίτευξης των επιχειρησιακών στόχων ονομάζεται επίπτωση (impact). Ως παραδείγματα αναφέρονται η οικονομική απώλεια, η διακοπή λειτουργίας, η απώλεια καλής φήμης, κλπ.

Σημαντική είναι και η έννοια του κινδύνου (risk) που αναφέρεται στο ενδεχόμενο μια απειλή να εκμεταλλευτεί ευπάθειες αγαθών προκαλώντας ζημία. Αντίμετρο ή αλλιώς μέτρο ασφάλειας (safeguard, control, countermeasure) ονομάζεται το μέτρο διαχείρισης του κινδύνου. Εδώ περιλαμβάνονται πολιτικές, κανόνες, διαδικασίες, οδηγίες, οργανωσιακές πρακτικές ή δομές διαχειριστικής, τεχνικής ή νομικής φύσεως. Υπάρχει και ο όρος υπόλοιπο κινδύνου που αναφέρεται στον κίνδυνο που απομένει μετά την εγκατάσταση των μέτρων ασφάλειας.

5.1. Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Εμπειρικές μελέτες έχουν δείξει πως το ένα τρίτο του χρόνου των υπεύθυνων για την ασφάλεια πληροφοριακών συστημάτων αφιερώνεται σε τεχνικά θέματα και τα δύο τρίτα στην ανάπτυξη πολιτικών διαδικασιών, σε μελέτες ανάλυσης κινδύνων, στη διαμόρφωση σχεδίων για επιχειρησιακή συνέχεια και σε δράσεις εκπαίδευσης του προσωπικού σχετικά με την ασφάλεια. Γενικώς είναι αποδεκτό ότι το προσωπικό αποτελεί πολύ μεγαλύτερη απειλή για την ασφάλεια πληροφοριών σε σχέση με τα πρόσωπα εκτός του οργανισμού. Το επίπεδο ασφάλειας πληροφοριών εξαρτάται από τα αποδεκτά επίπεδα κινδύνου που έχει καθορίσει ένας οργανισμός, τη λειτουργικότητα του πληροφοριακού συστήματος και το κόστος που διατίθεται για την ύπαρξη της ασφάλειας.

Το σύνολο των αλληλοσυσχετιζόμενων δραστηριοτήτων που χρησιμοποιεί πόρους για το μετασχηματισμό των εισροών σε εκροές είναι γνωστό ως διεργασία (process). Η ασφάλεια πληροφοριών είναι μια διεργασία. Η πληροφορία αποτελεί περιουσιακό στοιχείο κάθε οργανισμού κι επακολούθως η προστασία του αποτελεί ευθύνη της διοίκησης κι είναι επομένως θέμα ανθρώπων, θέμα διαχείρισης. Οι ενέργειες υλοποίησης μέτρων ασφάλειας αναφέρονται ως στοιχεία της διαχείρισης ασφάλειας πληροφοριών. Για το συντονισμό και τη συσχέτιση αυτών των ενεργειών είναι απαραίτητη η θέσπιση στόχων αναφορικά με την ασφάλεια πληροφοριών και για την επίτευξη αυτών χρησιμοποιείται ένα σύστημα διαχείρισης πληροφοριών.

Ως σύστημα διαχείρισης καλείται ένα πλαίσιο πολιτικών, διαδικασιών, οδηγιών και πόρων για την επίτευξη στόχων. Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ – Information Security Management System) είναι το τμήμα του συνολικού συστήματος διαχείρισης του οργανισμού που αφορά την ασφάλεια πληροφοριών[167]. Για την αποτελεσματικότητα ενός ΣΔΑΠ[168] οι δραστηριότητες δε θα πρέπει να αποκλίνουν από τους στόχους της καθ' αυτής επιχείρησης. Οι απαιτήσεις οι σχετικές με την ασφάλεια θα πρέπει να προσδιοριστούν ύστερα από μελέτη κι ανάλυση της διαχείρισης κινδύνου. Το ΣΔΑΠ χρειάζεται να έχει την υποστήριξη όλης της διοίκησης και να είναι συμβατό με την οργανωσιακή κουλτούρα.

Για τη διαχείριση της Ασφάλειας Πληροφοριών υπάρχουν διάφορες μεθοδολογίες που χρησιμοποιούν ή στηρίζονται σε κάποιο από τα πολλά πρότυπα που έχουν αναπτυχθεί. Μια διαδεδομένη μέθοδος ελέγχου και βελτίωσης διαδικασιών κατά την ανάπτυξη ενός

[167] Κάτσικας Σωκράτης Κ., "Διαχείριση της Ασφάλειας Πληροφοριών", Εκδόσεις Πεδίο & Σωκράτης Κ.Κάτσικας, Αθήνα 2014, σελ. 52

[168] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών είναι η μέθοδος Plan-Do-Check-Act (PDCA). Αυτή η μέθοδος αποτελείται από τέσσερα επαναληπτικά βήματα. Στο βήμα *Σχεδιασμός* (Plan) μελετάται η ασφάλεια πληροφοριών στον οργανισμό, θέτονται οι στόχοι και ορίζονται οι τρόποι επίτευξης αυτών. Στο βήμα *Υλοποίηση* (Do) θέτονται σε εφαρμογή τα μέτρα που τέθηκαν κατά τη φάση του σχεδιασμού. Εν συνεχεία, γίνεται *Έλεγχος* (Check) απόκλισης απ' τους αρχικούς στόχους και έλεγχος των τελικών αποτελεσμάτων. Στο τέταρτο βήμα *Δράση* (Act) γίνονται ενέργειες διόρθωσης και βελτίωσης των μέτρων.

Το ΣΔΑΠ στην ουσία αφορά μία ενιαία διεργασία που δέχεται ως είσοδο τις απαιτήσεις ασφάλειας του οργανισμού και παρέχει ως έξοδο τη διαχείριση της ασφάλειας πληροφοριών. Στη φάση του *σχεδιασμού* αναλύεται κι εκτιμάται η επικινδυνότητα ασφάλειας των πληροφοριών. Δηλαδή, πραγματοποιείται:

- Στήριξη από τη Διοίκηση.
- Καθορισμός πεδίου εφαρμογής (υπολογιστικά συστήματα, κλπ.).
- Απογραφή πληροφοριακών αγαθών.
- Μελέτη ανάλυσης κι εκτίμησης επικινδυνότητας.
- Καθορισμός απαιτήσεων ασφάλειας.
- Δημιουργία πολιτικής ασφάλειας.

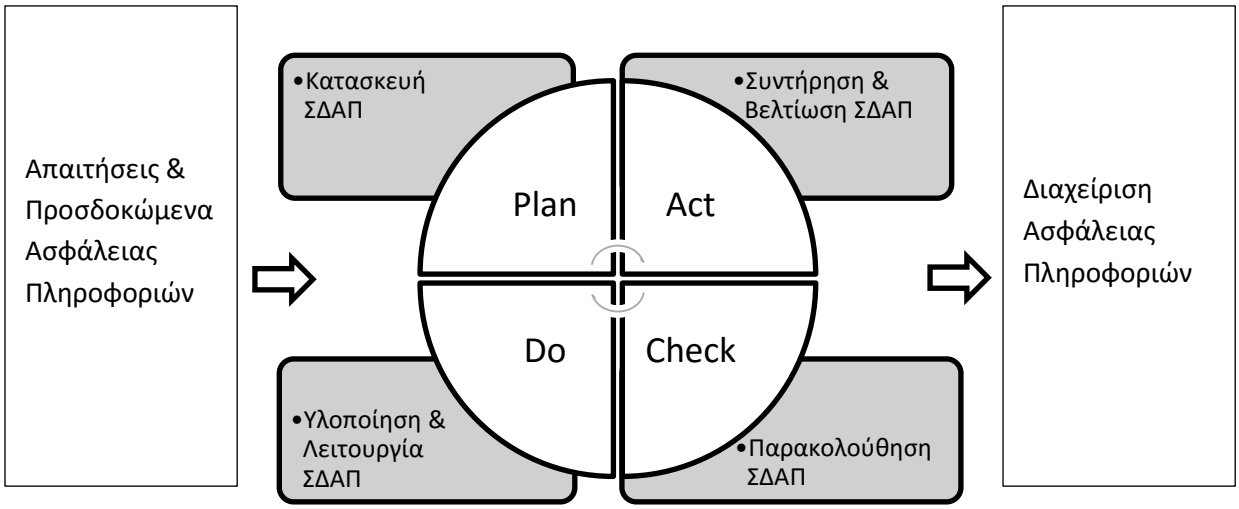
Στη φάση της *υλοποίησης* ακολουθείται μελέτη που σκοπό έχει τη μείωση της επικινδυνότητας με τη διαλογή κι εφαρμογή των κατάλληλων μέτρων προστασίας. Δηλαδή, εφαρμόζεται:

- Σχέδιο Διαχείρισης Επικινδυνότητας.
- Κατανομή ρόλων και αρμοδιοτήτων.
- Υλοποίηση ΣΔΑΠ.
- Δράσεις ενημέρωσης και κατάρτισης του προσωπικού.
- Υλοποίηση διαδικασιών έγκαιρης ανίχνευσης και αντιμετώπισης περιστατικών ασφάλειας.

Στη φάση *έλεγχος* γίνεται αξιολόγηση των αποτελεσμάτων σύμφωνα με τους αρχικά τιθέμενους στόχους και πραγματοποιείται μια αναφορά αξιολόγησης στη διοίκηση. Η διαδικασία του ελέγχου είναι επαναληπτική και γίνεται από το αρμόδιο τμήμα εσωτερικού ελέγχου. Στο στάδιο της *δράσης* εκτελούνται ενέργειες που έχουν κριθεί απαραίτητες για τη βελτίωση της συνολικής διεργασίας διαχείρισης της ασφάλειας πληροφοριών. Ενημερώνεται η διοίκηση κι ελέγχεται κι αξιολογείται η ίδια η διαδικασία βελτίωσης των μέτρων προστασίας. Συνδυάζοντας τα τέσσερα βήματα της μεθοδολογίας PDCA με το

πρότυπο ISO/IEC 27001 ορίζεται το πλαίσιο της Διαχείρισης Ασφάλειας Πληροφοριών, όπως παρουσιάζεται στο παρακάτω γράφημα.

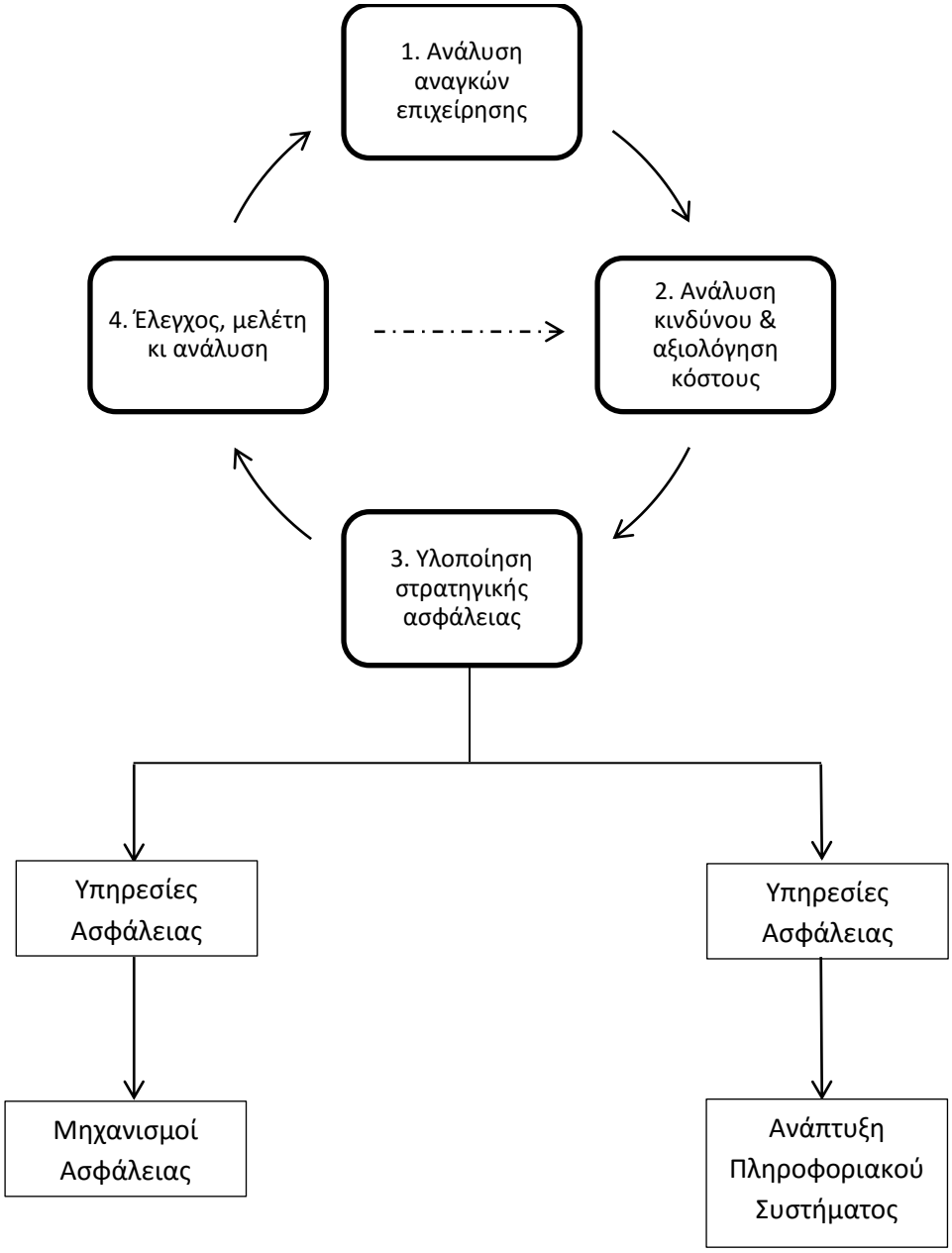
Γράφημα 5.1: Διαχείριση Ασφάλειας Πληροφοριών κατά ISO/IEC 27001.



Πηγή: Ιωάννης Μαυρίδης, Ασφάλεια Πληροφοριών στο Διαδίκτυο, σελ. 208 ISBN: 978-960-603-193-9,

Η υπόθεση ότι η ασφάλεια είναι ζήτημα τεχνολογικής φύσεως είναι λανθασμένη. Ο Baskerville σημείωσε ότι τα πληροφοριακά συστήματα και η ασφάλεια πρέπει να διαχωριστούν διαφορετικά θα υπάρξουν συγκρούσεις και διαφωνίες για το σύστημα και την ασφάλεια. Το μοντέλο που παρουσιάζεται παρακάτω αναπτύχθηκε λαμβάνοντας υπόψη το παραπάνω θέμα και παρουσιάζεται ως μια κυκλική επαναληπτική διαδικασία σχεδιασμού κι ανάπτυξης μιας στρατηγικής ασφάλειας πληροφοριών.

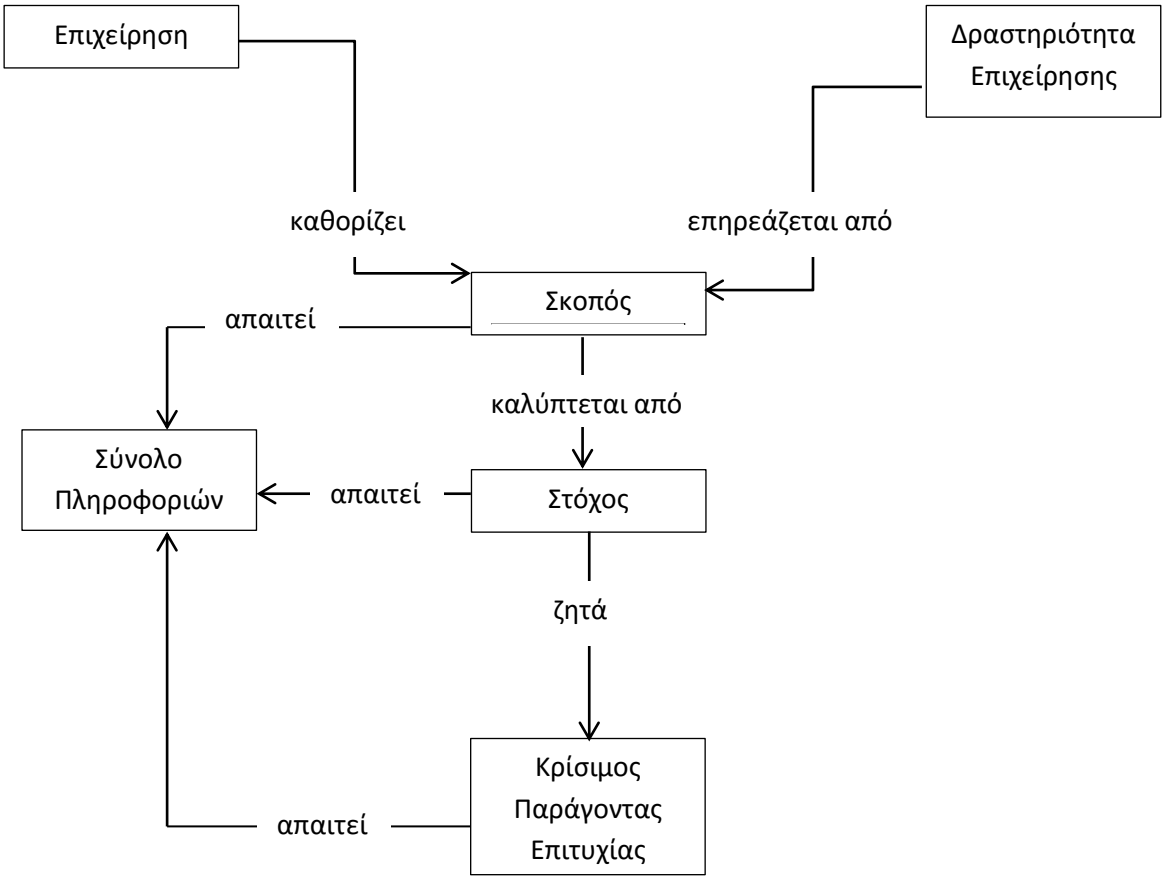
Γράφημα 5.2: Μοντέλο Στρατηγικής Πληροφοριακού Συστήματος



Πηγή: Baskerville, R. (1993), "Information systems security design methods: implications for information systems development", ACM Computing Surveys, Vol. 25 No. 4, pp. 375-414

Η ανάλυση αναγκών επιχείρησης είναι το πρώτο βήμα για τη δημιουργία και τη διατήρηση μιας στρατηγικής ασφάλειας πληροφοριών που θα πρέπει να αντανακλά την ολική αποστολή και τους στόχους που έχει θέσει μια επιχείρηση.

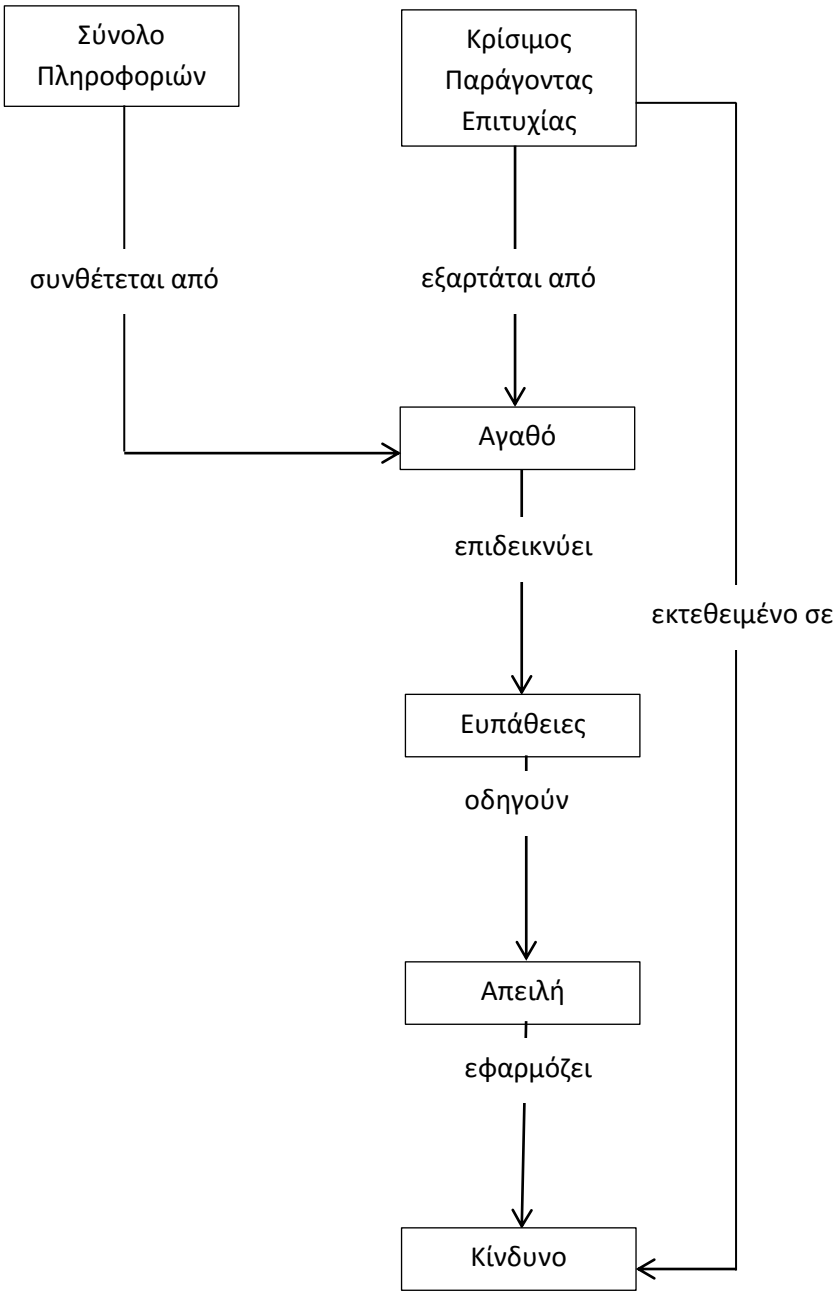
Γράφημα 5.3: Ανάλυση αναγκών επιχείρησης



Πηγή: N. Kolokotronis C. Margaritis P. Papadopoulou P. Kanellis D. Martakos, "An integrated approach for securing electronic transactions over the Web", Benchmarking: An International Journal, 2002, Vol. 9 Iss 2 pp. 166 – 181- Permanent link to this document: http://dx.doi.org/10.1108/14635770210421836

Η ανάλυση κινδύνου κι η αξιολόγηση κόστους συγκεκριμενοποιεί τους παράγοντες απ' το προηγούμενο βήμα που είναι κρίσιμοι για την πηγή πληροφόρησης. Πιθανές ευπάθειες κι απειλές πρέπει να εξετάζονται σε όλα τα επίπεδα. Παράλληλα, πρέπει να πραγματοποιείται αξιολόγηση του κόστους πιθανής ζημίας σχετιζόμενη με το κόστος πρόληψης από συγκεκριμένη απειλή συμπεριλαμβάνοντας στον υπολογισμό το χρόνο, τα έξοδα και τους πόρους που θα διατεθούν στην κάθε περίπτωση. Ο κάθε κίνδυνος πρέπει να κατηγοριοποιείται με βάση την πιθανότητα αυτού να συμβεί και τις επιπτώσεις που ενδέχεται να φέρει.

Γράφημα 5.4: Ανάλυση κινδύνου

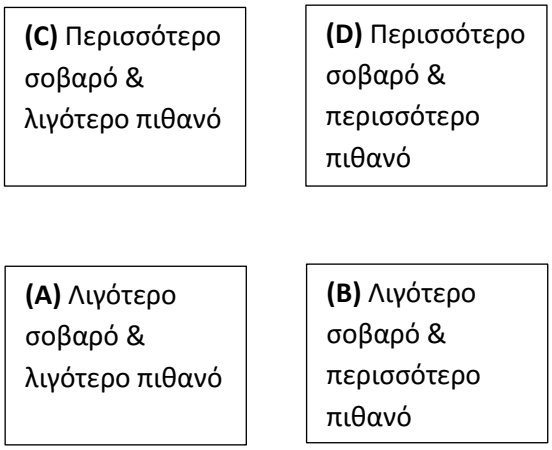


Πηγή: N. Kolokotronis C. Margaritis P. Papadopoulou P. Kanellis D. Martakos, (2002),"An integrated approach for securing electronic transactions over the Web", Benchmarking: An International Journal, Vol. 9 Iss 2 pp. 166 – 181- Permanent link to this document: http://dx.doi.org/10.1108/14635770210421836

Η υλοποίηση στρατηγικής ασφάλειας αναφέρεται στην εγγύηση της αποτελεσματικότερης χρήσης των πόρων. Η πληροφορία που συσσωρεύεται απ' τα προηγούμενα βήματα χρησιμοποιείται για α) ταυτοποίηση υπηρεσιών ασφάλειας που πρέπει να παρέχονται από τεχνικής άποψης και για β) επέκταση της ανάλυσης του συστήματος και σχεδιασμού καθηκόντων κατά την εφαρμογή των επιχειρηματικών

διαδικασιών. Στη διαδικασία αυτή συμπεριλαμβάνεται η εξέταση παρόμοιων αναφορών από άλλες επιχειρήσεις και η εφαρμογή καλών πρακτικών. Διαφορετικά επίπεδα δεδομένων χρειάζονται διαφορετική παροχή ασφάλειας.

Γράφημα 5.5: Κατηγοριοποίηση κινδύνου



Πηγή: N. Kolokotronis C. Margaritis P. Papadopoulou P. Kanellis D. Martakos, (2002),"An integrated approach for securing electronic transactions over the Web", Benchmarking: An International Journal, Vol. 9 Iss 2 pp. 166 – 181- Permanent link to this document: http://dx.doi.org/10.1108/14635770210421836

Το τελευταίο βήμα που αφορά τον έλεγχο, τη μελέτη και την ανάλυση μπορεί να εκτελεστεί μέσω της χρήσης πληθώρων εργαλείων που είναι ευρέως διαθέσιμα από προμηθευτές λογισμικού. Η αποτελεσματική χρήση τους μπορεί να καθορίσει την ανάγκη περαιτέρω ανάλυσης κι επανεξέτασης του επιπέδου κινδύνου κατά τη λειτουργία του συστήματος. Σε αυτό το βήμα μπορεί να εντοπιστούν μειονεκτήματα της εφαρμοζόμενης στρατηγικής ή σημαντικά κενά απ' την αλλαγή των σκοπών ή των δραστηριοτήτων της επιχείρησης.

Οι μηχανισμοί ασφάλειας και οι μεμονωμένες λύσεις που εφαρμόζονται απ' τους οργανισμούς, προσφέρουν λύση ως προς την ασφάλεια, αλλά μόνο σε ότι έχει να κάνει με το πεδίο εφαρμογής. Για αυτό είναι επιτακτική η ανάγκη ορισμού ενός πλαισίου, στη βάση του οποίου να αντιμετωπίζεται με ολιστική προσέγγιση το πρόβλημα της ασφάλειας πληροφοριών. Στις δράσεις αυτές συμπεριλαμβάνονται θεσμικές, οργανωσιακές αλλά και κοινωνικές δράσεις.

Οι θεσμικές κατηγοριοποιούνται σε κανονιστικές και νομικές. Παράδειγμα κανονιστικής ρύθμισης αποτελούν τα πρότυπα και οι κώδικες δεοντολογίας που

συμπληρώνουν την υπάρχουσα νομοθεσία. Μια άλλου είδους κατηγοριοποίηση των θεσμικών ρυθμίσεων μπορεί να γίνεται με βάση το γεωγραφικό πεδίο εφαρμογής τους, έχοντας έτσι διεθνείς, περιφερειακές, εθνικές και τοπικές ρυθμίσεις. Τέλος, οι συγκεκριμένες ρυθμίσεις μπορούν να κατηγοριοποιούνται με το τομεακό πεδίο εφαρμογής τους. Σε περίπτωση που μια θεσμική ρύθμιση εφαρμόζεται σε πάνω από έναν τομείς τότε υπάρχει οριζόντια θεσμική ρύθμιση. Αν όμως η θεσμική ρύθμιση αφορά έναν τομέα, τότε υπάρχει κάθετη θεσμική ρύθμιση.

Οι οργανωσιακές ρυθμίσεις έχουν να κάνουν με τα μέτρα οργάνωσης που πρέπει να παίρνονται προκειμένου να διασφαλιστεί η ασφάλεια των πληροφοριών. Παράδειγμα αποτελεί μια στρατηγική και οι σχετικές πολιτικές.

Ένα πρότυπο είναι ένα σύνολο αποδεκτών κριτηρίων, μεθόδων και διεργασιών ή πρακτικών. Τα πρότυπα μπορεί να προκύπτουν από ενώσεις εταιρειών ή οργανισμών προτυποποίησης κατόπιν έρευνας και ευρύτερης συμφωνίας. Προτυποποίηση είναι η διεργασία ανάπτυξης και υλοποίησης τεχνικών προτύπων. Προκειμένου να εξασφαλιστεί η συμμόρφωση ενός οργανισμού με συγκεκριμένες προδιαγραφές χρειάζεται αυτός να αξιολογείται με σκοπό την απόκτηση του αντίστοιχου πιστοποιητικού συμμόρφωσης (πιστοποίηση). Η πιστοποίηση ορίζει τις διαδικασίες αξιολόγησης και ελέγχου ενός οργανισμού. Τα πιο γνωστά πρότυπα ασφάλειας πληροφοριών είναι η σειρά ISO/IEC 27000 και τα Common Criteria.

5.2. Η σειρά προτύπων ISO27k

Η δημιουργία ενός ΣΔΑΠ άρχισε τέλη της δεκαετίας του ’80 όταν παρουσιάστηκε η πρόταση των «άριστων ελαχίστων μέτρων ασφάλειας (baseline best controls)», στην Αγγλία και στις ΗΠΑ κυρίως. Η ιδέα αυτή αφορούσε στη δημιουργία ενός καταλόγου με τα αποτελεσματικά μέτρα ασφάλειας που πρέπει ούτως ή άλλως να εφαρμόσει ένας οργανισμός. Το 1990 συγκροτήθηκε μια ομάδα εκπροσώπων επιχειρήσεων απ’ τη βρετανική κυβέρνηση προωθώντας την πρόταση προκύπτοντας κατά αυτόν τον τρόπο ένας κώδικας καλής πρακτικής με αντικείμενο τη διαχείριση της ασφάλειας πληροφοριών, ο οποίος υιοθετήθηκε το 1995 απ’ το βρετανικό οργανισμό προτυποποίησης (BSI – British Standards Institute) ως BS 7799-1. Μετά από δυο χρόνια δημοσιεύτηκε το πρότυπο BS 7799-2 το οποίο περιέγραφε τις προδιαγραφές του ΣΔΑΠ. Το δεύτερο πρότυπο χρησίμευε ώστε να χρησιμοποιηθεί ως πρότυπο συμμόρφωσης για τη δυνατότητα πιστοποίησης του ΣΔΑΠ κατά BS 7799-1.

Το 1997-8 έγιναν επιτυχείς δοκιμές του συστήματος και ξεκίνησαν να δείχνουν το ενδιαφέρον τους για αυτά τα πρότυπα κι άλλες χώρες, όπως η Σουηδία, η Αυστραλία, η Ινδία, η Ολλανδία. Μέχρι τέλη του 1999 τα πρότυπα είχαν υιοθετηθεί από 20 χώρες.

Το 2000 το βρετανικό πρότυπο BS 7799-1 υποβλήθηκε στο ISO/IEC ως ISO/IEC 17799 και το 2002 αναριθμήθηκε σε ISO/IEC 27002. Ακολούθως, το 2005 δημοσιεύτηκε το BS 7799-2 ως ISO/IEC 27001. Η σειρά ISO27k έχει σχεδιαστεί όμοια με τη σειρά ISO 9000, παρέχει συστάσεις καλών πρακτικών για τη διαχείριση πληροφοριών και κινδύνων και τα μέτρα ασφάλειας μέσα στο περιβάλλον ενός ΣΔΑΠ. Η παρούσα κατάσταση των προτύπων της σειράς παρουσιάζεται ακολούθως. Το έτος δημοσίευσης ακολουθεί τον αριθμό σειράς μετά την άνω και κάτω τελεία, π.χ. το ISO/IEC 27000:2016 είναι το πρότυπο 27000 που δημοσιεύτηκε το έτος 2016. Αναφέρονται ο αριθμός σειράς και το αντικείμενο των προτύπων[169].

Πίνακας 5.1: Τα δημοσιευμένα πρότυπα της σειράς ISO27k

ISO/IEC 27000:2016 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Συστήματα διαχείρισης της ασφάλειας των πληροφοριών - Επισκόπηση και λεξιλόγιο
ISO/IEC 27001:2013, ISO/IEC 27001:2013/Cor 1:2014, ISO/IEC 27001:2013/Cor 2:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Συστήματα διαχείρισης της ασφάλειας των πληροφοριών - Απαιτήσεις
ISO/IEC 27002:2013 , ISO/IEC 27002:2013/Cor 1:2014 , ISO/IEC 27002:2013/Cor 2:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κώδικας πρακτικής για τους ελέγχους ασφάλειας των πληροφοριών
ISO/IEC 27003:2010 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Πληροφορίες διαχείρισης της ασφάλειας των οδηγιών εφαρμογής του συστήματος. Περιγράφει τη διεργασία λήψης έγκρισης απ'τη διοίκηση και την υλοποίηση του ΣΔΑΠ κι ορίζει το έργο υλοποίησής του και παρέχει οδηγίες για το σχεδιασμό του έργου ΣΔΑΠ για να αποτελέσει σχέδιο υλοποίησης αυτού.
ISO/IEC 27004:2009 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Πληροφορίες διαχείρισης της

[169] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on&includesc=true

ασφάλειας των οδηγιών εφαρμογής του συστήματος. Δίνει κατευθυντήριες γραμμές για τη χρήση μετρήσεων ώστε να εκτιμηθεί η αποτελεσματικότητα ενός υλοποιούμενου ΣΔΑΠ με βάση το ISO/IEC 27001.
ISO/IEC 27005:2011 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Πληροφορίες διαχείρισης των κινδύνων ασφαλείας
ISO/IEC 27006:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης συστημάτων διαχείρισης της ασφάλειας των πληροφοριών
ISO/IEC 27007:2011 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για τον έλεγχο των συστημάτων διαχείρισης της ασφάλειας των πληροφοριών
ISO/IEC TR 27008:2011 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για τους ελεγκτές σχετικά με τους ελέγχους ασφάλειας των πληροφοριών
ISO/IEC 27010:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Διαχείριση της ασφάλειας των πληροφοριών για διατομεακές και δια-οργανωτικές επικοινωνίες
ISO/IEC 27011:2008 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για τη διαχείριση της ασφάλειας των πληροφοριών για τους οργανισμούς τηλεπικοινωνιών με βάση το πρότυπο ISO / IEC 27002
ISO/IEC 27013:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Καθοδήγηση για την ολοκληρωμένη εφαρμογή του ISO / IEC 27001 και ISO / IEC 20000-1
ISO/IEC 27014:2013 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Διακυβέρνηση της ασφάλειας των πληροφοριών
ISO/IEC TR 27015:2012 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για τη διαχείριση της ασφάλειας των πληροφοριών για τις χρηματοπιστωτικές υπηρεσίες
ISO/IEC TR 27016:2014 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Διαχείριση της ασφάλειας των πληροφοριών - Οργανωτική οικονομία

ISO/IEC 27017:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κώδικας πρακτικής για τους ελέγχους ασφάλειας των πληροφοριών με βάση το πρότυπο ISO / IEC 27002 για τις υπηρεσίες cloud
ISO/IEC 27018:2014 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κώδικας πρακτικής για την προστασία των προσωπικά αναγνωρίσιμων πληροφοριών (PII-ΠΑΠ) στα δημόσια σύννεφα λειτουργώντας ως επεξεργαστές ΠΑΠ
ISO/IEC TR 27019:2013 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για τη διαχείριση της ασφάλειας των πληροφοριών με βάση το πρότυπο ISO / IEC 27002 για συστήματα ελέγχου τεχνολογικής διαδικασίας ειδικά για τον κλάδο κοινής ωφέλειας ενέργειας
ISO/IEC TR 27023:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Χαρτογραφώντας τις αναθεωρημένες εκδόσεις του προτύπου ISO / IEC 27001 και ISO / IEC 27002
ISO/IEC 27031:2011 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για την τεχνολογία της πληροφορίας και της επικοινωνίας ετοιμότητα για την επιχειρησιακή συνέχεια
ISO/IEC 27032:2012 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Οδηγίες για την ασφάλεια στον κυβερνοχώρο
ISO/IEC 27033-1:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Η ασφάλεια των δικτύων - Μέρος 1: Επισκόπηση και έννοιες
ISO/IEC 27033-2:2012 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Η ασφάλεια των δικτύων - Μέρος 2: Κατευθυντήριες γραμμές για τον σχεδιασμό και την υλοποίηση της ασφάλειας των δικτύων
ISO/IEC 27033-3:2010 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Η ασφάλεια των δικτύων - Μέρος 3: σενάρια δικτύωσης Αναφοράς - Απειλές, τεχνικές σχεδιασμού και θέματα ελέγχου
ISO/IEC 27033-4:2014 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Η ασφάλεια των δικτύων - Μέρος 4: Εξασφάλιση των επικοινωνιών μεταξύ των δικτύων που χρησιμοποιούν πύλες ασφαλείας

ISO/IEC 27033-5:2013 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Η ασφάλεια των δικτύων - Μέρος 5: Η εξασφάλιση των επικοινωνιών σε όλα τα δίκτυα που χρησιμοποιούν Εικονικά Ιδιωτικά Δίκτυα (VPNs)
ISO/IEC 27034-1:2011 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας – Αίτηση Ασφάλειας - Μέρος 1: Επισκόπηση και έννοιες
ISO/IEC 27034-1:2011/Cor 1:2014
ISO/IEC 27034-2:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Αίτηση Ασφάλειας - Μέρος 2: Οργάνωση κανονιστικό πλαίσιο
ISO/IEC 27035:2011 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Πληροφορίες διαχείρισης περιστατικών ασφαλείας
ISO/IEC 27036-1:2014 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Ασφάλεια των πληροφοριών για τις σχέσεις με τον προμηθευτή - Μέρος 1: Επισκόπηση και έννοιες
ISO/IEC 27036-2:2014 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - ασφάλεια των πληροφοριών για τις σχέσεις με τον προμηθευτή - Μέρος 2: Απαιτήσεις
ISO/IEC 27036-3:2013 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Ασφάλεια των πληροφοριών για τις σχέσεις με τον προμηθευτή - Μέρος 3: Κατευθυντήριες γραμμές για την τεχνολογία της πληροφορίας και της επικοινωνίας ασφάλεια της αλυσίδας εφοδιασμού
ISO/IEC 27037:2012 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για τον προσδιορισμό, την επιλογή, την απόκτηση και διατήρηση των ψηφιακών αποδεικτικών στοιχείων
ISO/IEC 27038:2014 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Προδιαγραφή για την ψηφιακή επιμέλεια
ISO/IEC 27039:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Επιλογή, εγκατάσταση και λειτουργία των συστημάτων ανίχνευσης εισβολών (IDP)

ISO/IEC 27040:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Ασφάλεια αποθήκευσης
ISO/IEC 27041:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Καθοδήγηση για τη διασφάλιση της καταλληλότητας και της επάρκειας της μεθόδου διερεύνησης περιστατικών
ISO/IEC 27042:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Κατευθυντήριες γραμμές για την ανάλυση και την ερμηνεία των ψηφιακών αποδεικτικών στοιχείων
ISO/IEC 27043:2015 Η τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Αρχές διερεύνησης των περιστατικών και των διαδικασιών

Τα πρότυπα ISO/IEC 27001 και ISO/IEC 27006 είναι τα μόνα πρότυπα που μπορούν να χρησιμοποιηθούν για πιστοποίηση από τρίτα μέρη. /μια επιχείρηση μπορεί να πιστοποιηθεί από ανεξάρτητους φορείς για τη συμμόρφωση του ΣΔΑΠ με το ISO/IEC 27001 ενώ ένας φορέας πιστοποίησης μπορεί να διαπιστευτεί σύμφωνα με το ISO/IEC 27006. Τα υπόλοιπα πρότυπα δίνουν κατευθύνσεις γενικής φύσεως ή σε συγκεκριμένους τομείς[170].

Το ISO/IEC 27001 είναι ένα πρότυπο[171] για συστήματα διαχείρισης ασφάλειας πληροφοριών (ISMS) κι ανήκει στην οικογένεια προτύπων ISO/IEC 27000. Τα πρότυπα περιλαμβάνουν εκατοντάδες πιθανούς ελέγχους και μηχανισμούς ελέγχου[172]. Σκοπός του προτύπου είναι να θέσει προδιαγραφές για το σχεδιασμό, την υλοποίηση, τη λειτουργία, την παρακολούθηση, τον έλεγχο και τη συντήρηση ενός ΣΔΑΠ. Περιέχει επίσης προδιαγραφές για την εκτίμηση και διαχείριση κινδύνων. Το πρότυπο εφαρμόζετι σε όλους τους τύπους οργανισμών.

Το πρότυπο ISO/IEC 27001:2013 αποτελεί το διεθνές πρότυπο για την ασφάλεια πληροφοριών, έχει αυστηρές απαιτήσεις σε όλους τους τομείς που επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των δεδομένων. Όλα αυτά, από την ασφάλεια των εγκαταστάσεων, τη διαχείριση του ανθρωπίνου δυναμικού, τις διαδικασίες οργάνωσης, τις διαδικασίες λειτουργίας, τις συνεταιριστικές σχέσεις, τις πελατειακές σχέσεις, τη συμμόρφωση με νομικές απαιτήσεις,

[170] Κάτσικας Σωκράτης Κ., "Διαχείριση της Ασφάλειας Πληροφοριών", Εκδόσεις Πεδίο & Σωκράτης Κ.Κάτσικας, Αθήνα 2014, σελ. 61
[171] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
[172] http://www.microsoft.com/online/legal/v2/el-gr/MOS_PTC_Security_Audit.htm

μέχρι την ασφάλεια των υποδομών επικοινωνιών και πληροφορικής, τη συνεχή εκπαίδευση προσωπικού και το σχεδιασμό επιχειρησιακής συνέχειας[173].

Ένας οργανισμός μπορεί να αποκτήσει πιστοποίηση ISO 27001 για τα συστήματα διαχείρισης ασφάλειας πληροφοριών (ISMS) που διαθέτει, η οποία κατά κανόνα βασίζεται στα Πρότυπα Ασφάλειας Πληροφοριών[174] ISO 27002.

5.3. Το Οργανωσιακό Πλαίσιο Ασφάλειας

Η Πολιτική Ασφάλειας αναφέρεται στο οργανωσιακό πλαίσιο της Ασφάλειας Πληροφοριών. Το οργανωσιακό πλαίσιο περιλαμβάνει έγγραφα για ***πολιτικές, κανόνες, διαδικασίες και οδηγίες***. Το σύνολο αυτών των εγγράφων καλείται Σχέδιο Ασφάλειας. Το πλαίσιο ασφάλειας αποτελεί κεντρικό σημείο αναφοράς για την επικοινωνία μεταξύ των εμπλεκομένων για να αναπτυχθεί κοινή αντίληψη περί του θέματος ασφάλεια και για να διευκολυνθεί η συνεργασία μεταξύ τους.

Πολιτική Ασφάλειας

Η πολιτική (policy) είναι μια τυπική και σύντομη δήλωση που εκφράζει τις γενικές πεποιθήσεις, τους σκοπούς, τους στόχους και τις διαδικασίες σε συγκεκριμένο θέμα. Οι πολιτικές ορίζουν τους στόχους και συνοδεύονται από κανόνες και οδηγίες. Η συμμόρφωση στην πολιτική είναι υποχρεωτική και η μη-συμμόρφωση ισοδυναμεί με πειθαρχικό παράπτωμα. Στις επιχειρήσεις συναντώνται διάφορα είδη πολιτικών ασφάλειας πληροφοριών. Στο υψηλότερο επίπεδο ανήκει η οργανωσιακή πολιτική ασφάλειας πληροφοριών που περιέχει: α) στόχους του οργανισμού σχετικά με την ασφάλεια πληροφοριών, β) καθήκοντα εμπλεκομένων, γ) υποστήριξη της Διοίκησης ως προς τη συμμόρφωση, δ) πλάνο ελέγχου διαδικασιών και ε) πλάνο κατάλληλης κατάρτισης προσωπικού.

Στο αμέσως χαμηλότερο επίπεδο, κάθε επιμέρους πολιτική ασφάλειας πληροφοριών σχετίζεται με συγκεκριμένες ομάδες ανθρώπων εντός του οργανισμού και καλύπτει συγκεκριμένες θεματικές περιοχές. Παραδείγματα αποτελούν η πολιτική ελέγχου πρόσβασης, η πολιτική ασφάλειας επικοινωνιών, η πολιτική κρυπτογραφικών τεχνικών, η πολιτική ιδιωτικότητας και προστασίας πληροφοριών προσωπικού χαρακτήρα, κ.ά.

---

[173] http://www.bsigroup.com/en-GB/iso-27001-information-security/
[174] http://www.microsoft.com/online/legal/v2/el-gr/MOS_PTC_Security_Audit.htm

Τα άλλα στοιχεία του πλαισίου

Ο όρος *κανόνες* (standards) αναφέρεται σε απαιτήσεις που είναι υποχρεωτικές κι υποστηρίζουν τις πολιτικές. Οι κανόνες καλύπτουν θέματα που αφορούν το είδος της χρήσης του υλικού, του λογισμικού, του πρωτοκόλλου, του προσωπικού που θα είναι υπεύθυνο. Η *διαδικασία* (procedure) σχετίζεται με τα βήματα που πρέπει να ακολουθηθούν για την επίτευξη του τελικού σκοπού. Οι διαδικασίες σκιαγραφούν τον τρόπο προστασίας των πόρων κι αποτελούν μηχανισμούς επιβολής πολιτικών. Οι οδηγίες (guidelines) αφορούν δηλώσεις, εντολές διοικητικές που σκοπό έχουν την επίτευξη των στόχων μιας πολιτικής, δεν είναι όμως υποχρεωτικές κι αποτελούν υποδείξεις στους χρήστες. Λόγω της αλλαγής του περιβάλλοντος, οι οδηγίες αλλάζουν συχνά.

5.4. Ευρωπαϊκή Ένωση και Προστασία Δεδομένων

Πρόσφατα, η Ευρωπαϊκή Ένωση, μέσω της Οδηγίας της ΕΕ για την προστασία των δεδομένων[175], εφαρμόζει κανόνες προστασίας προσωπικών δεδομένων πιο αυστηρούς από αυτούς των Η.Π.Α. και τις περισσότερες άλλες χώρες/περιοχές. Για την επιβολή αυτών των κανόνων, η ΕΕ απαγορεύει τη μεταφορά προσωπικών δεδομένων εκτός των συνόρων της, δηλαδή δεν επιτρέπεται μεταφορά σε άλλες χώρες, εκτός της περίπτωσης που συντρέχουν οι συνθήκες που η μεταφορά είναι νόμιμη μέσω αναγνωρισμένων μηχανισμών, όπως για παράδειγμα μέσω του μηχανισμού πιστοποίησης "Safe Harbor".

Για να επιτραπεί η συνεχής ροή πληροφοριών, η Ευρωπαϊκή Επιτροπή προχώρησε σε σύναψη σύμβασης με το Υπουργείο Εμπορίου των Η.Π.Α., με βάση την οποία οι οργανισμοί των Η.Π.Α. δύνανται να αποκτήσουν ίδια πιστοποίηση συμμόρφωσης με τις βασικές αρχές του πλαισίου ασφαλείας Safe Harbor που προσομοιάζονται σε γενικές γραμμές στις απαιτήσεις της Οδηγίας[176].

Για να κατορθώσει μια επιχείρηση να μεταφέρει δεδομένα από την ΕΕ στις Η.Π.Α. νόμιμα, ο οποιοσδήποτε οργανισμός στις Η.Π.Α. πρέπει να πιστοποιήσει δημόσια ότι συμμορφώνεται με τις βασικές αρχές του πλαισίου ασφάλειας Safe Harbor που ευθυγραμμίζονται με τους κανόνες της ΕΕ για την προστασία προσωπικών δεδομένων.

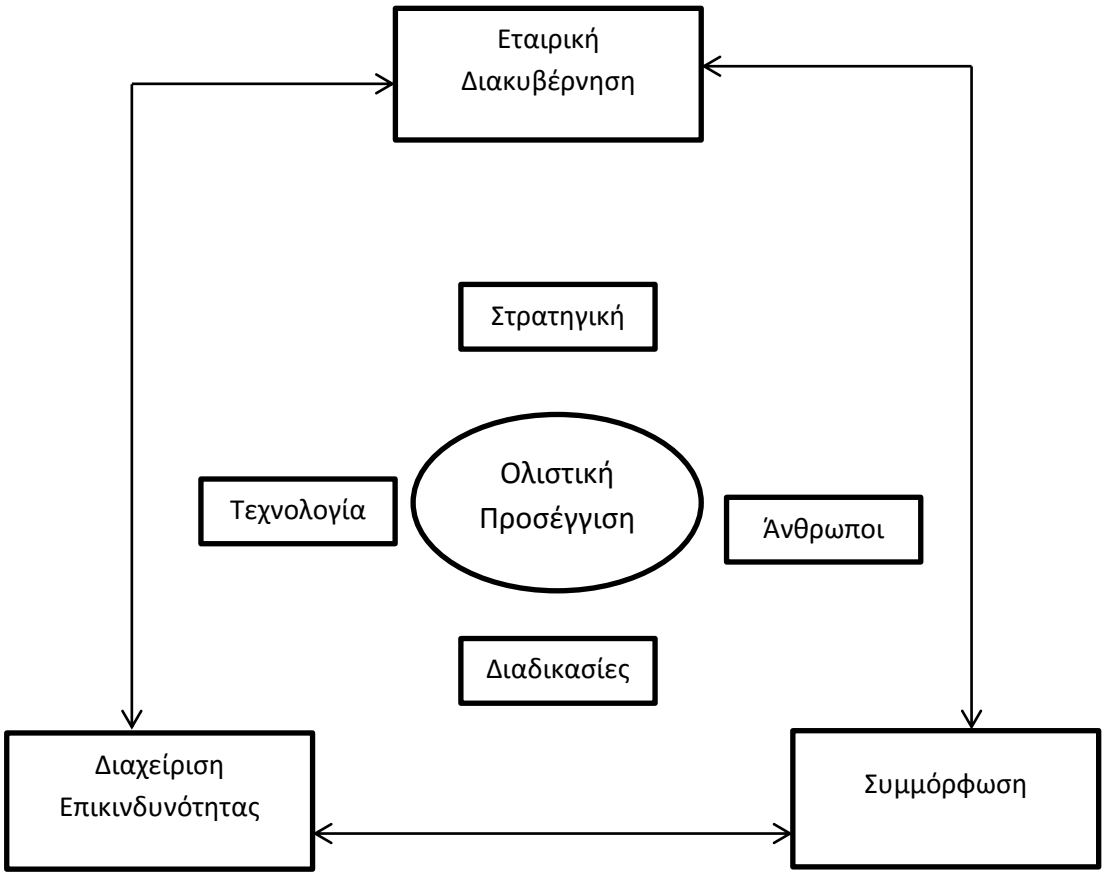
[175] http://www.export.gov/safeharbor/
[176] http://safeharbor.export.gov/list.aspx

5.5. Διακυβέρνηση – Επικινδυνότητα - Συμμόρφωση

Οι οργανισμοί έχουν αντιληφθεί πλέον ότι οι άξονες Διακυβέρνηση – Επικινδυνότητα – Συμμόρφωση επηρεάζουν σημαντικά τη λειτουργία του κι ουσιαστικά αλληλοσυμπληρώνονται κι άρα πρέπει να αντιμετωπίζονται ενιαία. Αυτοί οι άξονες, στη διεθνή βιβλιογραφία είναι γνωστοί με το ακρωνύμιο GRC από τα αρχικά των αντίστοιχων αγγλικών όρων Governance – Risk – Compliance. Η αντιμετώπιση αυτών ενιαία, ως σύνολο, αποτελεί απαίτηση στη σύγχρονη εποχή. Ο ορισμός[177] για το τρίπτυχο GRC έχει ως εξής: «είναι μία ολοκληρωμένη, ολιστική προσέγγιση σε επίπεδο εταιρικής διακυβέρνησης, επικινδυνότητας και συμμόρφωσης που εξασφαλίζει ότι ολόκληρος ο οργανισμός δρα ηθικά και σύμφωνα με το αποδεκτό επίπεδο ανάληψης επικινδυνότητας, τις εσωτερικές πολιτικές και τους εξωτερικούς κανονισμούς, δια μέσου της ευθυγράμμισης των στρατηγικών, των διαδικασιών, της τεχνολογίας και των ανθρώπων, βελτιώνοντας έτσι την αποδοτικότητα και την αποτελεσματικότητα της επιχείρησης.». Από αυτόν τον ορισμό προκύπτει το πλαίσιο αναφοράς ενιαίας διαχείρισης GRC, που παρουσιάζεται ακολούθως:

[177] Racz, N., Panitz, J., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (grc) status quo and software use: Results from a survey among large enterprises. Governance 1,1-2010.

Γράφημα 5.6: Πλαίσιο αναφοράς GRC.



Υπάρχουν διαθέσιμες στην αγορά ολοκληρωμένες λύσεις κι εξειδικευμένο λογισμικό GRC που ικανοποιούν για τους σχετικούς ελέγχους την ανάγκη αυτοματοποίησης. Η αυτοματοποίηση των διαδικασιών διευκολύνει σημαντικά στη συμμόρφωση με κάθε ρυθμιστικό πλαίσιο, στη διενέργεια εσωτερικών ελέγχων, στην αποτελεσματικότητα και καθιστά ευκολότερη τη διαδικασία εντοπισμού απειλών.

Κεφάλαιο 6: Ηλεκτρονικό Έγκλημα

6.1. Ορισμός ηλεκτρονικού εγκλήματος

Το ηλεκτρονικό έγκλημα ή «έγκλημα στον κυβερνοχώρο» ή «e-έγκλημα» ή «ψηφιακό έγκλημα τεχνολογίας» είναι ένα φαινόμενο ιδιαίτερα δημοσιευμένο, αλλά η αύξηση της παγκόσμιας διασύνδεσης είναι άρρηκτα συνδεδεμένη με την ανάπτυξη της σύγχρονης εγκληματικότητας στον κυβερνοχώρο. Κάθε εγκληματική δραστηριότητα που περιλαμβάνει έναν υπολογιστή είτε ως μέσο, στόχο ή ένα μέσο για τη διαιώνιση περαιτέρω εγκλημάτων εμπίπτει στο πεδίο εφαρμογής του εγκλήματος στον κυβερνοχώρο[178]. Μια γενικευμένη ερμηνεία του εγκλήματος στον κυβερνοχώρο μπορεί να είναι «παράνομες πράξεις όπου ο υπολογιστής αποτελεί είτε ένα εργαλείο ή στόχο ή και τα δύο μαζί».

Η διάδοση της ψηφιακής τεχνολογίας και η σύγκλιση των συσκευών πληροφορικής και επικοινωνίας έχουν αλλάξει τον τρόπο με τον οποίο γίνεται η κοινωνικοποίηση καθώς και η επιχειρηματικότητα[179]. Ενώ είναι συντριπτικά θετική η εξέλιξη της τεχνολογίας, υπάρχει όμως και η σκοτεινή της πλευρά. Το έγκλημα ακολουθεί την ευκαιρία που υπάρχει για τη διάπραξή του. Σχεδόν κάθε πρόοδος συνοδεύεται από μια αντίστοιχη ομάδα εστίασης που πρέπει να αξιοποιηθεί για εγκληματικούς σκοπούς[180].

«Το έγκλημα στον κυβερνοχώρο» έχει χρησιμοποιηθεί για να περιγράψει ένα ευρύ φάσμα αδικημάτων, συμπεριλαμβανομένων των αδικημάτων κατά δεδομένων ηλεκτρονικών υπολογιστών και συστημάτων (όπως το "hacking"), υπολογιστών που σχετίζονται με πλαστογραφία και απάτη (όπως «phishing»), αδικημάτων με σεξουαλικό περιεχόμενο (όπως η διάδοση της παιδικής πορνογραφίας) και αδικημάτων με πνευματικά δικαιώματα (όπως η διάδοση πειρατικού περιεχομένου).

Η μαγεία των ψηφιακών φωτογραφικών μηχανών και η κοινή χρήση φωτογραφιών στο διαδίκτυο αξιοποιείται από εγκληματίες παιδικής πορνογραφίας. Η ευκολία της ηλεκτρονικής τραπεζικής και των online πωλήσεων παρέχει πρόσφορο έδαφος για απάτες. Η ηλεκτρονική επικοινωνία, όπως το ηλεκτρονικό ταχυδρομείο (email) και τα μηνύματα SMS μπορούν να χρησιμοποιηθούν για καταδίωξη και παρενόχληση. Η ευκολία με την οποία τα ψηφιακά μέσα μπορούν να μοιραστούν έχει οδηγήσει σε μια έκρηξη παραβίασης

[178] Rolf H. Weber, Internet of things: Privacy issues revisited, computer law & security review 31, 618–627, Published by Elsevier Ltd, 2015

[179] Soudabeh Vahdati & Niloofar Yasini, Factors affecting internet frauds in private sector: A case study in Cyberspace Surveillance and Scam Monitoring Agency of Iran, Computers in Human Behavior 51, 180–187, Elsevier Ltd., 2015

[180] Paul Hunton, Data attack of the cybercriminal: Investigating the digital currency of cybercrime, Computer law & security review 28 (2012) 201e207

πνευματικών δικαιωμάτων. Η αυξανόμενη εξάρτηση από υπολογιστές και ψηφιακά δίκτυα κάνει από μόνη της την τεχνολογία ένα δελεαστικό στόχο είτε για την απόκτηση πληροφοριών ή ως μέσο που προκαλεί αναστάτωση και ζημίες. Σημαντική επίσης είναι η χρήση των μέσων κοινωνικής δικτύωσης και κυρίως του Facebook τα τελευταία χρόνια. Η ελευθερία έκφρασης και η δυνατότητα να σχολιάζει ο κάθε χρήστης σε οποιαδήποτε δημοσίευση που έχει κάνει πρόσωπο ή επιχείρηση και η πρόσβαση σε ανταλλαγή μηνυμάτων με άτομα που δεν υπάρχει εμπιστοσύνη σχετικά με την πραγματική ταυτότητα των χρηστών κάνει την απάτη ακόμα ευκολότερη[181].

6.2. Φορείς Ασφάλειας κατά του Ηλεκτρονικού Εγκλήματος

- *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος*

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙΔΗΕ) είναι αυτοτελής κεντρική υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας. Με το Π.Δ. 178/2014 προβλέφθηκε η ίδρυση και η διάρθρωσή της με έδρα την Αθήνα καθώς και η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη.

Αποστολή της αποτελεί η πρόληψη, η έρευνα και η καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Σχετικά με την εσωτερική της δομή αποτελείται από πέντε τμήματα[182] προστασίας του χρήστη κι ασφάλειας του Κυβερνοχώρου. Πιο συγκεκριμένα διαθέτει (α) Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών, (β) Τμήμα Καινοτόμων Δράσεων και Στρατηγικής, (γ) Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, (δ) Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και (ε) Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων.

- *Διεθνής Ένωση Αρχηγών Αστυνομίας*

Έναν επιπλέον φορέα ασφάλειας αποτελεί η *Διεθνής Ένωση Αρχηγών Αστυνομίας* (IACP[183]) που φιλοξενεί το ετήσιο εκπαιδευτικό συνέδριο Δικαίου Επιβολής Διαχείρισης Πληροφοριών το οποίο εστιάζει στην πληροφορική της ασφάλειας και της εγκληματικότητας στον κυβερνοχώρο.

---

[181] Serra Inci Celebi, How do motives affect attitudes and behaviors toward internet advertising and Facebook advertising?, Computers in Human Behavior 51 (2015) 312–324, Elsevier Ltd.

[182] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=53864&Itemid=378&lang=

[183] http://www.iacp.org/

➢ *Ευρωπαϊκή Ένωση*

Επιπροσθέτως, η Ευρωπαϊκή Ένωση (ΕΕ) έχει δημιουργήσει ένα σώμα που ονομάζεται το *φόρουμ του εγκλήματος στον κυβερνοχώρο* και μερικά από τα ευρωπαϊκά κράτη μέλη έχουν υπογράψει Σύμβαση του Συμβούλιου της Ευρώπης για το ηλεκτρονικό έγκλημα το οποίο στοχεύει στην τυποποίηση του Ευρωπαϊκού νόμου σχετικά με το έγκλημα στον κυβερνοχώρο.

➢ *ENISA*

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών[184] (ENISA), αποτελεί ευρωπαϊκό κέντρο εμπειρογνωσίας για την ασφάλεια στον κυβερνοχώρο. Ουσιαστικά βοηθά τα κράτη μέλη να εξοπλίζονται και να προετοιμάζονται για πρόληψη, εντοπισμό κι αντιμετώπιση προβλημάτων που αφορούν την ασφάλεια των πληροφοριών. Παρέχει συμβουλές και λύσεις τόσο σε φορείς του δημόσιου και του ιδιωτικού τομέα των χωρών της ΕΕ όσο και στα θεσμικά όργανα της ΕΕ. Επιπλέον, δημοσιεύει εκθέσεις και μελέτες για την ασφάλεια στον κυβερνοχώρο. Αυτές οι μελέτες είναι σχετικές με την ασφάλεια στο υπολογιστικό νέφος, την προστασία των δεδομένων, τις τεχνολογίες για τη βελτίωση της προστασίας, την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπίστευσης για τις ηλεκτρονικές συναλλαγές και τον εντοπισμό απειλών στον κυβερνοχώρο.

6.3. Η εγκληματικότητα σε άλλες ηπείρους

Τα αποτελέσματα εθνικών ερευνών των ΗΠΑ επιβεβαιώνουν την εικόνα που σχηματίζεται σχετικά με το ότι το έγκλημα στον κυβερνοχώρο είναι σταθερά και δραματικά υπό αύξηση. Μια από τις πιο διάσημες πράξεις εθνικής έρευνας για τις Ηνωμένες Πολιτείες είναι η «Έρευνα Υπολογιστών του εγκλήματος και της Ασφάλειας» που διεξήχθη από το Ινστιτούτο Ασφάλειας υπολογιστών, με τη συμμετοχή του Ομοσπονδιακού Γραφείου Ερευνών Υπολογιστών του Intrusion Squad στο Σαν Φρανσίσκο.

Επιπλέον, πολλές διεθνείς πηγές προειδοποιούν ότι η Μέση Ανατολή γίνεται όλο και πιο σημαντική πηγή εγκληματικότητας στον κυβερνοχώρο. Για παράδειγμα, η Σαουδική Αραβία κατατάσσεται ως η ηγετική χώρα της περιοχής που αποτελεί στόχο και πηγή κακόβουλων δραστηριοτήτων σε απευθείας σύνδεση (online). Είναι επίσης η νούμερο ένα πηγή κακόβουλων επιθέσεων με βάση το Συμβούλιο Συνεργασίας του

[184] http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_el.htm#goto_2

Κόλπου. Η Αίγυπτος[185] είναι μία από τις χώρες με τα περισσότερα περιστατικά «ψαρέματος» (phishing) στον κόσμο, με περίπου 1.763 περιστατικά phishing και στην κατάταξη είναι αρκετά κοντά με άλλες χώρες στην περιοχή, όπως τη Σαουδική Αραβία, τα Ηνωμένα Αραβικά Εμιράτα και το Κατάρ. Δεν είναι δύσκολο να δούμε ότι τα εγκλήματα στον κυβερνοχώρο αυξάνονται στην περιοχή λόγω της αύξησης της βάσης χρηστών με φτωχή ευαισθητοποίηση ως προς την ασφάλεια και έλλειψη κανονισμών. Λόγω των θρησκευτικών κινήτρων και των πολιτικών ζητημάτων της περιοχής, οι χάκερ (hackers) αποστέλλουν με επιτυχία πολιτικά ή θρησκευτικά μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου προτρέποντας τους χρήστες να ανοίξουν τα συνημμένα αρχεία, μολύνοντας έτσι τους υπολογιστές με κακόβουλο λογισμικό, προκειμένου να επιτεθούν ουσιαστικά στην υποδομή της Μέσης Ανατολής όπως στις ιστοσελίδες επιχειρήσεων που δρουν μέσω του ηλεκτρονικού εμπορίου, στις τράπεζες, στις τηλεπικοινωνίες των κυβερνητικών υπηρεσιών.

Όταν γίνεται αναφορά για έγκλημα στον κυβερνοχώρο, συνήθως εννοούνται δύο μεγάλες κατηγορίες του αδικήματος. Κατά το πρώτο, ένας υπολογιστής συνδεδεμένος σε ένα δίκτυο είναι ο στόχος στο αδίκημα. Αυτή είναι η περίπτωση των επιθέσεων στην εμπιστευτικότητα, ακεραιότητα ή/ και στη διαθεσιμότητα του διαδικτύου.

Η άλλη κατηγορία αποτελείται από παραδοσιακά αδικήματα, όπως κλοπή, απάτη, και πλαστογραφία που διαπράττονται με τη βοήθεια των ηλεκτρονικών υπολογιστών συνδεδεμένα σε δίκτυο, τα δίκτυα υπολογιστών και συναφείς τεχνολογίες πληροφορικής και επικοινωνίας. Το έγκλημα στον κυβερνοχώρο κυμαίνεται από ηλεκτρονική απάτη, κλοπή και πλαστογραφία, παραβιάσεις της ιδιωτικής ζωής, τη διάδοση υλικού επιβλαβούς περιεχομένου και του οργανωμένου εγκλήματος. Σε πολλές περιπτώσεις, στη συγγραφή νομοθετημάτων εμπεριέχονται ορισμοί, ωστόσο οι νομοθέτες δεν δίνουν πάντα καλές ερμηνείες[186].

Ένα από τα σημαντικότερα προβλήματα για ακριβή ορισμό του εγκλήματος στον κυβερνοχώρο είναι η έλλειψη συγκεκριμένων στατιστικών δεδομένων για τα αδικήματα αυτά. Δεδομένου ότι η αναφορά του εγκλήματος είναι προαιρετική, τα αριθμητικά στοιχεία είναι σχεδόν σίγουρα πολύ χαμηλότερα από την πραγματική εμφάνιση του συναφούς δικτύου εγκλήματος[187].

[185] M. El–Guindy, Cybercrime in the Middle East. ISSA J. 17, 2008
[186] D. Shinder, Scene of the Cybercrime, Walthman, Syngress, New York, 2002
[187] Kunz, M., & Wilson, P. Computer crime and computer frauds (pp. 13–22). University of Maryland, Department of Criminology and Criminal Justice, Report to the Montgomery County Criminal Justice Coordinating Commission, 2004

Στο Δέκατο Συνέδριο των Ηνωμένων Εθνών για την Πρόληψη του Εγκλήματος και Θεραπεία των δραστών, σε ένα εργαστήριο αφιερωμένο στα θέματα των εγκλημάτων που σχετίζονται με τα δίκτυα υπολογιστών, το έγκλημα στον κυβερνοχώρο είχε διαχωριστεί σε δύο κατηγορίες και ορίστηκε:

(α) με τη στενή έννοια ως κάθε παράνομη συμπεριφορά που κατευθύνεται μέσω των ηλεκτρονικών πράξεων που στοχεύουν στην ασφάλεια των συστημάτων πληροφορικής και την επεξεργασία των δεδομένων από αυτές.

(β) με τη γενικότερη έννοια ως κάθε παράνομη συμπεριφορά που διαπράττεται μέσω ή σε σχέση με ένα σύστημα ηλεκτρονικού υπολογιστή ή του δικτύου, συμπεριλαμβανομένων των εγκλημάτων αυτών ως παράνομη κατοχή και προσφορά ή ενοχλητική πληροφορία μέσω ενός συστήματος υπολογιστή ή δικτύου.

Το έγκλημα στον κυβερνοχώρο, σύμφωνα με τους εν λόγω ορισμούς περιλαμβάνει υπολογιστές και δίκτυα. Στην έννοια έγκλημα στον κυβερνοχώρο, η λέξη «κυβερνο" συνήθως αναφέρεται στην τέλεση ποιοτικά νέων αδικημάτων που διευκολύνονται από την τεχνολογία των πληροφοριών ή ενσωματώνουν το κυβερνοχώρο σε πιο παραδοσιακές δραστηριότητες.

Το έγκλημα στον κυβερνοχώρο είναι ένας από τους ταχύτερα αναπτυσσόμενους τομείς της εγκληματικότητας. Όλο και περισσότεροι εγκληματίες εκμεταλλεύονται την ταχύτητα, την ευκολία και την ανωνυμία ότι οι σύγχρονες τεχνολογίες προσφέρουν ένα ευρύ φάσμα για τη διάπραξη εγκληματικών δραστηριοτήτων[188]. Στο παρελθόν, το έγκλημα στον κυβερνοχώρο διαπράττονταν από άτομα ή μικρές ομάδες ατόμων. Ωστόσο, πλέον υπάρχει μια αναδυόμενη τάση με τα παραδοσιακά συνδικάτα του οργανωμένου εγκλήματος και επαγγελματίες με εγκληματολογικό μυαλό που εργάζονται από κοινού συγκεντρώνοντας τους πόρους τους και την εμπειρογνωμοσύνη τους. Χαρακτηριστικό παράδειγμα αποτελεί στις μέρες μας ο πόλεμος που έχει ξεκινήσει διαδικτυακά[189] από τους Anonymous με το ISIS.

Το έγκλημα στον κυβερνοχώρο είναι παγκόσμιο έγκλημα[190]. Ως εξηγείται σε ευρωπαϊκή έκθεση τα εγκλήματα που σχετίζονται με ηλεκτρονικούς υπολογιστές διαπράχθηκαν σε κυβερνοχώρο και δεν σταματούν τα σύνορα στα συμβατικά των κρατών.

[188] Elis, N., Monday, May 12, 2014. Can big data predict the next cyber attack? Jerusalem Post. http://www.jpost.com/Enviro-Tech/Can-big-data-predict-the-next-cyber-attack-351957

[189] http://tvxs.gr/news/kosmos/oi-anonymous-kiryksan-ton-diadiktyako-polemo-sto-islamiko-kratos

[190] K.W. Müller, M. Dreier, M.E. Beutel, E. Duven, S. Giralt, K.Wolfling, A hidden type of internet addiction? Intense and addictive use of social networking sites in adolescents, Computers in Human Behavior 55, 172e177, Elsevier Ltd., 2016

Μπορούν να διαπράττονται από οπουδήποτε και από οποιονδήποτε χρήστη του υπολογιστή.

6.4. Το μέγεθος του προβλήματος και λόγοι για την ανάπτυξη της εγκληματικότητας στον κυβερνοχώρο

Γνωρίζοντας πόσο έγκλημα διαπράττεται μπορεί να βοηθήσει στο να παρθούν αποφάσεις σχετικά με τις δαπάνες για την ασφάλεια. Εκτιμήσεις εμπειρογνωμόνων σε θέματα ασφάλειας των ετήσιων απωλειών από την εγκληματικότητα στον κυβερνοχώρο κυμαίνονται από $555 εκατομμύρια σε περισσότερα από $13 δις, αλλά στην πραγματικότητα δεν υπάρχουν έγκυρες στατιστικές αναφορές σχετικά με τις απώλειες από αυτού του είδους το έγκλημα διότι δεν είναι γνωστό πόσες είναι οι υποθέσεις που δεν καταγγέλλονται. Ακόμα και όταν τα θύματα του κυβερνοχώρου έχουν επίγνωση των εγκλημάτων, δεν αναφέρουν τις απώλειές τους, ιδιαίτερα αν οι απώλειες αυτές μπορούν εύκολα να κρυφτούν. Με βάση άρθρο από το Πανεπιστήμιο [191]Gdansk με τη δυναμική ανάπτυξη της χρήσης του Διαδικτύου από τις επιχειρήσεις έχει αυξηθεί ραγδαία ο αριθμός των απειλών του υπολογιστή και του επιπέδου των κινδύνων που σχετίζονται με αυτές. Σύμφωνα με την έκθεση Ponemon, «Ο αντίκτυπος της εγκληματικότητας στον κυβερνοχώρο στις Επιχειρήσεις», κάθε εβδομάδα υπάρχει ένας μέσος όρος 66 επιτυχημένων επιθέσεων στον κυβερνοχώρο που προκαλούν διαταραχές. Οι στοχευμένες επιθέσεις κοστίζουν $214.000. Οι δαπάνες προκύπτουν από εγκληματολογική έρευνα, επενδύσεις στο κόστος της τεχνολογίας και στην ανάκτηση της φήμης του «ονόματος» της επιχείρησης.

Τα θύματα μπορεί μερικές φορές να χάσουν περισσότερα από την αναφορά αυτών των εγκλημάτων από ό, τι χάνουν ουσιαστικά από το ίδιο το έγκλημα. Η «ντροπή», η εκτροπή του προσωπικού στην προετοιμασία στοιχείων και μαρτυριών, τα νομικά έξοδα, τα αυξημένα ασφάλιστρα και η έκθεση των τρωτών σημείων και των αποτυχιών της ασφάλειας μπορούν όλα τα παραπάνω να προκύψουν από την αναφορά περιστατικών του εγκλήματος στον κυβερνοχώρο.

Όπως κάθε πτυχή του εμπορίου και της επικοινωνίας έχει αλλάξει από το διαδίκτυο, το έγκλημα έχει εξελιχθεί επικερδές από τα εκατομμύρια των πιθανών θυμάτων που συνδέονται σε ένα παγκόσμιο δίκτυο. Υπάρχουν διάφοροι λόγοι για την αύξηση της εγκληματικότητας στον κυβερνοχώρο. Πρώτα απ 'όλα, η τεχνολογία για το ηλεκτρονικό

[191] Rafał Leszczyna, Cost assessment of computer security activities, Computer Fraud & Security, July 2013

έγκλημα έχει γίνει πιο εύκολα προσιτή, τα εργαλεία λογισμικού μπορούν να αγοραστούν σε απευθείας σύνδεση που επιτρέπει στο χρήστη να εντοπίσει ανοικτούς λιμένες ή ακόμα και να βρει τον κωδικό πρόσβασης. Αυτά τα εργαλεία επιτρέπουν σε ένα πολύ ευρύτερο φάσμα των ανθρώπων να γίνουν παραβάτες. Το έγκλημα στον κυβερνοχώρο αυξάνεται λόγω της εκθετικής συνδεσιμότητας, του αυξημένου επιπέδου γνώσης και της διαθέσιμης πληροφορίας διαδικτυακά. Σε σύγκριση με άλλα εγκλήματα και αδικήματα γενικά απαιτείται μικρότερη επένδυση και μπορεί να πραγματοποιηθεί σε διάφορες τοποθεσίες, χωρίς γεωγραφικούς περιορισμούς και δίχως να λαμβάνονται υπόψη τα σύνορα.

6.5. Το μέλλον της εγκληματικότητας στον κυβερνοχώρο

Στον αναπτυσσόμενο κόσμο του διαδικτύου, τόσο στην προσωπική ζωή όσο και στην επαγγελματική, το έγκλημα στον κυβερνοχώρο αποτελεί ένα διαρκώς αυξανόμενο πρόβλημα. Η τιμωρία για αυτού του είδους τα εγκλήματα έχει γίνει ένα νέο πεδίο προς διερεύνηση του εγκλήματος και της επιβολής του νόμου. Το έγκλημα στον κυβερνοχώρο έχει δώσει στους εγκληματίες τη δυνατότητα να δρουν πέρα από τα σύνορα. Όταν μια πόρτα παραμένει ανοικτή, το εγκληματικό στοιχείο θα βρει τρόπο να μπει. Σε αυτή την περίπτωση, η πόρτα για το έγκλημα είναι το Διαδίκτυο[192].

Τα εγκλήματα στον κυβερνοχώρο είναι τεράστια σε έκταση. Κυμαίνονται από ατομική πράξη κι εκτείνονται σε μια αυξανόμενη επιθυμία διεθνούς οργανωμένου εγκλήματος. Οι απάτες (scams) μέσω του Διαδικτύου είναι ανεξέλεγκτες. Αποστέλλονται μηνύματα μέσω ηλεκτρονικού ταχυδρομείου και ιστοσελίδων, που προσπαθούν να παρασύρουν τα ανυποψίαστα θύματα σε ιστούς για εξαπάτηση. Τα προγράμματα Spy bots και Trojan προσπαθούν να εισχωρήσουν σε ευαίσθητες προσωπικές και επιχειρηματικές πληροφορίες, να συγκεντρώσουν όσα στοιχεία μπορούν με πρόθεση για εγκληματική χρήση.

Τα εγκλήματα πιο προσωπικού χαρακτήρα αφθονούν επίσης σε ολόκληρο το Διαδίκτυο. Πολλοί ιστότοποι γνωριμιών και αρκετά μέσα κοινωνικής δικτύωσης είναι γεμάτα με απατεώνες που παίζουν επικίνδυνα παιχνίδια με αρκετά θύματα. Αυτή η κοινωνική αλληλεπίδραση γίνεται έγκλημα όταν το άτομο πέφτει θύμα από άτομα που χρησιμοποιούν το Διαδίκτυο για να ενισχύσουν τις ανασφάλειες τους, ενεργώντας σε βάρος τους. Δυστυχώς, τα παιδιά είναι τα συχνότερα θύματα αυτού του είδους εγκλημάτων.

[192] Cyber and Technology Enables Crimes (2013). Retrieved from https://www.crimecommission.gov.au/sites/default/files/CYBER%20AND%20TECHNOLOGY%20ENABLED%20CRIME%20JULY%202013.pdf

Εξάλλου, τίτλοι ειδήσεων συχνά περιλαμβάνουν ιστορίες θυμάτων με αυτά για εγκλήματα στον κυβερνοχώρο.

Ορισμένα θύματα έχουν δεχθεί προσωπικές παραβιάσεις διαπραγμένες από εγκληματίες με απευθείας σύνδεση σε παιχνίδια κι εμφανίζονται στην ουσία ως απλοί παίκτες. Η διατήρηση της ασφάλειας στο Διαδίκτυο έχει γίνει όλο και πιο δύσκολη υπόθεση. Υπάρχει ένα σύνολο από εταιρείες που ασχολείται με τέτοια προβλήματα. Η διαμόρφωση νέων νόμων για την επίτευξη περισσότερης ασφάλειας αποτελεί γεγονός. Πρέπει να τονιστεί σε αυτό το σημείο ότι από τη στιγμή που τα εγκλήματα γίνονται ηλεκτρονικά, δεν υπάρχει αποτύπωμα που να μην μπορεί να εξιχνιαστεί. Όλα υπάρχουν στο διαδίκτυο. Αυτό αποτελεί πλέον μια παγκόσμια αρένα και η ενίσχυση νόμων για την προστασία των πολιτών θα γίνεται όλο κι εντονότερη.

Το Ίντερνετ των πραγμάτων (Internet of Things - IoT) είναι κι αυτό που πρέπει να ληφθεί υπόψη για το μέλλον της εγκληματικότητας. Έχει προβλεφθεί ήδη κατά τον τελευταίο αιώνα, αλλά έχει μπει στο επίκεντρο του ενδιαφέροντος τα τελευταία 15 χρόνια περίπου. Είναι ένα όραμα το οποίο προβλέπει δυνητικά δισεκατομμύρια «Πράγματα», όπως για παράδειγμα είναι οι έξυπνες συσκευές και οι αισθητήρες, που συνδέονται μεταξύ τους με τη χρήση μηχανής με μηχανή, ενεργοποιώντας την τεχνολογία μέσω του Διαδικτύου ή άλλων τρόπων συνδεσιμότητας που είναι βασισμένα [193]σε IP (IP-based).

Σε ένα έξυπνο κτίριο - όπου τα συστήματα κυμαίνονται από HVAC (θέρμανση, αερισμό και κλιματισμό), από τον έλεγχο του φωτισμού και τη πρόσβαση απ' την πόρτα ως την παρακολούθηση βίντεο και των ανελκυστήρων, όλα είναι συνδεδεμένα μεταξύ τους - μια απειλή για την ασφάλεια σχετική με τη διατάραξη ρεύματος ή φωτισμού θα μπορούσε να προκαλέσει απώλεια ζωής, αν το κτίριο αναφέρεται σε νοσοκομείο. Σε κτίρια γραφείων, ένα στοιχείο ελέγχου πρόσβασης πόρτας που είναι χακαρισμένο θα μπορούσε να προσφέρει σε έναν εισβολέα μη εξουσιοδοτημένη πρόσβαση. Τα προβλήματα που σχετίζονται με συσκευές IoT δεν είναι απλά υποθετικά. Ένα παράδειγμα μιας απειλής είναι το σκουλήκι Stuxnet, το οποία έχει την ικανότητα να διαταράσσει τον έλεγχο ενός βιομηχανικού συστήματος, προκαλώντας εκτεταμένες ζημιές. Στην εγκληματικότητα από το IoT, πρέπει να ληφθεί μια διαφορετική στάση. Πρέπει η ασφάλεια να ληφθεί υπόψη ήδη

[193] Manyika, J; Chui, M; Bisson, P; Woetzel, J; Dobbs, R; Bughin, J; Aharon, D. 'Unlocking the potential of the Internet of Things'. McKinsey Global Institute, June 2015 http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

από το σχεδιασμό, πριν την κατασκευή του προϊόντος. Δεν μπορεί να «βιδωθεί», προστεθεί στη συνέχεια[194].

6.6. Η χρήση κλεμμένων οικονομικών πληροφοριών

Οι παραβάτες χρησιμοποιούν τα προσωπικά στοιχεία των θυμάτων με ποικίλους τρόπους. Μεταξύ των πιο συνηθισμένων παραδειγμάτων χρήσης είναι (FTC 2004, online):

- Κλήση στον εκδότη της πιστωτικής κάρτας για αλλαγή της διεύθυνσης αποστολής της χρέωσης του λογαριασμού της κάρτας του θύματος, μετά την οποία ο λογαριασμός χρεώνεται κι άρα πραγματοποιείται ζημία στο θύμα. Επειδή ο λογαριασμός του θύματος αποστέλλεται σε διαφορετική διεύθυνση, μπορεί να περάσει κάποιο χρονικό διάστημα πριν το θύμα συνειδητοποιήσει ότι υπάρχει κάποιο πρόβλημα. Στην Περιφέρεια της Delaware, ένας κατηγορούμενος καταδικάστηκε σε ποινή φυλάκισης 33 μηνών και $160,910.87 για την αποκατάσταση, και ένας άλλος κατηγορούμενος σε φυλάκιση 41 μηνών και $126,298.79 για αποκατάσταση λόγω της διάθεσης των ονομάτων και των αριθμών κοινωνικής ασφάλισης (ΑΜΚΑ) υψηλόβαθμων στρατιωτικών σε μια ιστοσελίδα στο διαδίκτυο και τη χρήση των στοιχείων αυτών για τη δημιουργία πιστωτικών καρτών online.
- Το άνοιγμα νέων λογαριασμών πιστωτικής κάρτας στο όνομα του θύματος. Όταν χρησιμοποιούνται οι πιστωτικές κάρτες και δεν πληρώνονται οι λογαριασμοί, αυτές οι καθυστερήσεις αποπληρωμής αποστέλλονται στο λογαριασμό του θύματος τις οποίες καλείται να πληρώσει.
- Πραγματοποίηση τηλεφωνικών κλήσεων. Στις Ηνωμένες Πολιτείες ο κατηγορούμενος είχε εμπλακεί σε ένα σύστημα hacking που χρησιμοποιούσε οικιακούς υπολογιστές για ηλεκτρονική πρόσβαση σε πολλά από τα μεγαλύτερα τηλεφωνικά συστήματα στις Ηνωμένες Πολιτείες για τη λήψη χιλιάδων αριθμητικών καρτών (κωδικοί πρόσβασης). Ο κατηγορούμενος, ο οποίος ομολόγησε την ενοχή του για την κατοχή των συσκευών πρόσβασης μη εξουσιοδοτημένων και της απάτης ηλεκτρονικών υπολογιστών, χρησιμοποιώντας προσωπικούς υπολογιστές για την απόκτηση πρόσβασης σε ένα τηλεφωνικό σύστημα υπολογιστή για το κατέβασμα και τη μεταφορά χιλιάδων κωδικών

[194] Colin Tankard, The security issues of the Internet of Things, Digital Pathways, Computer Fraud & Security, 2015

πρόσβασης που σχετίζονται με τους αριθμούς καρτών της εταιρείας. Κατά τη λήψη αυτών των κωδικών, ο κατηγορούμενος χρησιμοποιώντας ένα πρόγραμμα του υπολογιστή που είχε δημιουργήσει για να αυτοματοποιήσει τη μεταφόρτωση, και ανέθεσε στους συνωμότες του το πώς να χρησιμοποιήσουν το πρόγραμμα. Ο κατηγορούμενος παραδέχθηκε ότι η ζημία που υπέστη η εταιρεία ως αποτέλεσμα της εγκληματικής συμπεριφοράς του ήταν $955.965. Καταδικάστηκε σε φυλάκιση 18 μηνών και σε $10.000 για αποκατάσταση.

- Μπορούν να πλαστογραφήσουν επιταγές, πιστωτικές, χρεωστικές κάρτες, ή να επιτρέψουν ηλεκτρονικές μεταβιβάσεις σε άλλο όνομα, και να υποκλέψουν τον τραπεζικό λογαριασμό θυμάτων. Ένα παράδειγμα αποτελεί το γεγονός μιας γυναίκας που μόλις είχε επιστρέψει από τις διακοπές της και βρήκε ότι η αδελφή της είχε κάνει χρήση της πιστωτικής της κάρτας ($584) και είχε διαπράξει δόλιες δραστηριότητες στο όνομα της αδελφής της. Το θύμα δεν παρέλαβε ποτέ τίποτα από αυτά που είχε χρεωθεί. Επιπλέον, όταν άνοιξε τα μηνύματα του ηλεκτρονικού ταχυδρομείου της ανακάλυψε ότι δεν είχε πρόσβαση, διότι η αδελφή της είχε κλέψει την ταυτότητά της.
- Την κήρυξη πτώχευσης με άλλο όνομα για την αποφυγή πληρωμής χρεών για την αποφυγή τυχόν έξωσης κι οποιασδήποτε πληρωμής.
- Η αγορά ενός αυτοκινήτου με τη λήψη δανείου σε άλλο όνομα. Στις Ηνωμένες Πολιτείες, ο εναγόμενος καταδικάστηκε για τη χρήση της ημερομηνίας γέννησης καθώς και του Αριθμού Μητρώου Κοινωνικής Ασφάλισης του θύματος για την εφαρμογή της δράσης του on-line με σκοπό την υποκλοπή πιστωτικών καρτών από τρεις εταιρείες ώστε να εφαρμόσει την αγορά σε απευθείας σύνδεση για δάνειο $15.000. Στην πραγματικότητα χρησιμοποιούσε τα έσοδα του δανείου για το αυτοκίνητο ως επένδυση σε δική του επιχείρηση. (Ο κατηγορούμενος, αφού ομολόγησε την ενοχή του για την κλοπή της ταυτότητας του θύματος καταδικάστηκε σε ποινή φυλάκισης 7 μηνών και σε $27.000 για αποκατάσταση).

6.7. Ηλεκτρονικό Έγκλημα

Πέραν της βελτίωσης της ποιότητας της ζωής μέσω της τεχνολογίας, υπεισέρχονται και παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας οι οποίες θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα» ή «Ηλεκτρονική απάτη». Σύμφωνα με το Λεξικό της Νέας Ελληνικής Γλώσσας του Γ. Μπαμπινιώτη (αναφέρεται *στον Οδηγό*

Προστασίας Καταναλωτών 2005), «απάτη» είναι: (1) μεθοδευμένη (μη νόμιμη ή νομιμοφανής) ενέργεια, που αποσκοπεί στην παραπλάνηση (εξαπάτηση) κάποιου, ώστε να ωφεληθεί αυτός χάριν του οποίου γίνεται η συγκεκριμένη ενέργεια, (2) αξιόποινη συμπεριφορά (πράξη ή παράλειψη) κατά την οποία, κάποιος με σκοπό να αποκομίσει είτε ο ίδιος είτε και τρίτος παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή, με την παρουσίαση εν γνώσει του ψευδών γεγονότων ως αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων[195].

Ως «Ηλεκτρονικά Εγκλήματα» θεωρούνται οι αξιόποινες εγκληματικές πράξεις που σε μεγάλο βαθμό υπαγορεύονται από οικονομικούς λόγους και τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων. Μεγάλος αριθμός online απατών αντικατοπτρίζουν τις υπάρχουσες απάτες κι άλλες παρουσιάζουν τη μοναδικότητά τους στην εποχή μας[196]. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου[197]. Σύμφωνα με τους Kunz & Wilson όμως, αυτοί οι όροι χρησιμοποιούνται χωρίς διάκριση κι έτσι θα ισχύσει και στην παρούσα εργασία. Οι απάτες αυτές αφορούν σε επιβλαβείς κώδικες που θέτουν σε κίνδυνο εμπιστευτικά δεδομένα[198].

Βασική αρχή στις απάτες που διαπράττονται μέσω Διαδικτύου είναι να πείσουν το θύμα να καταβάλλει ένα μικρό, αρχικό χρηματικό ποσό, με σκοπό να εξασφαλίσει ένα πολύ μεγαλύτερο στο μέλλον (π.χ. νιγηριανές απάτες) ή γενικότερα να πείσουν το θύμα για την ασφάλεια των διαδικτυακών συναλλαγών με σκοπό στη συνέχεια να του αποσπάσουν μεγάλα χρηματικά ποσά (απάτες με πιστωτικές κάρτες κ.ά.). Οι συνηθέστεροι κίνδυνοι που παρουσιάζονται στις ηλεκτρονικές συναλλαγές είναι οι εξής δέκα[199].

1. *Διακίνηση μηνυμάτων με απατηλό περιεχόμενο:* είναι γνωστή υπό τον όρο «Ισπανικό Λόττο» κι αφορά τη μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των

[195] Karl de Leeuw and Jan Bergstra, The History of Information Security: A Comprehensive Handbook 2007 Elsevier B.V., http://www.cybercrimes.net
[196] Wang, S. Y. K., & Wilson, H., The evolutional view of the types of identity thefts and online frauds in the era of the internet. Internet Journal of Criminology, 12 (ISSN 2045–6743), 2011
[197] http://bit.ly/1PHF0Gu
[198] Soudabeh Vahdati, Niloofar Yasini, Factors affecting internet frauds in private sector: A case study in Cyberspace Surveillance and Scam Monitoring Agency of Iran, Computers in Human Behavior 51 (2015) 180–18,7 2015
[199] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=53816&Itemid=0&lang=&lang=#4

εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου, στην οποία όμως ποτέ δεν δήλωσαν συμμετοχή. Η εν λόγω απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων. Οι αποστολείς αυτών των μηνυμάτων, για να γίνουν πιστευτοί, συνοδεύουν τα μηνύματά τους με πλαστά πιστοποιητικά όσον αφορά την υποτιθέμενη ηλεκτρονική κλήρωση.

2. *Επιχειρησιακές Απάτες (Business/Employment Schemes):* Πρόκειται για διαδικτυακές αγγελίες που αναρτώνται σε ιστοσελίδες εύρεσης εργασίας ή αποστέλλονται μέσω e-mail στο θύμα και περιγράφουν ιδιαίτερα ελκυστικές θέσεις εργασίας ιδίως στο εξωτερικό. Ορισμένοι δράστες δημιουργούν ιστοσελίδα της εταιρείας, στην οποία αναρτούν πληροφορίες για την απατηλή αγγελία προκειμένου να γίνουν περισσότερο πειστικοί. Οι υποψήφιοι εργαζόμενοι πρέπει να τους γνωστοποιήσουν τα προσωπικά τους στοιχεία, καθώς και να τους αποστείλουν αντίγραφα εγγράφων τους, για την διεκδίκηση της θέσης εργασίας. Τα θύματα είναι άτομα που συμπληρώνουν αιτήσεις για θέσεις εργασίας ενώ στην πραγματικότητα τα στοιχεία τους χρησιμοποιούνται για την αγορά εμπορευμάτων με πίστωση.

3. *Απάτες πιστωτικής / χρεωστικής κάρτας (Credit/Debit Card Frauds):* Η χρήση πιστωτικών καρτών στο διαδίκτυο, για τη διεκπεραίωση πάσης φύσεως συναλλαγών, έχει δημιουργήσει νέες δυνατότητες για τη διάπραξη εγκλημάτων[200]. Ουσιαστικά, είναι η μη εξουσιοδοτημένη χρήση της τραπεζικής κάρτας μέσω κλοπής προσωπικών δεδομένων από ιστοσελίδες για την απόκτηση χρημάτων με δόλο. Πραγματοποιούνται με την αλίευση των ευαίσθητων προσωπικών δεδομένων ώστε να επιτευχθεί η παράνομη μεταφορά χρημάτων σε λογαριασμούς μελών τους που μένουν στην Ελλάδα ή κάνουν αγορές διάφορων προϊόντων στο όνομα του ιδιοκτήτη της κάρτας. Η κύρια μέθοδος πραγματοποιείται συνήθως με έναν από τους ακόλουθους δύο τρόπους.

   α) Αποκτάται φυσική πρόσβαση στα στοιχεία των πιστωτικών καρτών των πολιτών κι εν συνεχεία αυτά χρησιμοποιούνται σε διαδικτυακές αγορές. Στην ουσία πρόκειται για μη εξουσιοδοτημένη πρόσβαση (*unauthorized access*).

[200] M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwise, B. Graveland, D.McKinney, J. Mulcahy, C. Wueest, In: Symantec Global Internet Security Threat Report. Trends for 2009. Technical Report, Symantec Corporation, Cupertino, 2010.

Αφορά την απόκτηση πρόσβασης σε πόρους μέσω ενός υπολογιστή χωρίς άδεια (συνήθως μέσω χρήσης hacking [201]ή Trojans[202]).

β) Αυτός ο τρόπος αφορά τη διάδοση των στοιχείων απ' τους ίδιους τους χρήστες του διαδικτύου οι οποίοι τα διαθέτουν άθελά τους σε κακόβουλους χρήστες. Πιο συγκεκριμένα, το θύμα λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου (spam e-mails - αυτές οι απάτες γνωστές κι ως *απάτες «ψαρέματος»/ Phising)* από Ίδρυμα στον οποίο τηρεί λογαριασμό και του ζητείται να συμπληρώσει τα στοιχεία του διαφορετικά ο λογαριασμός θα κλείσει. Αυτό το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα, με αποτέλεσμα το θύμα να χορηγεί τα απαραίτητα στοιχεία. Τα κέρδη των δραστών παγκοσμίως υπερβαίνουν το ένα δισεκατομμύριο ευρώ σε ετήσια βάση[203].

4. *Απάτες «pharming»:* Αυτή η απάτη αποτελεί παραλλαγή του «phishing». Περιγράφει την παρέμβαση τρίτων στον DNS εξυπηρετητή (DNS server) μιας ιστοσελίδας που έχει ως στόχο την ανακατεύθυνση του προγράμματος περιήγησης σε άλλες ψεύτικες ιστοσελίδες. Το pharming μπορεί να γίνει μέσω αλλοίωσης: 1) του «host» file ενός Η/Υ, ανακατευθύνοντας έτσι σε ψευδή προορισμό, 2) του «router» ενός δικτύου LAN ή ακόμη και του firmware ενός router, πετυχαίνοντας έτσι ο δράστης το σκοπό του, και 3) ενός DNS server αλλοιώνοντας την κίνηση όλων των χρηστών του διαδικτύου που εξυπηρετείται από αυτούς.

5. *Απάλειψη Χρέους (Debt Elimination):* Αφορά ιστοσελίδες που υπόσχονται τη διαχείριση και την εξάλειψη του χρέους νοικοκυριών και επιχειρηματιών, διαφημίζοντας νόμιμους τρόπους για την αντιμετώπιση του χρέους από πιστωτικές κάρτες και των στεγαστικών δανείων. Αυτό που ζητείται είναι η καταβολή ενός αρχικού ποσού, η αποστολή όλων πληροφοριών που σχετίζεται με τα εν προκειμένω δάνεια και τις πιστωτικές κάρτες. Τέλος, ζητείται εξουσιοδότηση προς το άτομο που θα φέρει εις πέρας όλη τη διαδικασία. Ο διαμεσολαβητής εκδίδει ομόλογα και γραμμάτια προς τους δανειστές που φιλοδοξούν να ικανοποιήσει

[201] Το hacking συνήθως αναφέρεται στην απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα μέσω δεξιοτήτων, τακτικής και λεπτομερούς γνώσης.
[202] Ένα Trojan είναι ένα πρόγραμμα που εμφανίζεται καλοήθες, αλλά στην πραγματικότητα περιέχει επιβλαβή προγράμματα (π.χ. ένα συνημμένο μήνυμα που φέρει ιούς).
[203] Christian Konradt, Andreas Schilling, Brigitte Werners , Phishing: An economic analysis of cybercrime perpetrators, computers & security 58 (2016) 39–46

νόμιμα όλα τα χρέη. Από το θύμα είναι απαραίτητη η καταβολή ενός ποσοστού της αξίας των χρεών που θα καλυφθούν από το διαμεσολαβητή.

6. *Απάτες Πυραμίδας/ Ponzi (Ponzi/Pyramid Schemes):* Η συγκεκριμένη απάτη σχετίζεται με διαδικτυακά πυραμιδικά συστήματα εργασίας από το σπίτι. Οι επενδυτές προσελκύονται σε δόλιο πρόγραμμα γεμάτο υποσχέσεις όσον αφορά τα κέρδη. Ωστόσο, αυτές οι επενδύσεις είναι μη πραγματικές με αποτέλεσμα οι επενδυτές να χάνουν ακόμα και την αρχική τους επένδυση..

7. *Spam:* είναι η λήψη μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου που παρέχει σε παραλήπτες προσφορές. Ο σκοπός των μηνυμάτων spam είναι να κάνει τους πελάτες να σκεφτούν ότι πρόκειται να λάβουν τις αγορές τους σε χαμηλή τιμή. Πριν τη συναλλαγή ζητείται από τους παραλήπτες να καταθέσουν τον αριθμό της πιστωτικής τους κάρτας για την αγορά καθώς κι άλλα προσωπικά δεδομένα[204]. Χαρακτηριστικό παράδειγμα αποτελεί πρόσφατα στο Facebook η απάτη απ 'όπου οι χρήστες έρχονται αντιμέτωποι με διαφημίσεις που εξαπλώνονται μέσω παραβιασμένων λογαριασμών του Facebook. Τον έλεγχο έχουν πάρει οι κυβερνοεγκληματίες χρησιμοποιώντας malware και τακτικές κοινωνικής μηχανικής. Χωρίς συγκατάθεση, δημοσιεύονται φωτογραφίες που διαφημίζουν μεγάλη έκπτωση σε γυαλιά επώνυμα ηλίου. Όταν γίνεται απόπειρα αγοράς σε ψεύτικα e-shops, αντιμετωπίζονται διάφοροι κίνδυνοι[205].

8. *Αυτόνομα κακόβουλα προγράμματα*: όπως οι γνωστοί σε όλους Ιοί, τα Σκουλήκια και οι Δούρειοι Ίπποι (Trojan Horses).

9. *«Απάτες 419» ή «Νιγηριανές Απάτες»:* Αποστέλλονται μηνύματα σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας έχει αποβιώσει και ο παραλήπτης του μηνύματος έχει επιλεγεί ούτως ώστε να κληρονομήσει αυτός την περιουσία και χρειάζεται να διαθέσει το λογαριασμό του ώστε να αποκτήσει κάποιο ποσοστό επί της περιουσίας αυτής. Τα λεφτά αναφέρεται ότι πρέπει να μεταφερθούν σε τραπεζικό λογαριασμό του εξωτερικού. Άλλη περίπτωση αφορά άτομα από τη Νιγηρία που υποστηρίζεται ότι αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται

[204] www.cybercc.gr
[205] http://www.welivesecurity.com/2016/04/06/buying-ray-bans-dont-fall-for-this-facebook-scam/

από εγκληματικές πράξεις, υποσχόμενοι για τη συνεργασία υψηλό ποσοστό αμοιβής.

Πολλές φορές και στις δύο περιπτώσεις ζητείται από το θύμα κάποιο αποδεικτικό έγγραφο, οι αποστολείς προσκομίζουν τα σχετικά πλαστά έγγραφα, τα οποία φαίνονται αυθεντικά κι επίσημα, πείθοντάς τους στην ουσία και πέφτοντας στην παγίδα.

10. *Ιός ransomware – CryptoWall* ή αλλιώς «ο ιός των 100€»: Οι δράστες εκμεταλλευόμενοι τις αδυναμίες του Η/Υ του θύματος, του μεταφέρουν κακόβουλο λογισμικό ενώ περιηγείται στο διαδίκτυο. Το λογισμικό αυτό εμφανίζει στην οθόνη ένα μήνυμα που δείχνει ότι προέρχεται από τη Δίωξη Ηλεκτρονικού Εγκλήματος κι απαιτεί την καταβολή πρόστιμου ύψους 100 € για αδικήματα του Ποινικού Κώδικα που διέπραξε κατά την πλοήγησή του. Η καταβολή γίνεται με τη χρήση προπληρωμένων καρτών paysafe ή ucash. Αυτός ο ιός έχει πανευρωπαϊκή παρουσία. Πολλοί χρήστες έχουν πέσει θύματα κι έχουν καταβάλλει κιόλας χρηματικό ποσό.

    Το «CryptoWall» αποτελεί εξέλιξη του κακόβουλου λογισμικού «Cryptolocker». Εξαπλώνεται μέσω μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου, χρησιμοποιώντας ένα εξελιγμένο σύστημα κρυπτογράφησης, κλειδώνει όλα τα ψηφιακά αρχεία και τα δεδομένα που είναι αποθηκευμένα στον υπολογιστή του χρήστη, ενώ για να ξεκλειδωθούν τα αρχεία του, πρέπει να καταβληθεί χρηματικό ποσό (ransom). Η καταβολή γίνεται μέσω ανώνυμου προγράμματος περιήγησης, με τη χρήση του ψηφιακού νομίσματος bitcoin (BTC), κατόπιν μηνύματος που εμφανίζεται στον χρήστη, με οδηγίες για την πραγματοποίηση της πληρωμής.

    10.α) *Κινητά τηλέφωνα και διαδικτυακές παγίδες*: Η χρήση των smartphones αυξάνεται συνεχώς. Θύτες, προκαλούν απάτες εκατομμυρίων ευρώ από την αγοραπωλησία εφαρμογών software για κινητά τηλέφωνα. Συνήθως ζητείται από τον ανυποψίαστο χρήστη, να εισάγει το κινητό του τηλέφωνο προκειμένου να αποκτήσει την εφαρμογή που έχει επιλέξει. Στη συνέχεια, ξεκινούν οι υπέρογκες χρεώσεις στον αριθμό του, που έχει αποδεχτεί ο ίδιος χωρία να το καταλάβει.

    10.β) Ηλεκτρονικές Δημοπρασίες (Auctions): Ένα είδος απάτης που αφορά τις διαδικτυακές δημοπρασίες. Εστιάζουν κυρίως στην διαστρεβλωμένη παρουσίαση του προϊόντος ή στην μη παράδοση του.

Κεφάλαιο 7: Προβλέψεις

7.1. Πρόβλεψη Απατών με Χρονολογικές Σειρές

Με τον όρο χρονολογικές σειρές νοείται μία σειρά από παρατηρήσεις που λαμβάνονται σε ορισμένες χρονικές στιγμές ή περιόδους οι οποίες μπορεί να ισαπέχουν ή και όχι μεταξύ τους. Κατ' αυτόν τον τρόπο, η τρέχουσα τιμή μίας μεταβλητής εκφράζεται ως συνάρτηση των προηγούμενων τιμών με χρονική υστέρηση. Με άλλα λόγια, η χρονολογική σειρά μπορεί να θεωρηθεί ως στοχαστική διαδικασία πεπερασμένου πλήθους παρατηρήσεων, δηλαδή η πραγματοποίηση μίας διαδικασίας $X_1, X_2, \dots, X_t$, όπου X η τυχαία μεταβλητή και t η χρονική στιγμή. Η χρησιμοποίηση αυτών είναι ραγδαία τις τελευταίες τρεις δεκαετίες, κυρίως μετά τη δημοσίευση της εργασίας των Box & Jenkins[206].

Στόχος είναι να δημιουργηθεί ένα χρονοδιάγραμμα, του οποίου η μελέτη του θα δώσει εικόνα της διαχρονικής εξέλιξης φαινομένων. Αφορά τη μετατροπή πληροφοριών από κανονικά χρονικά διαστήματα σε στατιστικά μέτρα. Γνωστοί μέθοδοι ανάλυσης χρονοσειρών αποτελούν (α) η μέθοδος της αυτοσυσχέτισης, στην οποία η χρονοσειρά αναπαριστάται με ένα δυναμικό μοντέλο όπου οι παρατηρήσεις θεωρούνται συναρτήσεις του παρελθόντος, και (β) η μέθοδος της φασματικής ανάλυσης η οποία αναπαριστά τη χρονοσειρά με ένα κινητικό μοντέλο που οι παρατηρήσεις θεωρούνται συναρτήσεις του χρόνου.

Οι παρατηρήσεις είναι συγκεκριμένες τιμές ή συγκεκριμένες πραγματοποιήσεις τυχαίων μεταβλητών. Αυτές οι τυχαίες μεταβλητές αποτελούν μέρος μίας άπειρης σειράς από τυχαίες μεταβλητές. Αυτή η άπειρη ακολουθία ονομάζεται στοχαστική ή τυχαία διαδικασία ή στοχαστική ανέλιξη και παρουσιάζεται ως {Xt:t=0,1,2,...}. Η έννοια της στοχαστικής διαδικασίας είναι ανάλογη της έννοιας του πληθυσμού και αυτή της συγκεκριμένης πραγματοποιήσεως είναι ανάλογη αυτής του δείγματος[207].

Οι χρονολογικές σειρές διακρίνονται σε συνεχείς χρονολογικές σειρές και σε διακριτές. Συνεχείς είναι αυτές όπου η τιμή του X(t) φαινομένου παρατηρείται συνεχώς, π.χ. η παρακολούθηση των σεισμών αποτελεί συνεχή χρονολογική σειρά. Διακριτές απ' την άλλη είναι αυτές όπου η τιμή του φαινομένου καταγράφεται σε ορισμένα χρονικά διαστήματα. Στην παρούσα μελέτη, οι χρονοσειρές που μας ενδιαφέρουν είναι οι διακριτές.

[206] Lon-Mu Liu, Gregory B. Hudak in collaboration with George E. P. Box, Mervin E. Muller , George C. Tiao, FORECASTING AND TIME SERIES ANALYSIS USING THE SCA STATISTICAL SYSTEM Copyright Scientific Computing Associates Corp., 1992-1994, Chicago, Illinois 60607-3528 U.S.A.

[207] Θαλασσινός Ελευθέριος, Υποδείγματα χρονολογικών σειρών: Θεωρία, εφαρμογές, Εκδόσεις Σταμούλης, 1986

Οι τιμές των χρονοσειρών παρουσιάζουν ορισμένα χαρακτηριστικά που είναι γνωστά ως συνιστώσες της χρονοσειράς. Οι συνιστώσες αυτές είναι α) η *τάση* η οποία είναι η μακροχρόνια ομαλή κεντρική κίνηση και μπορεί να είναι ανοδική, καθοδική ή σύνθετη, β) η *κυκλικότητα*, που είναι η συστηματική κύμανση που δημιουργείται γύρω από την τάση κι επαναλαμβάνεται με μικρή, μεγάλη ή πλήρη ομοιομορφία κατά περιόδους μεγαλύτερες του ενός χρόνου, γ) η *εποχικότητα,* η περιοδική δηλαδή βραχυχρόνια κίνηση που εμφανίζεται εντός του έτους κι επαναλαμβάνεται σε όλες τις ακολουθούμενες ετήσιες χρονικές περιόδους και δ) η τυχαία κύμανση που διαμορφώνεται ανεξαρτήτως του χρόνου κι ονομάζεται άρρυθμος παράγοντας, λόγω της τυχαίας συμπεριφοράς της.

Η στατιστική ανάλυση της χρονοσειράς αποβλέπει στο διαχωρισμό των συνιστωσών που την αποτελούν. Δηλαδή, η αφαίρεση της τάσης είναι απαραίτητη όταν χρειάζεται να μελετηθεί η συμπεριφορά της χρονοσειράς. Η ανάλυση των χρονοσειρών αφορά τον προσδιορισμό και την αξιολόγηση κάθε συνιστώσας. Η διαδικασία που ακολουθείται σχετίζεται με α) τον προσδιορισμό της μακροχρόνιας τάσης, β) τον προσδιορισμό της εποχικότητας, γ) την απαλοιφή εποχικών κυμάνσεων, δ) την απαλοιφή τάσης, ε) τον προσδιορισμό κυκλικών κυμάνσεων και στ) την απαλοιφή αυτών.

7.2. Μέτρα Χρονολογικών Σειρών

Βασική έννοια των χρονολογικών σειρών αποτελεί η γραφική παράσταση που αφορά την καμπύλη που παράγεται σε ένα σύστημα ορθογωνίων αξόνων, όπου ο οριζόντιος παριστάνει το χρόνο κι ο κατακόρυφος τις μετρούμενες τιμές στο αντίστοιχο χρονικό διάστημα. Μέσω αυτής γίνονται κάποιες γρήγορες διαπιστώσεις. Μέσος όρος (μ) μίας χρονολογικής σειράς είναι η μέση τιμή όλων των τιμών της.

$$\mu = \frac{1}{N}\sum_{t=1}^{N} X(t_t)$$

με $X(t_t), t = 1,2,3, \dots N$ να συμβολίζει τη χρονολογική σειρά

μ: μέση τιμή

N: χρονικές στιγμές

Διασπορά είναι ο μέσος όρος των τετραγώνων των αποκλίσεων από τη μέση τιμή.

$$\sigma^2 = \frac{1}{N-1}\sum_{t=1}^{N}(X(t_t) - \mu)^2$$

Τυπική απόκλιση (σ) μίας χρονολογικής σειράς είναι η τετραγωνική ρίζα της διασποράς. Η τυπική απόκλιση είναι πιο διαισθητική σαν έννοια από ότι είναι η διασπορά.

$$\sigma = \sqrt{\sigma^2} = \sqrt{\frac{1}{N-1}\sum_{t=1}^{N}(X(t_t) - \mu)^2}$$

Γύρω απ' τις τιμές μ±σ βρίσκονται τα περισσότερα σημεία της χρονολογικής σειράς. Αλλά υπάρχουν και χρονολογικές σειρές όπου τα μέτρα μ και μ±σ δε δίνουν καλή περιγραφή της πραγματικής μέσης τιμής. Η αιτία είναι πως υπάρχει τάση και η πραγματική μέση τιμή αλλάζει με το χρόνο. Συνεπώς, ένα μοντέλο για την τάση είναι απαραίτητο. Αν υποτεθεί αυθαίρετα ότι η τάση ακολουθεί κάποια γνωστή κατανομή, σαν πρώτη προσέγγιση μπορεί να γίνει αποδεκτό ότι η μέση τιμή μεταβάλλεται γραμμικά ως προς τον χρόνο. Συστηματοποιώντας τη διαδικασία κατασκευής μοντέλου για την τάση κατασκευάστηκε ο κινητός μέσος όρος. Στις χρονολογικές σειρές, εκτός από τη μακροχρόνια τάση συναντάται κυκλική κύμανση, εποχιακή κι ακανόνιστη μεταβολή.

Στη μακροχρόνια τάση η τιμή της μεταβλητής τείνει είτε να αυξάνεται είτε να ελαττώνεται για μεγάλο χρονικό διάστημα. Μερικές απ' τις μεθόδους προσδιορισμού της μακροχρόνιας τάσης είναι η μέθοδος των δυο μέσων σημείων, των κινητών μέσων, της ευθείας ελαχίστων τετραγώνων κι αυτή της καμπύλης ελαχίστων τετραγώνων. Η τάση, εξαιτίας του μακροχρόνιου χαρακτήρα της, δε μπορεί να διακριθεί με σαφήνεια αν τα διαθέσιμα στοιχεία δεν καλύπτουν σχετικά μακροχρόνιο διάστημα, συνήθως 10 και παραπάνω χρόνια.

Στην κυκλική κύμανση σε μία μακροχρόνια περίοδο παρατηρούνται αυξομειώσεις της τιμής της μεταβλητής γύρω από γραμμή τάσης με μικρή, μεγάλη ή πλήρη ομοιομορφία, κατά περιόδους μεγαλύτερες του έτους. Ουσιαστικά, για μία χρονική σειρά παρατηρήσεων, τα σημεία της χρονολογικής σειράς βρίσκονται πάνω (peak) απ' τη γραμμή τάσης και στη συνέχεια, για άλλη χρονική σειρά τιμών, τα σημεία είναι κάτω (trough) από αυτή τη γραμμή. Η ανοδική εξέλιξη κύμανσης μεταξύ του κάτω και του άνω σημείου καμπής ονομάζεται ανοδική φάση. Καθοδική φάση είναι η αμέσως επόμενη καθοδική εξέλιξη της κύμανσης μεταξύ του άνω σημείου καμπής και του κάτω σημείου καμπής που ακολουθεί. Ο χρόνος μεταξύ δύο διαδοχικών κάτω ή άνω σημείων καμπής αποτελεί την περίοδο ή το χρονικό μήκος της κυκλικής κύμανσης. Πρακτικά, οι κυκλικές αυξομειώσεις είναι δύσκολες

ως προς την αντιμετώπιση γιατί η κυκλική κίνηση δεν ακολουθεί κανένα κανονικό μοντέλο, βασικά κινείται απρόβλεπτα.

Οι χρονολογικές σειρές που παρουσιάζουν περιοδικές ή αλλιώς εποχιακές μεταβολές είναι αρκετά χρήσιμες αφού ακολουθούν κανονικό μοντέλο κι έτσι δύναται να δώσουν αξιόπιστες προβλέψεις για το μέλλον. Διαφορετικά είναι γνωστές με τον όρο περιοδική βραχυχρόνια κίνηση που εκδηλώνεται κι εξαντλείται πλήρως εντός του έτους κι επαναλαμβάνεται σε όλες τις ετήσιες χρονικές περιόδους. Η εποχική συνιστώσα έχει περίοδο το έτος, καθώς εντός αυτού εξαντλεί όλες τις ανοδικές και καθοδικές κινήσεις της. Όμως υπάρχουν και χρονολογικές σειρές που παρουσιάζουν ακανόνιστες μεταβολές που είναι άλλοτε μικρές άλλοτε μεγάλες, μια θετικές και μια αρνητικές, χωρίς καμία κανονικότητα. Η κύμανση αυτή είναι γνωστή κι ως άρρυθμος παράγοντας, λόγω της τυχαίας συμπεριφοράς της. Αυτές οι μεταβολές μπορεί να είναι συμπτωματικές, οφειλόμενες σε απρόβλεπτα γεγονότα και τυχαίες. Υπάρχουν τιμές δηλαδή που βρίσκονται σε προφανή απόκλιση από τις υπόλοιπες. Οι τιμές αυτές μπορεί να δημιουργήσουν σοβαρά προβλήματα στη μοντελοποίηση κι άρα να χρειαστεί ειδική μεταχείριση αφού προσδιοριστεί το αίτιο.

Για τον ορισμό ενός μοντέλου χρονολογικών σειρών απαιτείται ο καθορισμός όλων των κοινών κατανομών μίας ακολουθίας, δηλαδή των πιθανοτήτων, διαδικασία που είναι εξαιρετικά δύσκολη. Αντ' αυτού χρησιμοποιούνται ροπές μικρότερης τάξης με την υπόθεση της στασιμότητας. Στάσιμη αποκαλείται μια χρονολογική σειρά εάν δεν υπάρχει συστηματική αλλαγή του μέσου όρου και της διασποράς της στο χρόνο.

7.3. Στατιστική ανάλυση χρονοσειρών

Η ανάλυση των χρονοσειρών συνίσταται στον προσδιορισμό και την αξιολόγηση κάθε συνιστώσας της χρονοσειράς και την αξιοποίηση των συμπερασμάτων που προκύπτουν. Η στατιστική ανάλυση χρονοσειρών αποβλέπει στο διαχωρισμό των συνιστωσών που την αποτελούν. Όταν πρέπει να μελετηθεί η συμπεριφορά της χρονοσειράς χωρίς την τάση, η αφαίρεσή της είναι απαραίτητη. Η κυκλική συνιστώσα έχει μεγάλη σημασία κυρίως όταν γίνεται λόγος για οικονομική δραστηριότητα και μελετάται συνήθως ανεξάρτητα. Η αφαίρεση της εποχικότητας διευκολύνει τη σύγκριση τιμών μιας χρονοσειράς. Η μελέτη των συνιστωσών έχει ως αποτέλεσμα τη μελέτη του παρελθόντος και την εξέταση μελλοντικών προοπτικών.

Για τη λήψη πρόβλεψης, τα βήματα που ακολουθούνται στην ανάλυση χρονοσειράς

είναι (α) εξασφάλιση σταθερής συμπεριφοράς χρονοσειράς, (β) εξασφάλιση μη ύπαρξης περιοδικότητας, (γ) εξασφάλιση καταλληλότητας μοντέλου, (δ) εκτίμηση αγνώστων παραμέτρων και (ε) χρήση μοντέλου για πρόβλεψη.

7.4.1 Η συνάρτηση αυτοσυσχέτισης (AutoCorrelation Function- ACF)

Ο συντελεστής αυτοσυσχέτισης αποτελεί ένα στατιστικό δείκτη που χρησιμοποιείται για τον καθορισμό της τυχαιότητας ή μη της χρονοσειράς, δηλαδή δείχνει τη συσχέτιση της χρονοσειράς με τον εαυτό της. Μαθηματικώς εκφράζεται ως ο λόγος της συνδιακύμανσης προς το γινόμενο των τετραγωνικών ριζών των διακυμάνσεων δυο μεταβλητών. Ισχύει ότι 1≤ρ≤1, όπου ρ συντελεστής συσχέτισης. Ουσιαστικά, ο συντελεστής συσχέτισης δίνει ένα μέτρο για το βαθμό της σχέσης των δυο μεταβλητών. Μέσω αυτής της συνάρτησης γίνεται έλεγχος της τυχαιότητας των δεδομένων, της σταθερότητας της χρονοσειράς, της τάσης της, κλπ. Σε μία τυχαία χρονοσειρά, το 95% των συντελεστών βρίσκονται στο διάστημα ± 1.96/ n, όπου n είναι ο αριθμός των παρατηρήσεων. Εάν οι τιμές βρίσκονται εκτός των ορίων ±1.96, δηλαδή αν οι τιμές είναι στατιστικά διάφοροι του μηδενός, τότε υπάρχει συσχέτιση και η χρονοσειρά δε θεωρείται τυχαία.

Για ρ=±1, ισχύει ότι έχουμε τη μεγίστη δυνατή συσχέτιση, εάν ρ>0 υπάρχει θετική συσχέτιση, η οποία όσο πιο κοντά στο 1, τόσο πιο ισχυρή, εάν ρ<0 υπάρχει αρνητική συσχέτιση, η οποία όσο πιο κοντά στο -1, τόσο πιο ισχυρή. Για ρ=0 δεν υπάρχει καμία συσχέτιση μεταξύ των δυο μεταβλητών.

7.4.2 Η συνάρτηση μερικής αυτοσυσχέτισης (Partial AutoCorrelation Function- PACF)

Οι συντελεστές μερικής αυτοσυσχέτισης μετρούν το βαθμό της σχέσης μεταξύ των y_t και y_{t-k} όταν οι επιδράσεις όλων των άλλων χρονικών υστερήσεων 1,2,3, ...,k-1 έχουν αφαιρεθεί.

7.5. Ανάλυση Χρονολογικών Σειρών

Λευκός θόρυβος

Η χρονοσειρά αποτελείται από ανεξάρτητες τυχαίες μεταβλητές με ίδια κατανομή (independent and identically distributed, iid) στην περίπτωση που οι τυχαίες μεταβλητές έχουν ίδια κατανομή κι είναι ανεξάρτητες μεταξύ τους. Μια τέτοιου είδους χρονοσειρά είναι εντελώς τυχαία, δεν περιέχει αυτοσυσχετίσεις κι είναι γνωστή επίσης ως λευκός θόρυβος (white noise). Αν τα στοιχεία της ακολουθούν κανονική κατανομή Gauss, τότε η

χρονοσειρά λέγεται Γκαουσιανός λευκός θόρυβος (Gaussian white noise). Με λίγα λόγια, είναι μία ακολουθία ασυσχέτιστων τυχαίων μεταβλητών για τις οποίες ισχύει Ε(e_t)=0 και Var(e_t)= $\sigma^2_{e_t}$, t=1,2,...,n

Τυχαίος περίπατος

Ο τυχαίος περίπατος (random walk) είναι μία ακολουθία παρατηρήσεων όπου οι μεταβλητές είναι ανεξάρτητες, ισόνομες και τυχαίες. Είναι μία μη στάσιμη χρονοσειρά, όπου το κάθε στοιχείο της προκύπτει από το προηγούμενο με την πρόσθεση μιας τυχαίας τιμής, δηλαδή $X_{t=} X_{t-1} + e_t$, e_t: χρονοσειρά λευκού θορύβου.

Στασιμότητα

Η στασιμότητα αποτελεί βασικό χαρακτηριστικό των χρονολογικών σειρών. Ο διαχωρισμός των διάφορων χαρακτηριστικών μίας χρονολογικής σειράς είναι απαραίτητος και ιδίως αυτός ανάμεσα στα στάσιμα και τα μη-στάσιμα χαρακτηριστικά. Τα στοχαστικά μοντέλα φανερώνουν ότι ο μέσος, η διακύμανση και οι αυτοσυνδιακυμάνσεις δεν εξαρτώνται από τον χρόνο t. Στοιχεία ύπαρξης μη στασιμότητας απ' την άλλη θεωρούνται η ύπαρξη τάσης, εποχικότητας, η αλλαγή της μεταβλητότητας συναρτήσει του χρόνου, κ.α.

Η προσέγγιση Box-Jenkins

Αυτή η προσέγγιση ασχολείται με την αναγνώριση ενός ιδιαίτερου στατιστικού υποδείγματος που μπορεί να προσαρμοστεί σε μια δεδομένη χρονολογική σειρά και βασίζεται στην προσεκτική παρατήρηση των συναρτήσεων αυτοσυσχέτισης και μερικής αυτοσυσχέτισης. Έχουν διαμορφωθεί τρεις στάσιμες στοχαστικές διαδικασίες, α) η αυτοπαλινδρομική (AR), β) η τεχνική του κινητού μέσου (MA), και γ) η μικτή διαδικασία (ARMA). Λόγω του γεγονότος ότι οι περισσότερες χρονοσειρές δεν είναι στάσιμες, υπάρχει ομάδα μη στάσιμων διαδικασιών οι οποίες μπορούν να μετασχηματιστούν σε στάσιμες μέσω φίλτρου που δεν εξαρτάται από το χρόνο. Η τεχνική Box-Jenkins Auto-Regressive Integrated Moving Average δίνει μορφή υποδείγματος πιο γενική, ως συνάρτηση αυτοπαλινδρομούμενων όρων, κινούμενου μέσου και μιας σταθεράς. Επίσης, στο εκτιμώμενο μοντέλο περιλαμβάνεται ένας τύπος εποχικού και ένας τύπος μη εποχικού παράγοντα. Η γενική του μορφή είναι γνωστή ως εξής: *ARIMA(p,d,q)(P,D,Q)s* ,όπου:

- p: η τάξη αυτοπαλινδρόμησης του μη εποχικού παράγοντα,
- d: η τάξη προς τα πίσω διαφορών του μη εποχικού παράγοντα,

- q: η τάξη κινούμενου μέσου του μη εποχικού παράγοντα,

- P: η τάξη αυτοπαλινδρόμησης του εποχικού παράγοντα,

- D: η τάξη των προς τα πίσω διαφορών του εποχικού παράγοντα,

- Q: η τάξη κινούμενου μέσου του εποχικού παράγοντα,

- s: η εποχικότητα της χρονοσειράς.

Η προσέγγιση των Box-Jenkins είναι μια μέθοδος εύρεσης υποδείγματος ARIMA που να παριστάνει ικανοποιητικά τη στοχαστική διαδικασία από την οποία προήλθε το δείγμα. Περιλαμβάνει τρία στάδια, την ταυτοποίηση (identification), την εκτίμηση (estimation) και το διαγνωστικό έλεγχο (diagnostic checking).

Στο πρώτο στάδιο, επιλέγεται ένα δοκιμαστικό μοντέλο για να δείξει αν υπάρχουν βασικά χαρακτηριστικά στη χρονοσειρά, γίνεται γραφική απεικόνιση της μεταβλητής της χρονοσειράς και των συναρτήσεων συσχέτισης και γίνεται εξειδίκευση ενός ARIMA υποδείγματος με βάση τις πληροφορίες από το δείγμα. Καθορίζονται οι τιμές των p,d,q. Προκειμένου να προκύψει το συμπέρασμα ότι η σειρά είναι στάσιμη ή όχι, εξετάζεται η συμπεριφορά της δειγματικής συνάρτησης αυτοσυσχέτισης. Αν οι αυτοσυσχετίσεις συγκλίνουν προς το μηδέν, τότε η σειρά μάλλον είναι στάσιμη, αν φθίνουν με αργό ρυθμό, είναι ένδειξη ότι η σειρά είναι μη στάσιμη κι άρα πρέπει να γίνει στάσιμη. Αν μια μεταβλητή χαρακτηρίζεται από τάση, τότε χρησιμοποιούνται πρώτες, δεύτερες κ.τ.λ. διαφορές για να μετατραπεί η σειρά σε στάσιμη. Με τη μέθοδο των διαφορών εξαλείφεται η τάση, μέσω δημιουργίας μιας νέας χρονοσειράς από τις διαφορές μεταξύ διαδοχικών όρων. Αφού η σειρά γίνει στάσιμη, προσδιορίζεται η τάξη του υποδείγματος ARIMA που βασίζεται στις δειγματικές απλές και μερικές αυτοσυσχετίσεις.

Στο δεύτερο στάδιο της εκτίμησης εκτιμώνται οι παράμετροι του μοντέλου ύστερα από την προσαρμογή του στα δεδομένα. Ελέγχεται η σημαντικότητα των παραμέτρων, προβλέπεται το μέρος της χρονοσειράς που χρησιμοποιείται γι’ αυτό το σκοπό και γίνεται αποδοχή ή απόρριψη του μοντέλου. Ακολουθεί επομένως η εκτίμηση των p παραμέτρων της αυτοπαλίνδρομης διαδικασίας και των q παραμέτρων της διαδικασίας κινητού μέσου.

Στο τελευταίο στάδιο γίνεται διάγνωση που σχετίζεται με την τελική αποδοχή ή απόρριψη του μοντέλου. Ελέγχεται κατά πόσο ταιριάζει το υπόδειγμα με τα δεδομένα, εφαρμόζονται στατιστικοί έλεγχοι για τη σημαντικότητα των παραμέτρων και τη συμπεριφορά των καταλοίπων και την τάξη του υποδείγματος. Εδώ περιλαμβάνονται διαδικασίες υπολογισμού διαστημάτων εμπιστοσύνης, υπολογισμός του τυπικού σφάλματος και άλλων στατιστικών μεγεθών με σκοπό την ποσοτική εκτίμηση της

σημαντικότητας των συντελεστών του μοντέλου, τον έλεγχο της κανονικότητας των υπόλοιπων (residuals).

ARIMA

Οι διαφορές πρώτης τάξης, σε ένα τυχαίο περίπατο, οδηγούν σε διαδικασία λευκού θορύβου. Γενικά όμως, μία στάσιμη στοχαστική διαδικασία που προκύπτει παίρνοντας διαφορές κάποιας τάξης δεν είναι λευκός θόρυβος αλλά ARMA(p,q) στάσιμη διαδικασία.

Οι Box – Jenkins, για μία μη στάσιμη χρονοσειρά προτείνουν τη χρήση διαφορών πρώτης, δεύτερης ή d τάξεως για την επίτευξη στασιμότητας. Έτσι προσαρμόζεται ένα μοντέλο ARMA(p,q). Αυτό εφαρμόζεται σε μία ολοκληρωμένη σειρά d τάξεως και καλείται αυτοπαλίνδρομο ολοκληρωμένο μοντέλο κινητού μέσου τάξεως (p,q,d) - ARIMA(p,q,d). Πιο απλά, η διαδικασία ARIMA(p,q,d) 'διαφορίζεται' d φόρες και παράγει διαδικασία ARMA(p,q). Οι 3 συντελεστές έχουν ως εξής: p: παράμετρος αυτοπαλινδρόμησης (AR), d: βαθμός διαφορικού μετασχηματισμού/ ο αριθμός d των διαφορών που απαιτούνται για να γίνει η σειρά στάσιμη, q: τάξη μετακινούμενου μέσου (MA).

Τα μοντέλα ARIMA συνδυάζουν τις ιδιότητες τριών διαφορετικών υπομοντέλων α) αυτοπαλινδρόμησης (autoregression), β) ολοκλήρωσης (integration) και γ) εξομάλυνσης με μετακινούμενο μέσο (moving average).

Εποχικό υποδείγμα ARIMA (SARIMA)

Το εποχικό μέρος ενός υποδείγματος ARIMA έχει την ίδια δομή με αυτή του μη-εποχικού υποδείγματος. Έχει δηλαδή έναν παράγοντα AR, έναν παράγοντα MA και μια τάξη διαφορών. Ορίζεται ως ARIMA(p.d.q)x(P,D,Q), όπου P: ο αριθμός των εποχικών αυτοπαλίνδρομων όρων (SAR), D: ο αριθμός των εποχικών διαφορών και Q: ο αριθμός των εποχικών όρων κινητού μέσου (SMA).

7.6. Αξιολόγηση

Προκειμένου να αξιολογηθεί ένα μοντέλο ως προς την προβλεπτική του ικανότητα, χρησιμοποιούνται διάφορα κριτήρια, όπως:

- Η ρίζα του μέσου τετραφωνικού σφάλματος (RMSE), με τύπο:

$$\sqrt{\frac{\sum_t^M (y_t^f - y_t^a)^2}{N}}$$

όπου,
y_t^f : οι προβλεπόμενες τιμές,

y_t^a: οι παρατηρούμενες τιμές και

N: ο αριθμός των χρονικών περιόδων

- Το μέσο απόλυτο σφάλμα (MAE), με τύπο:

$$MAE = \frac{1}{N}\sum_{\tau=1}^{N}\left|y_t^f - y_t^a\right|$$

- Το μέσο απόλυτο ποσοστιαίο σφάλμα (MAPE), με τύπο:

$$MAPE = \frac{1}{N}\sum_{\tau=1}^{N}\left|\frac{y_t^f - y_t^a}{y_t^a}\right|$$

Μέσω των παραπάνω τύπων εξετάζεται η ακρίβεια του υποδείγματος και κατά πόσον οι προβλεπόμενες τιμές ακολουθούν τις στην ουσία τις πραγματικές. Όσο πιο κοντά στο μηδέν οι παραπάνω τιμές, τόσο πιο καλή θεωρείται η πρόβλεψη.

Εν συνεχεία, για τη διαλογή του καταλληλότερου υποδείγματος χρησιμοποιείται το κριτήριο Akaike (AIC) που έχει τον ακόλουθο τύπο:

$$AIC = \ln\frac{\sum \acute{\varepsilon}_t^2}{T} + \frac{2k}{T}$$

όπου:

$\sum \acute{\varepsilon}_t^2$: το άθροισμα των τετραγώνων των καταλοίπων,

Τ: το πλήθος των παρατηρήσεων και

κ: το πλήθος των παραμέτρων που εκτιμώνται.

Επιπλέον, σημαντικό είναι να εκτιμηθεί το διάστημα εμπιστοσύνης, το οποίο διατυπώνεται με βάση τη διακύμανση του σφάλματος πρόβλεψης. Αποτελεί ουσιαστικό κριτήριο υποδηλώνοντας την καταλληλότητα κι ακρίβεια της πρόβλεψης.

Περαιτέρω, εξετάζονται και τα κατάλοιπα, τα οποία θα πρέπει να μην αυτοσυσχετίζονται. Η ύπαρξη αυτοσυσχέτισης μπορεί να δείξει ότι υπάρχει ανεπαρκής προσαρμογή του υποδείγματος, κι άρα θα πρέπει να γίνουν τροποποιήσεις.

Για να είναι έγκυρες οι προβλέψεις, θα πρέπει το διάστημα λήψης δεδομένων να είναι παρόμοιο με το διάστημα πρόβλεψης και η πρόβλεψη πρέπει να είναι πεπερασμένη σε πλήθος στοιχείων και να αντιστοιχεί σε μέγεθος στο 10% του μεγέθους του δείγματος δεδομένων.

7.7. Προβλέψεις

Βασικός σκοπός της μελέτης των μοντέλων των χρονοσειρών, δηλαδή της εξειδίκευσης κι εκτίμησης ενός μοντέλου, όπως του αυτοπαλίνδρομου (AR), του κινητού μέσου (MA), του μεικτού (ARMA), του αυτοπαλίνδρομου ολοκληρωμένου κινητού μέσου (ARIMA) είναι η διενέργεια προβλέψεων. Δηλαδή, σύμφωνα με το εκτιμώμενο μοντέλο και τις υπάρχουσες πληροφορίες να γίνει πρόβλεψη της τιμής της χρονολογικής σειράς στην περίοδο t μέχρι τη χρονική περίοδο t, κ.ο.κ.

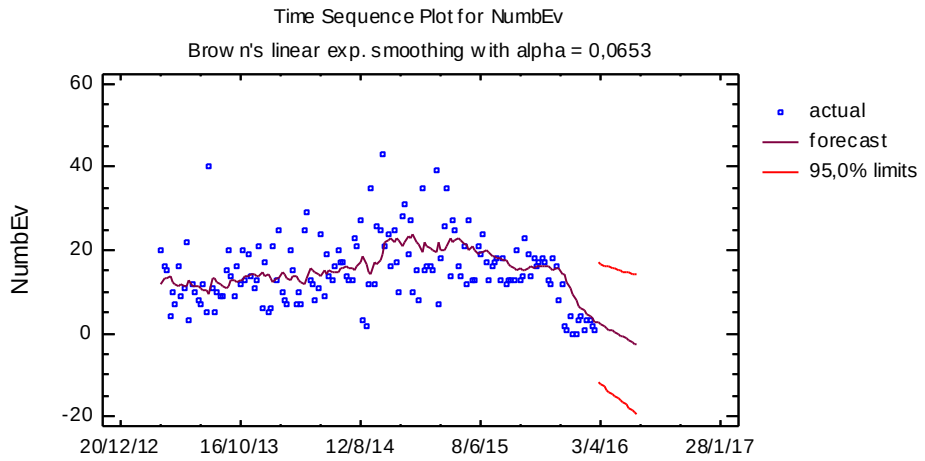
Η πρόβλεψη των μελλοντικών τιμών μίας παρατηρούμενης χρονοσειράς αποτελεί σημαντικό πρόβλημα για πολλές εφαρμογές. Για να πραγματοποιηθεί μια πρόβλεψη χρησιμοποιούνται παρατηρήσεις μέχρι την πιο πρόσφατη χρονική στιγμή. Θεωρώντας την παρατηρούμενη χρονοσειρά από μία στοχαστική διαδικασία, το πρόβλημα που μελετάται είναι η πρόβλεψη της χρονικής σειράς για k χρονικά βήματα μπροστά από τη χρονική στιγμή t $X_t(k)$, ενώ η πραγματική αλλά άγνωστη τιμή στην χρονική στιγμή t είναι X_{t+k}. Το σφάλμα πρόβλεψης είναι η διαφορά της πραγματικής πρόβλεψης απ' την πρόβλεψη της χρονικής σειράς για k χρονικά βήματα. Η βέλτιστη πρόβλεψη είναι η εκτίμηση του στοιχείου X_{t+k} της με βάση τα προηγούμενα στοιχειά της X_t. Καλή χαρακτηρίζεται μια πρόβλεψη αν έχει αμεροληψία (unbiasedness) κι αποτελεσματικότητα (efficiency). Συνδυάζοντας τα παραπάνω, καλύτερη είναι αυτή που ελαχιστοποιεί το μέσο τετραγωνικό σφάλμα πρόβλεψης για κάθε βήμα πρόβλεψης k.

Παρακάτω θα γίνει ανάλυση και μελέτη μοντέλων πρόβλεψης αναφορικά με τα ηλεκτρονικά εγκλήματα που έχουν πραγματοποιηθεί στην Ελλάδα τα τελευταία τρία χρόνια. Τα δεδομένα έχουν προκύψει από τη βάση δεδομένων της Ηλεκτρονικής Δίωξης Εγκλήματος και έχει ληφθεί υπόψη η εβδομαδιαία πραγματοποίηση απατών στην Ελλάδα. Για την ακρίβεια, τα δεδομένα αφορούν όχι όλες τις πραγματοποιημένες απάτες, αλλά μόνο όσες έχουν καταγγείλει τα αντίστοιχα θύματα. Η σχετική ανάλυση θα γίνει μέσω της χρήσης του στατιστικού πακέτου Statgraphics.

Με βάση το μοντέλο προκύπτουν εβδομαδιαίες προβλέψεις των ακολουθούμενων ηλεκτρονικών εγκλημάτων για το διάστημα Μάρτιος του 2016 έως τον Ιούλιο του 2016. Τα στοιχεία που θα χρησιμοποιηθούν είναι εβδομαδιαίες καταγγελλόμενες υποθέσεις ηλεκτρονικών απατών στην Ελλάδα σύμφωνα με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. Ο αριθμός των παρατηρήσεων είναι εβδομαδιαίος, ίσος με 156 και ξεκινούν από τον Απρίλιο του 2013.

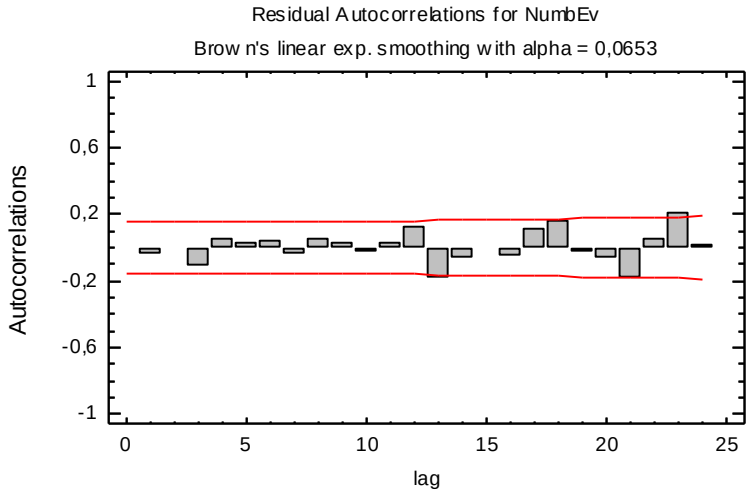
Αρχικά, για τον εντοπισμό του μοντέλου που θα ερμηνεύει καλύτερα τα δεδομένα της χρονοσειράς των ηλεκτρονικών απατών στην Ελλάδα, θα πρέπει να εξεταστεί κατά πόσο υπάρχει εποχικότητα. Όπως φαίνεται στο γράφημα της χρονοσειράς, τα γεγονότα έχουν μια μη ισορροπημένη τάση. Εκτιμάται ότι οι απάτες με το πέρασμα του χρόνου θα μειώνονται και η κλίση, ενώ αρχικά ήταν ελαφρώς ανοδική, στην πορεία προκύπτει να είναι καθοδική. Το πλήθος των απατών, διαχρονικά δεν παραμένει σταθερό.

Γράφημα 7.1: Γράφημα χρονοσειράς ηλεκτρονικών απατών

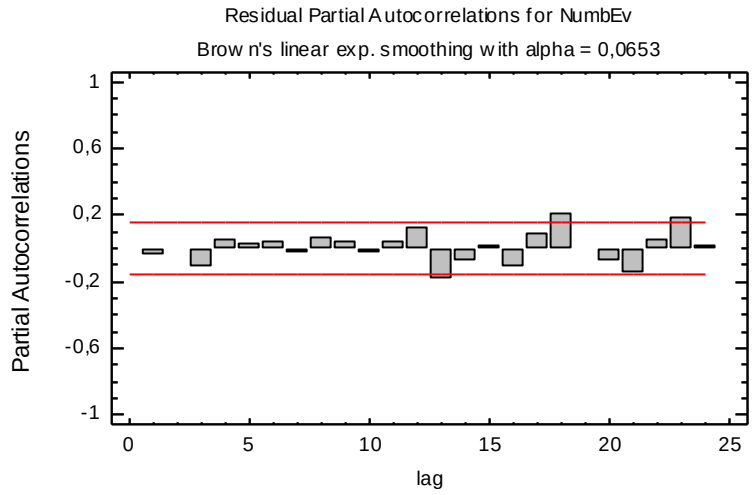


Παρατηρώντας τα γραφήματα αυτοσυσχέτισης καταλοίπων (ACF) και μερικής αυτοσυσχέτισης καταλοίπων (PACF) του επιλεγμένου μοντέλου (*Brown's linear exp. smoothing with alpha = 0,0653*), παρατηρείται ότι η χρονοσειρά παρουσιάζει εποχικότητα, δεδομένου ότι οι μπάρες εκτείνονται πέρα της χοάνης.

Γράφημα 7.2: Γράφημα αυτοσυσχέτισης καταλοίπων χρονοσειράς ηλεκτρονικών απατών

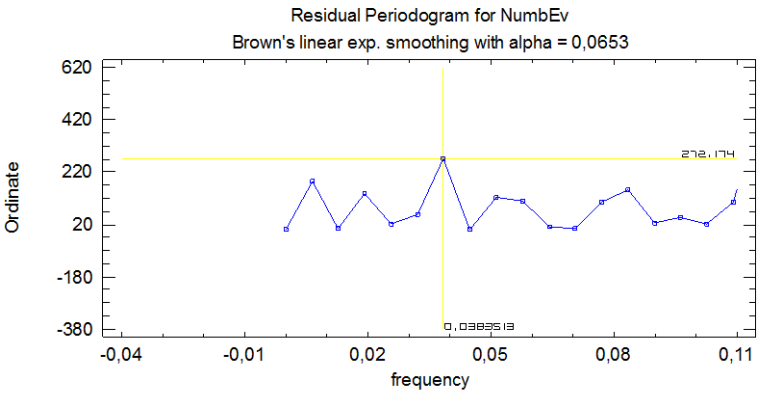


Γράφημα 7.3: Γράφημα μερικής αυτοσυσχέτισης καταλοίπων χρονοσειράς ηλεκτρονικών απατών



Οι μπάρες που προεξέχουν στο γράφημα αυτοσυσχέτισης καταλοίπων (ACF) είναι 2 ενώ το στο γράφημα μερικής αυτοσυσχέτισης καταλοίπων (PACF) προεξέχουν 3. Με αυτόν τον τρόπο καθορίζεται ο μέγιστος βαθμός των τάξεων των συντελεστών MA, SMA και AR, SAR, που μπορούν να είναι έως 2 και 3 αντίστοιχα, στο μοντέλο ARIMA που θα χρησιμοποιηθεί για την πρόβλεψη.

Γράφημα 7.4: Περιοδόγραμμα καταλοίπων χρονοσειράς ηλεκτρονικών απατών



Με βάση τα παραπάνω, η χρονοσειρά των ηλεκτρονικών απατών είναι εποχική με εποχικότητα 26 εβδομάδες, και προσδιορίστηκε από το περιοδόγραμμα ως εξής: s= 1/0,0383513 = 26,07474. Όπου 0,0383513 η τετμημένη της πρώτης μεγάλης κορυφής κοντά στην πρώτη περίοδο.

Εφαρμόζοντας την εποχικότητα, τα δεδομένα συνοπτικά με βάση το Statgraphics έχουν ως εξής:

- Data variable / Μεταβλητή: NumbEv – Number of Events – Πραγματοποιημένα Γεγονότα
- Number of observations / Αριθμός παρατηρήσεων = 156
- Start index / Ημερομηνία έναρξης γεγονότων = 1/4/13
- Sampling interval / Εβδομαδιαία αξιοποίηση δείγματος = 7,0 day(s)
- Seasonality / Εποχικότητα = 26 εβδομάδες

Για την εξάλειψη της εποχικότητας χρησιμοποιήθηκαν πρώτης τάξεως εποχικές διαφορές. Τα μοντέλα που εξετάστηκαν είναι:

A. ARIMA(0,1,1)x(1,1,1)26 με σταθερά
B. Simple moving average of 3 terms
   Seasonal adjustment: Multiplicative
C. Simple exponential smoothing with alpha = 0,1456
   Seasonal adjustment: Multiplicative
D. Brown's linear exp. smoothing with alpha = 0,0674
   Seasonal adjustment: Multiplicative
E. Simple exponential smoothing with alpha = 0,1409

Πίνακας 7.1: Σύγκριση των εξεταζόμενων μοντέλων

Model	*RMSE*	*MAE*	*ME*
(A)	6,71412	5,35941	0,473725
(B)	8,31887	5,50782	-0,204266
(C)	7,27155	4,8353	-0,346144
(D)	7,20781	4,80788	-0,464709
(E)	7,39069	5,57907	-0,399585

Το προτεινόμενο μοντέλο είναι το (A) ARIMA(0,1,1)x(1,1,1)26 με σταθερά, έχοντας τη μικρότερη τιμή ρίζας του μέσου τετραγωνικού σφάλματος- RMSE, όπως φαίνεται στον παραπάνω πίνακα. Εξετάζοντας τη συμπεριφορά των καταλοίπων παρατηρείται πως το μοντέλο (A) ARIMA(0,1,1)x(1,1,1)26 με σταθερά έχει την ένδειξη OK και στους πέντε ελέγχους των καταλοίπων.

Οι έλεγχοι που πραγματοποιούνται είναι οι παρακάτω:

- RUNS = Έλεγχος ροών πάνω και κάτω

- RUNM = Έλεγχος ροών πάνω και κάτω από τη διάμεσο
- AUTO = Box-Pierce έλεγχος για αυτοσυσχέτιση
- MEAN = Έλεγχος διαφοράς μέσου στο 1ο και 2ο μισό
- VAR = Έλεγχος διαφοράς διασποράς στο 1ο και 2ο μισό

Πίνακας 7.2: Έλεγχοι καταλοίπων

Model	*RMSE*	*RUNS*	*RUNM*	*AUTO*	*MEAN*	*VAR*
(A)	6,71412	OK	OK	OK	OK	OK
(B)	8,31887	OK	OK		OK	*
(C)	7,27155	OK	OK		OK	OK
(D)	7,20781	OK	OK		OK	OK
(E)	7,39069	OK	OK	OK	OK	OK

Το αποτέλεσμα αυτών των ελέγχων είναι αυτό που καθορίζει κατά πόσο ένα μοντέλο είναι κατάλληλο για τα δεδομένα. Η ένδειξη OK σε όλους τους παραπάνω ελέγχους δείχνει πως το πρώτο κι επιλεχθέν μοντέλο είναι και το πιο κατάλληλο για να χρησιμοποιηθεί για τη διενέργεια της πρόβλεψης με βάση τα δεδομένα που έχουμε.

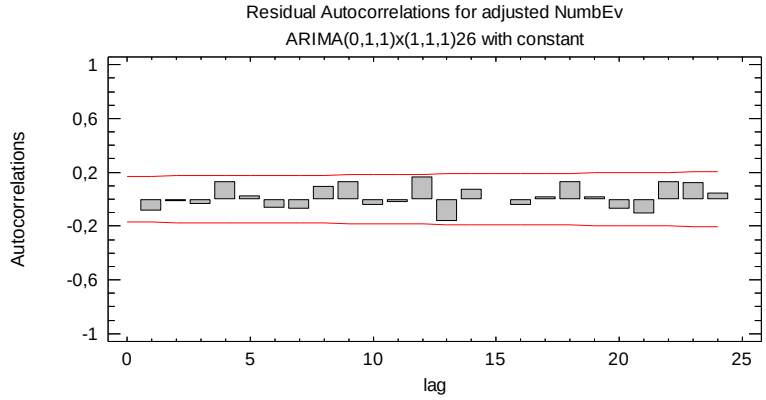
Πίνακας 7.3: Έλεγχος παραμέτρων του μοντέλου ARIMA(0,1,1)x(1,1,1)26 με σταθερά

Parameter	*Estimate*	*Stnd. Error*	*t*	*P-value*
MA(1)	0,891341	0,041102	21,6861	0,000000
SAR(1)	-0,473926	0,0805285	-5,8852	0,000000
SMA(1)	0,813048	0,0369615	21,9971	0,000000
Mean	-0,127491	0,0325426	-3,91766	0,000146
Constant	-0,187912			

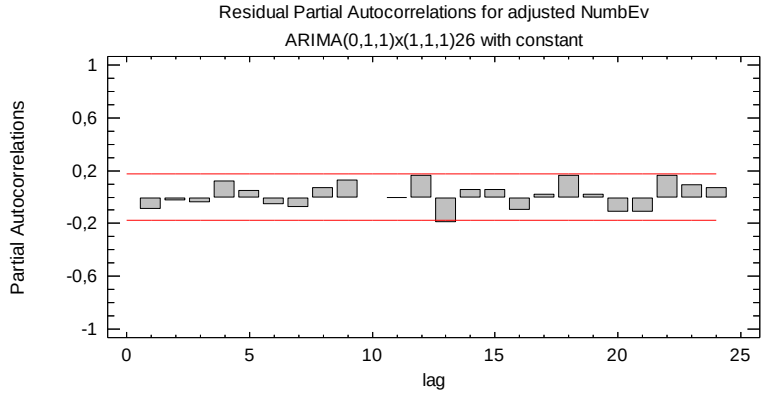
Στον πίνακα του ελέγχου των παραμέτρων του επιλεχθέντος μοντέλου πρόβλεψης (Πίνακας 7.3) αξιολογείται η στατιστική σημαντικότητα των συντελεστών του. Δεδομένου ότι το P-value των συντελεστών του μοντέλου είναι μικρότερο από 0,10, οι συντελεστές είναι στατιστικά σημαντικοί και διάφοροι του μηδενός σε βαθμό εμπιστοσύνης 95%.

Επιπλέον, στο γράφημα αυτοσυσχέτισης καταλοίπων (ACF) καμία μπάρα δεν προεξέχει από τη χοάνη, ενώ στο γράφημα μερικής αυτοσυσχέτισης καταλοίπων (PACF) προεξέχει οριακά μία μόνο μπάρα.

Γράφημα 7.5: Γράφημα αυτοσυσχέτισης καταλοίπων χρονοσειράς ηλεκτρονικών απατών



Γράφημα 7.6: Γράφημα μερικής αυτοσυσχέτισης καταλοίπων χρονοσειράς ηλεκτρονικών απατών



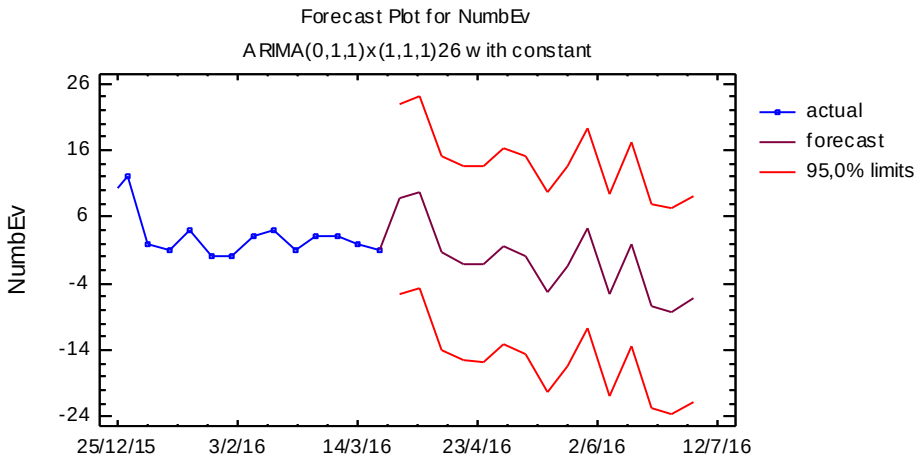
Βάσει των παραπάνω, το μοντέλο είναι κατάλληλο για να γίνουν οι προβλέψεις που αφορούν το διάστημα 15 εβδομάδων, από τον Μάρτιο έως και τον Ιούλιο του έτους 2016. Οι προβλέψεις που δίνει το μοντέλο και το αντίστοιχο διάστημα εμπιστοσύνης παρουσιάζονται στον πίνακα που ακολουθεί.

Πίνακας 7.4: Πρόβλεψη ηλεκτρονικών απατών στην Ελλάδα με τη χρήση του ARIMA(0,1,1)x(1,1,1)26

	Πρόβλεψη	***Διάστημα Εμπιστοσύνης 95,0%***	
Εβδομάδα	***Κεντρική Τιμή***	***Κάτω Όριο***	***Άνω Όριο***
28/3/16	9	0	23
4/4/16	10	0	24
11/4/16	1	0	15
18/4/16	0	0	14
25/4/16	0	0	14
2/5/16	2	0	16
9/5/16	0	0	15
16/5/16	0	0	10
23/5/16	0	0	14
30/5/16	4	0	19
6/6/16	0	0	10
13/6/16	2	0	17
20/6/16	0	0	8
27/6/16	0	0	7
4/7/16	0	0	9

Παρατηρείται μείωση στα γεγονότα που αφορούν τις καταγγελίες που σχετίζονται με ηλεκτρονικές απάτες. Ειδικότερα στις τελευταίες προβλεπόμενες εβδομάδες, οι καταγγελίες τείνουν να μειώνονται σε σημείο που να είναι μηδενικές οι υποθέσεις, και άρα να μην παρουσιάζονται ηλεκτρονικές απάτες. Στο παρακάτω διάγραμμα φαίνεται πιο ξεκάθαρα η φθίνουσα τάση.

Γράφημα 7.7: Γράφημα πρόβλεψης της χρονοσειράς ηλεκτρονικών απατών



Για το προβλεπόμενο διάστημα οι συνολικές ηλεκτρονικές απάτες είναι ελάχιστες κι ίσες με 28 περίπου καταγγελίες, ενώ για το αντίστοιχο διάστημα της προηγούμενης χρονιάς οι υποθέσεις ήταν τόσες και παραπάνω μάλιστα, μόλις σε μια εβδομάδα. Όπως προκύπτει, αυτή η μη αναμενόμενη, με βάση τη λογική, μείωση οφείλεται σε πολλούς παράγοντες που σχετίζονται με τις δύσκολες καταστάσεις που περνάει αυτή η χώρα τα τελευταία χρόνια κι ιδίως αυτήν την περίοδο που υπήρξε και θέμα ανασυγκρότησης στην εσωτερική οργάνωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος. Ο τελευταίος παράγοντας φαίνεται να παίζει ουσιαστικό ρόλο στη μείωση των υποθέσεων.

7.8. Συμπεράσματα

Αξιόποινες εγκληματικές πράξεις τελούνται πλέον με τη χρήση ηλεκτρονικών υπολογιστών κυρίως κι όχι με τη χρήση όπλων. Οι κύριες μορφές κυβερνοεγκλημάτων που έχουν εξιχνιασθεί από το Τμήμα Ηλεκτρονικού Εγκλήματος στην Ελλάδα σχετίζονται με απάτες μέσω Διαδικτύου, παιδική πορνογραφία, cracking και hacking, διακίνηση-πειρατεία λογισμικού, πιστωτικές κάρτες, διακίνηση ναρκωτικών κι έγκλημα στα chat rooms. Σε αυτήν την εργασία έχει γίνει εστίαση στην πρώτη κατηγορία.

Όπως επισημαίνεται από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, η έρευνα των ηλεκτρονικών εγκλημάτων είναι αρκετά δύσκολη και χρονοβόρα διαδικασία. Οι χρήστες του Διαδικτύου που ερευνώνται και που έχουν καταγγελθεί στην υπηρεσία διαπράττουν αξιόποινες πράξεις λαμβάνοντας διάφορα διαδικτυακά μέτρα προστασίας, καθιστώντας τον εντοπισμό αρκετά δύσκολη υπόθεση.

Ο συνδυασμός τεχνικών μέσων μαζί με τον ανθρώπινο παράγοντα είναι η χρυσή τομή για τα βέλτιστα αποτελέσματα. Σε περίπτωση ύπαρξης των τεχνολογικών μέσων χωρίς την κατάλληλη εξειδίκευση του προσωπικού ή την ύπαρξη καταρτισμένου προσωπικού, αλλά την έλλειψη πόρων, είναι δυνατό τα αποτελέσματα που σχετίζονται με τη διευθέτηση των απατών να μην είναι τα επιθυμητά. Τα αποτελέσματα της έρευνας υπονοούν είτε ότι ο παραπάνω συνδυασμός είναι άριστος κι άρα δεν υπάρχουν πολλές περιπτώσεις ηλεκτρονικών απατών που να καταγγέλλονται ή ότι η εμπιστοσύνη των χρηστών θυμάτων είναι ανύπαρκτη ως προς τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος κι άρα δεν μπαίνουν στη διαδικασία της καταγγελίας. Υπάρχει το ενδεχόμενο να θεωρούν τόσο την εξειδίκευσή όσο και τους πόρους αρκετά ελλιπή.

Μια επιπλέον παράμετρος που δύναται να δικαιολογεί τα αποτελέσματα της έρευνας είναι η νομοθεσία του κράτους και τα προβλήματα που παρουσιάζει με τις συνεχείς πολιτικές αλλαγές. Όπως είχε αναφέρει ο Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος, Υποστράτηγος κ. Εμμανουήλ Σφακιανάκης, τον οποίο ευχαριστώ ιδιαίτερα για την κάθε δυνατή πληροφορία που παρείχε για την εκπόνηση αυτής της εργασίας, «Η τεχνολογική υποδομή μαζί με τη νομοθεσία είναι απολύτως αναγκαίες για την σωστή τεκμηρίωση των υποθέσεων που έχουν εξιχνιαστεί και αφορούν ηλεκτρονικά εγκλήματα. Στην περίπτωση που θα υπάρχει τεχνολογική υποδομή χωρίς την κατάλληλη νομοθεσία, μέσα από την οποία θα οριοθετούνται οι εγκληματικές συμπεριφορές, τότε θα έχουμε πρόβλημα ως προς την απονομή δικαιοσύνης». Κι εδώ ουσιαστικά τίθεται το θέμα της εμπιστοσύνης κι αν αξίζει να κάνει κάποιος χρήστης – θύμα καταγγελία από τη στιγμή που μπορεί η υπόθεσή του να διαρκέσει αρκετά μεγάλο χρονικό διάστημα, να διαθέσει πόρους και ψυχολογική επένδυση, και στην τελική να υπάρχει αμφισβήτηση κι ως προς το αν θα αποδοθεί δικαιοσύνη.

Σύμφωνα με δημοσιεύσεις αλλά και την κοινή λογική, λόγω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και του διαδικτύου αναπτύσσονται καθημερινά τεράστιες δυνατότητες όχι μόνο χρήσης, αλλά και κατάχρησης που σχετίζονται με την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα εμπλουτίζεται μέρα με τη μέρα και η πιθανότητα εμφάνισης νέων μορφών στο μέλλον επιβάλλει την επένδυση από τους αντίστοιχους φορείς στο θέμα αυτό καθώς και τη διασυνοριακή συνεργασία. Κι εδώ όμως, αν και γίνονται προσπάθειες, δυστυχώς τις τελευταίες μέρες υπάρχει κλονισμός μέχρι και για το πόσο θα υφίσταται η Ευρωπαϊκή Ένωση, με τη Μεγάλη Βρετανία ήδη να βρίσκεται σε διαδικασίες αποχώρησης ως κράτος μέλος.

Επιπλέον, πολλές είναι και οι πολιτικές αλλαγές στην Ελλάδα. Προβλήματα εντοπίστηκαν κι ως προς την εσωτερική οργάνωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος που ο επί χρόνια επικεφαλής της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, Υποστράτηγος Μανώλης Σφακιανάκης, μετατέθηκε σε άλλο τμήμα του Αρχηγείου της ΕΛ.ΑΣ, κλονίζοντας ακόμα περισσότερο τη γνώμη του κοινού για το έργο της Διεύθυνσης, καθώς ήταν ο ίδιος που έστησε τη Δίωξη Ηλεκτρονικού Εγκλήματος και είχε σημειώσει σημαντικές επιτυχίες στο ενεργητικό του. Πραγματοποιήθηκαν κι άλλες μεταθέσεις προσωπικού καθιστώντας μάλλον πιο δύσκολη την τέλεση του έργου τους ως προς την εστίαση στην εξιχνίαση νέων επιθέσεων.

Με βάση έρευνα που διεξήγαγε η Στατιστική Υπηρεσία, η Ελλάδα κατατάσσεται στην 26η θέση μεταξύ των 28 κρατών μελών της Ε.Ε. του Δείκτη Ψηφιακής Οικονομίας και Κοινωνίας (DESI) για το 2016, συγκαταλέγοντάς τη στην ομάδα των χωρών που παρουσιάζουν υστέρηση. Όπως επισημαίνεται στη σχετική έκθεση, η Ελλάδα υστερεί από την πλευρά της ζήτησης, με χαμηλό επίπεδο ψηφιακών δεξιοτήτων, κι αυτό διότι μόλις το 63% του πληθυσμού είναι τακτικοί χρήστες του διαδικτύου, ενώ υπάρχει ένα 30% που δεν έχει χρησιμοποιήσει ποτέ το διαδίκτυο.

Υπαρκτό είναι και το έλλειμμα εμπιστοσύνης ως προς τις ηλεκτρονικές αγορές κι ηλεκτρονικές συναλλαγές κι είναι μόλις 37% το ποσοστό των Ελλήνων χρηστών του διαδικτύου που έχουν ανταλλάξει συμπληρωμένα έντυπα με τη δημόσια διοίκηση μέσω διαδικτύου.

Η ανάγκη για περισσότερη ενασχόληση με το θέμα των ηλεκτρονικών απατών πάντως έχει γίνει σαφής, και ότι θα πρέπει να δοθεί περισσότερη εστίαση σε αυτό το θέμα. Πιο συγκεκριμένα, έχει προκύψει από έρευνες ότι ο αριθμός των πτυχιούχων θετικών επιστημών, τεχνολογίας, μηχανικής και μαθηματικών (STEM) έχει αυξηθεί ελαφρά στην ΕΕ, αλλά οι μισοί σχεδόν Ευρωπαίοι, με ποσοστό 45% δε διαθέτουν βασικές ψηφιακές δεξιότητες, όπως για παράδειγμα είναι η αποστολή ηλεκτρονικών μηνυμάτων ή η εγκατάσταση νέων ηλεκτρονικών συσκευών. Υπάρχει πρόθεση από την Επιτροπή να αντιμετωπίσει αυτό το θέμα με τις ψηφιακές δεξιότητες και να επενδύσει περισσότερο στη σχετική κατάρτιση, στο πλαίσιο του προσεχούς προγράμματος δράσης για τις δεξιότητες στην ΕΕ.

Στην Ευρώπη, μόνο το 16% των μικρομεσαίων επιχειρήσεων πραγματοποιούν αγοραπωλησίες μέσω διαδικτύου καθιστώντας τις ηλεκτρονικές απάτες λιγότερες απ’ ότι

αν το ποσοστό των ΜΜΕ ήταν μεγαλύτερο. Αντίστοιχα, στην Ελλάδα δικαιολογείται με αυτόν τον τρόπο ο μικρός αριθμός των υποθέσεων.

Τέλος, αξίζει να επισημανθεί ότι ο αριθμός των Ευρωπαίων χρηστών του διαδικτύου που έρχονται σε επικοινωνία με τις αρχές ηλεκτρονικά, παραμένει σταθερός και ίσος με 32%. Συνεπώς, με όλες τις παραπάνω συνθήκες και τα γεγονότα που συμβαίνουν στην Ελλάδα, η φθίνουσα τάση πραγματοποίησης καταγγελιών στην Ηλεκτρονική Δίωξη, μέχρι και η μηδενική τάση δικαιολογούν τα εν προκειμένω αποτελέσματα της έρευνας.

Ελληνική Βιβλιογραφία

1 Αλευρομαγείρου, Σ., Ηλεκτρονικό εμπόριο και νομικά θέματα. ΑΤΕΙ Κρήτης, Πτυχιακή εργασία, 2007

2 Ανδρέου Πέτρος, Πέππα Ηλέκτρα, Παπακωνσταντίνου Κωνσταντίνα, "Ηλεκτρονικό Εμπόριο (e-commerce)", Πανεπιστήμιο Αιγαίου, 2002.

3 Ανδρουλάκη Ε., Κατασκευή ενός πληροφοριακού συστήματος για ηλεκτρονικό εμπόριο εταιρίας. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2009

4 Αποστόλου Κ., και Καρακατσάνη Α., Εμπιστοσύνη του ηλεκτρονικού καταστήματος στις ηλεκτρονικές συναλλαγές, ΑΤΕΙ Κρήτης, πτυχιακή εργασία, 2008

5 Βασιλείου Ε. Καζαντζάκη Ε., Recommendation systems. ΤΕΙ Μεσολογγίου Διπλωματική εργασία, 2006

6 Γιάννης Β. Σαμαράς, Γκιούρδας Μ., (μετάφραση) Efraim Turban, David King, Jae Kyu Lee, Michael Chung, Ηλεκτρονικό εμπόριο - Αθήνα, 2002. - σελ. 398

7 Διαμαντάκης Π., Η χρήση του διαδικτύου από τις επιχειρήσεις. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2011

8 Δουκίδης Γ- Θεμιστικλέους Μ- Δράκος Β- Παπαζαφιροπούλου Ν., Ηλεκτονικό Εμπόριο, Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 1998

9 Δουκίδης Γ. και Φραιδάκη Κ, Καταγραφή του Ηλεκτρονικύ Εμπορίου Β-C στην Ελλάδα: Αντιλήψεις και συμπεριφορά των online καταναλωτών, Εργαστήριο Ηλεκτρονικού Εμπορίου (ELTRUN), 2010

10 Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., (1998), σελ. 18 'Ηλεκτρονικό Εμπόριο,' Οικονομικό Πανεπιστήμιο Αθηνών

11 Θαλασσινός Ελευθέριος, Ανάλυση χρονολογικών σειρών: μεθοδολογία Box-Jenkins, Εκδόσεις Σταμούλης, 1991

12 Θαλασσινός Ελευθέριος, Υποδείγματα χρονολογικών σειρών: Θεωρία, εφαρμογές, Εκδόσεις Σταμούλης, 1986

13 Καλογέρα Ασημίνα, 'Στρατηγική και εφαρμογές e-banking' Πτυχιακή Εργασία ΤΕΙ Καβάλας, 2005

14 Κάτσικας Σωκράτης Κ., "Διαχείριση της Ασφάλειας Πληροφοριών", Εκδόσεις Πεδίο & Σωκράτης Κ.Κάτσικας, Αθήνα 2014, σελ. 45

15 Κρητικός Κ., Το ηλεκτρονικό εμπόριο ως εργαλείο ανάπτυξης των τραπεζικών εργασιών. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2008

16 Μαρκάκη Σ., B2B επιχειρείν. Η συμβολή του ηλεκτρονικού εμπορίου. ΑΤΕΙ Κρήτης, πτυχιακή εργασία, 2010

17 Μαυρίδης Ιωάννης, Ασφάλεια Πληροφοριών στο Διαδίκτυο, σελ. 208 ISBN: 978-960-603-193-9, Copyright © ΣΕΑΒ- ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ, 2015

18 Μπατσίνης Ν., Δέλιας Π., Τσαφαράκης Σ., Ηλεκτρονικό εμπόριο και εικονικές επιχειρήσεις. Εκδόσεις Πολυτεχνείου Κρήτης «Χανιά», 2006

19 Μπατσίνης Ν., Δέλιας Π., Τσαφαράκης Σ., Ηλεκτρονικό εμπόριο και εικονικές επιχειρήσεις. Εκδόσεις Πολυτεχνείου Κρήτης «Χανιά», 2006

20 Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.16)

21 Πάγκαλος Γ. και Μαυρίδης Ι., «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις: ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002, ISBN 906-516-018-8 (σελ.181)

22 Πασχόπουλος Α. & Σκάλτσας Π., Ηλεκτρονικό Εμπόριο: Ανάπτυξη & εφαρμογή επιχειρηματικής στρατηγικής και μάρκετινγκ στο διαδίκτυο, Εκδόσεις Κλειδάριθμος, Αθήνα 2001

23 Πασχοπουλος Α., Σκαλτσας Π., Ηλεκτρονικό Εμπόριο, εκδόσεις «Κλειδάριθμος» 2η έκδοση, 2000

24 Πάτσα, Χ., Αβαραμούδης, Β., Γκίκα, Σ., Πέτρου, Γ., (2005) ((Ηλεκτρονικό Επιχειρείν - Ηλεκτρονικό Εμπόριο>>, Equal Ανδρομέδα

25 Πολίτης Δ., Ηλεκτρονικές προμήθειες σχεδιασμός και εφαρμογή, Πανεπιστήμιο Πατρών, διπλωματική εργασία, 2011

26 Ρουμελιώτης Α., (2006), Ανάπτυξη πλατφόρμας ηλεκτρονικού εμπορίου. ΑΤΕΙ Ηρακλείου, πτυχιακή εργασία

27 Σαλτσογλίδης Α., Ανάπτυξη συστήματος ηλεκτρονικού εμπορίου, ΑΤΕΙ Κρήτης, Πτυχιακή εργασία, 2007

28 Συνανιώτη, Α., Φαρσαρώτας, Ι., «Ηλεκτρονική Τραπεζική», Αθήνα- Κομοτηνή: εκδόσεις Αντ. Σακούλας, 2004

29 Ταχαρίδου Βαρβάρα, Πανεπιστήμιο Μακεδονίας, Μεταπτυχιακό Πρόγραμμα στα Πληροφοριακά Συστήματα, 2004

30 Τσακαλίδης Α, Δρ Συρμακέσης Σ, Δρ.Τσώλης, Παν. Πατρών, Τμ Μηχ. Η/Υ e-εμπόριο e-επιχειρήν,
http://www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf

31 Φωτακοπούλου Δ., Ανάπτυξη Διαδικτυακής Εφαρμογής Ηλεκτρονικού Καταστήματος Παροχέα Ηλεκτρικής Ενέργειας. ΑΤΕΙ Κρήτης πτυχιακή εργασία, 2011

32 Χάλαρης Χρήστος, Οικονομία της κοινωνίας και της πληροφορίας , σελ. 14

Ξένη Βιβλιογραφία

1 Adams και Sasse, 1999; Albrechtsen και Hovden, 2009; Besnard και Arief, 2004; Furnell et al., 2007; Furnell et al.,2006

2 A. Kaponen, E-Commerce Electronic Payments, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2006

3 Akif Khan, «Bitcoin – payment method or fraud prevention tool?», Bitnet, Magazine: Computer Fraud & Security, p.16-19, 2015

4 Androulaki, E., Karame, G., Roeschlin, M., Scherer, T. and Capkun, S., "Evaluating user privacy in Bitcoin", 2012 available at: http://eprint.iarc.org/2012/596.pdf

5 Antoine Laronze Groine, Card Technology Today - Article, June 2009

6 Atwood J.W., Venkataiahgari A.K., Debbabi, M., Secure e-commerce transactions for multicast services. In IEEE International Conference on and Enterprise E-Commerce Technology, p. 18., 2006

7 Badra, M., Urien, P., Toward SSL integration in SIM smartcards. IEEE Wireless Communications and Networking Conference 2, 889–893, 2004

8 Barber, S., Boyen, X., Shi, E. and Uzun, E. , "Bitter to better – How to make bitcoin a better currency", 2012 available at: http://crypto.standford.edu/_xb/fc12/bitcoin.pdf

9 Barnes, S.J., Vidgen, R.T., "An integrative approach to the assessment of ecommerce quality", Journal o f Electronic Commerce Research, Vol.3, No.3, pp.114-127, 2003

10 Barry Scholnick, Nadia Massoud, Anthony Saunders, Santiago Carbo-Valverde, Francisco Rodrıguez-Fernandez, The economics of credit cards, debit cards and ATMs: A survey and some new evidence, Journal of Banking & Finance 32 (2008) 1468–1483

11 Baskerville, R. (1993), "Information systems security design methods: implications for information systems development", ACM Computing Surveys, Vol. 25 No. 4, pp. 375-414

12 Bella, G., Massacci, F., Paulson, L.C., Verifying the SET registration protocols. IEEE Journal on Selected Areas in Communications 21 (1), 77–87, 2003

13 Berlin, M., Mester, L.J., Credit card rates and consumer search. Review of Financial Economics 13, 179–198, 2004

14 Bicakci, K., Unal, D., Ascioglu, N., Adalier, O., Mobile authentication secure against man-in-the-middle attacks. Procedia Computer Science 34, 323–329 , 2014

15 Bisel, L.D., The role of SSL in cybersecurity. IT Professional 9 (2), 22–25, 2007

16 Bocij, Chaffey D., Greasley A. and Hichie S., Business Information Systems,Prentice Hall, 2006, 3rd Edition

17 BusinessWire, New VISA PayWave issuers and merchants sign up for faster, more

convenient payments, 2007

18 Chaudhary, A., Ahmad, K., Rizvi, M.A., E-commerce security through asymmetric key algorithm. International Conference Communication Systems and Network Technologies, 776–781, 2014

19 Choi, Soon-Yong, Stahl, Dale, Whinston, Andrew, "The economics of electronic commerce." Indianapolis: McMillan Technical Publishing, 1997

20 Christian Konradt, Andreas Schilling, Brigitte Werners , Phishing: An economic analysis of cybercrime perpetrators, computers & security 58 (2016) 39–46

21 Christin N, Egelman S, Vidas T, Grossklags J. It's all about the Benjamins: an empirical study on incentivizing users to ignore security advice. In: Danezis G, editor. Financial cryptography and data security SE e 2, vol. 7035. Berlin, Heidelberg: Springer; 2012

22 Colin Tankard, The security issues of the Internet of Things, Digital Pathways, Computer Fraud & Security, 2015

23 Condon, S., "Judge spares E-Gold directors jail time posted", 2013 available at: http://news.cnet.com/8301-13578_3-10104677-38.html

24 Cosima Rughinis & Razvan Rughinis, Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

25 Cottle, M., *The Government's Perilous Bitcoin Chase*, The Daily Beast, 2013

26 D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, in: Advances in Cryptology—CRYPTO'88, LNCS, vol. 403, Springer-Verlag, pp. 319–327, 1990

27 D. Chaum, B. den Boer, E. van Heyst, S. Mjolsnes, A. Steenbeek, Efficient offline electronic check, in: Advances in Eurocrypt'89, LNCS, vol. 434, Springer-Verlag, pp. 294–301, 1989

28 D. Chaum, Blind signatures for untraceable payments, in: Advances in Cryptology—CRYPTO'82, Plenum, New York, pp. 199–203, 1983

29 D. Shinder, Scene of the Cybercrime, Walthman, Syngress, New York, 2002

30 de Renesse, R., 2014. Research Forecast Report: Smartphone markets: worldwide trends, forecasts and strategies 2014–2018. http://www.analysysmason.com/smartphone-forecasts-2014

31 Du, L., Hu, X., Li, Y., Zhao, G., A CSK based SSL handshake protocol. IEEE International Conference on Network Infrastructure and Digital Content, 600–603 , 2009

32 Efraim Turban, Jae Lee, David King, Michael Chung, Ηλεκτρονικό εμπόριο: Αρχές, Εξελίξεις, Στρατηγική από τη σκοπιά του manager, Έκδοση Μ. Γκιούρδας, Αθήνα 2002

33 Eldridge, A., Is NFC the future of safe credit card processing? Business 2 Community, 2014

34 Elis, N., Monday, May 12, 2014. Can big data predict the next cyber attack? Jerusalem Post.

http://www.jpost.com/Enviro-Tech/Can-big-data-predict-the-next-cyber-attack-351957

35 Fagen Li, Mingwu Zhang, Tsuyoshi Takagi, Identity-based partially blind signature in the standard model for electronic cash - Mathematical and Computer Modelling 58 (2013) 196–203, 2012 Elsevier Ltd.

36 Fang-Yie Leu, Yi-Li Huang, Sheng-Mao Wang, A Secure M-Commerce System based on credit card transaction - Electronic Commerce Research and Applications 14 (2015) 351–360, Elsevier

37 FBI Directorate of Intelligence, Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Unlawful Activity, Wired Magazine, 2012

38 Fried, I., 2002. A building blessed with tech success, Plotkin, H., 1999. Beam me up some cash. HalPlotkin.com

39 Gary DeWaal Guy Dempsey , "New York BitLicense regulations virtually certain to significantly impact transactions in virtual currencies", Journal of Investment Compliance, Vol. 16 Iss 4 pp. 59 – 65, 2015 http://dx.doi.org/10.1108/JOIC-08-2015-0047

40 Gary DeWaal Guy Dempsey , (2015),"New York BitLicense regulations virtually certain to significantly impact transactions in virtual currencies", Journal of Investment Compliance, Vol. 16 Iss 4 pp. 59 - 65
http://dx.doi.org/10.1108/JOIC-08-2015-0047

41 Giorgio Merlonghi, "Fighting financial crime in the age of electronic money: opportunities and limitations", Journal of Money Laundering Control, Vol. 13 Iss 3 pp. 202 – 214, 2010 Permanent link to this document: http://dx.doi.org/10.1108/13685201011057118

42 Gold, S., 2014. The evolution of payment card fraud. Computer Fraud and Security (3), 12–17, 2014

43 Graebner, C., Ten days in Kenya with no cash, only a phone. Bloomberg Businessweek, 2014

44 Greenberg, A., Founder of Drug Site Silk Road Says Boom and Bust won't Kill His Black Market, Forbes, 2013, available at:
www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/

45 Guan, H.J., The research of SET-based electronic payment system model, International Conference on E-Business and Information System Security, 1–4 , 2009

46 Heggestuen, J., Alipay overtakes PayPal as the largest mobile payments platform in the world. Business Insider, 2014

47 Herley C. So long, and no thanks for the externalities. In: Proceedings of the 2009 workshop on new security paradigms workshop e NSPW '09. New York, New York, USA: ACM Press; 2009.

48 Hossein, Electronic commerce: principles and practice, Academic Press, 2002

49 Inglesant PG, Sasse MA. The true cost of unusable password policies. In: Proceedings of the 28th international conference on Human factors in computing systems e CHI ’10. New York, Press; 2010.

50 International Conference on Communication, Management and Information Technology (ICCMIT 2015)

51 J.-H. Yang, P.-Y. Lin, A mobile payment mechanism with anonymity for cloud computing, The Journal of Systems and Software (2015), http://dx.doi.org/10.1016/j.jss.2015.07.023

52 Java Card Platform Specification: Classic Edition; Application Programming Interface, Runtime Environment Specification, Virtual Machine Specification, Connected Edition; Runtime Environment Specification, Java Servlet Specification, Application Programming Interface, Virtual Machine Specification, Sample Structure of Application Modules, May 2009. URL: http://java.sun.com/javacard/3.0.1/specs.jsp.

53 Jeffrey Simser , "Bitcoin and modern alchemy: in code we trust", Journal of Financial Crime, Vol. 22 Iss 2 pp. 156 – 169, 2015 Permanent link to this document: http://dx.doi.org/10.1108/JFC-11-2013-0067

54 Jesdanun A., Apple Pay, Google Wallet, PayPal: pros and cons of mobile payment system, 2014

55 Jun Liu, Robert J. Kauffman, Dan Ma, Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem, Electronic Commerce Research and Applications 14 (2015) 372–391

56 K. Mayes, K. Markantonakis (Eds.), Smart Cards, Tokens, Security and Applications, Springer, 2008.

57 K.W. Müller, M. Dreier, M.E. Beutel, E. Duven, S. Giralt, K.Wolfling, A hidden type of internet addiction? Intense and addictive use of social networking sites in adolescents, Computers in Human Behavior 55, 172e177, Elsevier Ltd., 2016

58 Kalakota Ravi-Whinston B. Andrew, “Electronic Commerce: A Manager’s Guide”, Addison-Wesley 1997

59 Karl de Leeuw and Jan Bergstra, The History of Information Security: A Comprehensive Handbook 2007 Elsevier B.V., http://www.cybercrimes.net

60 Katten Muchin Rosenman LLP, “Bitcoin: Current US Regulatory Developments,” November 26, 2013

61 Katten Muchin Rosenman LLP,“Bitcoin: Current US Regulatory Developments,”, 2013

62 Krugman, P., “The antisocial network”, New York Times, 14 April, 2013

63 Kunz, M., & Wilson, P. Computer crime and computer frauds (pp. 13–22). University of Maryland, Department of Criminology and Criminal Justice, Report to the Montgomery

County Criminal Justice Coordinating Commission, 2004

64 Lee T., “Four reasons you shouldn’t buy bitcoins forbes”, 2013 available at: www.forbes.com

65 Li, Y., The design of the secure electronic payment system based on the SET protocol. International Conference on Computer Science and Information Technology, 29–33 , 2008

66 Lillington, K., 1999. PayPal puts dough in your palm. Wired.com, Reuters, 2002. PayPal execs enjoy deja woo-hoo. Wired.com

67 Lon-Mu Liu, Gregory B. Hudak in collaboration with George E. P. Box, Mervin E. Muller , George C. Tiao, FORECASTING AND TIME SERIES ANALYSIS USING THE SCA STATISTICAL SYSTEM Copyright Scientific Computing Associates Corp., 1992-1994, Chicago, Illinois 60607-3528 U.S.A.

68 Lu, S., Smolka, S.A., Model checking the secure electronic transaction (SET) protocol. In 7th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 358–364, 1999

69 M. Abe, E. Fujisaki, Howto date blind signatures, in: Advances in Cryptology—ASIACRYPT 1996, in: LNCS, vol. 1163, Springer-Verlag, 1996, pp 244–251

70 M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, S. Entwise, B. Graveland, D.McKinney, J. Mulcahy, C. Wueest, In: Symantec Global Internet Security Threat Report. Trends for 2009. Technical Report, Symantec Corporation, Cupertino, 2010.

71 Mahmoudi, N., Duman, E., Detecting credit card fraud by modified fisher discriminant analysis. Expert Systems with Applications 42 (5), 2510–2516, 2015

72 Manyika, J; Chui, M; Bisson, P; Woetzel, J; Dobbs, R; Bughin, J; Aharon, D. ‘Unlocking the potential
of the Internet of Things’. McKinsey Global Institute, June 2015
http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

73 Miers, I., Garman, C., Green, M. and Rubin, A., Zerocoin: Anonymous Distributed E-Cash from Bitcoin, IEEE Symposium on Security and Privacy, 2013 http://zerocoin.org/

74 Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi - “Cybercrime, Digital Forensics and Jurisdiction”, p.20 - Studies in Computational Intelligence 593, Springer 2015

75 Montgomery, K.C., Testimony on developing the framework for safe and efficient mobile payments. U.S. Senate Hearing, Washington, DC, 2012

76 Moyer, J.D., Hughes, B.B., ICTs: do they contribute to increased carbon emissions? Technol.

Forecast. Soc. Chang. 79, 919–931, 2012

77 Murck, P., “Bitcoin a webinar”, in Association of Financial Crime Specialists, Murck is general counsel to the Bitcoin Foundation, 2013

78 N. Kolokotronis C. Margaritis P. Papadopoulou P. Kanellis D. Martakos, "An integrated approach for securing electronic transactions over the Web", Benchmarking: An International Journal, 2002, Vol. 9 Iss 2 pp. 166 – 181- Permanent link to this document: http://dx.doi.org/10.1108/14635770210421836

79 N. Kolokotronis C. Margaritis P. Papadopoulou P. Kanellis D. Martakos, "An integrated approach for securing electronic transactions over the Web", Benchmarking: An International Journal, 2002, Vol. 9 Iss 2 pp. 166- 181 Permanent link to this document: http://dx.doi.org/10.1108/14635770210421836

80 Nabi, F., Secure business application logic for e-commerce systems - Computers and Security 24 (3), 208–217, 2005

81 Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2009 available at: http://bitcoin.org/bitcoin.pdf

82 New York State Department of Financial Services New York Codes, Rules, and Regulations. Part 200, Virtual Currencies, June 3, 2015

83 Norazah Mohd, S., Students’ demand for smartphones. Campus-Wide Inform. Syst. 30 (4), 236–248, 2013

84 O’Brien, M., Op Cit note 11, The US Attorneys Office, Southern District of NewYork, Indictments and Supporting Materials in US v. Liberty Reserve S.A. et al filed, 2013 and available at www.justice.gov/usao/nys/pressreleases/may13/libertyreserveetaldocuments.php

85 Odlyzko A. Economics, psychology, and sociology of security. In: Wright R, editor. Financial Cryptography Berlin, Heidelberg: Springer; 2003.

86 Online Retailing: Britain, Europe, US and Canada 2015’. Centre for Retail Research. www.retailresearch.org/onlineretailing.php

87 Oppliger, R., Hauser, R., Basin, D., SSL/TLS session-aware user authentication revisited. Computers and Security 27 (3–4), 64–70, 2008

88 Patricio E. Ramirez-Correa, F. Javier Rondan-Cataluna, Jorge Arenas-Gaitan, Elsevier, 2015

89 Paul Hunton, Data attack of the cybercriminal: Investigating the digital currency of cybercrime, Computer law & security review 28 (2012) 201e207

90 Petridou, S., Basagiannis, S., Towards energy consumption evaluation of the SSL handshake protocol in mobile communications. Annual Conference on Wireless On-demand Network

Systems and Services, 135–138, 2012

91 R.N. Akram, K. Markantonakis, Smart cards: State-of-the-art to future directions, invited paper, in: C. Douligeris, D. Serpanos (Eds.), IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2013, IEEE Computer Science, Athens, Greece, 2013

92 Racz, N., Panitz, J., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (grc) status quo and software use: Results from a survey among large enterprises. Governance 1,1-2010.

93 Rafał Leszczyna, Cost assessment of computer security activities, Computer Fraud & Security, July 2013

94 Raja Naeem Akram, Konstantinos Markantonakis, Damien Sauveron, Recovering from a lost digital wallet: A smart cards perspective extended abstract - http://dx.doi.org/10.1016/j.pmcj.2015.06.018 1574-1192/© 2015 Published by Elsevier B.V.

95 Rolf H. Weber, Internet of things: Privacy issues revisited, computer law & security review 31, 618–627, Published by Elsevier Ltd, 2015

96 Securities and Exchange Commission *SEC Charges Texas Man with Running Bitcoin Denominated Ponzi Scheme,* Washington: SEC, 2013

97 Serra Inci Celebi, How do motives affect attitudes and behaviors toward internet advertising and Facebook advertising?, Computers in Human Behavior 51 (2015) 312–324, Elsevier Ltd.

98 Shahiduzzaman, M., Alam, K., Information technology and its changing roles to economic growth and productivity in Australia. Telecommun. 38 (2), 125–135, 2014

99 Shedid, S.M., Kouta, M., Modified SET protocol for mobile payment: an empirical analysis. In International Conference on Software Technology and Engineering, vol. 1, V1-350–V1-355 , 2010

100 Sherif, M.H., Serhrouchni, A., Gaid, A.Y., Farazmandnia, F., SET and SSL: electronic payments on the Internet. IEEE Symposium on Computers and Communications, 353–358, 1998

101 Simser, J. , “Recovering the stolen sweets of fraud and corruption”, Working Paper Observatario de Economica a Gestao de Fraud, University of Porto, 2013

102 Simser, J., “Recovering the stolen sweets of fraud and corruption”, Working Paper Observatario de Economica a Gestao de Fraud, University of Porto, 2013

103 Soudabeh Vahdati & Niloofar Yasini, Factors affecting internet frauds in private sector: A

case study in Cyberspace Surveillance and Scam Monitoring Agency of Iran, Computers in Human Behavior 51, 180–187, Elsevier Ltd., 2015

104 Stevens, S., PayPass and PayWave pave the way for Apple Pay on your smartphone, 2014

105 Turban, Efraim, Ephraim McLean and James Wetherbe. Information Technology for Management: Transforming Organizations in the Digital Economy. New York: Wiley & Sons, 2004.

106 Wallace, B. (2011), "The rise and fall of bitcoin wired magazine", available at: www.wired.com/magazine/2011/11/mf_bitcoin/

107 Wang, S. Y. K., & Wilson, H., The evolutional view of the types of identity thefts and online frauds in the era of the internet. Internet Journal of Criminology, 12 (ISSN 2045–6743), 2011

108 Wash R. Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security e SOUPS '10. NY: ACM Press; 2010.

109 Wei, W., Li, J., Cao, L., Ou, Y., Chen, J., Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web 16 (4), 449–475, 2013

110 Wei-Kuei Chen, Efficient on-line electronic checks, Appl. Math. Comput. 162/ 1259–1263, 2005

111 Weirich D, Sasse MA. Pretty good persuasion. In: Proceedings of the 2001 workshop on New security paradigms e NSPW '01, 2001.

112 Wilhelm A., Putting Square's $5B valuation into context. TechCrunch, 2014

113 Yong, X., Jindi, L., Electronic payment system design based on SET and TTP, International Conference on E-Business and E-Government, 275–278, 2010

114 Zhao H., Liu R., A scheme to improve security of SSL. In Pacific-Asia Conference on Circuits, Communications and Systems, 401–404 , 2009

Ηλεκτρονικές Πηγές

1. www.FocusBari.gr
2. www.cybersource.com/en-EMEA/products/fraud_management/ukfraudreport2013/
3. Cyber and Technology Enables Crimes (2013). Retrieved from https://www.crimecommission.gov.au/sites/default/files/CYBER%20AND%20TECHNOLOGY%20ENABLED%20CRIME%20JULY%202013.pdf
4. Digital Consumers Are Frustrated: TrustInsight Study Reveals 17% of Online Shoppers Have Experienced Credit Card Declines'. 41st Parameter. www.the41.com/buzz/announcements/digital-consumers-are-frustratedtrustinsight-study-reveals-17-percentonline
5. Focus Bari, ELTRUN-Ηλεκτρονικό Εμπόριο B2C στην Ελλάδα, Ιούνιος 2009, http://www.focus.gr/default.asp?id=200050049&lcid=1032
6. http://bit.ly/1PHF0Gu
7. http://bitcoinx.gr/%CE%BC%CF%80%CE%BF%CF%81%CE%B5%CE%AF-bitcoin-%CE%B2%CE%BF%CE%B7%CE%B8%CE%AE%CF%83%CE%B5%CE%B9-%CE%B5%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1-%CE%B5%CE%BA%CF%84%CF%8C%CF%82-%CE%BA%CF%81%CE%AF%CF%83%CE%B7%CF%82/
8. http://bitcoinx.gr/bitcoin-%CE%BA%CE%B1%CE%B9-%CF%85%CF%80%CE%BF%CE%B4%CE%B9%CE%B1%CE%B9%CF%81%CE%AD%CF%83%CE%B5%CE%B9%CF%82/
9. http://bitcoinx.gr/bitstamp-%CE%B1%CE%B3%CE%BF%CF%81%CE%AC-bitcoin-%CE%BC%CE%B5-%CE%BA%CE%AC%CF%81%CF%84%CE%B5%CF%82/
10. http://dx.doi.org/10.1016/j.clsr.2013.01.009
11. http://dx.doi.org/10.1108/14635770210421836
12. http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf
13. http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf
14. http://eos.uom.gr/~mavla/emabo/content/18/papers/18_3.pdf
15. http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_el.htm#goto_2
16. http://nemis.cti.gr/ebusiness/distance_course.htm
17. http://safeharbor.export.gov/list.aspx
18. http://thalis.cs.unipi.gr/dpolemi/e-commerce/index.htm
19. http://tvxs.gr/news/kosmos/oi-anonymous-kiryksan-ton-diadiktyako-polemo-sto-islamiko-kratos
20. http://wdvl.com/internet/history
21. http://www.aegean.gr/culturaltec/dgavalas/ECommerce/slides/E-C_2005_04.pdf
22. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=53816&Itemid=0&lang=&lang=#4
23. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=53864&Itemid=378&lang=

24. http://www.bitcoingreece.gr/ : Οδηγίες εγκατάστασης Bitcoin
25. http://www.bsigroup.com/en-GB/iso-27001-information-security/
26. http://www.coinfox.info/news/4420-lyra-network-makes-bitcoin-available-to-35-000-french-and-global-merchants
27. http://www.creditcards.com/
28. http://www.export.gov/safeharbor/
29. http://www.iacp.org/
30. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
31. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on&includesc=true
32. http://www.microsoft.com/online/legal/v2/el-gr/MOS_PTC_Security_Audit.htm
33. http://www.microsoft.com/online/legal/v2/el-gr/MOS_PTC_Security_Audit.htm
34. http://www.sas.com/el_gr/insights/big-data/internet-of-things.html
35. http://www.sepe.gr/gr/research-studies/article/341165/xrisimo-epixeirimatiko-ergaleio-oi-ilektronikes-agores-symfwna-me-to-ergastirio-ilektronikoy-epixeir/
36. http://www.skai.gr/news/technology/article/310263/poso-megalo-einai-telika-to-internet/
37. http://www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf
38. http://www.vnikolopoulos.com/?p=194
39. http://www.welivesecurity.com/2016/04/06/buying-ray-bans-dont-fall-for-this-facebook-scam/
40. https://bitcoin.org/el/faq : Απορίες για το Bitcoin
41. https://blockchain.info/charts
42. https://books.google.gr/books?hl=en&lr=&id=EOjG84UvrHMC&oi=fnd&pg=PR13&dq=E-commerce+definition&ots=X8EKb7TFwq&sig=TP9tNQEHwnLLk50rRkj8wHGkPbU&redir_esc=y#v=onepage&q=E-commerce%20definition&f=false
43. https://www.cryptocoinsnews.com/bitstamp-adds-bitcoin-purchase-via-credit-card-in-germany-and-italy/
44. https://www.facebook.com/help/messenger-app/750020781733477/
45. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
46. https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network
47. https://www.vogogo.com/
48. Multos: The Multos Specification, Online. URL: http://www.multos.com/
49. Number of Transactions Per Day'. https://blockchain.info/charts/ntransactions
50. www.bitcoinfoundation.org
51. www.Coinmarketcap.com
52. www.cybercc.gr
53. www.elsevier.com/locate/cose
54. www.sepe.gr
55. www.tex.unipi.gr/undergraduate/notes/efarmoges_comp/kef6.pdf
56. www.torproject.org

57. www.worldwidewebsize.com
58. ‘LexisNexis True Cost of Fraud Study Says Merchants Are Incurring a $279 Loss For Every $100 of Fraud Losses’. LexisNexis, 2013. www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1379105834100604
59. http://dx.doi.org/10.1109/FiCloud.2014.39
60. http://www.iefimerida.gr/news/253125/i-ellada-proteleytaia-stin-ee-ston-deikti-psifiakis-oikonomias-kai-koinonias-2016#ixzz4CzZ4uO3T
61. http://www.statistics.gr/greeceinfigures?p_p_id=3&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_3_struts_action=%2Fsearch%2Fsearch&_3_redirect=%2Fgreece-in-figures&_3_keywords=%CF%87%CF%81%CE%AE%CF%83%CE%B7+%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85&_3_groupId=0
62. http://www.iefimerida.gr/news/253125/i-ellada-proteleytaia-stin-ee-ston-deikti-psifiakis-oikonomias-kai-koinonias-2016

Παράρτημα 1: Έκθεση του εγκλήματος στον κυβερνοχώρο και μέτρα ασφάλειας που λαμβάνουν οι τελικοί χρήστες στην Ευρωπαϊκή Ένωση

Σε μια έρευνα χρησιμοποιήθηκαν τα στοιχεία έρευνας μεγάλης κλίμακας από το Ευρωβαρόμετρο 77.2 / 2012 για να εξερευνηθεί η μεταβλητότητα σε δραστηριότητα απευθείας σύνδεσης, η έκθεση του εγκλήματος στον κυβερνοχώρο και τα μέτρα ασφαλείας των τελικών χρηστών στην Ευρωπαϊκή Ένωση (ΕΕ-27). Ενώ η ασφάλεια στον κυβερνοχώρο είναι μια υψηλής προτεραιότητας δραστηριότητα για τους εμπειρογνώμονες της ασφάλειας και τους ερευνητές, οι τελικοί χρήστες την διεξάγουν στο πλαίσιο της καθημερινής ζωής τους ως δραστηριότητα κοινωνικά υπόλογη και με περιορισμένους πόρους. Υποστηρίζεται ότι η συμπεριφορά περί ασφάλειας των τελικών χρηστών θα πρέπει να είναι σχετική με την εμπειρία τους ως θύματα κατά την καθημερινή τους τριβή με το διαδίκτυο. Μια οικολογική ανάλυση σε επίπεδο χωρών έδειξε ότι οι κοινωνίες με διαδεδομένη τη χρήση του Διαδικτύου έχουν Ανώτερη υποστήριξη ασφάλειας στον κυβερνοχώρο.

Δεδομένης της αρνητικής ανάδρασης βρόχου μεταξύ των απαντήσεων ασφαλείας που προέκυψε στη συγκεκριμένη έρευνα, η έκθεση εγκλήματος στον κυβερνοχώρο, καθώς και σε online δραστηριότητες, όσον αφορά σε ατομικό επίπεδο, καθιστά τη μοντελοποίηση γραμμικής συσχέτισης για στοιχεία της έρευνας ανέφικτη, και προτείνεται μια ανάλυση κατάταξης ως εργαλείο για την καλύτερη σύλληψη της μεταβλητότητας. Χρησιμοποιείται η ανάλυση Κ-μέσων συστάδων για το προσδιορισμό πέντε ειδών τελικών χρηστών στο θέμα της ασφάλειας των δραστηριοτήτων του έργου. Τα πέντε αυτά είδη είναι: «εξερευνητής», «αντιδραστικός», «συνετός», «τυχερός» και «περιστασιακός» χρήστης και γίνεται συζήτηση των προφίλ αυτών σε online δραστηριότητες και εμπειρίες.

Οι «συνετοί» χρήστες είναι σχετικά μη γνώστες για τις δημόσιες εκστρατείες που διοργανώνονται ως προς την ασφάλεια τους στο διαδίκτυο. Η ανάλυση κατάταξης είναι ένα παραγωγικό εργαλείο για την κατανόηση του προσανατολισμού των τελικών χρηστών ως προς το θέμα της ασφάλειας.

Υφίστανται τρεις κύριες απεικονίσεις τελικών χρηστών, που αντιπροσωπεύουν μια φαινομενικά παράλογη συμπεριφορά ως προς τους κανόνες περί ασφάλειας. Υπάρχουν οι «γνωστικά τεμπέληδες» χρήστες, που λειτουργούν με έναν οριοθετημένο ορθολογισμό που υπερεκτιμούν την παροντική άνεση/ ασφάλεια εις βάρος της προστασίας από μελλοντικούς κινδύνους. Επίσης, υπάρχουν οι «οικονομικά ορθολογικοί» χρήστες που ισοκαταλογίζουν τα δικά τους έξοδα με τα πλεονεκτήματα που παρέχουν σύμβουλοι ασφαλείας και

λαμβάνουν αποφάσεις σχετικά με τις συμβουλές των ειδικών για συμμόρφωση ως προς κάποιο επίπεδο ασφάλειας. Τέλος, υπάρχει και η κατηγορία χρηστών που χαρακτηρίζονται ως «κοινωνικοί» οι οποίοι είναι εναρμονισμένοι με την κοινωνική οργάνωση της δραστηριότητάς τους, στην οποία οι απαιτήσεις ασφάλειας αποτελούν μόλις ένα μικρό μέρος ενός ευρούς τοπίου των κοινωνικών κανόνων της εμπιστοσύνης και του συντονισμού που προσδιορίζουν τη δράση τους.

Και τα τρία μοντέλα εξερευνούν την αποστροφή από τον κίνδυνο καθώς και την αναζήτηση κινδύνου, αλλά προτείνουν διαφορετικούς περιορισμούς σχετικά με τη δραστηριότητα των χρηστών, δηλαδή (α) την αποφυγή υπερφορτωμένων ενημερώσεων, (β) την προτίμηση για οικονομική βελτιστοποίηση, και (γ) την άσκηση κοινωνικής ένταξης, αντίστοιχα. Ένα βασικό θέμα για την περιγραφή συμπεριφορών ασφαλείας των τελικών χρηστών αναφέρεται στην επίγνωση των κινδύνων (βλ. συνοπτική σύγκριση του πίνακα 1).

Πίνακας – Τα τρία θεωρητικά μοντέλα των τελικών χρηστών ως προς την ασφάλεια

	Γνωστικά τεμπέληδες χρήστες	**Οικονομικά ορθολογικοί χρήστες**	**Κοινωνικοί χρήστες**
Εστίαση στην απεικόνιση	Τεχνική αφέλεια λόγω πολλαπλών στόχων	Οικονομική ορθολογικότητα στο πλαίσιο της δραστηριότητας ενός ατόμου	Ανησυχίες αυτο-παρουσίασης; αξιόπιστοι φορείς κατά την άσκηση συντονισμένων δραστηριοτήτων
Επίγνωση κινδύνου των χρηστών	Όχι ιδιαίτερη ενημέρωση, οι κίνδυνοι είναι υποτιμημένοι	Η ενημέρωση είναι επαρκής, αντανακλώντας εκτιμώμενους προσωπικούς κινδύνους	Οι σχετικοί κίνδυνοι κοινωνικά είναι γνωστοί, μέσω της επικοινωνίας που δίνει νόημα στις προσωπικές εμπειρίες
Ορθολογικότητα	Περιορισμένη	Οικονομική, βασισμένη στην ανάλυση κόστους-οφέλους	Ο ορθολογισμός εμφανίζεται ως υποπροϊόν λογιστικών δραστηριοτήτων χρησιμοποιώντας λεξιλόγια που έχουν κατασκευαστεί

			κοινωνικά
Θεμελιώδες κίνητρο για την ενέργεια	Ικανοποίηση στόχων καταβάλλοντας ελάχιστη προσπάθεια	Βελτιστοποιώντας την άσκηση των προτιμήσεων	Επίτευξη θεμιτών στόχων και διατήρηση επιθυμητής ταυτότητας σε τοπική επίπεδο
Λόγοι για μικρή συμμόρφωση	Μικρή κατανόηση των κινδύνων και ελάχιστη τεχνική επίγνωση	Οι μέσες απώλειες του τελικού χρήστη από το έγκλημα στον κυβερνοχώρο είναι λίγες - το κόστος της ασφάλειας είναι υψηλό – Οι μελλοντικός δαπάνες και τα οφέλη είναι μειωμένες	Οι πρακτικές ασφαλείας είναι οι εξής: - Εμπόδια για ομαλή κοινωνική οργάνωση - Συνδέονται με μη αξιόλογες ταυτότητες

Πηγή: Cosima Rughinis & Razvan Rughinis, Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

Από τη σκοπιά των τεμπέληδων χρηστών η ευαισθητοποίηση για επίγνωση είναι κυρίως μια λειτουργία της κατανόησης απ' την πλευρά των χρηστών των επιγραμμικών τεχνολογιών και των κινδύνων και, αμοιβαίως η προσβασιμότητα σε λύσεις για θέματα ασφάλειας[208]. Αυτοί οι τελικοί χρήστες συνήθως απεικονίζονται τεχνικά ως αφελείς και είναι ευάλωτοι επειδή πρέπει να διαθέσουν γνωστικούς πόρους σε πολλαπλές, δύσκολες εργασίες που ουσιαστικά δεν κατέχουν.

Από τη σκοπιά των οικονομικά ορθολογικών χρηστών[209], η ευαισθητοποίηση αποτελεί κυρίως συνάρτηση της εμπειρίας από προσωπική απώλεια εξαιτίας της εγκληματικότητας στον κυβερνοχώρο, καθώς και των γενικών πληροφοριών που λαμβάνουν για παρόμοιες ζημίες που βιώνουν άλλοι. Η απώλεια εξαρτάται από την δραστηριότητα: διάφορα είδη των online δραστηριοτήτων μπορεί να επιβαρύνονται με

[208] Adams και Sasse, 1999; Albrechtsen και Hovden, 2009; Besnard και Arief, 2004; Furnell et al., 2007; Furnell et al.,2006

[209] Christin N, Egelman S, Vidas T, Grossklags J. It's all about the Benjamins: an empirical study on incentivizing users to ignore security advice. In: Danezis G, editor. Financial cryptography and data security SE e 2, vol. 7035. Berlin, Heidelberg: Springer; 2012.; Herley C. So long, and no thanks for the externalities. In: Proceedings of the 2009 workshop on new security paradigms workshop e NSPW '09. New York, New York, USA: ACM Press; 2009.

διαφορετικά είδη ζημιών. Επίσης, η συχνότητα της έκθεσης σε απευθείας σύνδεση αυξάνει τη συχνότητα των πραγματικών ζημιών που πραγματοποιούν το ρίσκο. Μια σημαντική παρατήρηση εδώ είναι ότι οι απώλειες είναι κατανεμημένες μεταξύ των διαφόρων συμμετεχόντων σε μια ρύθμιση του εγκλήματος στον κυβερνοχώρο, μέσα από διάφορες κοινωνικές ρυθμίσεις. Για παράδειγμα, στην περίπτωση χακαρισμένων τραπεζικών λογαριασμών, οι ζημίες επιβαρύνουν τόσο την τράπεζα όσο και τους τελικούς χρήστες και κατά συνέπεια, οι τελικοί χρήστες είναι συχνά προστατευμένοι από τους κινδύνους της εγκληματικότητας στον κυβερνοχώρο από ρυθμίσεις που μεταφέρουν τις χρηματοπιστωτικές απώλειες σε εταιρικούς φορείς. Επιπλέον, τα μέτρα ασφάλειας έχουν μη αμελητέα έξοδα[210]. Οι χρήστες απεικονίζονται ως οικονομικά ορθολογικοί φορείς οι οποίοι εκτιμούν τους κινδύνους και το κόστος της προστασίας με βάση τις δικές τους εμπειρίες και άλλων σχετικών και προσαρμόζουν τη συμπεριφορά τους για να ακολουθήσουν επαρκώς την δραστηριότητα ασφάλειας όπως την καταλαβαίνουν.

Από την σκοπιά των κοινωνικών χρηστών[211], η ευαισθητοποίηση δημιουργείται μέσα από προσωπικές εμπειρίες, και αυτές των άλλων, που ερμηνεύονται κοινωνικά[212] μέσω κοινών «λαϊκών μοντέλων». Επιπλέον, οι χρήστες δεν συμπεριφέρονται σύμφωνα με τυπικούς κανόνες και διαδικασίες, αλλά οι πράξεις τους είναι άκρως συμφραζόμενες πράγμα το οποίο αποτελεί και καλό αλλά και κακό νέο για τους σχεδιαστές των συστημάτων ασφαλείας, δεδομένου ότι οι κανόνες δεν ακολουθούνται, αλλά παράλληλα το πλαίσιο των τυπικών κανόνων παρέχει συχνά πολύτιμες πληροφορίες[213]. Οι κοινωνικοί χρήστες είναι υπόλογοι για τις πράξεις τους είτε λαμβάνοντας μέτρα ασφαλείας είτε όχι, σε ένα δεδομένο πλαίσιο, και σε μια δεδομένη κατάσταση κοινωνικής αλληλεπίδρασης. Οι εκτιμήσεις της κοινωνικής οργάνωσης της απώλειας είναι επίσης σημαντικές, καθώς και ζητήματα που αφορούν την κοινωνική οργάνωση της ευθύνης: οι χρήστες μπορεί να μην ευθύνονται πάντα για τις αποτυχίες της ασφάλειας, η οποία ευθύνη θα μπορούσε να αποδοθεί ουσιαστικά στην οργάνωση ως σύνολο, στον ίδιο τον εξοπλισμό, στην ειδική ταυτότητα και γνώση των επιτιθέμενων. Οι χρήστες απεικονίζονται ως έμπιστοι κοινωνικοί φορείς και ειδικευμένα στελέχη αυτο-παρουσίασης.

[210] Inglesant PG, Sasse MA. The true cost of unusable password policies. In: Proceedings of the 28th international conference on Human factors in computing systems e CHI ’10. New York, Press; 2010.
[211] Weirich D, Sasse MA. Pretty good persuasion. In: Proceedings of the 2001 workshop on New security paradigms e NSPW ’01, 2001.
[212] Wash R. Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security e SOUPS ’10. NY: ACM Press; 2010.
[213] Odlyzko A. Economics, psychology, and sociology of security. In: Wright R, editor. Financial Cryptography Berlin, Heidelberg: Springer; 2003.

Ακολουθεί παρουσίαση των αποτελεσμάτων της έρευνας αυτής που διεξήχθη σε 27 κράτη μέλη της Ε.Ε., αρχής γενομένης από το επίπεδο μεταβλητότητας της χώρας και στη συνέχεια φανερώνονται τα κοινωνικο-δημογραφικά στρώματα.

Μεταβλητότητα σε επίπεδο χώρας

Το πρώτο επίπεδο εξερεύνησης αφορά την περιγραφική ανάλυση της μεταβλητότητας της χώρας σε ατομικές εμπειρίες του κυβερνοεγκλήματος και συμπεριφοράς ασφάλειας, σε σχέση με τη χρήση του Διαδικτύου. Η χρήση του Διαδικτύου μετριέται ως ποσοστό των ερωτηθέντων που δηλώνουν ότι χρησιμοποιούν το Διαδίκτυο μια φορά την ημέρα ή αρκετές φορές την ημέρα. Οι εμπειρίες της εγκληματικότητας στον κυβερνοχώρο μετρώνται, για κάθε έναν μεμονωμένα, ως η καταμέτρηση των καταστάσεων όπου αυτός ή αυτή έχει αντιμετωπίσει αυτό το φαινόμενο, όπως:

- ✓ Η κλοπή ταυτότητας (κάποιος κλέβει τα προσωπικά δεδομένα και κάνει απομίμηση ταυτότητας).
- ✓ Λήψη emails που ζητούν με δόλο χρήματα ή προσωπικά στοιχεία.
- ✓ Online απάτες όπου τα αγαθά που αγοράζονται δεν παραδόθηκαν, ήταν πλαστά ή δεν αφορούσαν τίποτα σχετικό με το διαφημιζόμενο προϊόν.
- ✓ Δεν είναι σε θέση να έχουν πρόσβαση σε online υπηρεσίες λόγω των επιθέσεων στον κυβερνοχώρο.

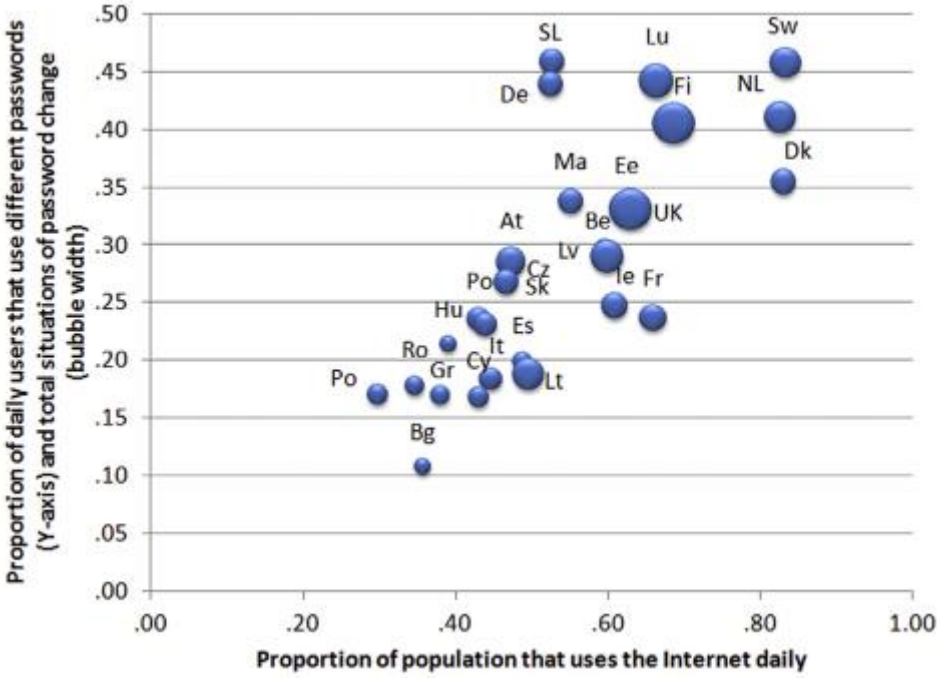
Η συμπεριφορά ασφάλειας μετράται για κάθε άτομο, μέσω της χρήσης antivirus και υψηλού επιπέδου κωδικό πρόσβασης. Ένας ασφαλής κωδικός πρόσβασης περιλαμβάνει δύο δείκτες: τη χρήση των πολλαπλών κωδικών πρόσβασης για πολλαπλές τοποθεσίες στον ιστότοπο και τον αριθμό των καταστάσεων όπου ο χρήστης έχει αλλάξει τον κωδικό πρόσβασης τα τελευταία 12 χρόνια στο e-mail, στα online μέσα κοινωνικής δικτύωσης, στην ιστοσελίδα αγορών που πραγματοποιεί και στις online τραπεζικές ιστοσελίδες.

Με βάση τη συσχέτιση της αναλογίας του επιπέδου της καθημερινής χρήσης του διαδικτύου σε κάθε χώρα με τους δείκτες της συμπεριφοράς στην ασφάλεια και την έκθεση σε εγκληματικότητα στον κυβερνοχώρο, εντοπίστηκε ότι σε οικολογικό επίπεδο, εφόσον είναι υψηλότερη η χρήση του Διαδικτύου, αυτό συμβάλλει στη δημιουργία κοινωνικών περιβαλλόντων και πολιτισμών που αφορούν ατομικές εμπειρίες ασφαλείας.

Δεδομένου ότι οι άνθρωποι που χρησιμοποιούν το Διαδίκτυο σπάνια ή καθόλου είναι λιγότερο πιθανό να αντιμετωπίσουν το έγκλημα στον κυβερνοχώρο και να λάβουν μέτρα ασφαλείας, η εκτιμώμενη συσχέτιση μεταξύ του ποσοστού των καθημερινών χρηστών και

της συχνότητας εμφάνισης της εγκληματικότητας στον κυβερνοχώρο θα ήταν μη λογική, ως εκ τούτου, έχει υπολογιστεί η έκθεση του εγκλήματος στον κυβερνοχώρο και η επίπτωση των μέτρων ασφαλείας μόνο για το τμήμα των καθημερινών χρηστών του Διαδικτύου, για κάθε χώρα, ελέγχοντας έτσι τη μεταβλητότητα που προκαλείται μέσω παρόμοιας συχνότητας των online δραστηριοτήτων.

Γράφημα 1– Scatterplot / Διάγραμμα σκεδασμού της χώρας σε επίπεδο μέσης χρήσης του Διαδικτύου (Χ-άξονας) και του ποσοστού των καθημερινών χρηστών που χρησιμοποιούν διαφορετικούς κωδικούς πρόσβασης για διαφορετικές περιοχές (άξονας Υ), με το μέγεθος της φούσκας να φανερώνει το μέσο αριθμό των καταστάσεων της αλλαγής του κωδικού πρόσβασης κατά τους τελευταίους 12 μήνες. Οικολογικό επίπεδο συσχέτισης Pearson: (α) καθημερινή χρήση και συνολική αλλαγή του κωδικού πρόσβασης: R=0,64, (β) καθημερινή χρήση και διαφορετικοί κωδικοί πρόσβασης R=0.74. Πηγή δεδομένων: Ευρωβαρόμετρο 77.2 / 2012, ανάλυση των συγγραφέων



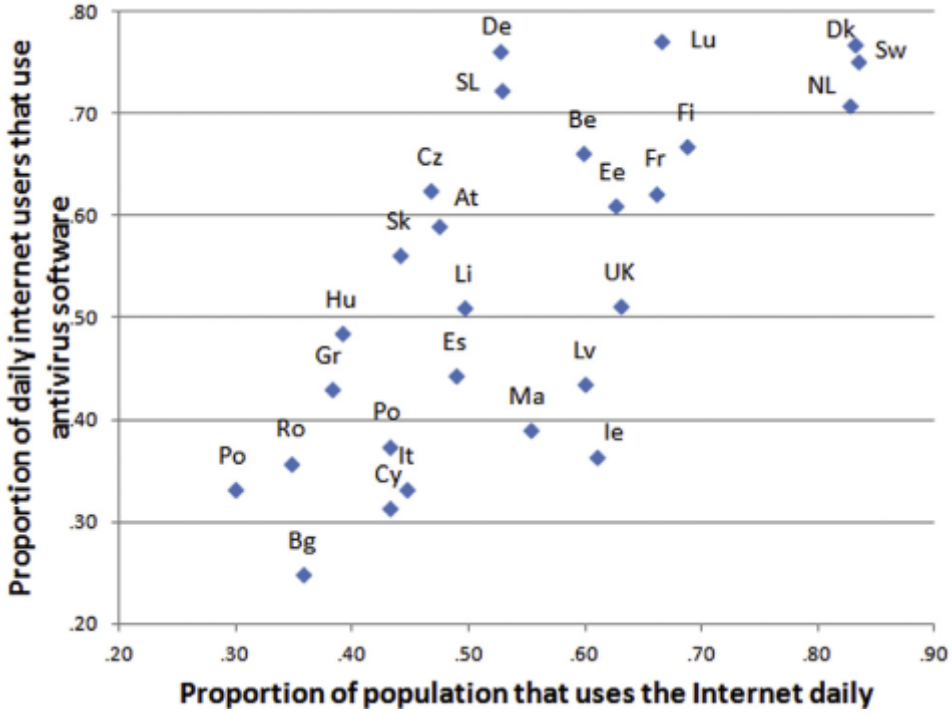
Πηγή: Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, Cosima Rughinis & Razvan Rughinis, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

Η προηγούμενη εικόνα εμφανίζει τη θετική συσχέτιση, σε οικολογικό επίπεδο, μεταξύ του ποσοστού των καθημερινών χρηστών του Διαδικτύου, στον άξονα Χ, και του

ποσοστού αλλαγής του κωδικού πρόσβασης μεταξύ των καθημερινών χρηστών στον άξονα Y (ο συντελεστής συσχέτισης Pearson είναι 0,64). Το μεγέθος των φυσαλίδων δείχνει το μέσο αριθμό των καταστάσεων της αλλαγής του κωδικού πρόσβασης κατά τους τελευταίους 12 μήνες για τους καθημερινούς χρήστες, το οποίο συσχετίζεται επίσης θετικά με τις αναλογίες καθημερινής χρήσης σε οικολογικό επίπεδο (ο συντελεστής συσχέτισης Pearson είναι 0,74). Φαίνεται ότι οι χώρες στις οποίες οι online δραστηριότητες είναι διάχυτες ενθαρρύνουν επίσης την ύπαρξη υγιούς/ ασφαλούς κωδικού πρόσβασης.

Στην ακόλουθη εικόνα παρατηρείται μια παρόμοια σχέση μεταξύ της δραστηριότητας στο Διαδίκτυο και της χρήση antivirus (η συσχέτιση Pearson είναι 0,71).

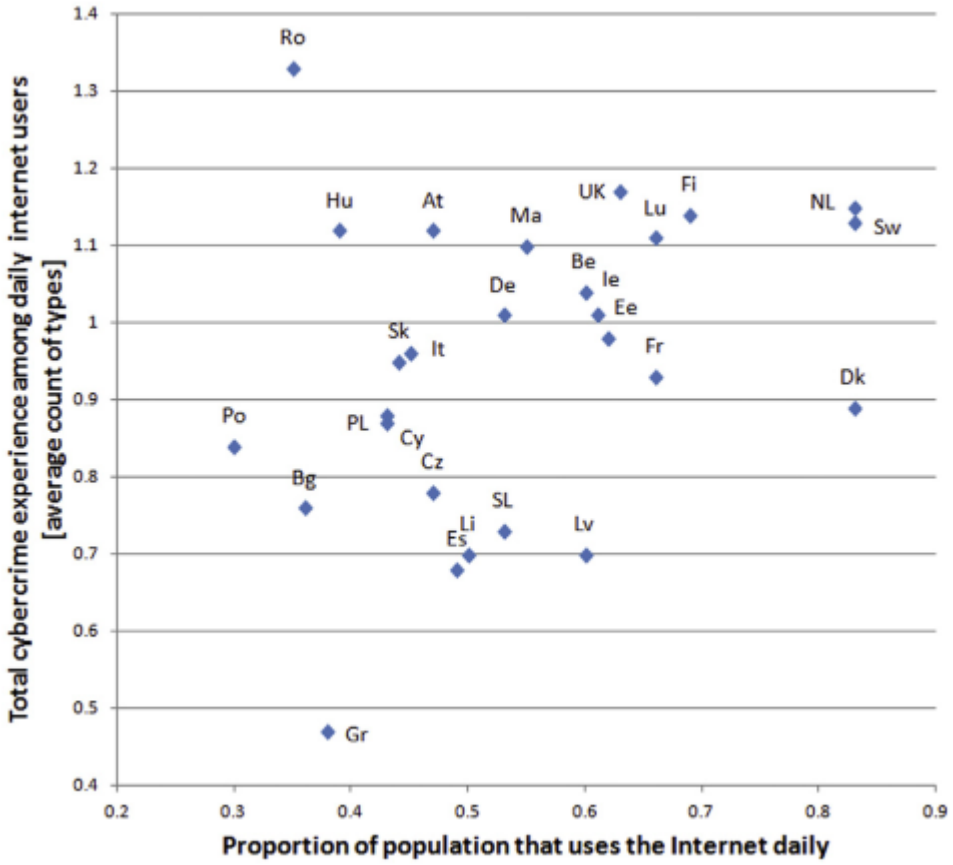
Γράφημα 2 - Scatterplot / Διάγραμμα σκεδασμού της χώρας σε επίπεδο μέσης χρήσης του Διαδικτύου και του antivirus χρησιμοποιούν για την καθημερινή χρήση του Διαδικτύου. Σε οικολογικό επίπεδο, ο συντελεστής Pearson είναι 0,71. Πηγή δεδομένων: Ευρωβαρόμετρο 77.2 / 2012, ανάλυση συγγραφέων



Πηγή: Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, Cosima Rughinis & Razvan Rughinis, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

Παρατηρήθηκε μια θετική αλλά ασθενέστερη σχέση με το οικολογικό επίπεδο μεταξύ του επιπέδου της χώρας της χρήσης του Διαδικτύου και τη μέση εμπειρία της εγκληματικότητας στον κυβερνοχώρο μεταξύ των καθημερινών χρηστών του Διαδικτύου:

Γράφημα 3 - Scatterplot / Διάγραμμα σκεδασμού χώρας του μέσου όρου της χρήσης του Διαδικτύου και της εμπειρίας του εγκλήματος στον κυβερνοχώρο. Οικολογικό επίπεδο συσχέτισης Pearson: 0,32 για όλα τα δεδομένα και 0,50 χωρίς τη Ρουμανία, την Ουγγαρία και την Ελλάδα. Πηγή δεδομένων: Ευρωβαρόμετρο 77.2 / 2012, ανάλυση συγγραφέων



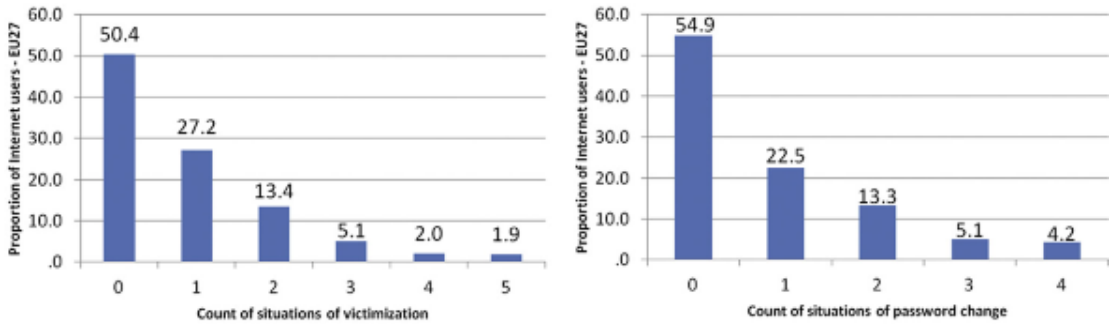
Πηγή: Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, Cosima Rughinis & Razvan Rughinis, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

Υπάρχουν δύο ενδιαφέρουσες ιδιαιτερότητες. Από τη μία πλευρά, η Ρουμανία και η Ουγγαρία έχουν εμφανώς ακραίες τιμές, με πολύ υψηλότερα επίπεδα εγκληματικότητας στον κυβερνοχώρο από την αναμενόμενη θέση τους, δεδομένου του χαμηλού ποσοστού

των καθημερινών χρηστών τους στο Διαδίκτυο. Στην πραγματικότητα, η Ρουμανία έχει τον υψηλότερο δείκτη εγκληματικότητας στον κυβερνοχώρο μεταξύ των 27 χωρών της ΕΕ και είναι δεύτερη ως προς τη χρήση του Διαδικτύου, μετά την Πορτογαλία. Η Ελλάδα φαίνεται επίσης να έχει μια απομακρυσμένη θέση, με χαμηλότερη αναφορά σε ποσοστά εγκληματικότητας στον κυβερνοχώρο από την αναμενόμενη. Παρόλα αυτά, ακόμη και αν εξαιρεθούν αυτές οι τρεις χώρες, η σχέση μεταξύ της εγκληματικότητας στον κυβερνοχώρο και τα πρότυπα χρήσης κάθε χώρας, είναι ασθενέστερη από τις ενώσεις που αφορούν τα μέτρα ασφαλείας (ο συντελεστής συσχέτισης Pearson είναι 0,50).

Σύμφωνα με το μοντέλο παλινδρόμησης για δύο εξαρτημένες μεταβλητές που αφορούν (α) τη συνολική εμπειρία του εγκλήματος στον κυβερνοχώρο (μετρούμενη ως καταμέτρηση των καταστάσεων στις οποίες ο ερωτώμενος έχει πέσει θύμα) και (β) τα λαμβανόμενα μέτρα για αλλαγή κωδικού πρόσβασης (που μετράται ως καταμέτρηση των καταστάσεων στις το οποίο ο εναγόμενος έχει αλλάξει τον κωδικό πρόσβασής του τους τελευταίους 12 μήνες), όπως φαίνεται στο παρακάτω γράφημα, οι δύο μεταβλητές δεν έχουν κανονική κατανομή.

Γράφημα 4 - Συνολική εμπειρία του εγκλήματος στον κυβερνοχώρο και Μέτρα για αλλαγή κωδικού πρόσβασης



(α) Εμπειρία εγκλήματος

(β) Αλλαγή κωδικού πρόσβασης

Όπως φαίνεται στο γράφημα, οι μεταβλητές έχουν κωδικοποιηθεί εκ νέου με 4 κατηγορίες: 0 (δεν αντιμετώπισε καμία κατάσταση εγκληματικότητας στον κυβερνοχώρο), 1 κατάσταση, 2 καταστάσεις, 3 ή περισσότερα καταστάσεις. Η αναφερόμενη κατηγορία και για τα δύο μοντέλα είναι 0 - καμία εμπειρία του εγκλήματος στον κυβερνοχώρο δεν εντοπίστηκε και δεν υπήρξε αλλαγή κωδικού πρόσβασης κατά τους τελευταίους 12 μήνες.

Ενώ υπάρχουν πολλές στατιστικά σημαντικές συσχετίσεις, αντανακλώντας το μεγάλο μέγεθος του δείγματος, η συνολική προβλεπτική ικανότητα του μοντέλου είναι χαμηλή. Μεγαλύτερα μεγέθη επίδρασης μπορούν να εντοπιστούν για τις εξής ηλικίες:

- ✓ Σε άτομα ηλικίας 65 ετών και άνω.
- ✓ Οι πιθανότητες για νεαρά άτομα ηλικίας 15-34 έχουν έρθει σε 3-5 περιπτώσεις εγκληματικότητας και είναι σχεδόν 2 αυτοί που δεν έχουν καθόλου σχετική εμπειρία.
- ✓ Οι περιπτώσεις αλλαγής κωδικού πρόσβασης είναι 3-4 αντί καμίας αλλαγής που είναι πάνω από 4.

Το εκπαιδευτικό επίτευγμα ως μετράται από την ηλικία αποφοίτησης αποτελεί επίσης ένα σχετικά ισχυρό προγνωστικό παράγοντα. Προκύπτει το συμπέρασμα ότι υπάρχουν σχετικά χαμηλά κοινωνικά στρώματα της έκθεσης σε έγκλημα στον κυβερνοχώρο και του κωδικού πρόσβασης, όταν αναλύονται ανεξάρτητα.

Προφίλ Χρηστών

Η εξερεύνηση γίνεται μέσω της ανάλυσης διασποράς. Χρησιμοποιήθηκε η συστάδα των Κ-μέσων (K-Means Cluster) για την ταξινόμηση των ερωτηθέντων, σύμφωνα με τους δείκτες συμπεριφοράς. Αποφασίστηκε ότι η 5-τύπου ταξινόμηση προσφέρει την καλύτερη επεξήγηση κι επίπεδο λεπτομέρειας. Οι πέντε αυτές κατηγορίες, έχουν λάβει το χαρακτηρισμό τους σύμφωνα με το online προσανατολισμό και είναι: «εξερευνητής», «αντιδραστικός», «συνετός», «τυχερός», και «περιστασιακός» χρήστης. Ο «εξερευνητής» και «περιστασιακός» χρήστης αντιπροσωπεύουν τα άκρα μιας συνεχούς δραστηριότητας έκθεσης και προστασία. Οι πρώτοι έχουν υψηλά επίπεδα και για τα τρία χαρακτηριστικά, ενώ τα τελευταία έχουν χαμηλά επίπεδα. Οι άλλες τρεις κατηγορίες αντιπροσωπεύουν ενδιάμεσα είδη κι ως επί το πλείστον διαφοροποιούνται από μοτίβα ασφαλείας.

Οι «τυχεροί» χρήστες αντιπροσωπεύουν μια ενδιαφέρουσα εμπειρική κατηγορία: έχουν υψηλή συχνότητα χρήσης, με μέση ποικιλομορφία των online δραστηριοτήτων, εμφανίζοντας ταυτόχρονα χαμηλή εμπειρία εγκληματικότητας στον κυβερνοχώρο και στρατηγικές χαμηλής προστασίας. Με άλλα λόγια φαίνονται να είναι τυχεροί. Τα συγχρονικά δεδομένα της έρευνας.

Υπάρχει διαφοροποίηση ως προς τους «συνετούς» από τους «αντιδραστικούς» τύπους ανάλογα με τους παρατηρήσιμους προσανατολισμούς της ασφάλειάς τους. Ένας «συνετός» χρήστης επιλέγει ως επί το πλείστον προειδοποιητικά μέτρα που μπορεί για

παράδειγμα να περιορίζουν την σε απευθείας σύνδεση δραστηριότητά τους κι επισκέπτονται μόνο αξιόπιστες ιστοσελίδες χρησιμοποιώντας μόνο το δικό τους υπολογιστή. Οι «αντιδραστικοί» χρήστες εμφανίζουν ελαφρώς υψηλότερη συχνότητα και την ποικιλία ως προς την απευθείας σύνδεση, αλλά έχουν και ελαφρώς υψηλότερες εμπειρίες κυβερνο-εγκλήματος. Ακόμα, δεν συμμετέχουν σε περιοριστικά μέτρα προστασίας, κάνοντας κυρίως μόνο χρήση της αλλαγής του κωδικού πρόσβασης τους. Όπως στους «εξερευνητές» αρέσει να έχουν υψηλό σκορ σε όλους τους δυνατούς τύπους λήψης μέτρων ασφάλειας, έτσι και στους «αντιδραστικούς» χρήστες αρέσει η συχνή αλλαγή κωδικών πρόσβασης, πιθανότατα ως αντίδραση ή πρόληψη κατά των εισβολών, σε αντίθεση με τους «εξερευνητές» που παρακολουθούν λιγότερο συμβουλές ασφάλειας, όπως είναι η χρήση διαφορετικών κωδικών πρόσβασης ή η χρήση λογισμικού προστασίας από ιούς.

Το ακόλουθο γράφημα απεικονίζει τα περιγράμματα της δραστηριότητας, των εμπειριών και των μέτρων ασφαλείας για τις πέντε συστάδες. Για παράδειγμα, οι χρήστες «εξερευνητής» και «συνετός» είναι παρόμοιοι ως προς την ένταση της ηλεκτρονικής δραστηριότητας, αλλά διαφέρουν ως προς την αντίδρασή τους στο έγκλημα στον κυβερνοχώρο. Οι πρώτοι εντείνουν την ύπαρξη υγιούς/ ασφαλέστερου κωδικού πρόσβασης, ενώ οι τελευταίοι αποσύρονται από τις online συναλλαγές.

Γράφημα 5- Προφίλ δραστηριότητας κυβερνο-ασφάλειας των τελικών χρηστών και εμπειρίας ως προς την εγκληματικότητα στον κυβερνοχώρο.

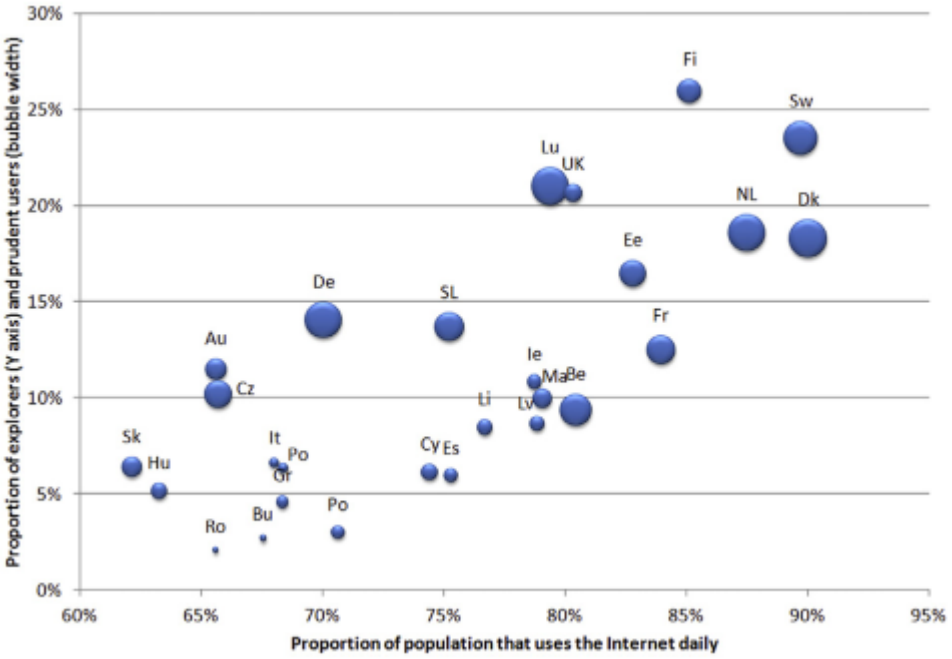
Πηγή: Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, Cosima Rughinis & Razvan Rughinis, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

Οι συσχετίσεις σε επίπεδο χώρας μεταξύ των αναλογιών των χρηστών σε μια συγκεκριμένη συστάδα και τα μέτρα της διείσδυσης στο Διαδίκτυο (De Argaez, 2013) είναι υψηλά για τους «εξερευνητές» (R= 0,87), τους «συνετούς» (R= 0,85), και τους «περιστασιακούς» χρήστες (R= -0,92). Είναι χαμηλότερα για τους «τυχερούς» (R= -0,57) και τους «αντιδραστικούς» χρήστες (R= -0,07). Η σχέση με τις εκτιμήσεις σε επίπεδο χώρας των καθημερινών χρηστών του Διαδικτύου είναι εξίσου υψηλή (βλ. Γράφημα). Αυτό δείχνει ότι οι προσανατολισμοί για «εξερευνητή» και «συνετό» χρήστη αναπτύσσονται ταυτόχρονα ως δύο εναλλακτικές για στάσεις ασφαλείας σε καλλιέργειες υψηλής διείσδυσης στο Διαδίκτυο, σε βάρος των «περιστασιακών» προσανατολισμών. Σε αντίθεση με τους «εξερευνητές» που, όταν έρχονται αντιμέτωποι με το έγκλημα στον κυβερνοχώρο, εντείνουν την προστασία τους, οι «συνετοί» χρήστες απαντούν σε εμπειρίες θυματοποίησης με την απόσυρσή τους από online συναλλαγές.

Αυτή η ανάλυση δείχνει ότι οι εκστρατείες ασφάλειας στο Διαδίκτυο και άλλες δημόσιες παρεμβάσεις μπορούν να αντιμετωπίσουν τη διακριτική κατηγορία των «συνετών» χρηστών, που περιλαμβάνουν ένα μεγάλο ποσοστό παλαιότερου και περισσότερο μορφωμένου κοινού με υψηλή διάχυση στο Διαδίκτυο. Είναι πιθανό να έχουν διαφορετικές συμπεριφορές τυπικής πλοήγησης από νεότερους χρήστες καθώς και διαφορετικά προβλήματα ασφάλειας εκτός από τους κινδύνους απρόσεχτων κοινοποιήσεων, εκφοβισμών σε απευθείας σύνδεση, και σεξουαλικής παρενόχλησης. Για την κατηγορία αυτή, οι δημόσιες παρεμβάσεις θα μπορούσαν να ενθαρρύνουν απαντήσεις σε θυματοποίηση που ενισχύουν την προστασία αντί να μειώνουν τη συμμετοχή.

Η διάκριση μεταξύ ασφαλούς δέσμευσης και προσεκτικής απόσυρσης από την online κοινότητα σπάνια τονίζεται στις δημόσιες εκστρατείες. Για τους «συνετούς» χρήστες, αυτό θα μπορούσε να αποτελέσει ένα σημαντικό μήνυμα, σε συμπεριφορικό επίπεδο, τονίζοντας ότι οι εκστρατείες ευαισθητοποίησης και ενημέρωσης παρουσιάζουν κινδύνους και μεθόδους ασφάλειας.

Γράφημα 6- Ποσοστό εξερευνητών (άξονας Υ) και ποσοστό συνετών χρηστών (πλάτος φυσαλίδων) ως συνάρτηση της αναλογίας του ποσοστού των καθημερινών χρηστών του διαδικτύου (άξονας Χ), 27 χώρες της ΕΕ. Πηγή δεδομένων: Ευρωβαρόμετρο 77.2 / 2012, ανάλυση συγγραφέων.



Πηγή: Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union, Cosima Rughinis & Razvan Rughinis, 2014 Elsevier Ltd., Computers & Security 43 III 125, www.elsevier.com/locate/cose

Παράρτημα 2: Πίνακας Δεδομένων

Ακολουθεί η παρουσίαση των πραγματικών τιμών σε καταγγελίες που πραγματοποιήθηκαν με βάση τα δεδομένα που λήφθηκαν από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και τη χρήση του Statgraphics.

Περίοδος	Πραγματικές τιμές	Προβλεπόμενες τιμές
1/4/13	20,0	12
8/4/13	16,0	13
15/4/13	15,0	13
22/4/13	4,0	14
29/4/13	10,0	12
6/5/13	7,0	12
13/5/13	16,0	11
20/5/13	9,0	12
27/5/13	11,0	11
3/6/13	22,0	11
10/6/13	3,0	13
17/6/13	12,0	11
24/6/13	10,0	11
1/7/13	8,0	11
8/7/13	7,0	11
15/7/13	12,0	10
22/7/13	5,0	10
29/7/13	40,0	10
5/8/13	11,0	13
12/8/13	5,0	13
19/8/13	10,0	12
26/8/13	9,0	12
2/9/13	9,0	11
9/9/13	15,0	11
16/9/13	20,0	12
23/9/13	14,0	13
30/9/13	9,0	13
7/10/13	16,0	12
14/10/13	12,0	13
21/10/13	20,0	13
28/10/13	13,0	14
4/11/13	19,0	14
11/11/13	14,0	14
18/11/13	11,0	14
25/11/13	13,0	14
2/12/13	21,0	14
9/12/13	6,0	15
16/12/13	17,0	14
23/12/13	5,0	14
30/12/13	6,0	13
6/1/14	21,0	12
13/1/14	13,0	13
20/1/14	25,0	13
27/1/14	10,0	15

3/2/14	8,0	14
10/2/14	7,0	13
17/2/14	20,0	13
24/2/14	15,0	14
3/3/14	7,0	14
10/3/14	10,0	13
17/3/14	7,0	13
24/3/14	25,0	12
31/3/14	29,0	13
7/4/14	13,0	16
14/4/14	12,0	15
21/4/14	8,0	15
28/4/14	11,0	14
5/5/14	24,0	14
12/5/14	9,0	15
19/5/14	19,0	14
26/5/14	14,0	15
2/6/14	13,0	15
9/6/14	16,0	15
16/6/14	20,0	15
23/6/14	17,0	16
30/6/14	17,0	16
7/7/14	14,0	16
14/7/14	13,0	16
21/7/14	13,0	16
28/7/14	23,0	15
4/8/14	21,0	16
11/8/14	27,0	17
18/8/14	3,0	18
25/8/14	2,0	17
1/9/14	12,0	15
8/9/14	35,0	14
15/9/14	12,0	17
22/9/14	26,0	17
29/9/14	25,0	18
6/10/14	43,0	19
13/10/14	21,0	22
20/10/14	24,0	22
27/10/14	16,0	23
3/11/14	25,0	22
10/11/14	17,0	23
17/11/14	10,0	22
24/11/14	28,0	21
1/12/14	31,0	22
8/12/14	19,0	23
15/12/14	27,0	23
22/12/14	10,0	24
29/12/14	15,0	22
5/1/15	8,0	21
12/1/15	35,0	20
19/1/15	15,0	22
26/1/15	16,0	21
2/2/15	16,0	20

9/2/15	15,0	20
16/2/15	39,0	19
23/2/15	7,0	22
2/3/15	18,0	20
9/3/15	26,0	20
16/3/15	35,0	21
23/3/15	14,0	23
30/3/15	27,0	22
6/4/15	25,0	23
13/4/15	16,0	23
20/4/15	14,0	22
27/4/15	21,0	21
4/5/15	12,0	21
11/5/15	27,0	20
18/5/15	13,0	21
25/5/15	13,0	20
1/6/15	21,0	19
8/6/15	19,0	19
15/6/15	24,0	19
22/6/15	17,0	20
29/6/15	13,0	20
6/7/15	16,0	19
13/7/15	17,0	18
20/7/15	18,0	18
27/7/15	13,0	18
3/8/15	18,0	17
10/8/15	12,0	17
17/8/15	13,0	17
24/8/15	13,0	16
31/8/15	13,0	16
7/9/15	20,0	15
14/9/15	13,0	16
21/9/15	14,0	15
28/9/15	23,0	15
5/10/15	19,0	16
12/10/15	14,0	16
19/10/15	18,0	16
26/10/15	16,0	16
2/11/15	17,0	16
9/11/15	18,0	16
16/11/15	17,0	16
23/11/15	13,0	16
30/11/15	12,0	16
7/12/15	18,0	15
14/12/15	16,0	16
21/12/15	8,0	16
28/12/15	12,0	14
4/1/16	2,0	14
11/1/16	1,0	12
18/1/16	4,0	11
25/1/16	0,0	10
1/2/16	0,0	8
8/2/16	3,0	7

15/2/16	4,0	6
22/2/16	1,0	5
29/2/16	3,0	4
7/3/16	3,0	4
14/3/16	2,0	3
21/3/16	1,0	3