Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Προστασία της Πληροφορίας στο Διαδίκτυο**
Ονοματεπώνυμο Φοιτητή	**Παναγιώτης Καλαμπαλίκης**
Πατρώνυμο	**Χρήστος**
Αριθμός Μητρώου	**ΜΠΠΛ**/08003
Επιβλέπων	**Αριστέα Σινανιώτη-Μαυρούδη**, **Καθηγήτρια**

Ημερομηνία Παράδοσης: **Οκτώβριος** 2012

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Αριστέα Σινανιώτη Καθηγήτρια	Χρήστος Δουληγέρης Καθηγητής	Δημήτριος Βέργαδος Επ. Καθηγητής

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου διατριβής, που υλοποιήθηκε στα πλαίσια του προγράμματος Μεταπτυχιακών Σπουδών «στην Πληροφορική» του Πανεπιστημίου Πειραιά για την απόκτηση Μεταπτυχιακού Διπλώματος στην Πληροφορική, ολοκληρώνεται ο κύκλος σπουδών μου,στο Πανεπιστήμιο Πειραιά.

Αρχικά θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου κ. Αριστέα Σινανιώτη, για τη δυνατότητα που μου έδωσε, να ασχοληθώ με το θέμα «η Προστασία της Πληροφορίας στο Διαδίκτυο» καθώς και για τις υποδείξεις που μου παρείχε τόσο κατά την εκπόνηση της παρούσας εργασίας όσο και στην παρουσίασή της.

Επίσης ευχαριστώ θερμά, τους συμμετέχοντες στην τριμελή επιτροπή για την εξέταση της εργασίας αυτής, κ. Χρήστο Δουληγέρη και κ. Δημήτριο Βέργαδο, για τις συμβουλές, υποδείξεις και παρατηρήσεις τους.

Θα ήθελα να εκφράσω την εκτίμηση μου και τις ευχαριστίες μου, σε όλο το διδακτικό προσωπικό του Μεταπτυχιακού Προγράμματος Σπουδών «Πληροφορική», του τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς καθώς και στους συναδέλφους αποφοίτους του εν λόγω προγράμματος για την αλληλεπίδραση και τον προβληματισμό που αναπτύχθηκε κατά τη διεξαγωγή αυτού.

Τέλος το μεγαλύτερο ευχαριστώ ανήκει στην οικογένειά μου, για την υποστήριξη και την ηθική συμπαράσταση που μου παρείχε κατά την διάρκεια των σπουδών μου.

Σε όσους συμβάλλουν στο δρόμο της γνώσης και της επιστήμης.

Περιεχόμενα

Συντομογραφίες

ΑΔΑΕ	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
ΑΠ	Αρχή πιστοποίησης
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Βλ.	Βλέπε
ΔτΑ	Δικαιώματα του Ανθρώπου (περιοδικό)
ΔΣΑΠΔ	Διεθνές Σύμφωνο περί Ατομικών και Πολιτικών Δικαιωμάτων
ΕΛΣΤΑΤ	Ελληνική Στατιστική Υπηρεσία
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΕΧΙ	Ένωση Ελλήνων Χρηστών Internet
ΚΕΠ	Κέντρα Εξυπηρέτησης Πολιτών
ΚτΠ	Κοινωνία της Πληροφορίας
ΜΜΕ	Μέσα Μαζικής Ενημέρωσης
Ν.	Νόμος
Ό.π	Όπου παραπάνω
ΤΠΕ	Τεχνολογία Πληροφοριών & Επικοινωνιών
ΤοΣ	Το Σύνταγμα (περιοδικό)
CMS	Σύστημα Διαχείρισης Περιεχομένου
DNS	Domain Name System
FTP	File Transfer Protocol - Πρωτόκολλο μεταφοράς αρχείων
HTTP	Πρωτόκολλο Μεταφοράς Υπερκειμένου
HTML	Γλώσσα δόμηση σελίδων του World Wide Web
XHTML	Εκτεταμένη γλώσσα σήμανσης υπερκειμένου.
IDS	Intrusion Detection System (Σύστημα Ανίχνευσης Εισβολής)
IRC	Internet Real Chat - Συζητήσεις πραγματικού χρόνου
IMAP	Πρωτόκολλο ηλεκτρονικού ταχυδρομείου
ISOC	Internet Society Club
ISP	Internet Service Provider (Παροχέας Internet)
ITU	Διεθνή Ένωση Τηλεπικοινωνιών
LAN	Local Area Network (τοπικό δίκτυο υπολογιστών)
POP3	Post Office Protocol (Πρωτόκολλο ηλεκτρονικού ταχυδρομείου)
SIS	Σύστημα πληροφοριών Σένγκεν
SMTP	Πρωτόκολλο ηλεκτρονικού ταχυδρομείου
SSL	Secure Socket Layer (πρωτόκολλο ασφαλής σύνδεσης)
TCP/IP	Πρωτόκολλο μεταφοράς δεδομένων στο Διαδίκτυο
UAC	Έλεγχος λογαριασμού χρήστη
URL	Uniform Resource Locator(διεύθυνση Παγκόσμιου Ιστού)
WAN	Wide Area Network (δίκτυο ευρείας περιοχής)
WWW	World Wide Web Παγκόσμιος πληροφοριακός ιστός

Κατάλογος εικόνων

Κατάλογος πινάκων

Κατάλογος σχημάτων

Περίληψη

Στην εποχή της παγκοσμιοποίησης η ραγδαία ανάπτυξη των νέων τεχνολογιών της πληροφορικής και του internet , δημιουργεί μια σύγχρονη κοινωνία που αντιστοιχεί στον όρο «Κοινωνία της Πληροφορίας» ή Κυβερνοχώρος. Σε αυτή την κοινωνία δημιουργούνται τεράστιες δυνατότητες και προοπτικές για τα μέλη της, με τη διακίνηση της πληροφορίας κάνοντας χρήση τεχνολογικών εργαλείων πληροφορικής και internet. Η πληροφορία αποκτά βαρύνουσα σημασία και ο κάτοχός της μεγάλη γνώση και ισχύ. Για το λόγο αυτό η πληροφορία πρέπει να προστατεύεται ιδιαίτερα αν περιλαμβάνει δεδομένα προσωπικού χαρακτήρα.

Με την παρούσα διπλωματική εργασία επιχειρείται αρχικά η μελέτη θεμάτων σχετικών με το Διαδίκτυο (στατιστικά στοιχεία, υπηρεσίες του Διαδικτύου, θετικά και αρνητικά στοιχεία, κοινωνικά δίκτυα), όπου αναδεικνύεται η δυναμική του internet και η ανάδειξή του σαν σύγχρονο βασικό μέσο επικοινωνίας. Στη συνέχεια γίνεται αναφορά σε θέματα ασφαλείας που πρέπει να υπάρχουν σε ένα σύστημα υπολογιστή. Καταγράφονται τρόποι παραβίασης της ιδιωτικότητας στο Διαδίκτυο (κακόβουλο λογισμικό), καθώς και επιθέσεις που μπορεί να υπάρξουν γενικότερα σε δίκτυα υπολογιστών. Στη συνέχεια προτείνονται τρόποι προστασίας των δεδομένων που προσφέρει η σύγχρονη Τεχνολογία και μετά η Νομική επιστήμη μέσα από το νομοθετικό πλαίσιο που έχει θεσπισθεί τόσο σε επίπεδο ευρωπαϊκό όσο και σε ελληνικό. Γίνεται επίσης εκτενής αναφορά σε ανεξάρτητες αρχές που βασική τους αποστολή είναι η εφαρμογή των νομοθετικών διατάξεων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Τέλος επιχειρείται εξαγωγή συμπερασμάτων για το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που προσφέρει η σύγχρονη τεχνολογία και το νομοθετικό πλαίσιο που εφαρμόζεται.

Abstract

In the era of globalization, the rapid growth of the new technologies of information and the Internet creates a modern society corresponding to the term “Society of Information” or “Cyberspace”. In this society huge potential and prospects for its members are created through the dissemination of information making use of the technological tools of computer science and the Internet. The information acquires utmost importance and its owner significant knowledge and power. For this reason, the information has to be especially protected if it includes specific personal data.

With the present diplomatic work, initially the study of subjects relevant to the Internet (statistical figures, services of the Internet, positive and negative aspects, social networks) is attempted where the dynamics of the Internet is demonstrated and also the fact that it has become a basic contemporary means of communication. Afterwards, issues that concern the safety measures that should be taken in a computer system are mentioned. Ways of the violation of privacy on the Internet (malicious computational) as well as attacks that may generally arise in computer networks are documented. Next, ways of the protection of data that modern technology and the Legal Science, through the legislative frame which has been established not only in Europe but also in Greece, offer are proposed. There is also an extensive reference to independent authorities whose basic mission is the implementation of legal ordinances in regard to the protection of specific personal data. Finally, a drawing of conclusions about the level of protection of specific personal data being offered by modern technology and the implemented legislative frame is attempted.

Εισαγωγή

Στη σύγχρονη εποχή της παγκοσμιοποίησης, η ραγδαία ανάπτυξη της τεχνολογίας της πληροφορικής και του Διαδικτύου επηρεάζει τομείς τόσο στην οικονομία όσο και στην ίδια την κοινωνία επιφέροντας μια σειρά αλλαγών στην εργασία, την εκπαίδευση, στις συναλλαγές, και σε μια σειρά άλλους τομείς. Παράλληλα, όμως, οι αυξημένες χάρη στην τεχνολογία, δυνατότητες συλλογής, επεξεργασίας και χρήσης πληροφοριών που αφορούν το άτομο, συνεπάγονται κινδύνους για επεμβάσεις στην ιδιωτική ζωή του ατόμου. Αυτή ακριβώς η ανησυχία από τους κινδύνους που διατρέχει ο ιδιωτικός βίος του σύγχρονου ανθρώπου, από τις αυξημένες δυνατότητες της πληροφορικής και των νέων τεχνολογιών δημιούργησε και την προβληματική για την προστασία των προσωπικών δεδομένων[1].

Δίκαια πολλοί υποστηρίζουν ότι το Διαδίκτυο είναι η επανάσταση των τελευταίων δεκαετιών, καθώς αυτό είναι εργαλείο στην οικονομία, στην επιστήμη, στην ενημέρωση, στη ψυχαγωγία, αποτελεί πηγή πληροφόρησης και αντικείμενο γνώσης, παρέχοντας πρόσβαση σε πολλές υπηρεσίες. Με την διαρκή εξέλιξη των νέων τεχνολογιών, οι χρήστες του διαδικτύου είναι πια σε θέση να επικοινωνούν με οποιοδήποτε μέρος του πλανήτη σύντομα και χωρίς ιδιαίτερο κόστος, να πραγματοποιούν ηλεκτρονικές αγορές, να το χρησιμοποιούν στην εργασία, στην εκπαίδευση, στην έρευνα, στην επιστήμη .Η χρήση του Διαδικτύου δίνει πρόσβαση σε κάθε είδους πληροφορία που χρειάζεται ο σύγχρονος άνθρωπος, μηδενίζει τις γεωγραφικές αποστάσεις , καταργεί τα σύνορα μεταξύ των κρατών, κάνει τον κόσμο να «φαντάζει» μικρός.

Η χρήση των νέων τεχνολογιών επικοινωνίας και του Διαδικτύου είναι βασικός μοχλός οικονομικής και κοινωνικής ανάπτυξης. Τα πληροφοριακά συστήματα γίνονται πολύτιμα εργαλεία εκσυγχρονισμού της δημόσιας διοίκησης και του κράτους ενώ στον ιδιωτικό τομέα χρησιμοποιούνται για την αποδοτικότερη οργάνωση της παραγωγής, διάθεσης προϊόντων και υπηρεσιών, καθώς μπορούν να αποθηκεύσουν να επεξεργαστούν και να συσχετίσουν πολλές πληροφορίες σε ελάχιστο χρόνο[2]. Η χρήση βασικών υπηρεσιών του Διαδικτύου όχι μόνο από τους ειδικούς της πληροφορικής, αλλά και από απλούς χρήστες διευκολύνει την άμεση επικοινωνία χωρίς περιορισμούς χρονικούς ή τοπικούς. Τα τελευταία μάλιστα χρόνια με την ανάπτυξη του web 2[3] και την τεράστια εξάπλωση των σελίδων κοινωνικής δικτύωσης (βλ. facebook, YouTube κ.α), η επικοινωνία έγινε πιο άμεση και διαδραστική, καθώς οι χρήστες ανταλλάσσουν απόψεις και σκέψεις online, βρίσκουν φίλους από τα παλιά και αποκτούν νέους, κάποιοι από τους οποίους μπορεί να βρίσκονται σε διαφορετικά γεωγραφικά σημεία του πλανήτη.

Όμως η χρήση του Διαδικτύου και των νέων τεχνολογιών πέρα από τα πλεονεκτήματα που προσφέρει στην κατεύθυνση της ανάπτυξης και της ευημερίας, εγκυμονεί και σοβαρούς κινδύνους προσβολής της ιδιωτικότητας του ατόμου, καθώς οι πληροφορίες που υπάρχουν και διακινούνται συνδέονται με συγκεκριμένα πρόσωπα. Έτσι οι πληροφορίες αυτές ανάγονται σε δεδομένα προσωπικού χαρακτήρα των ατόμων και έχουν σαν αντικείμενο την περιουσιακή

---

[1] Βλ.Ιγγλεζάκη Ι., Δίκαιο της πληροφορικής, β΄ έκδοση, εκδόσεις Σάκουλα, σελ 221

[2] Βλ.Αλεξανδροπούλου Αιγυπτιάδου Ε., Ζητήματα από το Δίκαιο της πληροφορικής, εκδόσεις Σάκουλα,2002, σελ 21

[3] Ο όρος Web 2.0 ,αναφέρεται στη νέα γενιά του Παγκόσμιου Ιστού όπου οι χρήστες μπορούν να μοιράζονται πληροφορίες, να συνεργάζονται online και να αλληλεπιδρούν μεταξύ τους χωρίς εξειδικευμένες γνώσεις σε θέματα υπολογιστών και δικτύων.

κατάσταση, την υγεία , τις θρησκευτικές και πολιτικές πεποιθήσεις, το ποινικό μητρώο, την επαγγελματική δραστηριότητα, τις κοινωνικές επαφές, την οικογενειακή κατάσταση την ερωτική ζωή και κάθε δραστηριότητα της προσωπικής ζωής. Η αποθήκευση των δεδομένων αυτών σε μεγάλες βάσεις δεδομένων, η γρήγορη ανάκλησή τους από αυτές σε συνδυασμό με την ταχύτητα διάδοσής τους, μπορεί να δώσουν μια πλήρη εικόνα για την προσωπικότητα του ατόμου σαν εργαζόμενο, καταναλωτή, πολίτη. Έτσι ο πολίτης είναι κάτω από το αδιάκριτο βλέμμα εκείνου που έχει πρόσβαση στην πληροφορία, που συνδέεται με τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν [4].

Σε μια παγκοσμιοποιημένη κοινωνία όπως η σημερινή υπάρχει μια κυρίαρχη αντίθεση. Από τη μια μεριά προβάλλει το αίτημα για ελεύθερη πρόσβαση στις πληροφορίες παντού με τη χρήση τεχνολογικών εργαλείων πληροφορικής και του Διαδικτύου. Από την άλλη κρίνεται επιτακτική η ανάγκη της προστασίας της ιδιωτικότητας του ατόμου και των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Λύση σε αυτό το πρόβλημα υπάρχει από την πλευρά της τεχνολογίας με τεχνικά μέτρα προστασίας αλλά και της νομικής με θέσπιση κατάλληλου νομοθετικού πλαισίου.

Αφορμή για την συγγραφή της παρούσας διατριβής αποτέλεσε ο προβληματισμός που αναδείχτηκε μέσα από τις παραδόσεις των μαθημάτων, «Νομική πληροφορική» με την Κα Σινανιώτη Αριστέα, «Ασφάλεια πληροφοριών» με την Κα Πολέμη Δέσποινα , «Κρυπτογραφία» με τον Κο Πατσάκη Κωνσταντίνο, «Δίκτυα Υπολογιστών» με τον Κο Δουληγέρη Χρήστο του Προγράμματος Μεταπτυχιακών Σπουδών «Πληροφορική» του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς.

Σκοπός αυτής της διατριβής είναι η μελέτη θεμάτων σχετικών με κινδύνους που ελλοχεύουν κατά τη χρήση συστημάτων πληροφορικής, επικοινωνίας και του Διαδικτύου, καθώς και τρόπων προστασίας που υπάρχουν σε επίπεδο τεχνολογικό και σε επίπεδο νομοθετικού πλαισίου.

Η εργασία αυτή εδώ αποτελείται από οκτώ κεφάλαια.

Στο πρώτο κεφάλαιο αυτής της εργασίας, γίνεται αναφορά σε θέματα του Διαδικτύου όπως: Βασικές υπηρεσίες , στατιστικά στοιχεία για τη χρήση του Διαδικτύου στον Κόσμο, στην Ευρώπη και στην Ελλάδα , τα θετικά και τα αρνητικά, κοινωνικά δίκτυα και το φαινόμενο Facebook.

Στο δεύτερο κεφάλαιο διαπραγματεύονται θέματα σχετικά με την ασφάλεια υπολογιστών-δικτύων όπως: Βασικές υπηρεσίες ασφαλείας, τρόποι παραβίασης της ιδιωτικότητας στο Διαδίκτυο, κατηγορίες επιθέσεων στα δίκτυα υπολογιστών , παράγοντες που βοηθούν τη διάδοση απειλών.

Στο τρίτο κεφάλαιο παρουσιάζονται μέτρα προστασίας από τη σκοπιά της τεχνολογίας όπως: Προγράμματα αντιϊκά (antivirus) ,Τείχος προστασίας (Firewall), Συστήματα ανίχνευσης εισβολέων (IDS), αντίγραφα ασφαλείας (Back Up), ασφάλεια ηλεκτρονικού ταχυδρομείου, κρυπτογραφία, ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές, πρωτόκολλο SSL (Secure Sockets Layer).

[4] Βλ.Αλεξανδροπούλου Αιγυπτιάδου Ε., Προσωπικά δεδομένα, εκδόσεις Σάκουλα,2007, σελ 21-22

Στο τέταρτο κεφάλαιο, εξετάζονται θέματα αναφορικά με το νομοθετικό πλαίσιο σε διεθνές επίπεδο και στην Ευρωπαϊκή Ένωση.

Το θέμα του πέμπτου κεφαλαίου περιέχει την ανάλυση θεμάτων σχετικών με το νομοθετικό πλαίσιο στην Ελλάδα αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα παρουσιάζονται βασικές διατάξεις του Συντάγματος και αναλύεται πιο διεξοδικά ο νόμος 2472/1997 όπου εξετάζονται: Η έννοια των προσωπικών δεδομένων, η διάκριση των δεδομένων σε απλά και ευαίσθητα, η επεξεργασία αυτών ,τα δικαιώματα του υποκειμένου. Στη συνέχεια παρουσιάζεται ο Ν. 2774/1999, ο Ν. 3471/2006 και ο Ν. 3917/2011.

Το έκτο κεφάλαιο αφιερώνεται στις Ανεξάρτητες Αρχές που είναι επιφορτισμένες με την εφαρμογή των νόμων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Παρουσιάζεται η Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα (Α.Π.Δ.Π.Χ) και ειδικότερα η αποστολή, η οργάνωση , οι αρμοδιότητες καθώς και σημαντικές αποφάσεις – γνωμοδοτήσεις της Αρχής. Στη συνέχεια αναφέρεται η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) καθώς και η Αρχή Διασφάλισης του Απορρήτου.

Στο έβδομο κεφάλαιο καταγράφονται προβληματισμοί και σκέψεις αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα και πως ο νομοθέτης πρέπει να είναι σε διαρκή επαγρύπνηση προκειμένου το νομοθετικό πλαίσιο να καλύπτει με επάρκεια την διαρκώς εξελισσόμενη τεχνολογία της Πληροφορικής και του Διαδικτύου. Στην κατεύθυνση αυτή βέβαια χρειάζεται και η βοήθεια των επιστημόνων της πληροφορικής με τη δημιουργία τεχνολογιών ασφαλείας που θα καλύπτουν τις εξελισσόμενες τεχνολογίες. Τέλος στο όγδοο κεφάλαιο προτείνεται η κατασκευή ασφαλούς ιστοσελίδας με τη χρήση του Συστήματος Διαχείρισης Περιεχομένου (Content Management Systems, CMS) joomla. Στο παράρτημα παρατίθενται περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ καθώς και έντυπα αιτήσεων καταγγελίας – προσφυγής στην ΑΠΔΠΧ.

Για τη συγγραφή της εργασίας χρησιμοποιήθηκε η βιβλιογραφική έρευνα, ενώ οι πηγές αντλήθηκαν από την ελληνική και ξένη βιβλιογραφία, περιοδικά σχετικά με την τεχνολογία της πληροφορικής , εφημερίδες, ιστοσελίδες με σχετικό περιεχόμενο.

Λέξεις Κλειδιά: Ιδιωτικότητα, προστασία πληροφορίας, προστασία δεδομένων προσωπικού χαρακτήρα, νομοθεσία περί ιδιωτικότητας, ασφάλεια υπολογιστών, ασφάλεια δικτύων, συμμετρική κρυπτογραφία, πρωτόκολλο ssl, Ανεξάρτητες Αρχές Προστασίας Προσωπικών δεδομένων, cms, joomla.

1 **ΚΕΦΑΛΑΙΟ**: **Το Διαδίκτυο** (Internet)

1.1 **Εισαγωγή**

Η ιδέα της δημιουργίας του Διαδικτύου έχει την αρχή της στα τέλη της δεκαετίας του 60, όταν το υπουργείο Άμυνας των ΗΠΑ αποφάσισε την κατασκευή ενός δικτύου υπολογιστών, το οποίο θα μπορούσε να λειτουργεί ακόμη και στην περίπτωση που μέρος του θα είχε καταστραφεί. Για να γίνει αυτό εφικτό έπρεπε να αναπτυχθούν και εφαρμοστούν νέες τεχνικές και τεχνολογίες στη δικτύωση των υπολογιστών, πράγμα που έγινε και δημιουργήθηκε ένα τέτοιο δίκτυο. Το δίκτυο αυτό μετά από συνεχείς βελτιώσεις αποτελεί σήμερα το Internet, γνωρίζει μεγάλη ανάπτυξη, συνδέει εκατομμύρια χρήστες και αποτελεί την μεγαλύτερη πηγή πληροφορίας, συνάντησης χρηστών, ανταλλαγής μηνυμάτων και ιδεών στον πλανήτη.

Σήμερα είναι ένα **παγκόσμιο δίκτυο υπολογιστών** που μπορούν και επικοινωνούν μεταξύ τους, είτε μεμονωμένοι είτε δίκτυα υπολογιστών (τοπικά –Local Area Networks/LAN's ή ευρείας περιοχής Wide Area Networks/Wan's). Από την παραπάνω δομή του το Internet, ως δίκτυο δικτύων, δικαιολογεί και την ελληνική ονομασία του Διαδίκτυο**.** Το Internet (**Inter**national **Net**work) ή Διαδίκτυο αναπτύχθηκε ως δίκτυο υπολογιστών και διασυνδεδεμένων δικτύων **(LANs, MANs και WANs**[5]**),** το οποίο καλύπτει τον πλανήτη. Ουσιαστικά πρόκειται για ένα δίκτυο δικτύων υπολογιστών, στο οποίο κάθε συνδεδεμένος χρήστης του είναι δυνητικά σε θέση να επικοινωνεί και να μεταφέρει δεδομένα σε/από οποιονδήποτε άλλο χρήστη ή ηλεκτρονικό υπολογιστή, ο οποίος είναι επίσης συνδεδεμένος στο δίκτυο. Για να επιτευχθεί η επικοινωνία μεταξύ των δικτύων υπολογιστών χρησιμοποιείται ένα κοινό πρωτόκολλο επικοινωνίας, το TCP/IP (Transmission Control Protocol/Internet Protocol) [6].

Στα χαρακτηριστικά του διαδικτύου, είναι πως συνδέει υπολογιστές διαφορετικών τύπων ως προς:

α) την υλική τους δομή (hardware),

β) την αρχιτεκτονική τους,

γ) το λειτουργικό σύστημα που χρησιμοποιούν, και

δ) το πρωτόκολλο δικτύωσης στο τοπικό τους δίκτυο.

Στο διαδίκτυο δεν υπάρχει κάποιος κεντρικός φορέας διεύθυνσης και λήψης αποφάσεων για τα ζητήματα εσωτερικής οργάνωσης, διαχείρισης και ελέγχου των πληροφοριών που διακινούνται. Το Διαδίκτυο δεν έχει κάποιον ιδιοκτήτη, **δεν ανήκει σε κανένα**, σε αντίθεση με τα επιμέρους δίκτυα υπολογιστών που το αποτελούν και συνήθως έχουν ιδιοκτήτη. Βέβαια για τα

---

[5] LAN: Local Area Network (τοπικό δίκτυο υπολογιστών).
WAN: Wide Area Network (δίκτυο ευρείας περιοχής)

[6] Για περισσότερα βλ: Αλεξανδρή Ν., Β. Μπελεσιώτη, Θ. Παναγιωτόπουλου, Εισαγωγή στην επιστήμη των υπολογιστών, Αθήνα 2004,σελ 167

επιμέρους προβλήματα που προκύπτουν έχουν δημιουργηθεί επιτροπές που επιλύουν θέματα και προβλήματα που παρουσιάζονται κάθε φορά. Τέτοιες επιτροπές είναι:

☞ **Internet Society**. Η επιτροπή Internet Society (ISOC) εγκρίνει και ενσωματώνει νέα πρότυπα, καθώς επιλύει και προβλήματα, όπως το πρόβλημα του μικρού αριθμού IP Διευθύνσεων[7].

☞ **InterNic** . Η επιτροπή που εκχωρεί και διαχειρίζεται διευθύνσεις ονομάτων χώρου(domain name) [8] .

☞ **I**nternet **E**ngineering **T**ask **F**orce (**IETF**). Αποστολή της συγκεκριμένης επιτροπής η επίλυση τεχνικών θεμάτων στην επικοινωνία των δικτύων λαμβάνοντας υπόψη την υπάρχουσα υποδομή[9].

1.2 **Βασικές έννοιες**

Δίκτυο υπολογιστών. Δίκτυο υπολογιστών είναι ένα σύνολο υπολογιστών που είναι συνδεδεμένοι μεταξύ τους με κανάλια επικοινωνίας και μπορούν να παράγουν να στέλνουν και να λαμβάνουν πληροφορίες[10]. Δύο ή περισσότεροι υπολογιστές θεωρούμαι ότι βρίσκονται σε δίκτυο όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες. Τα δίκτυα συνδέονται μεταξύ τους με συσκευές που λέγονται δρομολογητές (routers) ή πύλες (gateways). Το Διαδίκτυο είναι το "Δίκτυο των δικτύων" ένα σύνολο από διασυνδεδεμένους υπολογιστές και δίκτυα που συνδέονται μεταξύ τους βάσει καθορισμένων πρωτοκόλλων.

Πρωτόκολλα δικτύου. Λέγοντας πρωτόκολλα εννοούμε ένα σύνολο από συμβάσεις που ορίζουν με ποιο τρόπο, οι υπολογιστές που βρίσκονται σε ένα δίκτυο, ανταλλάσσουν μεταξύ τους τα δεδομένα , με ποιο τρόπο γίνεται ο έλεγχος για τυχόν λάθη και πως αντιμετωπίζονται αυτά.
Τα πρωτόκολλα που χρησιμοποιούνται και πάνω σε αυτά στηρίζεται η λειτουργία ενός δικτύου αλλά και του internet είναι το **TCP/IP** (**T**ransmission **C**ontrol **P**rogram/**I**nternet **P**rotocol). Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων που περιέχει το TCP ή Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μετάδοσης) και το IP ή Internet Protocol (Πρωτόκολλο Διαδικτύου). Η βασική λειτουργία των δύο αυτών πρωτοκόλλων είναι με την εγκαθίδρυση μιας σύνδεσης μεταξύ δύο υπολογιστών, η πληροφορία που αποστέλλεται σπάει σε μικρά κομμάτια που ονομάζονται πακέτα και ταξιδεύει μέσω πολλών διαφορετικών οδών για να φτάσει στον παραλήπτη όπου συναρμολογείται ξανά για να μπορεί να την χρησιμοποιήσει ο παραλήπτης.

---

[7] Διεθνή ένωση στην οποία μετέχουν περισσότεροι από 150 οργανισμοί και 6.000 μέλη από εκατό χώρες. Για περισσότερες πληροφορίες βλ. http://www.isoc.org.

[8] Το InterNIC είναι ο οργανισμός που διαχειρίζεται τις καταχωρήσεις ονομάτων χώρου βλ: http://www.internic.net

[9] Για πληροφορίες βλ.http://www.ietf.org

[10] Δουληγέρης Χρήστος Σημειώσεις του μαθήματος «Δίκτυα υπολογιστών» του Προγράμματος Μεταπτυχιακών Σπουδών «Πληροφορική» του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς

IP διεύθυνση (IP Address). Η IP διεύθυνση (IP Address) είναι η διεύθυνση ενός υπολογιστή στο Διαδίκτυο και τον προσδιορίζει μοναδικά. Μια διεύθυνση IP αποτελείται από 4 αριθμούς χωρισμένους με τελείες π.χ 147.102.154.12. Υπάρχουν δυναμικές διευθύνσεις IP οι οποίες δίνονται για να αναγνωρίζονται προσωρινές συσκευές όπως προσωπικοί υπολογιστές και στατικές διευθύνσεις IP που χρησιμοποιούνται για να αναγνωρίζονται ημι-μόνιμες συσκευές.

Domain Name System ή DNS. Το DNS ή αλλιώς Σύστημα Ονοματοδοσίας είναι ένας άλλος να προσδιορίζεται η ταυτότητα ενός υπολογιστή. Το σύστημα DNS μπορεί και αντιστοιχίζει ονόματα με διευθύνσεις IP. Ο λόγος χρησιμοποίησης αυτού του συστήματος είναι η δυσκολία που έχουν οι άνθρωποι στην απομνημόνευση αριθμητικών διευθύνσεων IP σε σχέση με τα ονόματα τα οποία θυμούνται ευκολότερα. Έτσι μια διεύθυνση IP αντιστοιχίζεται με ένα όνομα που είναι μοναδικό για τον κάθε υπολογιστή. Η μέθοδος αυτή είναι γνωστή σαν DNS (Domain Name System).

Ιστοσελίδα. Η ιστοσελίδα (Web Page) είναι ένα έγγραφο του παγκόσμιου ιστού (WWW) που αποτελείται από πληροφορίες οι οποίες έχουν την μορφή κειμένου, εικόνας, ήχου, βίντεο. Πολλές ιστοσελίδες μαζί συνιστούν ένα δικτυακό τόπο (web site). Υπάρχουν δύο είδη ιστοσελίδων: Οι στατικές οι οποίες δημιουργούνται τοπικά σε ένα υπολογιστή και αντιπροσωπεύουν την παλαιότερη τεχνολογία και οι δυναμικές οι οποίες δημιουργούνται σε ένα web server χρησιμοποιώντας κατάλληλα εργαλεία λογισμικού και «δείχνουν» την νέα τεχνολογία. Ένα τέτοιο ολοκληρωμένο σύστημα διαχείρισης περιεχομένου (cms), το οποίο δημιουργεί και διαχειρίζεται δυναμικές σελίδες, είναι το **joomla** το οποίο και θα παρουσιάσουμε στο κεφάλαιο 8. Για να δημιουργηθούν ιστοσελίδες χρησιμοποιείται η γλώσσα προγραμματισμού HTML ή η XHTML .Υπάρχουν βέβαια και προγράμματα που κατασκευάζουν πιο εύκολα ιστοσελίδες όπως το Dreamweaver το FrontPage κ.α.

Φυλλομετρητής ιστού. Ο φυλλομετρητής ιστού (web browser) είναι ένα πρόγραμμα περιήγησης στο Διαδίκτυο, το οποίο βοηθά το χρήστη να επισκέπτεται διάφορες ιστοσελίδες και να αλληλεπιδρά με πληροφορίες που βρίσκονται σε αυτές με μορφή κειμένου, ήχου, βίντεο, παιχνιδιών ή και υπερσυνδέσμων που παραπέμπουν σε άλλες τοποθεσίες ιστού.

Web server. Ο όρος Web server παραπέμπει σε ένα ή πολλούς ηλεκτρονικούς υπολογιστές (hardware), όπου φιλοξενούνται οι ιστοσελίδες που συγκροτούν ένα δικτυακό τόπο. Μπορεί να είναι και λογισμικό (software) που μας επιτρέπει μέσω του Internet και με την βοήθεια του πρωτοκόλλου HTTP να αποκτούμε πρόσβαση σε ιστοσελίδες που είναι αποθηκευμένες σε αυτόν. Υπάρχουν διάφορα είδη Web Server όπως οι dedicated servers, οι load balancing servers, οι database servers. Επίσης, καθένας μπορεί να μετατρέψει τον ηλεκτρονικό υπολογιστή του σε έναν Web Server εγκαθιστώντας κατάλληλο λογισμικό που να συνδέει τον υπολογιστή του με το Internet[11]. Γνωστοί Web Server είναι ο Apache Server , ο IIS Server , ο Nginx Server κ.α.

[11] Βλ. http://www.webvistas.org/topic/451-%CF%B9-web-servers/

1.3 Η ιστορία του Διαδικτύου

Στη δεκαετία του '50 κατά τη διάρκεια του Ψυχρού Πολέμου οι Ηνωμένες Πολιτείες βρίσκονταν σε συνεχή στρατιωτικό και τεχνολογικό ανταγωνισμό με το αντίπαλο δέος, τη Σοβιετική Ένωση. Το 1955 ο Αμερικανός πρόεδρος Eisenhower ανακοίνωσε την πρόθεση της χώρας του να θέσει σε τροχιά γύρω από τη Γη έναν μικρό δορυφόρο, δίνοντας έτσι το σύνθημα για μία κούρσα για την κατάκτηση του Διαστήματος. Η κούρσα αυτή τερματίστηκε μόλις δύο χρόνια αργότερα, με την εκτόξευση του δορυφόρου Sputnik I στις 4 Οκτωβρίου 1957. Το πλήγμα που δέχθηκε το γόητρο των ΗΠΑ ήταν τόσο ισχυρό, ώστε για πρώτη φορά μετά τη ρίψη της ατομικής βόμβας δεκατρία χρόνια νωρίτερα η χώρα ένιωσε τρωτή. Θέλοντας λοιπόν να προστατευτούν από μια πιθανή πυρηνική επίθεση των Ρώσων δημιούργησαν την υπηρεσία προηγμένων αμυντικών ερευνών ARPA (Advanced Research Project Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency) στις μέρες μας. Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί ένα δίκτυο επικοινωνίας το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση. Έτσι δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET[12] το οποίο εγκαταστάθηκε και λειτούργησε το 1969.

Αρχικά, το ενδιαφέρον του ARPA επικεντρώθηκε σε τεχνολογικά θέματα στρατιωτικού ενδιαφέροντος, που θα εξασφάλιζαν την εδαφική ακεραιότητα των ΗΠΑ, όπως η έρευνα για το Διάστημα, η βαλλιστική πυραύλων, η διεξαγωγή και παρακολούθηση πυρηνικών δοκιμών. Πολύ σύντομα μετατράπηκε στο σημαντικότερο ερευνητικό κέντρο στρατιωτικών θεμάτων, διαθέτοντας έναν τεράστιο προϋπολογισμό, προσλαμβάνοντας δεκάδες κορυφαίους επιστήμονες και προωθώντας τη συνεργασία με τα πιο αξιόλογα ερευνητικά εργαστήρια στη χώρα. Έτσι, η ανάγκη για συνεχή επικοινωνία και συνεργασία με ιδρύματα που βρίσκονταν διάσπαρτα σε διάφορες και αρκετά απέχουσες μεταξύ τους τοποθεσίες, οδήγησε αναπόφευκτα στην έρευνα στον τομέα των επικοινωνιών.

Το παρακάτω χρονοδιάγραμμα, δίνει συνοπτικά την ιστορία του Διαδικτύου καθώς και τους σημαντικότερους σταθμούς αυτού[13].

1934: Ο Βέλγος εμπειρογνώμονας , Paul Otlet, με τη χρήση της τότε τεχνολογίας, όπως το τηλέφωνο και το ράδιο ,οραματίστηκε κάτι που έμοιαζε σε δομή με το σημερινό διαδίκτυο.

---

[12] Το αρχικό θεωρητικό υπόβαθρο δόθηκε από τον Τζ. Λικλάιντερ (J.C.R. Licklider) που μιλούσε για το "γαλαξιακό δίκτυο". Η θεωρία αυτή υποστήριζε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το επόμενο θέμα που προέκυπτε ήταν ότι το δίκτυο αυτό θα έπρεπε να ήταν αποκεντρωμένο έτσι ώστε ακόμα κι αν κάποιος κόμβος του δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές. Τη λύση σε αυτό έδωσε ο Πολ Μπάραν (Paul Baran) με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων του Λέοναρντ Κλάινροκ (Leonard Kleinrock), που υποστήριζε ότι πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο Στηριζόμενο λοιπόν σε αυτές τις τρεις θεωρίες δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET, βλ: http://el.wikipedia.org/wiki/Διαδίκτυο επίσης http://el.wikipedia.org/wiki/ARPANET

[13] Βλ: http://www.livescience.com/20727-internet-history.html.

1958: Στο Υπουργείο Άμυνας των ΗΠΑ ιδρύεται η Υπηρεσία Προηγμένων Έργων Έρευνας (Advanced Research Projects Agency- ARPA) με στόχο την εξέλιξη της επιστήμης και της τεχνολογίας στα πλαίσια του Αμερικανικού στρατού.

1961: Γίνεται η πρώτη δημοσίευση που αφορά στη θεωρία Μεταγωγής Πακέτων (Packet Switching) από τον Leonard Kleinrock «Information Flow in Large Communication Nets» [14].

1964: Δημοσιεύεται μελέτη από τον Paul Baran για τα κατανεμημένα δίκτυα μεταγωγής πακέτων : «On Distributed Communications Networks[15].

1965: Δύο υπολογιστές στο εργαστήριο Lincoln του MIT επικοινωνούν μεταξύ τους την τεχνολογία «packet-switching».

1967: Δημοσιεύεται το πρώτο σχέδιο του δικτύου ARPANET από τον L.Roberts. Η δημοσίευση φέρει τον τίτλο "Multiple Computer Networks and Intercomputer Communication».

1968: Η εταιρεία BBN παρουσιάζει την τελική έκδοση του Interface Message Processor υπογράφοντας σύμβαση για το ARPANET.

1969: Χρηματοδοτείται και εγκαθίσταται η πρώτη υλοποίηση του ARPANET με 4 κόμβους (mini computers μνήμης 12K) διαφορετικού λειτουργικού συστήματος και γραμμές ταχύτητας 50kbps. Αργότερα, μέχρι το τέλος του 1971 θα έχουν συνδεθεί στο ARPANET συνολικά 23 κόμβοι. Στις 29 Οκτωβρίου το Πανεπιστήμιο της Καλιφόρνια, στο Λος Άντζελες, το Ινστιτούτο Ερευνών του Στάνφορντ, το Πανεπιστήμιο της Καλιφόρνια, στη Santa Barbara και το Πανεπιστήμιο της Γιούτα εγκαθιστούν τους πρώτους κόμβους επικοινωνίας. Το πρώτο μήνυμα που στέλνεται είναι «Lo», ένα μήνυμα από τον φοιτητή Charles Kline για σύνδεση (Login) στον υπολογιστή του Ινστιτούτου Ερευνών του Στάνφορντ. Ωστόσο το μήνυμα δεν ολοκληρώθηκε καθώς το σύστημα του Στάνφορντ κατέρρευσε.

1970 : Γίνεται η πρώτη δημοσίευση που αφορά στο πρωτόκολλο επικοινωνίας του δικτύου ARPANET από τους C.S. Carr, S. Crocker, V.G. Cerf με τίτλο, "HOST-HOST Communication Protocol in the ARPA Network". Τίθεται σε λειτουργία το δίκτυο ALOHAnet, το οποίο θα συνδεθεί με το ARPANET δύο χρόνια αργότερα.

1972: Ανακοινώνεται στην ευρύτερη επιστημονική κοινότητα η λειτουργία του ARPANET και αποφασίζεται η υποστήριξη της έρευνάς του. Ο Ray Tomlinson της BBN παρουσιάζει το e-mail και χρησιμοποιεί για πρώτη φορά το σύμβολο @ κατά τη νέα υλοποίηση του προγράμματος ηλεκτρονικού ταχυδρομείου του ARPANET. Υλοποιείται το πρώτο σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου. Επιδεικνύεται για πρώτη φορά η υπηρεσία chat και διαμορφώνονται οι προδιαγραφές της υπηρεσίας telnet. Η Ομάδα Εργασίας Διαδικτύωσης (INWG) βρίσκεται αντιμέτωπη με την πρόκληση της θέσπισης πρωτοκόλλων.

1973: Η Παγκόσμια δικτύωση γίνεται πραγματικότητα, καθώς το Πανεπιστήμιο του Λονδίνου και το Royal Radar Establishment, στη Νορβηγία, συνδέονται στο ARPANET. Ο όρος Διαδίκτυο μόλις έχει γεννηθεί. Το ARPANET έχει γίνει πλέον διεθνές και απαριθμεί περίπου 2000 χρήστες.

---

[14] Βλ: http://www.lk.cs.ucla.edu/LK/Bib/REPORT/PhD

[15] Βλ: http://www.rand.org/publications/RM/baran.list.html

Λειτουργεί το πρώτο δίκτυο Ethernet[16] με όνομα Alto Aloha System. Διαμορφώνονται οι προδιαγραφές της υπηρεσίας μεταφοράς αρχείων FTP και του πρωτοκόλλου NVP (Network Voice Protocol) που καθιστούν δυνατή την πρώτη τηλεδιάσκεψη στο ARPANET.

1974: Γεννιέται ο πρώτος πάροχος υπηρεσιών διαδικτύου (ISP) μία εμπορική έκδοση του ARPANET , γνωστή ως Telenet. Ο Vinton Cerf και ο Bob Kahn (το δίδυμο που από πολλούς αναγνωρίζονται ως οι πατέρες του διαδικτύου) δημοσιεύουν το «Πρωτόκολλο για τη διαδικτυακή σύνδεση», που παρουσιάζουν τις λεπτομέρειες για τον σχεδιασμό του TCP (Πρωτόκολλο Ελέγχου Μεταφοράς).

1975: Λειτουργεί η πρώτη mailing list στο ARPANET, ενώ στο e-mail υλοποιούνται οι δυνατότητες απάντησης και προώθησης μηνυμάτων.

1976: Η Βασίλισσα Ελισάβετ Β' πατάει το κουμπί αποστολής για το πρώτο e-mail της.

1978: Το πρωτόκολλο TCP χωρίζεται στο TCP και το IP.

1979: Δημιουργείται το USENET όπου φιλοξενούνται ειδήσεις και ομάδες συζήτησης.

1981: Το Εθνικό Ίδρυμα Επιστημών των ΗΠΑ (NSF) προβλέπει επιδοτήσεις για τη δημιουργία Δικτύου για την ανταλλαγή πληροφοριών και την παροχή υπηρεσιών μεταξύ επιστημόνων των πανεπιστημίων.

1982: Το Transmission Control Protocol (TCP) και το Internet Protocol (IP) αναγνωρίζονται ως η «Σουίτα Πρωτοκόλλων Διαδικτύου» για το ARPANET.Αυτό έχει ως αποτέλεσμα τη σύνδεση του Διαδικτύου με το πρωτόκολλο TCP /IP, το οποίο ακόμα και σήμερα παραμένει το βασικό πρωτόκολλο για το Διαδίκτυο. Δημιουργείται το EUnet (European UNIX Network) που συνδέει αρχικά το Ηνωμένο Βασίλειο, τη Σουηδία, τη Δανία και την Ολλανδία.

1983: Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) καθιερώνει τα γνωστά .edu, .gov, .com, .mil, .org, .net, και .int ως καταλήξεις για την ονομασία ιστοσελίδων. Οι νέες ονομασίες είναι πολύ ευκολότερες από αυτές που υπήρχαν μέχρι τότε όπως 123.456.789.10.

1984: Ο William Gibson συγγραφέας του Neuromancer χρησιμοποιεί για πρώτη φορά τον όρο «Κυβερνοχώρος».

1985: Στις ΗΠΑ, όλα τα πανεπιστημιακά ιδρύματα συνδέονται μέσω του νέου Nation Science Foundation Net (NSFNet), το οποίο εξασφαλίζει πρόσβαση σε όλους τους φοιτητές και το προσωπικό των πανεπιστημίων. Παραχωρείται το πρώτο domain name (symbolics.com) και ακολουθούν άλλα, κυρίως από εκπαιδευτικά ιδρύματα (π.χ. berkeley.edu, ucla.edu κ.ά.).

1986: Στο NSFnet, το Δίκτυο του Εθνικού Ιδρύματος Επιστημών επιτυγχάνεται για πρώτη φορά απευθείας σύνδεση «υπερυπολογιστών» με ταχύτητες 56.000 bits το δευτερόλεπτο, η τυπική ταχύτητα ενός dial-up modem. Με την πάροδο του χρόνου αυτή η ταχύτητα επιτυγχάνεται σε όλο το NSFnet, αλλά και στα περιφερειακά του δίκτυα, πραγματοποιώντας ουσιαστικά μια επέκταση του Διαδικτύου σε όλες τις ΗΠΑ. Το NSFnet ήταν ουσιαστικά ένα

[16] Βλ: http://www.ethermanage.com/ethernet/ethernet.html

δίκτυο από τα πολλά δίκτυα, μέσω των οποίων συνδέονταν ακαδημαϊκοί χρήστες στο ARPANET.

1987: Τα hosts στο Διαδίκτυο ξεπερνούν τις 20.000. Η Cisco παρουσιάζει το πρώτο router.

1988: Υπάρχει πλέον παγκόσμια επέκταση του Διαδικτύου καθώς έχουν δημιουργηθεί πολλά εθνικά κ.ά. δίκτυα που συνδέονται σε αυτό. Εμφανίζεται το πρώτο worm, το οποίο επηρεάζει τη λειτουργία περίπου 6000 από τους 60000 εξυπηρετητές του δικτύου. Υλοποιείται το IRC(Internet Relay Chat).

1989: Ο World.std.com γίνεται ο πρώτος εμπορικός πάροχος για πρόσβαση στο Διαδίκτυο μέσω dial-up.

1990: Σταματάει η λειτουργία του δικτύου ARPANET. Ούτως ή άλλως, οι περισσότεροι κόμβοι του διαδικτύου έχουν ήδη συνδεθεί με άλλα δίκτυα. Λειτουργεί ο πρώτος Internet provider, που προσφέρει σύνδεση στο Internet μέσω τηλεφώνου, με το όνομα «The World comes on-line (world.std.com)». Μαζί με χώρες όπως η Αυστρία, η Ισπανία, κ.ά., η Ελλάδα συνδέεται στο Διαδίκτυο μέσω του δικτύου NSFNET.

1991: Ο Tim Berners-Lee, επιστήμονας από το CERN, αναπτύσσει για πρώτη φορά την HTML. Σήμερα αποτελεί την κύρια γλώσσα σήμανσης για τις ιστοσελίδες. Το CERN παρουσιάζει και εισάγει για πρώτη φορά το **W**orld **W**ide **W**eb, το γνωστό σε όλους μας **«www».** Σαν πρώτος web-server λειτουργεί ο nxoc01.cern.ch που αργότερα θα μετονομαστεί σε info.cern.ch. Το πρόγραμμα φυλλομετρητής διατίθεται ελεύθερα και στη 2η έκδοσή του στηρίζεται στη χρήση της γλώσσας HTML (HyperText Markup Language). Έτσι, το διαδίκτυο (ένας χώρος υπολογιστών και καλωδίων) χρησιμοποιείται για να φιλοξενήσει τον παγκόσμιο ιστό (ένα χώρο δεσμών υπερκειμένου). Υλοποιείται ο Archie, η πρώτη μηχανή αναζήτησης και ανάκτησης αρχείων.

1992: Δίνεται σε χρήση η εξελιγμένη μηχανή αναζήτησης Veronica και χρησιμοποιείται για πρώτη φορά ο όρος "surfing the Internet" (πλοήγηση στο Διαδίκτυο). Συνδέεται στο NSFNET και η Κύπρος.Τα πρώτα αρχεία ήχου και βίντεο κυκλοφορούν στο διαδίκτυο. Η φράση «σερφάρω στο διαδίκτυο» διαδίδεται και γίνεται ευρέως γνωστή.

1993: Ο αριθμός των ιστοσελίδων ανέρχεται στις 600 και ο Λευκός Οίκος, αλλά και ο ΟΗΕ μπαίνουν στο διαδίκτυο. Ο Marc Andreesen δημιουργεί το πρώτο πρόγραμμα περιήγησης στο διαδίκτυο το Mosaic, στο Πανεπιστήμιο του Ιλινόι. Οι υπολογιστές που συνδέονται στο NSFnet από τους 2.000 το 1985 φτάνουν το 1993 σε 2 εκατομμύρια. Το NSF ηγείται μίας προσπάθειας για δημιουργία μίας νέας αρχιτεκτονικής του διαδικτύου, ώστε να μπορέσει να αξιοποιηθεί και εμπορικά. Η εξέλιξη και η πτώση των τιμών των προσωπικών υπολογιστών (PCs) κάνει το διαδίκτυο γνωστό στο ευρύ κοινό που δεν ανήκει στην πανεπιστημιακή κοινότητα.

1994: Γεννιέται η Netscape Communications. Αρχίζουν οι απευθείας συνδέσεις στο Internet ενώ εμφανίζονται και οι πρώτες διαφημίσεις στο hotwired.com.

1995: Οι Compuserve, America Online και Prodigy παρέχουν πρόσβαση στο Διαδίκτυο. Στον κυβερνοχώρο βγαίνουν και οι Amazon.com, Craiglist και eBay. Το NSFnet θεωρείται πλέον παρωχημένο και η εμπορική εκμετάλλευση του διαδικτύου είναι πλέον γεγονός. Στις 23 Μαΐου η εταιρεία SUN ανακοινώνει την πλατφόρμα και τη γλώσσα JAVA. Ακολουθεί η ανάπτυξη της JAVAscript. Ξεκινάει η εμπορική διάθεση των domain names. Εμφανίζονται η VRML (εικονικά περιβάλλοντα) και τα collaborative tools. Οι νέες εκδόσεις του προγράμματος περιήγησης των

Windows ’95 βρίσκονται στα χέρια μόνο των κατασκευαστών ηλεκτρονικών υπολογιστών, ύστερα από σχετική απόφαση του υπουργείου Δικαιοσύνης. Αντίθετα ο browser της Netscape παραμένει ελεύθερος και δωρεάν στο διαδίκτυο.

1996: Ο ανταγωνισμός μεταξύ των προγραμμάτων περιήγησης εντείνεται, κυρίως μεταξύ των δύο μεγάλων εταιρειών της Microsoft και της Netscape. Δίνονται 7 νέες καταλήξεις domain, οι: .firm, .store, .web, .arts, .rec, .info, .nom.

1997: Εμφανίζεται η τεχνολογία Push. Αυτή είναι η χρονιά και του Multicasting.

1998: Γεννιέται η Google η μηχανή αναζήτησης που άλλαξε οριστικά τον τρόπο περιήγησης στο διαδίκτυο. Γίνονται οι πρώτες δημοσιεύσεις για τη γλώσσα XML. Αυτή είναι η χρονιά των portals και του διαδικτυακού εμπορίου.

1999: Η AOL αγοράζει τη Netscape. Η ανταλλαγή αρχείων Peer-to-peer γίνεται πραγματικότητα με τη δημιουργία του Napster, προκαλώντας μεγάλη δυσαρέσκεια στη μουσική βιομηχανία. Πραγματοποιούνται οι πρώτες διαδικτυακές ηλεκτρονικές τραπεζικές συναλλαγές.

2000: Σκάει η λεγόμενη «φούσκα dot-com». Πολλές εταιρείες του διαδικτύου καταρρέουν οικονομικά. Η Yahoo! και eBay έχουν τεράστιες απώλειες, λόγω του ζητήματος των προσωπικών δεδομένων, ενώ η AOL συγχωνεύεται με την Time Warner. Δίνονται 7 νέες καταλήξεις domain, οι: .aero, .biz, .coop, .info, .museum, .name, .pro.

2001: Γίνονται οι πρώτες μεταδόσεις με χρήση του Internet2. Υλοποιείται το πλήρες σύνολο χαρακτήρων Unicode.Ομοσπονδιακός δικαστής κλείνει το Napster σε μία προσπάθεια να δώσει τέλος στην ελεύθερη διακίνηση υλικού, για το οποίο αναγνωρίζονται πνευματικά δικαιώματα.

2003: Ο ιός Slammer SQL εξαπλώνεται σε όλο τον κόσμο μέσα σε 10 λεπτά. Πρωτοεμφανίζονται τα Myspace, Skype και Safari.

2004: Το Facebook μπαίνει στο διαδίκτυο και η εποχή της κοινωνικής δικτύωσης μόλις αρχίζει. Την ίδια χρονιά παρουσιάζει ο browser Mozilla Firefox.

2005: Ξεκινά το Youtube.com

2006: Η AOL αλλάζει επιχειρηματικό πλάνο προσφέροντας τις περισσότερες υπηρεσίες δωρεάν, με τα έσοδα της να στηρίζονται κυρίως στις διαφημίσεις. Πρώτη συνάντηση και για το Φόρουμ για τη Διακυβέρνηση του Διαδικτύου.

2009: Η 40η επέτειος του Internet.

2010: Το Facebook φτάνει τα 400 εκατομμύρια ενεργούς χρήστες.

2011: Twitter και Facebook παίζουν σημαντικό ρόλο στην οργάνωση και ενημέρωση στις εξεγέρσεις της «Αραβική Άνοιξης», το επαναστατικό κύμα στη Μέση Ανατολή και τη Βόρεια Αφρική[17].

[17] Βλ: http://www.e-yliko.gr/htmls/pc_use/internetstory.aspx επίσης http://www.livescience.com/20727-internet-history.html

1.4 Βασικές υπηρεσίες Διαδικτύου

Ηλεκτρονικό Ταχυδρομείο (electronic **mail e-mail)**

Το ηλεκτρονικό ταχυδρομείο είναι η υπηρεσία του Διαδικτύου που χρησιμοποιείται πάρα πολύ, ενώ οι πρώτες μορφές της χρονολογούνται από την αρχή του ARPANET.Το ηλεκτρονικό ταχυδρομείο ή email είναι η υπηρεσία που επιτρέπει την αποστολή μηνυμάτων μεταξύ δύο ή περισσότερων χρηστών με ηλεκτρονικό τρόπο. Τα μηνύματα αυτά μπορεί να έχουν επισυναπτόμενα αρχεία με εικόνες, κείμενο, βίντεο, ήχο- μουσική κ.λ.π. Το ηλεκτρονικό ταχυδρομείο έχει σχεδόν μηδαμινό κόστος ενώ τα μηνύματα παραδίδονται ταχύτατα σε σχέση με το συμβατικό ταχυδρομείο. Με τη χρήση του email καταργείται στην ουσία η αναμονή σε ταχυδρομεία.

Τα προγράμματα διαχείρισης e-mail είναι αρκετά φιλικά προς το χρήστη και δεν απαιτούν εξειδικευμένες γνώσεις για το χειρισμό τους. Τέτοια προγράμματα είναι το Outlook ,το Windows Live Mail, Eudora, pegasus mail, Opera Mail, ThunderBird κ.α Ανάμεσα στις δυνατότητες που παρέχονται είναι η παράδοση του ίδιου μηνύματος σε πολλούς παραλήπτες, ενημέρωση λήψης του μηνύματος στον αποστολέα, καθώς και αυτόματη διαχείριση και ταξινόμηση των εισερχόμενων μηνυμάτων ανά κατηγορία, περιεχόμενο, αποστολέα κ.λ.π. Κατά την αποστολή του μηνύματος δεν είναι απαραίτητο να είναι παρών ο παραλήπτης για τη λήψη του μηνύματος, καθώς αυτό παραμένει στον απομακρυσμένο εξυπηρετητή αλληλογραφίας μέχρι να συνδεθεί ο χρήστης και να το λάβει στον προσωπικό του υπολογιστή. Το ηλεκτρονικό ταχυδρομείο στηρίζει την λειτουργία του στα πρωτόκολλα POP3[18] (**P**ost **O**ffice **P**rotocol) SMTP[19] (**S**imple **M**ail **T**ransfer **P**rotocol) και IMAP[20] (**I**nternet **M**essage **A**ccess **P**rotocol). Τα μηνύματα τα διαχειρίζονται mail servers που τα αποθηκεύουν σε προσωπικό ηλεκτρονικό γραμματοκιβώτιο (mail box) του χρήστη, ώστε στη συνέχεια αυτός να τα μεταφέρει στον υπολογιστή του, μέσω ενός προγράμματος πελάτη(client), όπως είναι το Microsoft Outlook Express, το Mozilla κ.λ.π. Ο κάθε χρήστης αποκτά από τον παροχέα μια συγκεκριμένη και μοναδική παγκόσμια διεύθυνση (ηλεκτρονικό γραμματοκιβώτιο-mail box) ηλεκτρονικού ταχυδρομείου στην οποία βασίζεται η όλη λειτουργία της υπηρεσίας αυτής. Μια τέτοια

---

[18] Το POP3 αποτελεί εξέλιξη των προηγούμενων μορφών του πρωτοκόλλου, τα οποία ονομαζόταν ανεπίσημα POP1 και POP2. Ο όρος Post Office Protocol είναι πλέον συνώνυμος με το POP3, καθώς οι προηγούμενες μορφές του πρωτοκόλλου έχουν πλέον καταργηθεί στην πράξη.

[19] Το πρωτόκολλο Simple Mail Transfer Protocol (SMTP) είναι ένα σύνολο κανόνων υπεύθυνων για την μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο.Για να μπορεί ο χρήστης να χρησιμοποιήσει το ηλεκτρονικό ταχυδρομείο πρέπει πρώτα να συνδεθεί με έναν SMTP server. Το SMTP μεταφέρει μηνύματα μόνο μεταξύ υπολογιστών που λειτουργούν σαν mail servers. Δεν παραδίδει μηνύματα στο "γραμματοκιβώτιο" των χρηστών, ούτε τους επιτρέπει να παραλάβουν τα μηνύματά τους από τον mail server. Οι διαδικασίες αυτές γίνονται από το πρωτόκολλο POP3 για περισσότερα βλ: Jerry Honeycutt, MRY Ann Pike, μτφ, Ε.Γκαγκάτσιου, Πλήρης Οδηγός του Internet, 3η Αμερικάνικη Έκδοση,Γκιούρδας- Αθήνα, επίσης http://conta.uom.gr/conta/ekpaideysh/seminaria/M_Telecommunications/html/17/17-1.htm.

[20] Σε αντίθεση με το POP3, το πρωτόκολλο Internet Message Access Protocol (IMAP) που εμφανίστηκε αργότερα υποστηρίζει την ανάγνωση μηνυμάτων τόσο όταν ο χρήστης είναι συνδεδεμένος στο Διαδίκτυο όσο και αφού αποσυνδεθεί. Επίσης, αφήνει τα μηνύματα στον server έως ότου ο χρήστης αποφασίσει να τα διαγράψει. Έτσι, ο χρήστης μπορεί να διαβάζει τα email του από διάφορους υπολογιστές. Αντίθετα, το POP3 επιτρέπει την ανάγνωση των email μονάχα από τον υπολογιστή στον οποίο έχουν κατέβει.

διεύθυνση έχει μορφή, για παράδειγμα, username@sch.gr, όπου το πρώτο τμήμα πριν τον διαχωριστή @ είναι το όνομα του χρήστη και το δεύτερο του server.

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποτελείται από: α) την επικεφαλίδα (header), που περιέχει πληροφορίες όπως ο αποστολέας, ο παραλήπτης, η ημερομηνία αποστολής του μηνύματος (βλέπε πίνακα) β) το σώμα (body) που είναι το κυρίως περιεχόμενο του μηνύματος . Τα βασικά μέρη μιας επικεφαλίδας παρουσιάζονται στον παρακάτω πίνακα

To	Η ηλεκτρονική διεύθυνση (e-mail) του παραλήπτη
From	Η ηλεκτρονική διεύθυνση (e-mail) του αποστολέα
Subject	Το θέμα που έχει το μήνυμα
Date	Η ημερομηνία αποστολής του μηνύματος
Cc (Carbon copy)	Εδώ γράφεται μία ή περισσότερες διευθύνσεις παραληπτών που επιθυμούμε να γίνει κοινοποίηση του ίδιου μηνύματος
Bcc (Blind carbon copy)	Ίδια με την προηγούμενη κοινοποίηση Cc (Carbon copy) , με τη διαφορά ότι ο καθένας από τους παραλήπτες νομίζει ότι είναι ο μοναδικός παραλήπτης του μηνύματος (δεν μπορεί να δει τους υπόλοιπους).
Attachment	Επισυναπτόμενα αρχεία που επιθυμούμε να υπάρχουν στο ηλεκτρονικό μήνυμα.

Πίνακας 1. Τα βασικά μέρη επικεφαλίδας του e-mail

Η υπηρεσία του ηλεκτρονικού ταχυδρομείου προσφέρεται και μέσω ενός φυλλομετρητή (browser) και ονομάζεται **Web Mail**, όπου ο χρήστης έχει πρόσβαση στο ηλεκτρονικό ταχυδρομείο του μέσω του browser. Το WebMail είναι εφαρμογή ανάγνωσης και διαχείρισης ηλεκτρονικής αλληλογραφίας μέσω web. Προσφέρει πρόσβαση στα emails, από οποιονδήποτε υπολογιστή, οπουδήποτε (ακόμα και αν υπάρχει σύνδεση μέσω άλλου παροχέα ή από το εξωτερικό), με την εισαγωγή μόνο του username και του password. Για να γίνει χρήση του Web mail θα πρέπει ο πάροχος internet (Isp) να παρέχει αυτήν την υπηρεσία ή να μπορείτε να ανοίξετε μια συνδρομή σε μια υπηρεσία ηλεκτρονικού ταχυδρομείου (υπάρχουν συνδρομές δωρεάν και με πληρωμή). Γνωστές υπηρεσίες παροχής WebMail είναι το Gmail, Yahoo mail , Hotmail, InMail κ.α.

Παγκόσμιος πληροφοριακός ιστός (World Wide Web- www)

Ο Παγκόσμιος Ιστός ή World Wide Web (www) αποτελεί τη δημοφιλέστερη υπηρεσία του Διαδικτύου, τόσο που πολλοί την ταυτίζουν (λανθασμένα) με το Διαδίκτυο. Ο παγκόσμιος πληροφοριακός ιστός , δίνει τη δυνατότητα στο χρήστη να πλοηγηθεί σε πληροφορίες που βρίσκονται σε ιστοσελίδες με γραφικό και εύκολο τρόπο. Οι πληροφορίες βρίσκονται κατανεμημένες σε υπολογιστές σε μορφή εγγράφων, που καλούνται ιστοσελίδες και έχουν δομή

υπερκειμένου[21] ή υπερμέσου[22]. Οι ιστοσελίδες μπορεί να περιέχουν κείμενο, εικόνα , ήχο , βίντεο και επιτρέπουν μέσω των συνδέσμων την πλοήγηση του χρήστη σε αυτές, ή σε άλλες ιστοσελίδες. Αποτελεί την πολυμεσική όψη του Διαδικτύου δίνοντας τη δυνατότητα στους χρήστες για προσπέλαση, αλλά και για δημοσίευση πληροφοριών με εύκολο τρόπο. Δημιουργήθηκε το 1993 στο ερευνητικού κέντρο CERN, από τον Tim Berners-Lee.

Το πρωτόκολλο που επιτρέπει την πρόσβαση σε στοιχεία του παγκόσμιου Ιστού ονομάζεται hypertext tranfer protocol (**http**), πρωτόκολλο του επιπέδου εφαρμογής στην αρχιτεκτονική **TCP/IP**. Οι ιστοσελίδες είναι γραμμένες σε διάφορες γλώσσες σεναρίου (script languages), όπως η php, asp.net, javascript, ενώ βασίζονται κύρια στη γλώσσα HTML (Hyper Text Markup Language). Κάθε ιστοσελίδα στο Διαδίκτυο έχει μια μοναδική διεύθυνση που καλείται Uniform Resource Locator (**URL**), η οποία αποτελείται από το όνομα του υπολογιστή και το path της σελίδας, πράγμα που την καθιστά μοναδική[23].

Για παράδειγμα, η διεύθυνση www.unipi.gr/index.htm, αναλύεται ως εξής:

Protocol	Domain Name	Path
http://	**www.unipi.gr**	**/index.htm**

Πίνακας 2. Ανάλυση διεύθυνσης διαδικτύου (Uniform Resource Locator ,URL),

Τη γραφική παρουσίαση στην πλευρά του χρήστη την αναλαμβάνει ένα πρόγραμμα πελάτης, ο φυλλομετρητής (Web browser) ή περιηγητής που ουσιαστικά είναι ένα λογισμικό που επικοινωνεί με τους web servers , μέσω του πρωτοκόλλου HTTP. Αλληλεπιδρά με, κείμενα, εικόνες, βίντεο, μουσική, παιχνίδια και άλλες πληροφορίες συνήθως αναρτημένες σε μια ιστοσελίδα ενός ιστότοπου στον Παγκόσμιο Ιστό ή σε ένα τοπικό δίκτυο. Το κείμενο και οι εικόνες σε μια ιστοσελίδα μπορεί να περιέχουν υπερσυνδέσμους προς άλλες ιστοσελίδες του ίδιου ή διαφορετικού ιστότοπου. Ο Web browser επιτρέπει στον χρήστη την γρήγορη και εύκολη πρόσβαση σε πληροφορίες που βρίσκονται σε διάφορες ιστοσελίδες και ιστότοπους εναλλάσσοντας τις ιστοσελίδες μέσω των υπερσυνδέσμων. Οι φυλλομετρητές χρησιμοποιούν

---

[21] Το υπερκείμενο (αγγλ. hypertext) είναι ο μη γραμμικός τρόπος οργάνωσης πληροφοριών. Το υπερκείμενο θεωρείται μη γραμμικό κείμενο σε αντίθεση με το βιβλίο που θεωρείται γραμμικό. Η γραμμικότητα του βιβλίου έγκειται στο γεγονός ότι ο αναγνώστης οφείλει να διαβάζει τη μία σελίδα μετά την άλλη προκειμένου να κατανοήσει το περιεχόμενό του, δίχως να του δίδεται η δυνατότητα να "πλοηγείται" ελεύθερα εντός αυτού. Ο αναγνώστης έτσι αναγκάζεται να υπακούσει στους περιορισμούς που επιβάλλει ο συγγραφέας και το βιβλίο ως μέσο. Το υπερκείμενο ως μέσο έρχεται να ξεπεράσει τους περιορισμούς αυτούς επιτρέποντας την ελεύθερη πλοήγηση του αναγνώστη. Η πλοήγηση επιτυγχάνεται με την χρήση υπερσυνδέσμων. Επειδή οι υπερσύνδεσμοι αποτελούν τον κύριο μηχανισμό απόκλισης από τη γραμμικότητα αποτελούν θεμελιώδη έννοια στο υπερκείμενο. Ως τρόπος οργάνωσης (μέσω διασύνδεσης) το υπερκείμενο συναντιέται κυρίως στο χώρο των υπολογιστών και της Πληροφορικής. Ο Παγκόσμιος Ιστός χτίστηκε πάνω στις ιδέες του υπερκειμένου και αποτελεί μία ενσάρκωση (υλοποίηση) τέτοιου τρόπου διασύνδεσης και οργάνωσης πληροφοριών βλ: http://el.wikipedia.org/wiki/Υπερκείμενο επίσης Mark Gibbs & Richard Smith, Ταξιδεύοντας στο Internet, έκδοση Deluxe,μ.τ.φ Λ. Γατσώρης, Κ. Μπενέκος,εκδ. Anubis.

[22] Το Υπερμέσο (αγγλ. Hypermedia) ορίζεται ως ένα σύστημα που διαχειρίζεται ένα σύνολο πληροφοριών οι οποίες μπορούν να προσπελαστούν μη σειριακά. Το σύστημα αυτό αποτελείται από ενότητες πληροφοριών, οι οποίες ποικίλλουν αυθαίρετα ως προς τη μορφή και το περιχόμενο. Μπορούν να περιέχουν κείμενο, γραφικά, εικόνες, video, και animation, και συνδέονται με λογικούς συνδέσμους (links) ώστε να σχηματίζουν ένα δίκτυο πληροφοριών.

[23] Βλ Ν. Αλεξανδρή, Β. Μπελεσιώτη, Θ. Παναγιωτόπουλου, Εισαγωγή στην επιστήμη των υπολογιστών, Αθήνα 2004,σελ347

τη γλώσσα μορφοποίησης HTML για την προβολή των ιστοσελίδων, για αυτό η εμφάνιση μιας ιστοσελίδας μπορεί να διαφέρει ανάλογα με τον browser. Τέτοιοι φυλλομετρητές είναι ο Microsoft Internet Explorer, Mozilla Firefox, Google Chrome , Apple Safari, Opera, κ.ά.

Επειδή το πλήθος των ιστοσελίδων είναι πολύ μεγάλο, είναι αδύνατο να τις θυμόμαστε όλες. Για το λόγο αυτό κάνουμε την περιήγηση μας σε αυτές, συνήθως μέσω συνδέσμων από άλλες σελίδες ή από θεματικούς καταλόγους ή από τις μηχανές αναζήτησης που μας βοηθούν να εντοπίσουμε την ιστοσελίδα που θέλουμε.

Υπηρεσία Αναζήτησης πληροφοριών

Η αναζήτηση πληροφοριών στο Διαδίκτυο είναι μια χρήσιμη και δημοφιλής υπηρεσία. Επειδή υπάρχει μεγάλος όγκος αποθηκευμένης πληροφορίας η υπηρεσία αυτή βοηθά το χρήστη να βρίσκει πληροφορίες που υπάρχουν με βάση κάποια κριτήρια αναζήτησης. Η υπηρεσία αυτή διαθέτει εργαλεία αναζήτησης, όπως τις μηχανές αναζήτησης, τους θεματικούς καταλόγους, τις θεματικές πύλες, τις μεταμηχανές αναζήτησης. Η μηχανή αναζήτησης είναι μια υπηρεσία που διαθέτει μια βάση δεδομένων με καταγεγραμμένα στοιχεία για τις πληροφορίες που υπάρχουν στο Internet. Ο χρήστης αναζητεί αυτό που θέλει με βάση κάποια συγκεκριμένα κριτήρια - λέξεις κλειδιά (keywords) και η μηχανή αναζήτησης του παρουσιάζει τις διευθύνσεις εκείνες στις οποίες έχουν βρεθεί οι λέξεις κλειδιά. Γνωστές μηχανές αναζήτησης είναι η Google, Yahoo , Altavista, Lycos κ.λ.π.

Πρωτόκολλο Μεταφοράς Αρχείων (FTP)

Το Πρωτόκολλο Μεταφοράς Αρχείων(FTP[24]) είναι ένα πρωτόκολλο με ευρεία χρήση, σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet).Το πρωτόκολλο FTP επιτρέπει την ανταλλαγή αρχείων μεταξύ των υπολογιστών του Διαδικτύου. Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.λ.π. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα. Το FTP πρωτόκολλο όπως και το HTTP πρωτόκολλο , εκτελούνται επάνω στο TCP. Το FTP χρησιμοποιεί δυο παράλληλες συνδέσεις TCP για μεταφορά ενός αρχείου, μια σύνδεση ελέγχου (control connection) και μια σύνδεση δεδομένων (data connection). Η σύνδεση ελέγχου χρησιμοποιείται για αποστολή πληροφοριών ελέγχου ανάμεσα σε δυο υπολογιστές – πληροφοριών όπως όνομα χρήστη, κωδικό πρόσβασης, εντολές για αλλαγή ενός απομακρυσμένου καταλόγου και εντολές για "τοποθέτηση" και "λήψη" αρχείων. Η σύνδεση δεδομένων χρησιμοποιείται ώστε να κάνει την πραγματική αποστολή ενός αρχείου[25].

Ομάδες ειδήσεων- συζητήσεων (Usenet - Newsgroups)

[24] File Transfer Protocol

[25] Για περισσότερα Βλ: http://www.cnc.uom.gr/services/guides/ftp.pdf επίσης http://networking-basics.wikispaces.com

Η υπηρεσία Usenet[26] (Users' Network) είναι κατάλογοι με διευθύνσεις ηλεκτρονικού ταχυδρομείου χωρισμένοι σε ομάδες ανάλογα τα ενδιαφέροντα. Ο κάθε χρήστης μπορεί να στείλει μήνυμα σε κάποια ομάδα χρηστών που έχει κοινά ενδιαφέροντα με αυτόν. Τα μέλη της ομάδας αυτής μπορούν να το διαβάσουν και να απαντήσουν αν θέλουν σε αυτό. Η κάθε ομάδα ονομάζεται «ομάδα ειδήσεων» (newsgroup). Για να μπορεί να έχει κάποιος πρόσβαση σε αυτές τις ομάδες συζήτησης χρησιμοποιεί λογισμικά διαχείρισης ηλεκτρονικής αλληλογραφίας. Το όνομα του κάθε μηνύματος έχει συγκεκριμένη δομή και δείχνει τη θεματολογία. Τα ονόματα των ομάδων ειδήσεων έχουν μορφή παρόμοια μ' αυτή των διευθύνσεων του Internet, για παράδειγμα comp.binaries.ibm.pc. Το πρώτο συνθετικό του ονόματος δηλώνει τον γενικό τομέα ενδιαφέροντος. Τα κυριότερα προθέματα τομέων είναι τα εξής :

alt. Εναλλακτικές ομάδες ειδήσεων, με μεγάλη ποικιλία θεμάτων.

biz. Θέματα σχετικά με επιχειρήσεις.

comp. Ομάδες ειδήσεων για υπολογιστές.

misc. Διάφορα θέματα.

news. Θέματα σχετικά με το ίδιο το Usenet.

rec. Ψυχαγωγία.

sci. Επιστήμες.

soc. Κοινωνικά θέματα.

Για να έχει κάποιος πρόσβαση στην υπηρεσία Usenet, θα χρειαστεί το λεγόμενο πρόγραμμα ανάγνωσης ειδήσεων[27]. Υπάρχουν τόσο δωρεάν[28] προγράμματα ανάγνωσης όσο και κάποια επί πληρωμή πακέτα. Τα προγράμματα προτείνουν διάφορους τρόπους οργάνωσης των ομάδων συζήτησης που συμμετέχει κάποιος και επιτρέπουν την εγγραφή σε ομάδες συζητήσεων. Αυτό σημαίνει ότι νέα μηνύματα θα παραδίδονται αυτόματα όταν χρήστης κάνει σύνδεση με τον server Για να συνδεθούμε σε μια ομάδα ειδήσεων του Usenet, γράφουμε στη γραμμή διεύθυνσης το πρόθεμα news: και μετά τον τίτλο της ομάδας ειδήσεων που μας ενδιαφέρει, π.χ news:comp.Στη συνέχεια θα ανοίξει το παράθυρο μηνυμάτων και μετά από λίγο θα εμφανισθούν τα μηνύματα αυτής της ομάδας ειδήσεων, όπου σε κάθε μήνυμα βλέπουμε τον τίτλο του (Subject), τον αποστολέα (Sender) και την ημερομηνία αποστολής (Date).

Συζητήσεις πραγματικού χρόνου (Internet Real Chat)

[26] Το USENET δημιουργήθηκε από δύο αποφοίτους του Duke University τον Tom Truscott και τον Jim Ellis.Το λογισμικό που ανέπτυξαν δίνει τη δυνατότητα ανταλλαγής μηνυμάτων μεταξύ χρηστών διαφορετικών υπολογιστών, βλ: ό.π.,Mark Gibbs & Richard Smith, Ταξιδεύοντας στο Internet, έκδοση Deluxe,μ.τ.φ Λ. Γατσώρης, Κ. Μπενέκος,εκδ. Anubis.

[27] Ένα τέτοιο πρόγραμμα είναι το TweakNews βλ: http://www.tweaknews.gr/?page=home

[28] Ένα δημοφιλές πρόγραμμα ελεύθερο για την ανάγνωση άρθρων στο Usenet είναι το Free Agent,βλ: http://free-agent.en.softonic.com.

Το **IRC**[29] (**I**nternet **R**elay **C**hat) είναι μια υπηρεσία μέσω της οποίας, σε πραγματικό χρόνο (Real Time), μπορεί κάποιος χρήστης να επικοινωνήσει με άλλους χρήστες από όλο τον κόσμο. Όπως και σε άλλες υπηρεσίες του Internet, το IRC είναι μια εφαρμογή client/server. Για να μπορέσει κάποιος να χρησιμοποιήσει την υπηρεσία θα πρέπει να τρέχει ένα client[30] πρόγραμμα για το IRC και στη συνέχεια να συνδέεται σε ένα IRC Server. Υπάρχουν servers (IRC Servers), στους οποίους μπορεί να συνδεθεί κάποιος[31] προκειμένου να κάνει χρήση αυτής της υπηρεσίας του Internet. Μέσα στους servers υπάρχουν διάφορα κανάλια[32] (chat rooms), στα οποία μπορούν να συνδεθούν χρήστες που θέλουν να επικοινωνήσουν μεταξύ τους. Εκτός απ' τα κανάλια, μπορεί να γίνει chat σε επίπεδο χρήστη με χρήστη. Για την σύνδεση σε έναν chat server, χρειάζεται ένας φυλλομετρητής ιστού (π.χ Internet Explorer) και η επίσκεψη σε κάποια σελίδα που παρέχει αυτή τη δυνατότητα (web chat) είτε κάποιο πρόγραμμα για IRC. Δημοφιλέστερα προγράμματα για IRC είναι το Mirc[33] και το Pirch[34]. Υπάρχουν πολλοί ακόμα τρόποι για συνομιλία κειμένου: MSN messenger, Google Talk, ιστοσελίδες που δίνουν απευθείας αυτή τη δυνατότητα[35].

Τηλεδιάσκεψη (Videoconference)

Τηλεδιάσκεψη (Videoconference) είναι η αμφίδρομη επικοινωνία (ήχου, εικόνας και δεδομένων) σε πραγματικό χρόνο, μεταξύ δύο ή περισσοτέρων ατόμων ή ομάδων ατόμων που βρίσκονται σε απομακρυσμένα σημεία μεταξύ τους. Η τηλεδιάσκεψη είναι ένας νέος τρόπος για την επικοινωνία με άλλους ανθρώπους. Ο κάθε χρήστης που κάνει χρήση αυτής της υπηρεσίας τοποθετείται στιγμιαία στο ίδιο δωμάτιο με ένα άλλο χρήστη ή ομάδα χρηστών που ουσιαστικά βρίσκεται οπουδήποτε στον κόσμο. Αρχικά, η τηλεδιάσκεψη μοιάζει σαν να μιλάει ο χρήστης στην οθόνη του υπολογιστή του. Όμως μέσα σε λίγα λεπτά η οθόνη "εξαφανίζεται" και μιλάει σε ένα πραγματικό άτομο.

Μερικά συστήματα είναι σχεδιασμένα για χρήση από μια ομάδα ατόμων σε μια αίθουσα συσκέψεων. Άλλα είναι για χρήση από ένα ή δύο άτομα σε ένα γραφείο. Σε κάθε περίπτωση, υπάρχει εικόνα, ήχο και η αίσθηση ότι ο χρήστης βρίσκεται μαζί στο ίδιο δωμάτιο.

Υπάρχουν δυο είδη τηλεδιάσκεψης:

---

[29] Το IRC αναπτύχθηκε στα τέλη της δεκαετίας του '80 αρχικά για την αντικατάσταση του προγράμματος talk του UNIX βλ: Jerry Honeycutt & Mary Ann Pike, Πλήρης Οδηγός του Internet, 3η Αμερικάνικη έκδοση,1996 , μ.τ.φ Ε.Γκαγκάτσιου, Γκιούρδας, σελ 27.

[30] Τέτοιοι IRC Clients είναι :Microsoft Chat, Pirch32, Active Worlds Browser, VIRC96, Lol Chat, Orbit IRC, At Chat, Netpopup, MIRC 32-Bit, Internet Telecafe, FIRC96**.**

[31] Κάθε χρήστης που συνδέεται σε έναν irc server επιλέγει ένα ψευδώνυμο (nickname), με το οποίο εμφανίζεται και στους υπόλοιπους χρήστες**.**

[32] Τα κανάλια συζητήσεων είναι εικονικά κανάλια, όπου συνδέονται πολλοί χρήστες με κοινά ενδιαφέροντα, που συνήθως αναφέρονται στον τίτλο του καναλιού. Στα κανάλια αυτά ό,τι γράφετε είναι ορατό από όλους τους άλλους χρήστες στο ίδιο κανάλι και μπορούν όλοι να απαντήσουν.

[33] http://greek.almeethaq.net/lv/group/view/kl26887/mIRC.htm

[34] http://pirch.en.malavida.com

[35] http://imm.demokritos.gr/publications/books/INTERNET_RELAY_CHAT%20_IRC_.pdf

☞ Επικοινωνία μεταξύ 2 απομακρυσμένων σημείων που ονομάζεται σημείο προς σημείο (point to point).

☞ Επικοινωνία μεταξύ περισσότερων των 2 σημείων που ονομάζεται πολυδιάσκεψη (multipoint) και απαιτεί χρήση εξυπηρετητή τηλεδιάσκεψης (multipoint conference unit – MCU).

Για την πραγματοποίηση τηλεδιάσκεψης μέσω διαδικτύου, απαιτείται υπολογιστής με τεχνικά χαρακτηριστικά πολυμέσων(κάρτα ήχου, μικρόφωνο, ηχεία και κάμερα), καθώς επίσης και κατάλληλο λογισμικό, το οποίο να χρησιμοποιείται από όλους τους χρήστες της συγκεκριμένης επικοινωνίας.

Καθώς οι υπηρεσίες αυτού του τύπου γίνονται όλο και πιο δημοφιλείς στο Internet τα τελευταία χρόνια, έχει αναπτυχθεί πληθώρα εργαλείων που διαφημίζουν δυνατότητες τηλεδιάσκεψης μέσω φωνής και εικόνας. Λίγα όμως από αυτά τα εργαλεία υποστηρίζουν τα ανοικτά πρωτόκολλα επικοινωνίας που εξασφαλίζουν τη συμβατότητα μεταξύ διαφορετικών προγραμμάτων κλήσης. Τέτοια διεθνώς αναγνωρισμένα πρωτόκολλα τηλεδιάσκεψης είναι το δημοφιλέστερο αυτή τη στιγμή H.323[36] και το ανερχόμενο SIP. Το πρώτο υποστηρίζεται τόσο από τον εξειδικευμένο εξοπλισμό τηλεδιάσκεψης μεγάλων κατασκευαστών (Polycom, VCON, Tandberg, κ.α.) όσο και από απλό λογισμικό όπως το NetMeeting της Microsoft που είναι εγκατεστημένο σε κάθε υπολογιστή με λειτουργικό Windows. Το δεύτερο SIP, συντομογραφία του Session Initiation Protocol (Πρωτόκολλο εκκίνησης συνόδου), είναι ένα πρωτόκολλο σηματοδοσίας τηλεφωνίας IP που χρησιμοποιείται για την πραγματοποίηση, την τροποποίηση και τον τερματισμό τηλεφωνικών κλήσεων VOIP (**Vo**ice over **IP** ή τηλεφωνία μέσω διαδικτύου).Το SIP περιγράφει την επικοινωνία που χρειάζεται για την πραγματοποίηση μιας τηλεφωνικής κλήσης. Το SIP έχει κάνει πάταγο στον κόσμο του VOIP. Το πρωτόκολλο μοιάζει με το HTTP, βασίζεται σε κείμενο και είναι πολύ ανοιχτό και ευέλικτο. Ως εκ τούτου, έχει αντικαταστήσει σε μεγάλο βαθμό το πρότυπο H323 [37].

Τηλεφωνία μέσω Διαδικτύου (Voice over IP)

Η τηλεφωνία μέσω διαδικτύου(**Vo**ice over **IP** ή VoIP) προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα πλέον και στην ουσία χωρίς κόστος. Οι συνομιλίες αυτές παραδοσιακά γίνονταν αποκλειστικά μέσω Υπολογιστή που είναι συνδεδεμένος στο Διαδίκτυο (Internet) και διαθέτει μικρόφωνο, ακουστικά και το κατάλληλο λογισμικό. Η κλήση καταλήγει σε ένα άλλο Υπολογιστή , ανάλογα εξοπλισμένο, χωρίς να υπάρχει κάποια επιπλέον χρέωση, εκτός από αυτή της πρόσβασης στο Διαδίκτυο, αφού στη συγκεκριμένη επικοινωνία δεν μεσολαβεί κάποιος παραδοσιακός φορέας τηλεπικοινωνιών (π.χ. ΟΤΕ) παρά μόνο το Διαδίκτυο.

Σήμερα υπάρχει πληθώρα εφαρμογών, συμπεριλαμβανομένων των Asterisk, Voipbuster, ICQ, MSN Messenger, Skype, Ekiga κ.ά., οι οποίες προσφέρουν τηλεφωνία μέσω διαδικτύου.

[36] Το H323 είναι ένα σχετικά παλιό πρωτόκολλο και πλέον αντικαθίσταται από το πρωτόκολλο SIP(Session Initiation Protocol) βλ: http://www.3cx.gr/voip-sip/h323.php

[37] http://noc.auth.gr/services/voice-video/conferencing

Το πιο ευρέως διαδεδομένο από τα παραπάνω είναι το Skype[38], μια εξαιρετικά δημοφιλής εφαρμογή-υπηρεσία τηλεφωνία μέσω διαδικτύου με εκατομμύρια χρήστες ανά τον κόσμο.

Απομακρυσμένη σύνδεση- Telnet (Telecommunications Network)- SSH (Secure Shell).

Το Telnet είναι μια υπηρεσία του Internet που μας επιτρέπει να συνδεόμαστε με έναν απομακρυσμένο υπολογιστή και να δουλεύουμε αλληλεπιδραστικά στον υπολογιστή αυτό χρησιμοποιώντας τα προγράμματά του σαν να είμαστε άμεσα συνδεδεμένοι μαζί του. Έτσι το δικό μας τερματικό (προσωπικός υπολογιστής), μετατρέπεται σε τερματικό του απομακρυσμένου υπολογιστή ο οποίος ανταποκρίνεται στις εντολές μας. Το Telnet βασίζεται στην αρχιτεκτονική client/server: για να χρησιμοποιήσουμε το Telnet, εκτελούμε στον υπολογιστή μας ένα πρόγραμμα πελάτη για Telnet (Telnet client), ενώ στον απομακρυσμένο υπολογιστή εκτελείται ένα πρόγραμμα που ονομάζεται εξυπηρετητής Telnet (Telnet server). Ο Telnet server είναι ένας ταυτόχρονος εξυπηρετητής που μπορεί να ανταποκριθεί σε πολλές αιτήσεις συγχρόνως, δημιουργώντας μια νέα διεργασία για κάθε νέα αίτηση. Χρησιμοποιεί τα πρωτόκολλα Telnet[39] και SSH (Secure Shell). Για να είναι δυνατή η χρήση του εξυπηρετητή Telnet από κάποιο απομακρυσμένο χρήστη, ο χρήστης θα πρέπει να έχει δικαιώματα πρόσβασης (όνομα χρήστη και συνθηματικό) στον εξυπηρετητή. Έτσι στην αρχή της σύνδεσης ο χρήστης συνδέεται με κάποιον υπολογιστή δίνοντας στοιχεία αυθεντικοποίησής του (όνομα χρήστη -username και συνθηματικό -password)[40].

Από προεπιλογή, το Telnet δεν είναι εγκατεστημένο στα Windows, αλλά μπορεί να το εγκαταστήσει κάποιος ακολουθώντας τα παρακάτω βήματα:

• Πατώντας Έναρξη, Πίνακας ελέγχου, Προγράμματα και τέλος, Ενεργοποίηση ή απενεργοποίηση των δυνατοτήτων των Windows. Αν ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό πρόσβασης ή παρέχετε την επιβεβαίωση.

• Στο παράθυρο διαλόγου Δυνατότητες των Windows, επιλέξτε το πλαίσιο ελέγχου Πρόγραμμα-πελάτης Telnet. Κάντε κλικ στο κουμπί OK. Η εγκατάσταση ενδέχεται να διαρκέσει μερικά λεπτά[41]. Υπάρχουν επίσης προγράμματα που παρέχουν τέτοιες υπηρεσίες telnet.Ένα τέτοιο πρόγραμμα είναι το TeamViewer το οποίο διατίθεται και για δωρεάν χρήση.

Ασύρματο Διαδίκτυο

[38] Για περισσότερες πληροφορίες εγκατάσταση βλέπε: http://www.skype.com/intl/en/home επίσης http://skype.greek.toggle.com/ & http://pc-news.gr/component/content/article/11/266-whatisskype.html

[39] Η διαφορά του telnet και του SSH είναι ότι το telnet δεν χρησιμοποιεί κρυπτογράφηση (στέλνει όνομα χρήστη και κωδικό σαν απλό κείμενο μέσα από το δίκτυο) με αποτέλεσμα να υπάρχει η δυνατότητα υποκλοπής από κάποιον ενδιαφερόμενο. Το πρόβλημα αυτό έρχεται να το λύσει το πρωτόκολλο SSH, Secure Shell στο οποίο τα πάντα είναι κρυπτογραφημένα.

[40] http://conta.uom.gr/conta/ekpaideysh/seminaria/M_Telecommunications/html/17/17-3.htm

[41] Για περισσότερα βλ: http://windows.microsoft.com/el-GR/windows-vista/Telnet-frequently-asked-questions

Η ανάπτυξη του Ασύρματου Πρωτοκόλλου Εφαρμογής, (**W**ireless **A**pplication **P**rotocol ,WAP) σε συνδυασμό με τη χρήση σύγχρονων τεχνολογιών, 3G, GPRS δίνουν τη δυνατότητα στους χρήστες φορητών υπολογιστών ή κινητών τηλεφώνων να έχουν ασύρματη σύνδεση στο Διαδίκτυο. Κάνοντας χρήση αυτών των υπηρεσιών που προσφέρουν οι πάροχοι κινητής τηλεφωνίας ο χρήστης μπορεί μέσα από το κινητό του τηλέφωνο να κάνει χρήση internet χρησιμοποιώντας μια σειρά υπηρεσιών όπως, περιήγηση στο Internet, αναζήτηση πληροφοριών, αποστολή- λήψη email, εκτέλεση τραπεζικών συναλλαγών[42].

Ηλεκτρονικό εμπόριο (e-commerce)

Ηλεκτρονικό Εμπόριο(electronic-commerce),ορίζεται το εμπόριο παροχής αγαθών και υπηρεσιών που πραγματοποιείται από απόσταση με ηλεκτρονικά μέσα, βασιζόμενο δηλαδή στην ηλεκτρονική μετάδοση δεδομένων, χωρίς να καθίσταται αναγκαία η φυσική παρουσία των συμβαλλομένων μερών, πωλητή - αγοραστή. Περιλαμβάνει το σύνολο των διαδικτυακών διαδικασιών: ανάπτυξης , προώθησης, πώλησης ,παράδοσης, εξυπηρέτησης και πληρωμής για προϊόντα και υπηρεσίες. Πρόκειται για κάθε είδος εμπορικής συναλλαγής μεταξύ προσώπων (φυσικών και μη) που πραγματοποιείται με χρήση ηλεκτρονικών υπολογιστών που συνδέονται μεταξύ τους σε δίκτυα μέσω τηλεφωνικών γραμμών. Η χρήση τηλεπικοινωνιακών δικτύων δίνει την δυνατότητα πραγματοποίησης συναλλαγών από μακριά, χωρίς τη φυσική παρουσία του πελάτη, και χωρίς φυσικά την ανάγκη να υπάρχει πραγματικό κατάστημα!

Για να πραγματοποιηθεί μια τέτοια συναλλαγή χρειάζεται το κατάλληλο λογισμικό το οποίο επιτρέπει την Ηλεκτρονική Ανταλλαγή Δεδομένων (**E**lectronic **D**ata **I**nterchange –**EDI**[43]) μεταξύ των δύο μερών που εμπλέκονται στη συναλλαγή.

Το ηλεκτρονικό εμπόριο μπορεί να οριστεί από τέσσερις διαφορετικές οπτικές γωνίες:
● Επιχειρήσεις: Ως εφαρμογή νέων τεχνολογιών προς την κατεύθυνση του αυτοματισμού των συναλλαγών και της ροής εργασιών.

● Υπηρεσίες: Ως μηχανισμός που έχει στόχο να ικανοποιήσει την κοινή επιθυμία προμηθευτών και πελατών για καλύτερη ποιότητα υπηρεσιών, μεγαλύτερη ταχύτητα εκτέλεσης συναλλαγών και μικρότερο κόστος.

● Απόσταση: Ως δυνατότητα αγοραπωλησίας προϊόντων και υπηρεσιών μέσω του Internet ανεξάρτητα από τη γεωγραφική απόσταση.

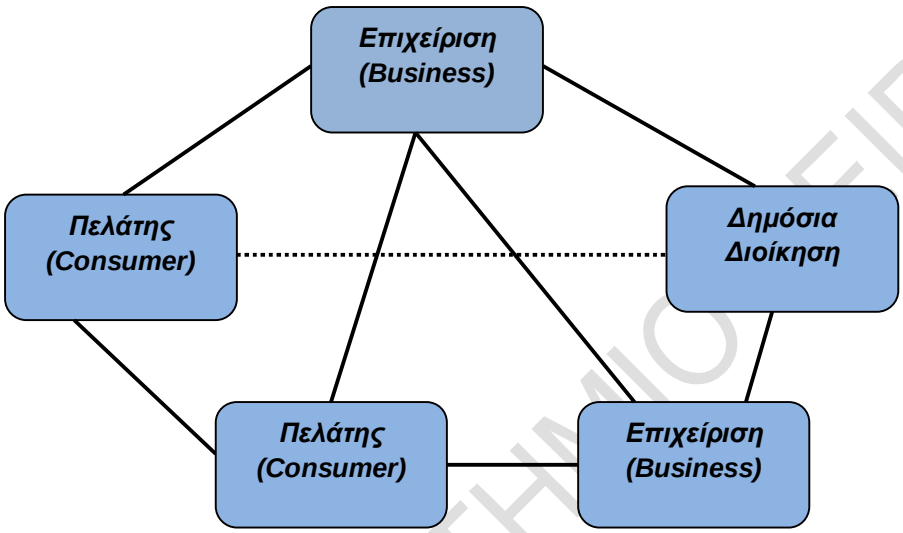
[42] Το 3G είναι η τεχνολογία που χρησιμοποιείται σε δίκτυα κινητής τηλεφωνίας για φωνή και δεδομένα, ενώ το GPRS είναι η τεχνολογία διακίνησης δεδομένων των δικτύων κινητής τηλεφωνίας 2G, για περισσότερα βλ: http://macnews.gr/forum/topic/107-%οδηγίες 3g-gprs%BD%CE%B1/.

[43] Δημιουργήθηκε στις αρχές της δεκαετίας του '70. Η EDI είναι μια κοινή δομή αρχείων που σχεδιάστηκε ώστε να επιτρέψει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσα από μεγάλα ιδιωτικά δίκτυα. Πρόκειται για την ηλεκτρονική ανταλλαγή εμπορικών και διοικητικών δεδομένων από υπολογιστή σε υπολογιστή, με την ελάχιστη παρέμβαση χειρόγραφων διαδικασιών. Τα δεδομένα αυτά είναι οργανωμένα σε αυτοτελή μηνύματα (τιμολόγια, παραγγελίες, τιμοκατάλογοι, φορτωτικές κλπ.), το περιεχόμενο και η δομή των οποίων καθορίζονται από κάποιο κοινώς αποδεκτό πρότυπο το οποίο είναι το EDIFACT (EDI For Administration, Commerce and Transportation) βλ: Ανέστης Καραυγουστής, Χρήση Νέων Τεχνολογιών στις επιχειρήσεις, ΥΠΕΠΘ-Γ.Γ.Ε.Ε.-Ι.Δ.Ε.Κ.Ε.,σελ 154.

● Επικοινωνία: Ως δυνατότητα παροχής πληροφοριών, προϊόντων ή υπηρεσιών, και πληρωμών μέσα από δίκτυα ηλεκτρονικών υπολογιστών Το εύρος των ανταλλαγών που διεξάγονται ηλεκτρονικά, έχει αυξηθεί ασυνήθιστα με την ευρεία χρήση του internet[44].

Είδη ηλεκτρονικού εμπορίου

Ανάλογα με το ποια είναι τα μέρη που πραγματοποιούν τις συναλλαγές έχουμε τις παρακάτω κατηγορίες ηλεκτρονικού εμπορίου(βλέπε σχήμα):



Σχήμα 1. Κατηγορίες ηλεκτρονικού εμπορίου

● Ηλεκτρονικό εμπόριο από επιχειρήσεις προς καταναλωτές (e-Commerce **B**usiness-**to**-**C**onsumer -**B2C**). Είναι πιο διαδεδομένη μορφή ηλεκτρονικού εμπορίου. Ο καταναλωτής μέσα από το ηλεκτρονικό κατάστημα και χωρίς να βγεί από το σπίτι του, έχει πρόσβαση σε μια τεράστια ποικιλία προϊόντων ή υπηρεσιών, τα οποία ανακαλύπτει, ενημερώνεται, συγκρίνει τιμές και αν επιθυμεί αγοράζει.

● Ηλεκτρονικό εμπόριο από επιχειρήσεις προς επιχειρήσεις (e-Commerce **B**usiness-**to**-**B**usiness - **B2B**). Οι εταιρείες χρησιμοποιούν το σύστημα **B2B** για γρηγορότερες συναλλαγές χωρίς λάθη, για έλεγχο των αποθεμάτων, αποτελεσματική αναπλήρωση των προϊόντων κ.λπ. Οι εφαρμογές **B2B** έχουν στόχο να βελτιώσουν και να απλοποιήσουν τις διάφορες επιχειρησιακές διαδικασίες μέσα σε μια εταιρεία, καθώς και να αυξήσουν την αποδοτικότητα των συναλλαγών μεταξύ εταιρειών που συνεργάζονται.

[44] Βλ: http://www.fcnet.gr/gr/overview/?id=51

.

● Ηλεκτρονικό εμπόριο από επιχειρήσεις προς κυβερνητικούς φορείς (e-Commerce **B**usiness-**to**- **G**overnment - **B2G**). Τέτοιες εφαρμογές **B2G** περιλαμβάνουν τη φορολογία, τις προμήθειες, τον τελωνειακό έλεγχο για τις εισαγωγές και εξαγωγές κ.λπ. Και αυτό γιατί το κράτος εμπλέκεται σχεδόν σε κάθε είδος επιχειρηματικής συναλλαγής καθ' όλη τη διάρκεια του εμπορικού κύκλου.

● Ηλεκτρονικό εμπόριο από καταναλωτές/πολίτες προς κυβερνητικούς φορείς (e-Commerce **C**onsumer/Citizen-**to**-**G**overnment -**C2G**). Οι εφαρμογές **C2G** περιλαμβάνουν συνήθως καταβολή φόρων, έκδοση πιστοποιητικών ή άλλων εγγράφων κ.λπ. Αν και δε μπορούμε να ορίσουμε απόλυτα τις συναλλαγές μεταξύ καταναλωτών ή πολιτών με κυβερνητικούς φορείς ως ηλεκτρονικό εμπόριο, μπορούμε να δούμε αρκετές **C2G** εφαρμογές στο πλαίσιο συναλλαγών που διεκπεραιώνονται αποτελεσματικότερα και αποδοτικότερα με τη χρήση συστημάτων και τεχνολογίας ηλεκτρονικού εμπορίου.

● Ηλεκτρονικό εμπόριο από καταναλωτές προς καταναλωτές (e-Commerce Consumer-to-Consumer - C2C): Σε αυτή την κατηγορία ο καταναλωτής πουλά απευθείας σε άλλους καταναλωτές. Παράδειγμα αποτελούν τα άτομα που κάνουν πωλήσεις μέσω καταχωρημένων αγγελιών, δικτυακών τόπων δημοπρασιών, όπου ο οποιοσδήποτε μπορεί να πουλήσει οτιδήποτε[45].

Τεχνολογίες υποστήριξης εφαρμογών ηλεκτρονικού εμπορίου

Οι εμπορικές συναλλαγές απαιτούν ασφάλεια και εμπιστευτικότητα. Στο ηλεκτρονικό εμπόριο αυτό επιτυγχάνεται με τεχνολογίες όπως:

☞ **Ψηφιακές υπογραφές**. Με την ψηφιακή υπογραφή έχουμε εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Η ψηφιακή υπογραφή έχει επιβεβαιωτική λειτουργία καθώς μας επιβεβαιώνει ότι το μήνυμα που λαμβάνει ο παραλήπτης ανήκει πράγματι στον αποστολέα και δεν έχει αλλοιωθεί,αλλά και εμπιστευτική λειτουργία, καθώς μόνο ο παραλήπτης είναι σε θέση να διαβάσει το μήνυμα και κανένας άλλος.

☞ **Επίπεδο ασφαλών συνδέσεων SSL** (Secure Socket Layer). Το πρωτόκολλο αυτό σχεδιάστηκε προκειμένου να πραγματοποιεί ασφαλή σύνδεση με τον εξυπηρετητή (server). Το SSL χρησιμοποιεί "κλειδί" δημόσιας κρυπτογράφησης, με σκοπό να προστατεύει τα δεδομένα καθώς "ταξιδεύουν" μέσα στο Internet.

☞ **Γραμμωτός κώδικας** (Barcode). Η τεχνολογία του γραμμωτού κώδικα αποτελεί τμήμα του γενικότερου τομέα των τεχνολογιών αυτόματης αναγνώρισης (Auto ID Technologies). Είναι ένα σύγχρονο εργαλείο, το οποίο βοηθά καταλυτικά στην ομαλή διακίνηση και διαχείριση (logistics) προϊόντων και υπηρεσιών.

☞ **Ασφαλείς ηλεκτρονικές συναλλαγές SET** (Secure Electronic Transactions). Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το πρότυπο αυτό, που δημιουργήθηκε από τη Visa και τη MasterCard, απολαμβάνει μεγάλης αποδοχής από την τραπεζική κοινότητα.

[45] Βλ: http://www.ea.gr/ep/agroweb/htmls/lessons/commerce1gr/12.htm

☞ **Έξυπνες Κάρτες** (Smart Cards). Έξυπνη κάρτα (smart card) είναι μια κάρτα, η οποία μοιάζει πολύ εξωτερικά με τη γνωστή πιστωτική κάρτα. Εσωτερικά, όμως, διαφέρει σημαντικά από αυτήν. Η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία(magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Οι "έξυπνες κάρτες" αποτελούν εξέλιξη των καρτών μαγνητικής λωρίδας (παθητικό μέσο αποθήκευσης, τα περιεχόμενα του οποίου μπορούν να διαβαστούν και να αλλαχθούν). Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν μεγάλη ποσότητα δεδομένων και παρέχουν δυνατότητες κρυπτογράφησης και χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια των περιεχομένων τους. Η τεχνολογία των έξυπνων καρτών προσφέρει απεριόριστες δυνατότητες χρήσης στη βιομηχανία, το εμπόριο και τη δημόσια διοίκηση[46].

1.5 Στατιστικά στοιχεία της χρήσης Διαδικτύου

Στην ενότητα αυτή παρουσιάζονται στατιστικά στοιχεία για την χρήση του Διαδικτύου στον υπόλοιπο κόσμο ,στην Ευρωπαϊκή Ένωση και στην Ελλάδα.

1.5.1 Χρήση Διαδικτύου παγκόσμια

Περίπου 2,3 δισ. άνθρωποι (32% του συνόλου) έχουν σήμερα πρόσβαση στο Διαδίκτυο σε όλο τον κόσμο, σύμφωνα με την Διεθνή Ένωση Τηλεπικοινωνιών (ITU). Εντυπωσιακή είναι η αύξηση που καταγράφει η χρήση του Διαδικτύου κυρίως στις αναπτυσσόμενες χώρες, όπως στην Αφρική που την περίοδο 2000-2011 καταγράφεται αύξηση 2.988% , Μέση Ανατολή με αύξηση 2.244% , Λατινική Αμερική με αύξηση 1.205% , Ασία με αύξηση 790% . Η ανάπτυξη του Ίντερνετ είναι ταχύτερη μεταξύ των νέων ηλικιακά ανθρώπων, με σχεδόν το μισό του online παγκόσμιου πληθυσμού να είναι κάτω των 25 ετών. Ο αριθμός αυτός αναμένεται να παρουσιάσει σταθερή αύξηση, καθώς η διείσδυση του Διαδικτύου εξακολουθεί να αναπτύσσεται στα σχολεία, σύμφωνα με την ITU. Ωστόσο, παρουσιάζονται χαοτικές ανισότητες[47] μεταξύ των κατοίκων διαφόρων περιοχών του πλανήτη, καθώς αρκετοί είναι αναγκασμένοι να συνδέονται με πολύ χαμηλές ταχύτητες, ενώ άλλοι δεν έχουν καθόλου πρόσβαση στο internet[48].

Για το λόγο αυτό αναπτύσσονται πρωτοβουλίες σε Διεθνές επίπεδο από επιστήμονες και ερευνητικούς φορείς με στόχο την εξάπλωση του Διαδικτύου σε περιοχές που το στερούνται.

---

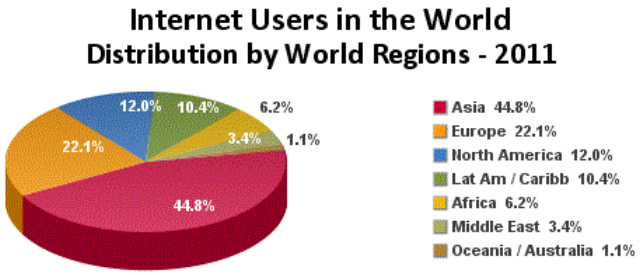
[46] Βλ: Ανέστης Καραυγουστής,ό.π., Χρήση Νέων Τεχνολογιών στις επιχειρήσεις, ΥΠΕΠΘ-Γ.Γ.Ε.Ε.-Ι.Δ.Ε.Κ.Ε.,σελ 159.

[47] Για παράδειγμα οι Ευρωπαίοι απολαμβάνουν το προνόμιο να έχουν στη διάθεσή τους προηγμένες ευρυζωνικές υπηρεσίες, γεγονός που σημαίνει ότι μπορούν να σερφάρουν στο Διαδίκτυο με πολύ μεγάλες ταχύτητες, ενώ οι κάτοικοι της Αφρικής αρκούνται σε πολύ πιο αργές ταχύτητες, βλ. δημοσίευμα εφημερίδας «Νέα», Παγκόσμιος πληθυσμός internet, 26/10/2011 στο: http://www.tanea.gr/kosmos/article/?aid=4668312.

[48] Σύμφωνα με στατιστικά δεδομένα που δημοσιεύτηκαν στο internetworldstats,Χρήση του Διαδικτύου του Παγκόσμιου Πληθυσμού μέχρι την 31η Δεκεμβρίου 2011 βλ: http://www.internetworldstats.com/stats.htm, βλ. επίσης: δημοσίευμα εφημερίδας «Νέα», Παγκόσμιος πληθυσμός internet, 26/10/2011 στο: http://www.tanea.gr/kosmos/article/?aid=4668312.

Μία από αυτές είναι το ahumanright.org[49], το οποίο ίδρυσε ο Ελληνοαμερικανός Κώστας Γραμμάτης, ερευνητής στο Εργαστήριο Πολυμέσων του Τεχνολογικού Ινστιτούτου της Μασαχουσέτης (MIT Media Lab).

Οι περισσότεροι χρήστες του internet βρίσκονται στην Ασία (περίπου οι μισοί ή το 44,8% του πίνακα) με χαμηλή σχετικά διείσδυση στον πληθυσμό (26,2%) και ανάπτυξη 789,6% την δεκαετία 2000-2011.Στη συνέχεια έρχεται η Ευρώπη με χρήστες που αντιπροσωπεύουν το 22,1% του πίνακα , μεγάλη διείσδυση στον πληθυσμό (61,3%) και ανάπτυξη 376,4% την δεκαετία 2000-2011.Την μεγαλύτερη πάντως διείσδυση στον πληθυσμό έχει η βόρεια Αμερική (78,6%) αντιπροσωπεύοντας το 12% του πίνακα, βλ. πίνακα.



ΠΑΓΚΟΣΜΙΑ χρήση του Διαδικτύου και στατιστικές πληθυσμών
31 Δεκέμβρη του 2011

Περιοχές του κόσμου	Πληθυσμός (2011 τεμ.)	Οι χρήστες του Internet 31 του Δεκέμβρη 2000	Οι χρήστες του Internet Τελευταία δεδομένα	Διείσδυση (Πληθυσμός%)	Ανάπτυξη 2000-2011	Χρήστες% του πίνακα
Αφρική	1.037.524.058	4.514.400	139.875.242	13,5%	2,988.4%	6,2%
Ασία	3.879.740.877	114.304.000	1.016.799.076	26,2%	789,6%	44,8%
Ευρώπη	816.426.346	105.096.093	500.723.686	61,3%	376,4%	22,1%
Μέση Ανατολή	216.258.843	3.284.800	77.020.995	35,6%	2,244.8%	3,4%
Βόρεια Αμερική	347.394.870	108.096.800	273.067.546	78,6%	152,6%	12,0%
Λατινική Αμερική / Καραϊβική και Ειρηνικός.	597.283.165	18.068.919	235.819.740	39,5%	1,205.1%	10,4%
Ωκεανία / Αυστραλία	35.426.995	7.620.480	23.927.457	67,5%	214,0%	1,1%
ΣΥΝΟΛΟ ΚΟΣΜΟΥ	6.930.055.154	360.985.492	2.267.233.742	32,7%	528,1%	100,0%

Πίνακας 3. Στατιστικά χρήσης Διαδικτύου παγκόσμια
Πηγή: http://www.internetworldstats.com/stats.htm

1.5.2 Χρήση Διαδικτύου στην Ευρώπη

Σύμφωνα με έρευνα της Mediascope Europe[50] , 426,9 εκ. Ευρωπαίοι μπαίνουν στο Internet κάθε βδομάδα (65%) με περισσότερους από το 1/3 αυτών (37%) να συνδέονται

[49] Το ahumanright.org δημιουργήθηκε με σκοπό να προωθήσει «τη δίκαιη και ίση πρόσβαση στο Ίντερνετ» και να βρει τη λύση που θα επιτρέπει σε όλους τους ανθρώπους να δικτυωθούν.Βλ: http://www.ahumanright.org

[50] Πανευρωπαϊκή έρευνα κατανάλωσης μέσων βλ στο: http://www.iabeurope.eu/research/mediascope-europe.aspx

χρησιμοποιώντας περισσότερες από μία συσκευές. Το 64% συνδέεται μέσω υπολογιστή (415,7 εκ.) και το 21% μέσω κινητού τηλεφώνου (139,2 εκ.). Η χρήση του διαδικτύου μέσω υπολογιστή είναι πιο δημοφιλής στη Νορβηγία και την Ελβετία (89%) και οι χρήστες είναι μεταξύ 25 – 44 ετών (44%). Οι mobile χρήστες είναι μεταξύ 16 – 24 ετών (30%), ενώ η χρήση του διαδικτύου μέσω κινητού τηλεφώνου είναι πιο δημοφιλής στη Μεγάλη Βρετανία, τη Νορβηγία και τη Σουηδία, όπου περισσότεροι από 4 στους 10 χρήστες συνδέονται μέσω κινητού.

Ο χρόνος που δαπανάται στο Internet διαφοροποιείται ανάλογα με την συσκευή που χρησιμοποιείται. Οι Ευρωπαίοι καταναλώνουν συνολικά 14,8 ώρες την εβδομάδα online. Εκείνοι που χρησιμοποιούν υπολογιστή καταναλώνουν κατά μέσο όρο 13,3 ώρες online, όσοι συνδέονται μέσω κινητού τηλεφώνου 9,4 ώρες ενώ όσοι συνδέονται μέσω tablets 9,3 ώρες την εβδομάδα. Για όσους συνδέονται μέσω παιχνιδοκονσόλας, οι ώρες ανέρχονται κατά μέσο όρο σε 6,8 την εβδομάδα. Τα σκήπτρα κατέχει η Βόρεια Ευρώπη με 86% πρόσβαση στο internet μέσω Η/Υ και 36% πρόσβαση στο internet μέσω κινητού τηλεφώνου, ακολουθεί η Δυτική Ευρώπη με 79% πρόσβαση στο internet μέσω Η/Υ και 31% πρόσβαση στο internet μέσω κινητού τηλεφώνου, έπεται η Νότια Ευρώπη με 59% πρόσβαση στο internet μέσω Η/Υ και 19% πρόσβαση στο internet μέσω κινητού τηλεφώνου και στην τελευταία θέση βρίσκεται η Κεντρική & Ανατολική Ευρώπη με 53% πρόσβαση στο internet μέσω Η/Υ και 14% πρόσβαση στο internet μέσω κινητού τηλεφώνου (Βλέπε πίνακα 4).

	% Πρόσβαση στο internet μέσω Η/Υ	% Πρόσβαση στο internet μέσω κινητού τηλεφώνου
Βόρεια Ευρώπη	86%	36%
Δυτική Ευρώπη	79%	31%
Νότια Ευρώπη	59%	19%
Κεντρική & Ανατολική Ευρώπη	53%	14%
Ευρωπαϊκός Μ.Ο	64%	21%

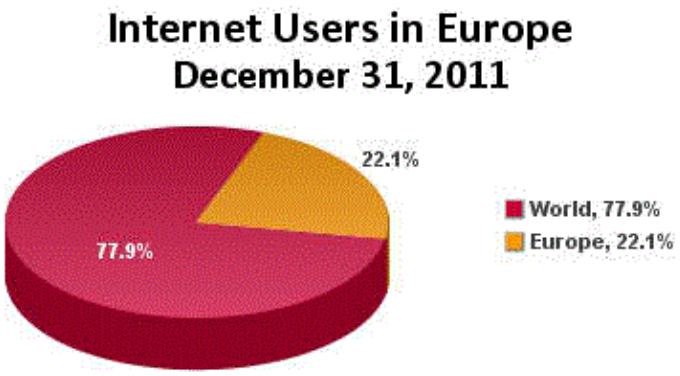
Πίνακας 4.Στατιστικά πρόσβασης στο Διαδίκτυο στην Ευρώπη Πηγή: Mediascope Europe 2012

Αυτό που ξεχωρίζει σε αυτή την έρευνα της Mediascope είναι το ποσοστό των «παραδοσιακών» μέσων που πλέον καταναλώνεται online μέσω Διαδικτύου(Εφημερίδες, Τηλεόραση, Ραδιόφωνο). Έτσι το 91% των χρηστών Internet ενημερώνεται online για τις ειδήσεις με πιο πιθανές τις ηλικίες 35-54 (93%) , το 73% των χρηστών Internet παρακολουθούν τηλεόραση online με πιο πιθανές τις ηλικίες 16-24 (83%) και τις ηλικίες 35-44 (81%), το 67% των χρηστών Internet ακούν ραδιόφωνο μέσω internet με πιο πιθανές τις ηλικίες 16-24 (81%) (βλ. πίνακα 5).

	Διαβάζουν νέα online	**Βλέπουν τηλεόραση online**	**Ακούνε ραδιόφωνο online**
16-24	89%	83%	81%
25-34	92%	70%	67%
35-44	93%	81%	78%
45-54	93%	70%	60%
55 +	90%	67%	57%
Άνδρες	93%	73%	68%
Γυναίκες	89%	74%	66%
Σύνολο Ευρώπης	***91%***	***73%***	***67%***

Πίνακας 5. Χρήση μέσων ενημέρωσης στο internet Πηγή: Mediascope Europe 2012

Οι χρήστες του Διαδικτύου στην Ευρώπη είναι 500.723.686 (ποσοστό 22,1% του πίνακα) , περίπου οι μισοί από αυτούς (232.935.740) έχουν facebook και η διείσδυση στον πληθυσμό είναι πολύ μεγάλη (61,3%).



Διαδίκτυο και το Facebook Χρήση στην Ευρώπη

ΕΥΡΩΠΗ	Πληθυσμός (2011 τεμ.)	Ποπ%. της Παγκόσμιας	Χρήστες του Διαδικτύου, 31-Δεκ-11	Διείσδυση (Πληθυσμός%)	Χρήστες Κόσμος%	Facebook 31-Μαρ-12
Ευρώπη	816.426.346	11,8%	500.723.686	61,3%	22,1%	232.935.740
Υπόλοιπος κόσμος	6.113.628.808	88,2%	1.766.510.056	28,9%	77,9%	602.589.540
ΣΥΝΟΛΟ ΚΟΣΜΟΥ	6.930.055.154	100,0%	2.267.233.742	32,7%	100,0%	835.525.280

Πίνακας 6. Στατιστικά χρήσης Διαδικτύου Ευρώπη
Πηγή: http://www.internetworldstats.com/stats.htm

Οι χώρες με τους περισσότερους χρήστες είναι κατά σειρά η Γερμανία με 13,5% του πίνακα και διείσδυση στον πληθυσμό 82,7%, ακολουθούν η Ρωσία με 12,3% του πίνακα και διείσδυση στον πληθυσμό 44,3%, η Μεγάλη Βρετανία με 10,5% του πίνακα και διείσδυση στον πληθυσμό 84,1%, η Γαλλία με 10,0% του πίνακα και διείσδυση στον πληθυσμό 77,2%, η Τουρκία με 7,3% του πίνακα και διείσδυση στον πληθυσμό 44,4%, η Ιταλία με 7,1% του πίνακα και διείσδυση στον πληθυσμό 58,7% και η Ισπανία με 6,1% του πίνακα και διείσδυση στον πληθυσμό 65,6%. Η Ελλάδα αντιπροσωπεύει το 1,0% του πίνακα με διείσδυση στον πληθυσμό 46,9%, βλ πίνακα 7, με αναλυτικά στοιχεία για κάθε χώρα.

Internet and Facebook Usage in Europe

EUROPE	Population (2011 Est.)	Internet Users, 31-Dec-11	Penetration (% Population)	Users % in Europe	Facebook 31-Mar-12
Albania	2,994,667	1,441,928	48.1 %	0.3 %	1,060,760
Andorra	84,825	68,740	81.0 %	0.0 %	36,760
Austria	8,217,280	6,143,600	74.8 %	1.3 %	2,766,540
Belarus	9,577,552	4,436,800	46.3 %	0.9 %	409,120
Belgium	10,431,477	8,489,901	81.4 %	1.7 %	4,634,220
Bosnia-Herzegovina	4,622,163	1,955,277	42.3 %	0.4 %	1,268,560
Bulgaria	7,093,635	3,464,287	48.8 %	0.7 %	2,386,800
Croatia	4,483,804	2,656,089	59.2 %	0.5 %	1,452,300
Cyprus	1,120,489	584,863	52.2%	0.1 %	553,860
Czech Republic	10,190,213	7,220,732	70.9 %	1.4 %	3,502,420
Denmark	5,529,888	4,923,824	89.0 %	1.0 %	2,835,120
Estonia	1,282,963	993,785	77.5 %	0.2 %	447,620
Faroe Islands	49,267	37,500	76.1 %	0.0 %	29,880
Finland	5,259,250	4,661,265	88.6 %	0.9 %	2,078,880
France	65,102,719	50,290,226	77.2 %	10.0 %	23,544,460
Germany	81,471,834	67,364,898	82.7 %	13.5 %	22,123,660
Gibraltar	28,956	20,200	69.8 %	0.0 %	18,800
Greece	10,760,136	5,043,550	46.9 %	1.0 %	3,562,120
Guernsey & Alderney	65,068	48,300	74.2 %	0.0 %	440
Hungary	9,976,062	6,516,627	65.3 %	1.3 %	3,751,300
Iceland	311,058	304,129	97.8 %	0.1 %	210,220
Ireland	4,670,976	3,122,358	66.8 %	0.6 %	2,093,960

Internet and Facebook Usage in Europe					
EUROPE	Population (2011 Est.)	Internet Users, 31-Dec-11	Penetration (% Population)	Users % in Europe	Facebook 31-Mar-12
Italy	61,016,804	35,800,000	58.7 %	7.1 %	20,889,260
Jersey	94,161	45,800	48.6 %	0.0 %	820
Kosovo	1,825,632	377,000	20.7 %	0.1 %	n/a
Latvia	2,204,708	1,540,859	69.9 %	0.3 %	319,300
Liechtenstein	35,236	28,826	81.8 %	0.0 %	11,880
Lithuania	3,535,547	2,103,471	59.5 %	0.4 %	983,440
Luxembourg	503,302	459,833	91.4 %	0.1 %	190,020
Macedonia	2,077,328	1,069,432	51.5 %	0.2 %	879,540
Malta	408,333	262,404	64.3 %	0.1 %	191,940
Man, Isle of	84,655	35,600	42.1 %	0.0 %	30,660
Moldova	4,314,377	1,429,154	33.1 %	0.3 %	221,220
Monaco	30,539	23,000	75.3 %	0.0 %	36,800
Montenegro	661,807	328,375	49.6 %	0.1 %	292,700
Netherlands	16,847,007	15,071,191	89.5 %	3.0 %	5,759,840
Norway	4,691,849	4,560,572	97.2 %	0.9 %	2,561,820
Poland	38,441,588	23,852,486	62.0 %	4.8 %	7,524,220
Portugal	10,760,305	5,455,217	50.7 %	1.1 %	4,174,000
Romania	21,904,551	8,578,484	39.2 %	1.7 %	4,161,340
Russia	138,739,892	61,472,011	44.3 %	12.3 %	5,237,420
San Marino	31,817	17,000	53.4 %	0.0 %	8,240
Serbia	7,310,555	4,107,000	56.2 %	0.8 %	3,173,440
Slovakia	5,477,038	4,337,868	79.2 %	0.9 %	1,889,160
Slovenia	2,000,092	1,420,776	71.0 %	0.3 %	670,660
Spain	46,754,784	30,654,678	65.6 %	6.1 %	15,682,800
Sweden	9,088,728	8,441,718	92.9 %	1.7 %	4,519,780
Switzerland	7,639,961	6,430,363	84.2 %	1.3 %	2,727,600
Turkey	78,785,548	35,000,000	44.4 %	7.3 %	30,963,100
Ukraine	45,134,707	15,300,000	33.9 %	3.1 %	1,686,500
United Kingdom	62,698,362	52,731,209	84.1 %	10.5 %	30,470,400
Vatican City State	832	480	57.7 %	0.0 %	20
TOTAL Europe	816,426,346	500,723,686	61.3 %	100.0 %	235,525,280

Πίνακας 7. Χρήστες Internet και Facebook στις Χώρες της Ευρώπης
Πηγή : http://www.internetworldstats.com/stats4.htm#europe

1.5.3 **Χρήση Διαδικτύου στην Ελλάδα**

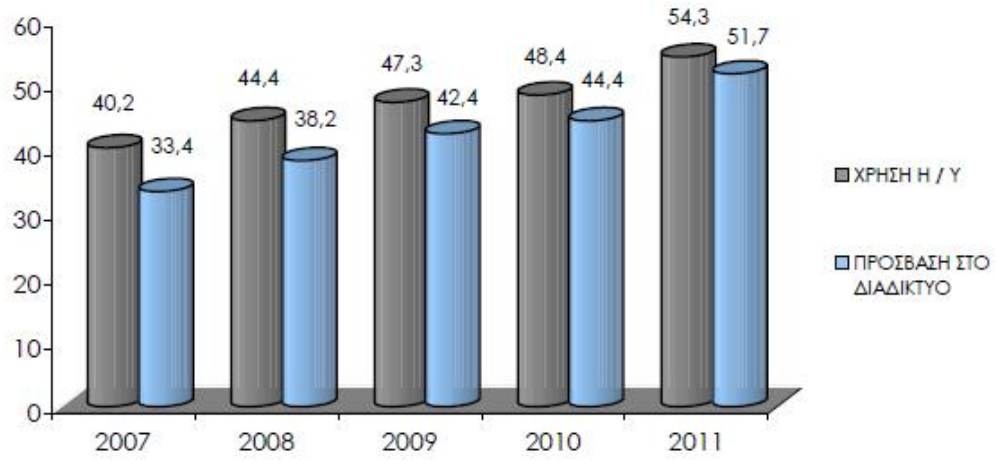
Η άποψη πως το Διαδίκτυο είναι μέρος της καθημερινής μας ζωής με αυξητικές τάσεις,- αλλά ακόμη αρκετά μακριά από τον ευρωπαϊκό μέσο όρο, επιβεβαιώνεται και από τα στατιστικά στοιχεία που δίνουν διάφοροι φορείς, όπως η ελληνική στατιστική υπηρεσία (ΕΛΣΤΑΤ), έρευνα της οποίας[51] θα παρουσιάσουμε στη συνέχεια :

Χρήση Ηλεκτρονικού Υπολογιστή και πρόσβαση στο Διαδίκτυο

Η ανοδική τάση των τελευταίων ετών συνεχίζεται, τόσο στη χρήση ηλεκτρονικού υπολογιστή όσο και στην πρόσβαση στο διαδίκτυο. Έτσι το Α΄ τρίμηνο του 2011, το ποσοστό των ατόμων που χρησιμοποίησαν ηλεκτρονικό υπολογιστή[52] ανέρχεται στο 54,3% και το ποσοστό των ατόμων που χρησιμοποίησαν το διαδίκτυο στο 51,7%. Την τελευταία πενταετία (2007 – 2011) η αύξηση που παρατηρείται ανέρχεται σε:

• 35,1% για χρήση ηλεκτρονικού υπολογιστή

• 54,8% για πρόσβαση στο διαδίκτυο



Σχήμα 2. Χρήση Η/Υ και πρόσβαση στο Διαδίκτυο Α΄ τρίμηνο ετών 2007-2011(% ατόμων) Πηγή : http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

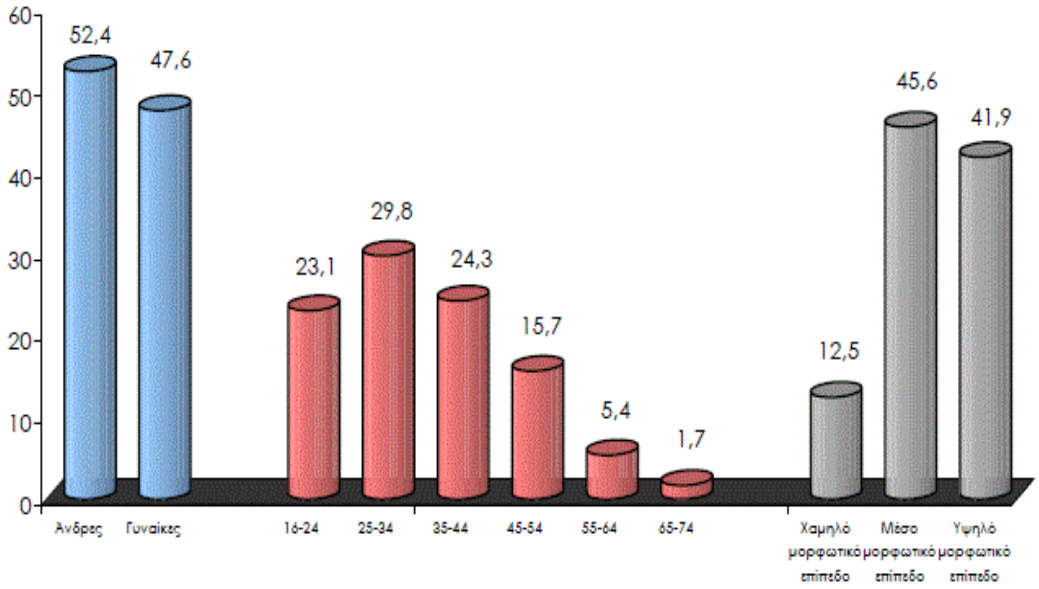
[51] Η έρευνα αναφέρεται στη χρήση τεχνολογιών πληροφόρησης και επικοινωνίας από τα νοικοκυριά για το έτος 2011
Βλ δελτίο τύπου ΕΛΣΤΑΤ, 13/6/2012 στο:
http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

[52] Η χρήση ηλεκτρονικού υπολογιστή ή και διαδικτύου μπορεί να έχει πραγματοποιηθεί από όλους τους χώρους πρόσβασης, δηλαδή κατοικία, χώρο εργασίας, χώρο εκπαίδευσης, γειτονικά, φιλικά ή συγγενικά σπίτια, ξενοδοχεία, internet cafés κλπ βλ. ό.π: έρευνα χρήσης τεχνολογιών πληροφόρησης και επικοινωνίας από τα νοικοκυριά έτους 2011 της ΕΛΣΤΑΤ στο:
http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

Προφίλ χρηστών διαδικτύου

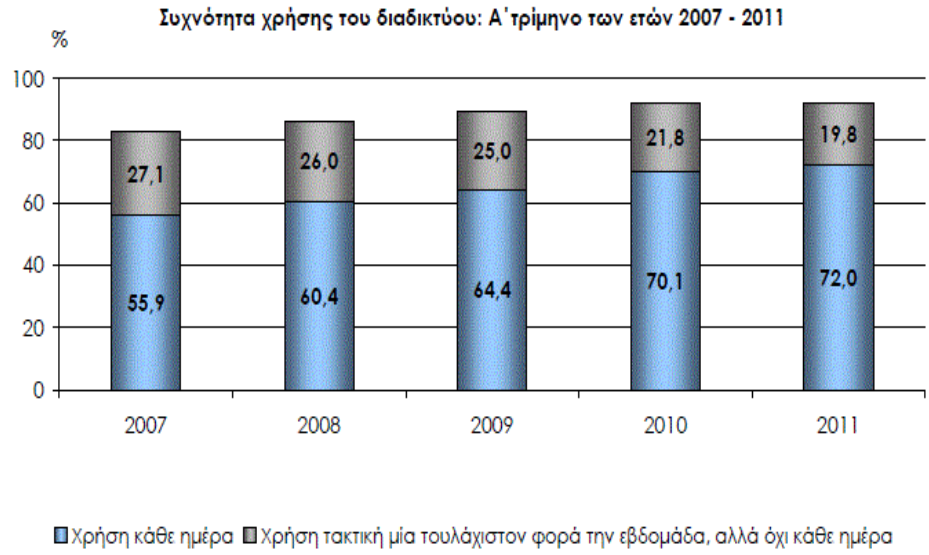
Σύμφωνα με τα αποτελέσματα της έρευνας, οι άνδρες χρησιμοποιούν περισσότερο το διαδίκτυο (52,4%) από ότι οι γυναίκες (47,6%). Αναφορικά με την ηλικία, οι περισσότεροι χρήστες του διαδικτύου (29,8%) ανήκουν στην ηλικιακή ομάδα 25-34 ετών ενώ το 15,7% στην ηλικιακή ομάδα 45-54 ετών και το 7,1% στην ηλικιακή ομάδα 55-74 ετών.

Όσον αφορά στο μορφωτικό επίπεδο, οι χρήστες μέσου μορφωτικού επιπέδου (απόφοιτοι δευτεροβάθμιας εκπαίδευσης και Ινστιτούτων Επαγγελματικής Κατάρτισης) είναι οι περισσότεροι με ποσοστό 45,6% ενώ οι χρήστες χαμηλού μορφωτικού επιπέδου (απόφοιτοι πρωτοβάθμιας εκπαίδευσης και γυμνασίου / κατώτερων τεχνικών σχολών) αποτελούν το 12,5% του συνόλου των χρηστών του διαδικτύου.



Σχήμα 3. Χρήση Διαδικτύου κατά φύλο , ηλικία και μορφωτικό επίπεδο(% ατόμων) Πηγή : http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

Συχνότητα χρήσης Διαδικτύου: Το Α΄ τρίμηνο του 2011, το 72,0% όσων χρησιμοποίησαν το διαδίκτυο έκανε καθημερινή χρήση του διαδικτύου, ποσοστό ελαφρά υψηλότερο από το αντίστοιχο ποσοστό του έτους 2010, ενώ το 91,8% έκανε τακτική χρήση, τουλάχιστον μία φορά την εβδομάδα, αλλά όχι κάθε ημέρα. Διαχρονικά, η εικόνα των τακτικών και καθημερινών χρηστών του διαδικτύου απεικονίζεται στο γράφημα που ακολουθεί:



Σχήμα 4. Συχνότητα χρήσης Διαδικτύου κατά φύλο , ηλικία και μορφωτικό επίπεδο(% ατόμων)
Πηγή : http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

Λόγοι χρήσης του διαδικτύου: Η αναζήτηση πληροφοριών και υπηρεσιών βρίσκεται στην κορυφή της λίστας των δραστηριοτήτων που πραγματοποιούνται μέσω διαδικτύου με ποσοστό 74,9%, ενώ το ποσοστό που καταγράφεται για όσους διάβασαν online ή «κατέβασαν» εφημερίδες και περιοδικά –δεύτερη περισσότερο πραγματοποιούμενη δραστηριότητα– είναι 72,9%. Αναλυτικά τα ποσοστά που καταγράφηκαν για την κάθε δραστηριότητα, κατά αύξουσα σειρά για το 2011, παρουσιάζονται στον πίνακα 8 που ακολουθεί:

Α/Α	ΔΡΑΣΤΗΡΙΟΤΗΤΑ	2010	2011	Μεταβολή % 2011/2010
1	Αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες	80,8	74,9	-7,3
2	Διάβασμα on-line ή «κατέβασμα» εφημερίδων και περιοδικών	57,2	72,9	27,5
3	Αναζήτηση πληροφοριών υγείας σχετικά με ασθένειες, διατροφή, κακώσεις, παράγοντες που βελτιώνουν την υγεία	50,1	58,5	16,8
4	Συμμετοχή σε ιστοσελίδες κοινωνικής δικτύωσης (δημιουργία προφίλ χρήστη, αποστολή μηνυμάτων κ.ά. στο Facebook, στο Twitter κλπ.)	46,9	54,3	15,8

5	Χρήση ηλεκτρονικών εγκυκλοπαιδειών (wikis) με σκοπό τη γνώση, για οποιοδήποτε θέμα	μ.δ. [53]	51,8	-
6	Χρήση υπηρεσιών για ταξίδια και καταλύματα	57,1	51,4	-10,0
7	Αναζήτηση πληροφοριών για επίσημη βαθμίδα εκπ/σης, για προσφορά εκπαιδευτικών προγραμμάτων κ.ά.	27,6	39,3	42,4
8	Πραγματοποίηση τηλεφωνικής κλήσης ή βιντεοκλήσης μέσω διαδικτύου	21,5	31,8	47,9
9	Διάβασμα και αποστολή γνώμης σε ιστοσελίδες για θέματα κοινωνικά ή πολιτικά	μ.δ. [41]	28,8	-
10	«Κατέβασμα» λογισμικού (εξαιρουμένου λογισμικού για παιχνίδια)	22,0	26,2	19,1
11	Αναζήτηση εργασίας ή αποστολή αιτήσεων για εύρεση εργασίας	13,7	25,0	82,5
12	Πραγματοποίηση τραπεζικών συναλλαγών	12,8	16,6	29,7
13	Συμμετοχή σε online διαβουλεύσεις ή ψηφοφορίες για τον καθορισμό κοινωνικών ή πολιτικών θεμάτων	μ.δ. [41]	9,6	-
14	Συμμετοχή σε online εκπαιδευτικά προγράμματα	4,7	8,6	83,0
15	Συμμετοχή σε ιστοσελίδες επαγγελματικής δικτύωσης	μ.δ. [41]	7,3	-
16	Πώληση αγαθών ή υπηρεσιών (e-Bay)	1,3	4,5	246,2

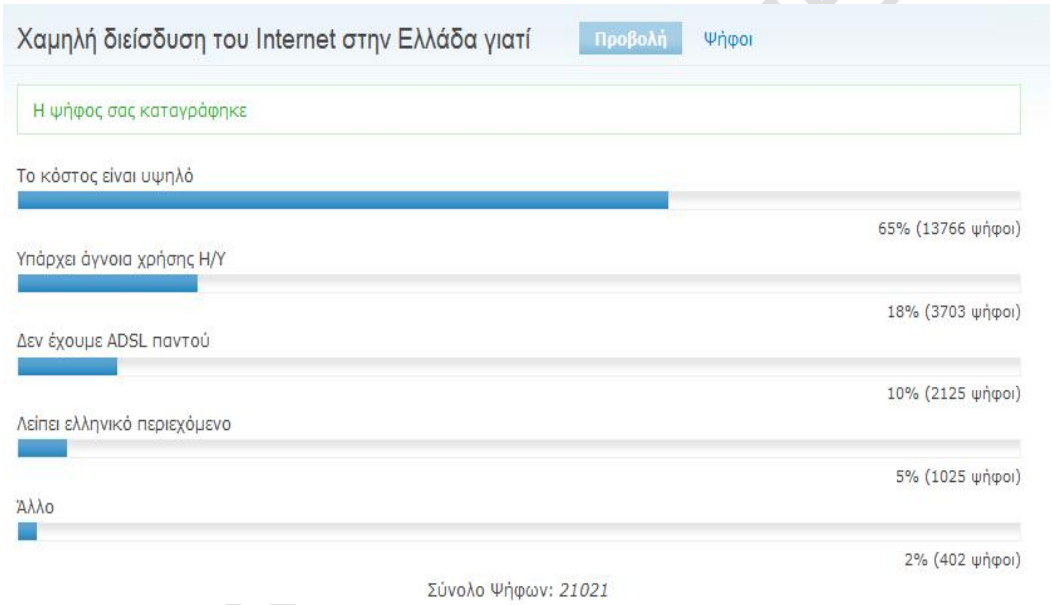
Πίνακας 8. Λόγοι χρήσης Διαδικτύου
Πηγή : http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

Συμπερασματικά για όλες σχεδόν τις δραστηριότητες καταγράφηκε αύξηση σε σχέση με το 2010. Μεγαλύτερη αύξηση (246,2%), έχει καταγραφεί για την πώληση αγαθών και υπηρεσιών (στο e-Bay κλπ.). Πολύ μεγάλες αυξήσεις επίσης καταγράφηκαν στη συμμετοχή σε online εκπαιδευτικά προγράμματα (83%) και στην αναζήτηση ή αποστολή αιτήσεων για εύρεση εργασίας (82,5%). Μεγάλες αυξήσεις, παρατηρούνται στην πραγματοποίηση τηλεφωνικών κλήσεων ή βιντεοκλήσεων μέσω διαδικτύου (47,9%), καθώς και στην αναζήτηση πληροφοριών για επίσημη βαθμίδα εκπαίδευσης, για προσφορά εκπαιδευτικών προγραμμάτων κ.ά. (42,4%). Αύξηση κατά 15,8% παρουσιάζει η συμμετοχή σε ιστοσελίδες κοινωνικής δικτύωσης (δημιουργία προφίλ χρήστη, αποστολή μηνυμάτων κ.ά. στο Facebook, στο Twitter κλπ.) ενώ

[53] μ.δ. Μη διαθέσιμη πληροφορία από την έρευνα του 2010.

αξίζει να σημειωθεί ότι η ηλικιακή ομάδα 25 – 34 ετών είναι αυτή που, κυρίως, επιδίδεται στην εν λόγω δραστηριότητα (35,9%)[54].

Βαθμός διείσδυσης του Διαδικτύου: Σχεδόν 1 στα 2 ελληνικά νοικοκυριά διαθέτει σύνδεση στο Διαδίκτυο. Δυναμικότεροι χρήστες του διαδικτύου αναδεικνύονται οι άνδρες, οι νέοι ηλικίας 16-24 ετών, τα άτομα υψηλού μορφωτικού επιπέδου και οι κάτοικοι των μεγάλων αστικών κέντρων. Η ηλικία παραμένει σημαντικός προσδιοριστικός παράγοντας της διείσδυσης του Διαδικτύου. Οι άνδρες συνεχίζουν να έχουν το προβάδισμα στη χρήση των νέων τεχνολογιών. Σταθερή η απόκλιση σε σχέση με την ΕΕ και για τα δύο φύλα. Η Αττική εμφανίζει τα μεγαλύτερα ποσοστά διείσδυσης, ενώ η Κεντρική Ελλάδα τους υψηλότερους δείκτες ανάπτυξης[55]. Βέβαια το ποσοστό διείσδυσης του Διαδικτύου στην Ελλάδα είναι κάτω από τον Μ.Ο της Ευρώπης (βλ προηγουμένη εικόνα) . Ο κυριότερος λόγος είναι το υψηλό κόστος, ο χαμηλός Διαδικτυακός αλφαβητισμός (18% σε σχέση με το Μ.Ο στην Ευρώπη που είναι 31%) και ότι δεν υπάρχει παντού ευρυζωνική σύνδεση.

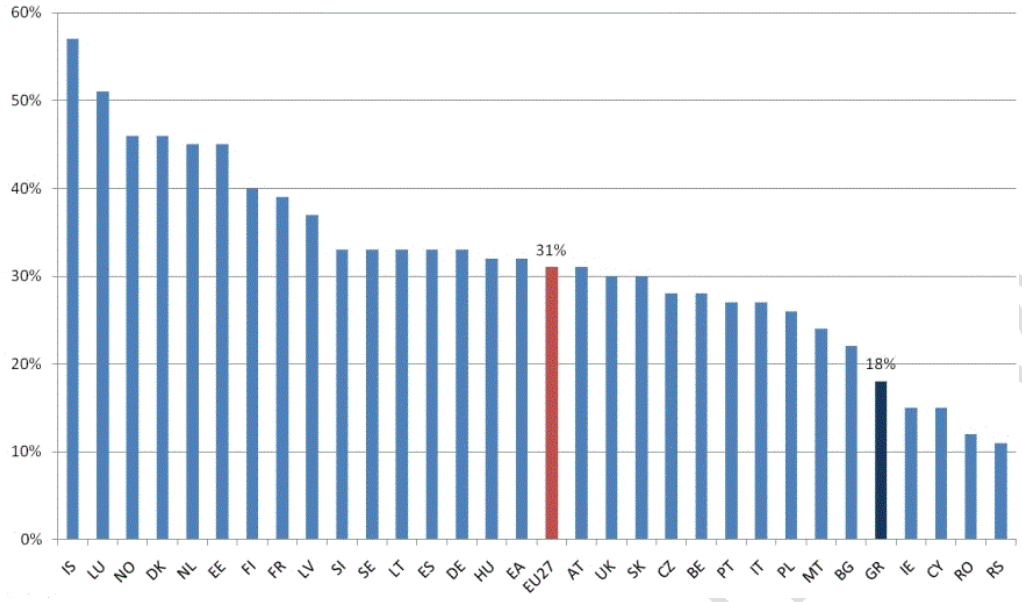


Σχήμα 5. Δημοσκόπηση για τη χαμηλή διείσδυση του internet στην Ελλάδα

Πηγή : http://www.eexi.gr/?q=node/17

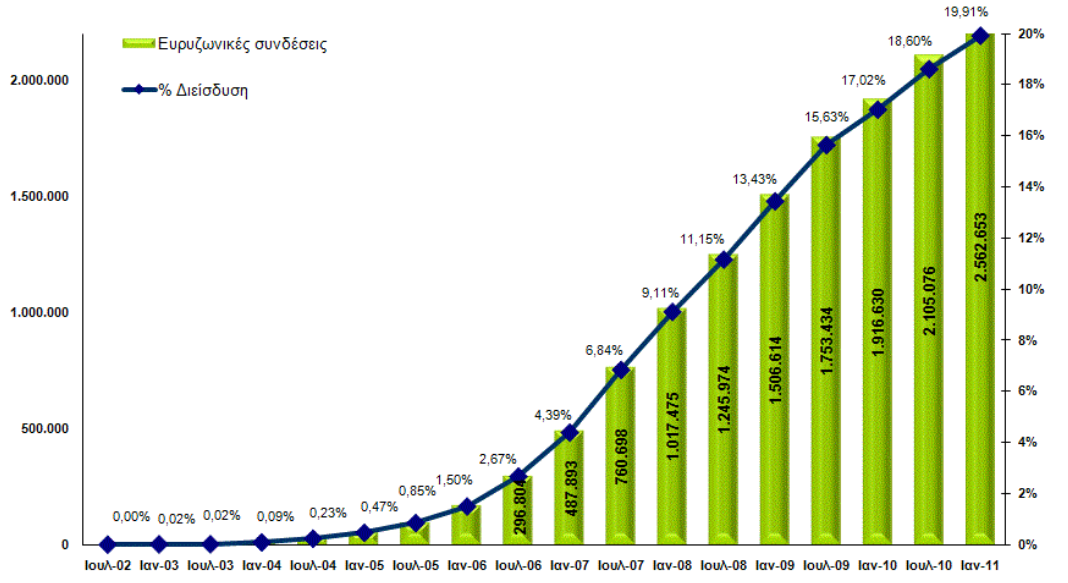
[54] Βλ δελτίο τύπου, ΕΛΣΤΑΤ, 13/6/2012 στο: http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases

[55] Βλ ταυτότητα χρηστών internet στην Ελλάδα,Μάρτιος 2010 στο: **http://www.observatory.gr**



Σχήμα 6. Διαδικτυακός Αλφαβητισμός στην Ευρώπη % του πληθυσμού με δεξιότητες χρήσης του Διαδικτύου

Πηγή : http://www.observatory.gr/page/default.asp?id=4



Σχήμα 7. Ευρυζωνικές συνδέσεις στην Ελλάδα % Διείσδυσης
Πηγή : http://www.observatory.gr/page/default.asp?id=4

1.6 **Τα θετικά στοιχεία του Διαδικτύου**

Η λειτουργία του Διαδικτύου σαν βασικού μέσου επικοινωνίας και η διείσδυση αυτού σε περισσότερα στρώματα της Κοινωνίας δημιουργεί πολλά θετικά γνωρίσματα και πλεονεκτήματα, μερικά από τα οποία είναι:

Επικοινωνία. Η λειτουργία του internet σαν μέσου επικοινωνίας και μάλιστα αμφίδρομου, συγκαταλέγεται στα βασικά πλεονεκτήματά του. Είναι αυτό που το κάνει να κερδίζει συνεχώς έδαφος έναντι άλλων μέσων επικοινωνίας, καθώς μπορούμε άμεσα να επικοινωνήσουμε ταχύτατα, με οποιονδήποτε σε όλο τον κόσμο, χωρίς περιορισμούς τόπου, χρόνου και με πολύ μικρό κόστος. Η επικοινωνία αυτή μπορεί να περιλαμβάνει από την αποστολή- λήψη e-mail, την αποστολή μηνυμάτων σε συσκευές επικοινωνίας (κινητά τηλέφωνα), την ζωντανή επικοινωνία με εικόνα και ήχο, την συνομιλία (chat).

Αναζήτηση πληροφοριών-εκπαίδευση. Η αναζήτηση πληροφορίας στο internet είναι από τα θετικά γνωρίσματά του, καθώς υπάρχει μεγάλος όγκος αποθηκευμένης πληροφορίας. Είναι γνωστή η φράση «πως αν δεν υπάρχει στο internet δεν υπάρχει πουθενά», που δείχνει τις τεράστιες δυνατότητες του Διαδικτύου για αποθήκευση και διακίνηση πληροφορίας. Η αναζήτηση πληροφορίας μπορεί να πραγματοποιηθεί σε σύντομο χρόνο, μέσα από τις μηχανές αναζήτησης, θεματικούς καταλόγους, ηλεκτρονικές βιβλιοθήκες, απλές ιστοσελίδες, ηλεκτρονικά βιβλία, ηλεκτρονικές εγκυκλοπαίδειες και λεξικά κ.λ.π.

Εκπαίδευση –έρευνα. Πέρα από από την απλή αναζήτηση πληροφορίας, το internet χρησιμεύει για την εκπαίδευση ατόμων μέσα από ανάγνωση επιστημονικών εργασιών- μελετών, Online μαθημάτων(διαφόρωνπανεπιστημίων,οργανισμών,εταιρειών),παρακολούθηση τηλεδιασκέψεων. Επίσης βοηθά στην ανάπτυξη της έρευνας σε κάθε επιστημονικό πεδίο καθώς ο χρήστης επιστήμονας μπορεί να έχει ενημέρωση για εργασίες που δημοσιεύονται σε επιστημονικά περιοδικά και συνέδρια. Ένα τέτοιο επιστημονικό πεδίο είναι της ιατρικής, όπου έρευνες για ιατρικά ζητήματα δημοσιεύονται στο Διαδίκτυο και όλοι μπορούν να ενημερωθούν άμεσα. Επίσης πολλές ιστοσελίδες στο Διαδίκτυο προσφέρουν πληροφορίες για διάφορες ασθένειες καθώς και on-line επικοινωνία με γιατρούς.

Ενημέρωση. Η χρήση του Διαδικτύου στον τομέα της ενημέρωσης έχει το χαρακτήρα της αμεσότητας της ταχύτητας και της πληρότητας. Έτσι ο χρήστης μαθαίνει τα γεγονότα που συμβαίνουν στον κόσμο μέσα από πολλαπλές ηλεκτρονικές πηγές (ειδησεογραφικά πρακτορεία, εφημερίδες, περιοδικά, ραδιοτηλεοπτικά μέσα, δικτυακούς τόπους ενημέρωσης, blogs, κοινωνικά δίκτυα κ.α)

Ψυχαγωγία-διασκέδαση. Και στον τομέα της ψυχαγωγίας το Διαδίκτυο υπερτερεί καθώς μπορεί να συνδυάζει πολλά παραδοσιακά μέσα. Έτσι ο χρήστης του Διαδικτύου μπορεί να ακούει ραδιόφωνο από όλο τον κόσμο, να βλέπει τηλεόραση, να ακούει την αγαπημένη του μουσική, να παρακολουθεί ντοκιμαντέρ της αρεσκείας του, να φέρνει στην οθόνη του υπολογιστή του κινηματογραφικές ταινίες, να διασκεδάζει με παιχνίδια κ.λ.π.

Διευκόλυνσή σε πολλούς τομείς της ζωής. Η χρήση του Διαδικτύου μας διευκολύνει σε πολλούς τομείς της καθημερινότητας εξοικονομώντας πολύτιμο χρόνο. Έτσι μπορούμε να πληρώνουμε λογαριασμούς, να πραγματοποιούμε τραπεζικές συναλλαγές, να διεκπεραιώνουμε θέματα που

έχουν σχέση με την εφορία[56] (κατάθεση φορολογικής δήλωσης, λήψη φορολογικής ενημερότητας, ενημέρωση εκκαθάρισης , λήψη κάρτα αποδείξεων, υποβολή δηλώσεων στοιχείων ακινήτων Ε9 , ειδοποίηση πληρωμής ή επιστροφής φόρου) ή με το δημόσιο[57] Επιπρόσθετα, υπάρχει η δυνατότητα υποβολής ηλεκτρονικής αίτησης προς τα ΚΕΠ για μία σειρά Διοικητικών διαδικασιών και εξυπηρετήσεων του πολίτη[58].

Ηλεκτρονικές εμπόριο. Χωρίς να βγει από το σπίτι του , ο χρήστης του Διαδικτύου μπορεί αφού περιηγηθεί σε ηλεκτρονικά καταστήματα, να κάνει τις αγορές του, οι οποίες θα του αποσταλούν στη διεύθυνση που θα δηλώσει. Επίσης και ο επιχειρηματίας μπορεί, κάνοντας χρήση κατάλληλων τεχνολογιών, να δημιουργήσει το ηλεκτρονικό του κατάστημα το οποίο και θα λειτουργεί παρέχοντας πωλήσεις από απόσταση , εξοικονομώντας έξοδα που θα είχε σε ένα συμβατικό κατάστημα. Εκτενέστερα το θέμα του ηλεκτρονικού εμπορίου αναλύεται σε προηγούμενη ενότητα (βλ. ενότητα 1.4. Βασικές υπηρεσίες Διαδικτύου).

1.7 Αρνητικές πλευρές της χρήσης του Διαδικτύου

Η χρήση του Διαδικτύου, όπως και κάθε μέσου επικοινωνίας δεν έχει μόνο θετικά αλλά και αρνητικά γνωρίσματα. Μερικές τέτοιες πλευρές καταγράφονται συνοπτικά παρακάτω, καθώς επίσης και σε άλλες ενότητες της εργασίας.

Απώλεια δεδομένων. Ο χρήστης του Διαδικτύου δέχεται την απειλή της κλοπής δεδομένων τόσο απλών και ευαίσθητων προσωπικών δεδομένων όσο και σημαντικών δεδομένων οικονομικής φύσης (αριθμοί πιστωτικών καρτών, κωδικοί για τραπεζικές συναλλαγές- e-Banking κ.α).

Ηλεκτρονικό έγκλημα. Στην Κοινωνία του Διαδικτύου, όπως και στην πραγματική Κοινωνία, υπάρχει το έγκλημα που εκδηλώνεται με τη μορφή κακόβουλου λογισμικού, εισβολής σε δίκτυα, επιθέσεις άρνησης εξυπηρέτησης, ανεπιθύμητης αλληλογραφίας (Spamming), επιθέσεις σε δικτυακούς τόπους, Phising (Ηλεκτρονικό Ψάρεμα), πειρατεία λογισμικού, διακίνηση υλικού παιδικής ή άλλης πορνογραφίας, αποπλάνηση ανηλίκων, παραβίαση Ιδιωτικότητας, εκφοβισμός (Cyber-bullying), επιθέσεις παρενόχλησης, διάφορες απάτες και επιβλαβείς συμπεριφορές, ξέπλυμα βρώμικου χρήματος, διαδικτυακή τρομοκρατία, ακατάλληλο περιεχόμενο, παρότρυνση για αυτοκτονία ή για μη νόμιμες ενέργειες κ.λ.π.

Εθισμός στο Διαδίκτυο. Η παρατεταμένη χρήση του Διαδικτύου για άντληση ικανοποίησης, μέσα από επισκέψεις σε σελίδες κοινωνικών δικτύων, σελίδες με βίαια ή άλλα παιχνίδια, σελίδες ηλεκτρονικού τζόγου, ακατάλληλου περιεχομένου έχει σαν αποτέλεσμα να εθίζει το χρήστη, καταναλώνοντας πολύτιμο χρόνο αλλά επιδρώντας ταυτόχρονα και στην ψυχική του υγεία.

Εξάρτηση. Η εξάρτηση από το Διαδίκτυο αποτελεί την πιο σύγχρονη μορφή εξάρτησης του ανθρώπου από την Τεχνολογία και μπορεί να μετατρέψει το Διαδίκτυο από σημαντικό εργαλείο

---

[56] Βλ http://www.gsis.gr/on_line_ypiresies/polites/e-polites.html

[57] Βλ http://government.gov.gr/%CF%8 υπηρεσίες-του-πολίτη%CE%B7

[58] Βλ http://www.kep.gov.gr/portal/page/portal/kep

βοήθειας του σύγχρονου ανθρώπου σε μέσον καταναγκασμού και ολοκληρωτικής απώλειας της ελευθερίας του. Η εξάρτηση στο Διαδίκτυο επηρεάζει ιδιαίτερα τους νέους και επιδρά σε αυτούς αρνητικά (Κοινωνική απομάκρυνση – απομόνωση, εγκληματικότητα, σχολική αποτυχία κ.α.) με επιπτώσεις στη σωματική τους υγεία (διατροφικές διαταραχές, παχυσαρκία, μειωμένη αθλητική δραστηριότητα, καθιστική ζωή , παραμέληση προσωπικής υγιεινής κ.α.) αλλά και στην ψυχική ισορροπία τους και ανάπτυξη.

Αλλοίωση γλώσσας. Σοβαρό πρόβλημα από τη συνεχή χρήση του διαδικτύου είναι η αλλοίωση που υφίσταται η γλώσσα μέσα από την απλοποιημένη χρήση της. Ένα τέτοιο παράδειγμα είναι η χρήση των greeklish[59] που χρησιμοποιείται κατά την επικοινωνία στο internet.

Προβλήματα διαπροσωπικών σχέσεων. Στα αρνητικά σημεία του internet καταγράφεται η αλλοτρίωση των ανθρώπινων σχέσεων και το έλλειμμα στην άμεση διά ζώσης επικοινωνία. Έτσι κάποιος επιλέγει να μιλήσει μέσω internet με ένα φίλο του, παρά να βρεθεί και να μιλήσει μαζί του. Αποτέλεσμα να χάνεται η αυθεντική επικοινωνία, τα συναισθήματα σε έναν διάλογο και οι εκφράσεις, με επακόλουθο να απομακρύνονται οι άνθρωποι μεταξύ τους και να αποξενώνονται, απομονωμένοι μπροστά στην οθόνη του υπολογιστή τους. Αυτό έχει σαν συνέπεια την καταστροφή των διαπροσωπικών σχέσεων. Πρόβλημα επίσης μπορεί να αποτελέσουν επικίνδυνες γνωριμίες με αγνώστους στο Διαδίκτυο οι οποίοι δηλώνουν ψεύτικες ταυτότητες και παραπλανούν τα θύματά τους.

Χειραγώγηση. Η λειτουργία του Διαδικτύου σαν πηγή Πληροφορίας, μπορεί να αποτελέσει και αρνητικές παρενέργειες από κάποιους, που στοχεύουν στην κατευθυνόμενη πληροφόρηση, προκαλώντας έλλειψη προσωπικής άποψης. Για το λόγο αυτό πρέπει να ελέγχεται η πηγή της Πληροφορίας και να διασταυρώνεται με άλλες πηγές. Εξάλλου πρέπει να χρησιμοποιούμε πηγές που οι πληροφορίες που δίνουν διακρίνονται για την αλήθεια και την αντικειμενικότητά τους.

1.8 Ιστοσελίδες κοινωνικής Δικτύωσης

Οι ιστοσελίδες κοινωνικής δικτύωσης αποτελούν εικονικές κοινότητες, όπου οι χρήστες του Διαδικτύου αφού γίνουν μέλη σε αυτές, έχουν τη δυνατότητα να δημιουργήσουν τα εικονικά τους προφίλ και να αναπτύξουν ένα δίκτυο επαφών, με το οποίο μπορούν να επικοινωνούν μέσω της ιστοσελίδας και να ανταλλάσσουν μηνύματα. Συνεισφορά στην εμφάνιση των κοινωνικών δικτύων και στη ραγδαία ανάπτυξή τους, έχει και η εξέλιξη του web με τη μετάβαση από το web 1.0 στην εποχή του web 2.0. Η εξέλιξη αυτή είχε σαν αποτέλεσμα να αλλάξει τη δομή και την ανάπτυξη του παγκόσμιου ιστού. Μία από τις σημαντικότερες αλλαγές στην εξέλιξη αυτή είναι η εμφάνιση των κοινωνικών δικτύων.

Ιδιαίτερο χαρακτηριστικό στοιχείο των κοινωνικών δικτύων του web αποτελεί το γεγονός ότι η ανάπτυξη τους ξεκίνησε από τους ίδιους τους χρήστες. Τα κοινωνικά δίκτυα γεννήθηκαν από κάτω προς τα πάνω, δεν είναι προϊόν κάποιας εταιρείας και άλλαξαν το Διαδίκτυο ποικιλοτρόπως. Η ιστορία της πρώτης ιστοσελίδας κοινωνικού δικτύου ξεκίνησε με την εμφάνιση της ιστοσελίδας sixdegrees.com το 1997.

---

[59] Ο όρος Greeklish (Γκρίκλις), προέρχεται από τις λέξεις **greek** (ελληνικά) και eng**lish** (αγγλικά) και είναι η ελληνική γλώσσα γραμμένη με λατινικό αλφάβητο.

Σχήμα 8. Sosial Network

πηγή: http://www.ereleases.com/prfuel/companies-skeptical-social-media

Οι πιο διαδεδομένες πλατφόρμες κοινωνικής δικτύωσης παγκοσμίως αυτή τη στιγμή είναι το Facebook, Youtube, Twitter, Ozone, Sina Weibo, Badoo , Linkedin,Tencent Weibo ,Zynga, Habbo [60] Myspace[61].

Η επιτυχία και η ραγδαία εξάπλωση των κοινωνικών δικτύων γεννάει αναμφίβολα και ερωτήματα: Είναι μια τάση της εποχής συνυφασμένη με την ανάπτυξη και εξέλιξη του internet; Ποια αναγκαιότητα προσελκύει τους ανθρώπους όλων των κοινωνικών επιπέδων να συμμετέχουν σε ένα τέτοιο δίκτυο; Η απάντηση σε αυτά τα ερωτήματα έχει να κάνει με την ίδια τη φύση του ανθρώπου, καθώς ο άνθρωπος όντως κοινωνικός, έχει ανάγκη από επικοινωνία με τους άλλους ανθρώπους. Θέλει να μιλήσει με άλλους για αυτά που τον απασχολούν, να σχολιάσει θέματα από την πολιτική επικαιρότητα, να μιλήσει για κοινωνικά ζητήματα. Να βρει φίλους από τα παλιά με τους οποίους έχασε επαφή. Να αναζητήσει νέους «φίλους» με κοινά

[60] Η κατάταξη έγινε με βάση τα οικονομικά μεγέθη και την αξία του καθενός. **Το Facebook** καταλαμβάνει την πρώτη θέση με αξία 29,11 δις δολαρίων και ακολουθούν το **Youtube** (18,09 δις) και το **Twitter** (13,30 δις). Στην τέταρτη θέση κατατάσσεται το **Ozone**, ένα δίκτυο που μπορεί να μην είναι πολύ γνωστό στη Δύση, αλλά είναι ιδιαίτερα δημοφιλές στην Κίνα και η αξία του υπολογίζεται σε 11,23 δις. Στην πρώτη δεκάδα συμπεριλαμβάνονται άλλα δύο κινεζικά δίκτυα το **Sina Weibo** (5η θέση) και το **Tencent Weibo** (8η θέση). Βλ. άρθρο εφημερίδας Βήμα, 6-3-2012,Γαλάνης Δημήτρης,στο: http://www.tovima.gr/media/article/?aid=447060

[61] Το κάποτε κυρίαρχο Myspace ανακοίνωσε συνεργασία με το μεγάλο του ανταγωνιστή, το Facebook, που έχει μετατραπεί σε μια από τις κινητήριες δυνάμεις του σύγχρονου Internet , βλ άρθ. Εφημερίδα Ελευθεροτυπία, 19-11-2010, στο: http://www.enet.gr/?i=news.el.article&id=225584

ενδιαφέροντα , επαγγελματικά ή χόμπι. Να συμμετέχει σε δίκτυα με εικονικά στοιχεία αποκτώντας ένα «άλλο εαυτό», αλληλεπιδρώντας με άλλους χρήστες χωρίς τους περιορισμούς και τις συμβατικότητες του πραγματικού κόσμου[62]. Η χρήση των κοινωνικών δικτύων έχει σαν αποτέλεσμα να επιτυγχάνονται και άλλοι στόχοι όπως πολιτικοί [63] , οικονομικοί [64] ή και άλλοι [65].

1.8.1 **Δημοφιλή κοινωνικά δίκτυα**

Το Facebook[66] είναι μια υπηρεσία κοινωνικής δικτύωσης στην οποία οι χρήστες μπορούν να επικοινωνήσουν με τους φίλους τους, να δημιουργήσουν νέες σχέσεις και να συγκροτήσουν ομάδες κοινού ενδιαφέροντος. Η τεράστια εξάπλωσή του φαίνεται από τους αριθμούς: 232.935.740 χρήστες στην Ευρώπη, 3.562.120 χρήστες στην Ελλάδα, 835.525.280 χρήστες σε όλο τον κόσμο[67]. Και όλα αυτά μέσα σε 6 χρόνια, κάνουν πραγματικά να μιλάμε για «το φαινόμενο facebook[68]». Για το λόγο αυτό θα ασχοληθούμε εκτενώς σε επόμενη ενότητα.

---

[62] Ένα τέτοιο δίκτυο είναι το Second Life (Δεύτερη Ζωή) είναι ένας εικονικός κόσμος που αναπτύχθηκε από τη Linden Lab, στις 23 Ιουνίου 2003 και είναι προσβάσιμο μέσω του Διαδικτύου. Είναι ένα δωρεάν πρόγραμμα για τον υπολογιστή που επιτρέπει στους χρήστες του να επικοινωνούν μεταξύ τους με εικονικούς εαυτούς (avatar) μέσα σε ένα πλήρως αλληλεπιδραστικό περιβάλλον βλ: http://xrisoikweb2.pbworks.com/w/page/8263756/Second%20Life..

[63] Συχνά οι πολιτικοί χρησιμοποιούν τα κοινωνικά δίκτυα για να έρθουν σε επαφή με τους πολίτες και να τους γνωστοποιήσουν τις θέσεις τους . Το επιτελείο του Μπαράκ Ομπάμα χρησιμοποίησε 16 δημοφιλή κοινωνικά δίκτυα όπως Facebok, Myspace, Youtube κ.τ.λ ώστε να κινητοποιήσει την ευρεία εμπλοκή του κοινού στις εκλογές. Σήμερα, η επίσημη σελίδα του στο Facebook αριθμεί πάνω από 19 εκατομμύρια «οπαδούς», ενώ ο λογαριασμός του στο Twitter συγκεντρώνει περίπου 7,5 εκατομμύρια «followers», βλ: άρθ. Γιάννης Ανδριτσόπουλος,εφημερίδα Νέα,20-04-2011 στο: http://www.tanea.gr/kosmos/article/?aid=4627714.

[64] Συχνά οι επιχειρήσεις χρησιμοποιούν τα κοινωνικά δίκτυα για να διαφημίσουν τα προϊόντα τους στην μεγάλη κοινότητα των χρηστών, στοχευμένα και αναλύοντας το προφίλ του κάθε χρήστη .

[65] Τα κοινωνικά δίκτυα έπαιξαν σημαντικό ρόλο στις εξεγέρσεις στον αραβικό κόσμο –Αίγυπτο ,Τυνησία, Λιβύη, βλ: http://journalism.gr/home/themata/63-first/226-dln-.html ή στο κίνημα των αγανακτισμένων βλ: http://news247.gr/eidiseis/koinonia/oi_laoi_ths_ghraias_alvionas_kseshkwnontai_gia_th_dhmokratia.1087848.html

[66] Η ιστορία του Facebook ξεκίνησε το 2004 στο πανεπιστήμιο Χάρβαρντ, όταν ο φοιτητής Μαρκ Ζούκερμπεργκ σκέφτηκε να δημιουργήσει ένα ηλεκτρονικό δίκτυο για την επικοινωνία μεταξύ των συμφοιτητών του. Στην αρχή το Facebook προοριζόταν μόνον για τους φοιτητές του Χάρβαρντ. Στη συνέχεια επεκτάθηκε και σε άλλα πανεπιστήμια , αλλά παρέμενε πάντα σε πλαίσια πανεπιστημιακά και μαθητικά. Το Σεπτέμβριο του 2006 η ιστοσελίδα όμως έγινε προσβάσιμη σε όλο τον κόσμο και από τότε ξεκίνησε η ραγδαία άνοδός του.

[67] Σύμφωνα με στατιστικά δεδομένα 31-03-2012 του internetworldstats , βλ.στο:
http://www.internetworldstats.com/stats4.htm

[68] Το facebook είναι τόσο δημοφιλές που η ιστορία του έγινε ταινία το 2010 με τίτλο «The social network», βλ. στο:
http://www.inews.gr/116/to-Facebook-egine-tainia.htm

Το YouTube ιδρύθηκε τον Φεβρουάριο του 2005, και το 2006 αγοράστηκε από την Google. Είναι μια υπηρεσία κοινωνικής δικτύωσης που επιτρέπει σε δισεκατομμύρια άτομα την αποθήκευση, αναζήτηση και αναπαραγωγή ψηφιακών ταινιών. Μέσα από την σελίδα του Youtube οι χρήστες μπορούν να παρακολουθήσουν τα βίντεο που ανήκουν σε άλλους χρήστες και να ανεβάσουν τα δικά τους βίντεο. Επίσης έχουν την δυνατότητα να σχολιάσουν τα βίντεο και τα τραγούδια που ακούν και να δείξουν αν τους αρέσουν ή όχι, απλά πατώντας ένα κουμπί. Όλοι μπορούν να βλέπουν τις αποθηκευμένες ψηφιακές ταινίες (βίντεο), ενώ τα εγγεγραμμένα μέλη μπορούν να αποθηκεύουν απεριόριστο αριθμό ταινιών με χρονικό όριο δεκαπέντε λεπτών το κάθε βίντεο. Μαζί με τις ταινίες φαίνεται και ο αριθμός των μελών που τις έχουν δει, ώστε να φαίνονται ποιες είναι οι πιο δημοφιλείς. Τα εγγεγραμμένα μέλη μπορούν να αφήσουν σχόλια στο κάθε βίντεο και να πατήσουν το κουμπί "Μου αρέσει" καθώς επίσης και να βαθμολογήσουν τα σχόλια άλλων χρηστών. Οι χρήστες μπορούν να επιλέξουν το περιεχόμενό τους να είναι δημόσιο ή ιδιωτικό για τους ίδιους και συγκεκριμένους χρήστες. Το YouTube αποτελεί τη μεγαλύτερη μηχανή αναζήτησης και παροχής βίντεο (σε χρήστες και όγκο περιεχομένου) [69].

Το twitter δημιουργήθηκε το 2006 και είναι μία υπηρεσία η οποία δίνει τη δυνατότητα στο χρήστη να κρατά επαφή, να ενημερώνει και να ενημερώνεται για τις καθημερινές δραστηριότητες των φίλων, των συγγενών και των ανθρώπων που τον ενδιαφέρουν μέσω του Internet. Το ενδιαφέρον των χρηστών για το Twitter έχει αυξηθεί κατακόρυφα τα τελευταία χρόνια[70] με αποτέλεσμα να είναι από τα πιο δημοφιλή κοινωνικά δίκτυα (τρίτο σε κατάταξη). Τα μηνύματα είναι μικρού μεγέθους έως και 140 χαρακτήρων, τα οποία βλέπουν όσοι έχουν επιλέξει να σας ακολουθούν μέσω της υπηρεσίας. Η διαδικασία αυτή ονομάζεται ***Twittering***, όσο και τα μηνύματα κινητής τηλεφωνίας. Τα μέλη μπορούν να ακολουθούν τα μηνύματα άλλων χρηστών καθώς και να απαντούν σε αυτά. Το δίκτυο όπως και άλλα κοινωνικά δίκτυα έχει απαγορευθεί στην Κίνα[71]. Το δίκτυο προσφέρει στους χρήστες του τη δυνατότητα να αναφέρουν ενόχληση από άλλα μέλη του δικτύου, των οποίων ο λογαριασμός μπορεί να ανασταλεί γι' αυτό το λόγο. Όταν ένας χρήστης δημοσιεύσει ένα μήνυμα, δεν είναι δυνατόν να το αλλάξει, αλλά μόνο να το διαγράψει[72].

Το Blogger είναι μια υπηρεσία[73] δημιουργίας ιστολογίων (web logs ή blogs). Οι χρήστες μπορούν να δημιουργήσουν ομάδες δημοσίευσης, να προσθέσουν τις δημοσιεύσεις άλλων σε δικές τους σελίδες (blog follow-up), να σχολιάζουν τις δημοσιεύσεις άλλων χρηστών, να προσθέσουν «αντιδράσεις» (reactions) σε δημοσιευμένα άρθρα, παρέχοντας προκαθορισμένα σχόλια (π.χ. «like it», «so and so» κλπ).Οι χρήστες δημοσιεύουν σε αυτά υλικό με τη μορφή κειμένου,

[69] Για περισσότερα βλ. http://www.youtube.com/t/about_youtube

[70] Βλ. http://www.google.com/trends/?q=twitter

[71] Βλ. http://www.gazzetta.gr/genikes-eidiseis/article/item/277901-kleinei-16-istotopoys-i-kina-6-syllipseis

[72] Η ιστοσελίδα του twitter : https://twitter.com

[73] Η υπηρεσία είναι της google και βρίσκεται στη διεύθυνση : www.blogger.com

φωτογραφιών ή βίντεο. Οι υπόλοιποι χρήστες μπορούν να προσθέτουν σχόλια και αντιδράσεις στο δημοσιευμένο υλικό[74].

Το δίκτυο LinkedIn[75], ιδρύθηκε τον Δεκέμβριο του 2002, αλλά ξεκίνησε επίσημα στις 5 Μαΐου του 2003[76]. Είναι μία υπηρεσία κοινωνικής δικτύωσης (social nerworking website) που εξειδικεύεται σε επιχειρηματικές δραστηριότητες. Δίνει τη δυνατότητα στους χρήστες να δημιουργήσουν ένα δίκτυο από υπάρχουσες και νέες επαγγελματικές επαφές (που αποκαλούνται συνδέσεις – connections). Όμως, προχωράει περισσότερο από αυτό. Όταν προσθέτεις μια νέα σύνδεση, οι συνδέσεις αυτής και οι συνδέσεις αυτών των συνδέσεων επίσης θα προστεθούν στο δικό σου δίκτυο. Αυτό προσφέρει σε έναν επαγγελματία απίστευτα μεγάλο πεδίο επαγγελματικών επαφών[77]. Στοχεύει στη δικτύωση επαγγελματιών και διευκολύνει τα μέλη του στη διατήρηση επαγγελματικών σχέσεων ακόμα και στην εύρεση εργασίας. Η δικτύωση των μελών επεκτείνεται σε 3 επίπεδα: κάθε μέλος διασυνδέεται αυτόματα με τους άμεσους γνωστούς του, αλλά και με τους γνωστούς των γνωστών του. Ο ιστοχώρος είναι διαθέσιμος σε έξι γλώσσες, Αγγλικά, Γαλλικά, Γερμανικά, Ιταλικά, Ισπανικά και Πορτογαλικά και σήμερα θεωρείται ο πιο επιτυχημένος ιστοχώρος κοινωνικής δικτύωσης για επαγγελματίες στον κόσμο, μετρώντας περισσότερους από 100 εκατομμύρια εγγεγραμμένους χρήστες[78].

Το flickr(προφέρεται Φλίκερ) είναι μια ιστοσελίδα[79], η οποία δημιουργήθηκε για να φιλοξενεί φωτογραφίες και βίντεο. Δημιουργήθηκε αρχικά από την εταιρία Ludicorp και ύστερα εξαγοράστηκε από την Yahoo. Η υπηρεσία χρησιμοποιείται συχνά από bloggers για να ενσωματώσουν τις φωτογραφίες τους στα blogs τους. Οι χρήστες του ανεβάζουν, οργανώνουν και δημοσιεύουν τις φωτογραφίες τους. Μπορούν να προσθέσουν άτομα που είναι επίσης μέλη του δικτύου και εμφανίζονται στις φωτογραφίες, καθώς και κατηγορίες, σημειώσεις, σχόλια και προτιμήσεις για συγκεκριμένες φωτογραφίες. Το flickr παρέχει δυνατότητες αναζήτησης φωτογραφιών με βάση παγκόσμια τοποθεσία, με βάση το μοντέλο της φωτογραφικής μηχανής με την οποία τραβήχτηκαν, αλλά και με βάση τις κατηγορίες ή ετικέτες που συνδέεται με τις φωτογραφίες[80].

1.8.2 **Το φαινόμενο** Facebook

Το Facebook αποτελεί τον αγαπημένο προορισμό εκατομμυρίων Ελλήνων χρηστών του Διαδικτύου. Σύμφωνα με έρευνα[81] που πραγματοποίησε το Εργαστήριο Ηλεκτρονικού

---

[74] Για περισσότερα βλ: http://support.google.com/blogger/bin/answer.py?hl=el&answer=175250

[75] Η σελίδα του: www.linkedin.com

[76] Βλ: http://press.linkedin.com/about

[77] Για περισσότερα βλ: http://social-net.gr/about/τι-είναι-το-linkedin

[78] βλ: http://mashable.com/2011/03/22/linkedin-surpasses-100-million-users-infographic/

[79] βλ: http://www.flickr.com

[80] Βλ: http://www.flickr.com/about

[81] Η έρευνα πραγματοποιήθηκε το 2009 και για την εκπόνηση της έρευνας δημιουργήθηκε από τους ερευνητές ένα group στο Facebook, το οποίο καλούσε όλους τους Έλληνες χρήστες του να συμμετάσχουν στην έρευνα συμπληρώνοντας ένα ερωτηματολόγιο, βλ περιοδικό Επιστημονικό Marketing Management, στο: http://www.epistimonikomarketing.gr/article_show.php?article_id=3113

Επιχειρείν (ELTRUN) του Οικονομικού Πανεπιστημίου Αθηνών, η πλειοψηφία του συνόλου των χρηστών (62%) που είναι εγγεγραμμένοι στο facebook δεν είναι εγγεγραμμένοι σε άλλη παρόμοια ιστοσελίδα. Ένα πολύ μεγάλο ποσοστό των χρηστών (59%) επισκέπτεται το facebook συχνότερα από 1 φορά την ημέρα. Το 34% των χρηστών επισκέπτεται το facebook 2-3 φορές ημερησίως και το 25% ακόμη πιο συχνά. Το 75% των χρηστών ξοδεύουν λιγότερο από 30 λεπτά σε κάθε τους επίσκεψη στο facebook. Το 50% δηλώνει μέσο χρόνο επίσκεψης λιγότερο από ένα τέταρτο της ώρας. Το αποτέλεσμα αυτό σε συνδυασμό με τη μέση συχνότητα επισκέψεων δείχνει πως ο μέσος χρήστης του facebook το επισκέπτεται αρκετές φορές την ημέρα και για μικρή διάρκεια, άρα γίνεται αναπόσπαστο μέρος της καθημερινότητας του. Το 92% των χρηστών δηλώνει πως ο βασικός λόγος χρήσης του facebook είναι η επικοινωνία με παλιούς φίλους και γνωστούς. Στη συνέχεια, ο δεύτερος επικρατέστερος λόγος χρήσης είναι η ενασχόληση με διάφορες εφαρμογές (τεστ γνώσεων & ευφυΐας, ερωτηματολόγια προτιμήσεων, φωτογραφίες & βίντεο, κ.ά.) και παιχνίδια που μπορεί να εγκατασταθούν στην ιστοσελίδα του facebook. Το 46% των χρηστών δηλώνει πως χρησιμοποιεί το facebook για να μαθαίνει προσωπικά στοιχεία φίλων και γνωστών. Οι νέες γνωριμίες και το «ηλεκτρονικό» φλερτ δεν αποτελούν για τους Έλληνες χρήστες ένα από τα βασικά κίνητρα χρήσης του facebook, αφού μόνο το 28% δηλώνει πως επισκέπτεται το facebook για αυτόν τον λόγο. Σύμφωνα με τα αποτελέσματα της έρευνας, σχεδόν το σύνολο των χρηστών εκμεταλλεύεται τη δυνατότητα που παρέχει το facebook για επανασύνδεση με παλιούς φίλους και γνωστούς και ένα πολύ μεγάλο ποσοστό των χρηστών επιδίδεται σε ένα νέο είδος “ηλεκτρονικού κουτσομπολιού”. Αναφορικά με το βαθμό εμπιστοσύνης των χρηστών προς το Facebook, το 33% των χρηστών δηλώνει πως εμπιστεύεται αρκετά ή πολύ το facebook και το 38% δηλώνει πως δεν το εμπιστεύεται καθόλου ή το εμπιστεύεται λίγο. Όσον αφορά τη σχέση που έχουν οι χρήστες με το facebook, είναι σχεδόν ή πολύ απαραίτητο στο 42% των χρηστών. Το ποσοστό αυτό επιβεβαιώνει την ιδιαίτερη σχέση που έχουν οι χρήστες του facebook με την συγκεκριμένη ιστοσελίδα.

Η ιστοσελίδα δίνει την δυνατότητα στους εγγεγραμμένους χρήστες να δημιουργήσουν τη δική τους προσωπική ιστοσελίδα χωρίς κανένα κόστος και χωρίς γνώσεις προγραμματισμού, ανοίγοντας ένα παράθυρο που θα τους κάνει γνωστούς στον έξω κόσμο και θα δώσει πληροφορίες και προσωπικά δεδομένα για αυτούς στους υπόλοιπους χρήστες που είναι «φίλοι». Σ’ αυτόν το χώρο μπορούν άτομα από οποιαδήποτε χώρα να επικοινωνήσουν, να μοιραστούν εικόνες, βίντεο, μουσική και ότι άλλο επιθυμούν χωρίς εμπόδια. Η εγγραφή μπορεί να δημιουργηθεί μέσα σε ελάχιστο χρόνο και μάλιστα είναι δωρεάν. Τα μέλη διατηρούν λίστα φίλων τους οποίους έχουν τη δυνατότητα να αναζητήσουν, να προσκαλέσουν ή να αποδεχτούν/αρνηθούν τη “φιλία” τους.

Στην αρχή ο κάθε χρήστης δημιουργεί το δικό του **προφίλ**, δίνοντας προσωπικές πληροφορίες που έχουν να κάνουν με στοιχεία της ταυτότητάς του (Επώνυμο, όνομα, ημερομηνία γέννησης, στοιχεία διεύθυνσης διαμονής και επικοινωνίας, κοινοποίηση προσωπικής-οικογενειακής κατάστασης, φύλο),κοινοποίηση στοιχείων συγγενικών και φιλικών προσώπων, στοιχεία που έχουν να κάνουν με το μορφωτικό επίπεδο και το επίπεδο σπουδών, στοιχεία εργασίας, πληροφορίες για μουσικά, λογοτεχνικά, κινηματογραφικά ή άλλα ενδιαφέροντα, στοιχεία που συγκροτούν την προσωπικότητα του κάθε χρήστη όπως ιδεολογικές, πολιτικές, θρησκευτικές πεποιθήσεις, καταναλωτικές συνήθειες.

Αυτό το προφίλ σε συνδυασμό με ανάρτηση φωτογραφιών συμβάλλει στην αναγνώριση και στο προσδιορισμό του κάθε χρήστη παρέχοντας πληροφορίες για αυτόν, αποτυπώνοντας την προσωπικότητά του. Πολλές φορές υπάρχει η αίσθηση στο χρήστη, ότι μπορεί να διαγράψει παλαιά δεδομένα και προσωπικές πληροφορίες και να προσθέσει νέες. Καλλιεργείται έτσι η αυταπάτη πως οι πληροφορίες που έχουν διαγραφεί εξαφανίζονται δια μαγείας. Όμως στην πραγματικότητα σε κάποιους έχουν μείνει γιατί, ότι δημοσιεύεται στο internet μπορεί να αποθηκευτεί σαν ηλεκτρονικό αρχείο.

Στη συνέχεια αφού έχει «οικοδομήσει» το προφίλ του, μπορεί να αποστείλει ή να αποδεχθεί αιτήματα φιλίας , να αναζητήσει παλιούς γνωστούς, συμμαθητές, φίλους μέσα από την πανίσχυρη **μηχανή αναζήτησης**. Έτσι σχηματίζεται μια μικρή κοινότητα που διαρκώς μεγαλώνει, καθώς τον βοηθάει η επιλογή « **άτομα που ίσως γνωρίζεις**» και αποτελούνται από τους φίλους των φίλων. Μπορεί να εκφράσει τις σκέψεις ,τα προβλήματα που τον απασχολούν, τα συναισθήματά του! Μέσα από την υπηρεσία **news feed** ο χρήστης μαθαίνει για ότι έχουν

κοινοποιήσει οι επαφές του καθώς και οποιαδήποτε αλλαγή έχουν ή πρόκειται να πραγματοποιήσουν αυτοί στο άμεσο μέλλον (π.χ να παραβρεθούν σε μια εκδήλωση ή μια συναυλία, ή ένα πάρτυ. Μέσα από την **υπηρεσία ανταλλαγής μηνυμάτων** (on line instant messaging) βλέπει ποιοι είναι συνδεδεμένοι στο face book και μπορεί να συνομιλήσει μαζί τους σε πραγματικό χρόνο. Μπορεί επίσης να κάνει **βιντεοκλήση** στον χρήστη «φίλο» που είναι online και να επικοινωνήσει μαζί του με εικόνα και ήχο. Υπάρχει επίσης η δυνατότητα να **ανεβάζει φωτογραφίες** τόσο δικές του όσο και φίλων του οι οποίες σε συνδυασμό με άλλες προσωπικές πληροφορίες μέσα από το προφίλ και το **status** που δημοσιεύει να μπορεί να σχηματισθεί η πλήρης εικόνα για τον χρήστη, και να αποτελέσουν για κάποιους μια καλή ενασχόληση να συγκεντρώνουν τέτοια στοιχεία για διαφορετικούς σκοπούς[82]. Στην κατεύθυνση αυτή βοηθά και η σύγχρονη τεχνολογία με τη χρήση «έξυπνων κινητών τελευταίας τεχνολογίας», τα οποία όταν χρησιμοποιούνται από τους χρήστες για περιήγηση στο internet , χρήση του GPS, υπηρεσιών της Google, «βοηθούν» στο να **προσδιορίζουν τη θέση του χρήστη**[83].

Τα κοινωνικά δίκτυα όμως δεν είναι φιλανθρωπικά ιδρύματα, αλλά εταιρείες που η λειτουργία τους στηρίζεται σε μεγάλο βαθμό στη διαφήμιση και μάλιστα στη στοχευμένη διαφήμιση με βάση τη συμπεριφορά και το καταναλωτικό προφίλ του κάθε χρήστη[84]. Έτσι συγκεντρώνονται πληροφορίες για κάθε χρήστη , μέσα από το προφίλ , το status, ηλεκτρονικά παιχνίδια και άλλες εφαρμογές που λειτουργούν στην πλατφόρμα του facebook και εξυπηρετούν αυτό το σκοπό.

1.9 **Το μέλλον του Διαδικτύου**

Το Διαδίκτυο αρχικά φτιάχτηκε για να υπηρετήσει στρατιωτικούς σκοπούς στη συνέχεια όμως δόθηκε στο ευρύ κοινό. Ουσιαστικά η ραγδαία εξάπλωσή του παρουσιάζεται στις τελευταίες δύο δεκαετίες και σε αυτό συνεισφέρουν οι εξελίξεις στον τηλεπικοινωνιακό τομέα και στην ανάπτυξη της Πληροφορικής. Το πέρασμα από την εποχή του Web 1.0, της μονόδρομης επικοινωνίας όπου η πληροφορία αναζητείται και διαβάζεται, στην εποχή του Web 2.0 όπου κυριαρχεί η συμμετοχή, η συνεργασία η δυναμική αλληλεπίδραση μεταξύ των χρηστών, δείχνει το δρόμο που οδηγεί η ραγδαία ανάπτυξη του internet. Το διαδίκτυο αυτή τη στιγμή εξαπλώνεται ολοένα και πιο γρήγορα, όπως συνέβη και παλιότερα με άλλα μέσα επικοινωνίας όπως το τηλέφωνο, το ραδιόφωνο ή η τηλεόραση.

Σύμφωνα με τον Sir Tim Berners-Lee δημιουργό του World Wide Web « το Διαδίκτυο πρέπει να βρει έναν τρόπο ώστε να μπορούν οι χρήστες να διαχωρίζουν τις φήμες από την πραγματική επιστήμη. Για το λόγο αυτό απαιτούνται νέα συστήματα που θα αξιολογούν τα sites ανάλογα με την εγκυρότητα της γνώσης που προσφέρουν. Επίσης να αναζητεί τρόπους να

---

[82] Υπάρχει ιστοσελίδα με τίτλο "We Know What You're Doing , συγκεντρώνει στοιχεία που είναι δημόσια αναρτημένα από το Facebook σύμφωνα με τα παρακάτω κριτήρια: Ποιος θέλει να απολυθεί; (Who wants to get fired;), Ποιος έχει μεθύσει το προηγούμενο βράδυ; (Who's hangover;),Ποιος παίρνει ναρκωτικά; (Who's taking drugs;), Ποιος έχει αινούργιο αριθμό τηλεφώνου; (Who's got a new telephone number;) βλ: http://www.weknowwhatyouredoing.com

[83] Η υπηρεσία Latitude της Google είναι μια δυνατότητα του Google Maps for mobile της εφαρμογής δηλαδή Google Maps για κινητά τηλέφωνα που όχι μόνο καταγράφει τη θέση στην οποία βρίσκεσαι αλλά εμφανίζει τη θέση των φίλων μας που έχουν εγκαταστήσει και εξουσιοδοτήσει την εφαρμογή. Έτσι μέσα από το κινητό βλέπεις τη θέση του δικτύου φίλων σου ανά πάσα στιγμή. Βλ: http://www.phonet.gr/tag/latitude/ επίσης http://www.maclife.gr/forum/showthread.php/2088-Google-Latitude

[84] Βλ. Κ. Λαμπρινουδάκης, Σ. Γκρίτζαλης, Λ. Μήτρου, Σ. Κάτσικας, Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Εκδόσεις Παπασωτηρίου 2010, σελ. 634.

φέρει το διαδίκτυο πιο κοντά στην κινητή τηλεφωνία. Μια τέτοια κίνηση θα αύξανε τη χρήση του στην Αφρική και άλλες φτωχές περιοχές του πλανήτη όπου υπάρχουν λίγοι υπολογιστές αλλά πολλές συσκευές κινητού τηλεφώνου. Επιπλέον, χρειάζεται να γίνει διερεύνηση πώς μπορούν να αξιοποιηθούν οι δυνατότητες του internet από αυτούς που δεν μπορούν να διαβάσουν ή να γράψουν , ίσως χρησιμοποιώντας νεύματα ή στίξη»[85].

Η τεράστια ανάπτυξη του Διαδικτύου φέρνει και αλλαγές στον ορισμό των διευθύνσεων IP .Έτσι από 32 bits που αποθηκεύεται μια διεύθυνση (IPV 4[86] με δυνατότητα 2^{32} = 4.294.967.926 διευθύνσεων) θα φτάσει στα 128 bits (IPV 6[87] με δυνατότητα 2^{128} = 340 x 10^{36} διευθύνσεων), αριθμός πολύ μεγάλος για να καλύψει όχι μόνο το παρόν αλλά και το μέλλον.

Οι νέες δυνατότητες θα επεκταθούν σε εφαρμογές των πολυμέσων σε πολλές δραστηριότητες καθημερινές (επικοινωνίες, τραπεζικές συναλλαγές, ηλεκτρονικό εμπόριο). Η εμφάνιση επίσης των υπολογιστών δικτύου (NetPC[88]) αναμένεται να φέρει νέες εφαρμογές με πολλές δυνατότητες στην εκπαίδευση από απόσταση, στην έρευνα, στην εργασία. Βασική προϋπόθεση βέβαια οι γραμμές μεταφοράς των δεδομένων για να μπορέσουν να ανταποκριθούν στις τεράστιες ανάγκες των χρηστών και στη μεγάλη ταχύτητα που απαιτεί μια εφαρμογή πολυμέσων[89].

Το διαδίκτυο θα εξελιχθεί σε βασικό στοιχείο της καθημερινής μας ζωής, διαδραματίζοντας ρόλο ανάλογο εκείνου που έπαιξε η τηλεόραση τα τελευταία 30 χρόνια. Οι ρυθμοί ανάπτυξής του δείχνουν ότι σύντομα θα είναι τόσο κοινό και διαδεδομένο όσο το ηλεκτρικό ρεύμα και το τηλέφωνο. Το 2020 είναι πολύ πιθανό να μη μιλάμε μόνο για ψηφιακή οικονομία, αλλά και για ψηφιακή κοινωνία. Στη νέα του μορφή το δίκτυο θα πάψει να είναι περιορισμένο στην οθόνη του υπολογιστή – θα το συναντάμε όπου κι αν βρισκόμαστε με τη βοήθεια μεγάλης ποικιλίας συσκευών και με ταχύτητες πολύ καλύτερες από τις σημερινές[90].

2 ΚΕΦΑΛΑΙΟ: Ασφάλεια υπολογιστών –Δικτύων

2.1 Γενικά

Στην εποχή της ραγδαίας ανάπτυξης υπολογιστικών και πληροφοριακών συστημάτων, της γιγάντωσης του intenet ,των ιών και των χάκερ, της ηλεκτρονικής απάτης και του ηλεκτρονικού

[85] Από τη συνέντευξη του Sir Tim Berners-Lee στο BBC δημιουργό του World Wide Web, βλ στο: http://www.oteacademy.gr/eidisi/% ανησυχίες-για-το-μέλλον-του-internet

[86] IPv6: είναι το ακρωνύμιο του «Internet Protocol version 4», που σημαίνει «Πρωτόκολλο Διαδικτύου Έκδοση 4.

[87] IPv6: είναι το ακρωνύμιο του «Internet Protocol version 6», που σημαίνει «Πρωτόκολλο Διαδικτύου Έκδοση 6, για περισσότερα βλ: http://www.ipv6-taskforce.gr/

[88] NetPC: Υπολογιστές αποκλειστικής σύνδεσης στο internet , χαμηλού κόστους.

[89] Βλ:Καράκος Α., Διαδίκτυο Παγκόσμιος Ιστός και τεχνικές Προγραμματισμού, Εκδόσεις Γκιούρδας, Αθήνα 2009,σελ.54

[90] http://pacific.jour.auth.gr/internet/page2.htm.

εγκλήματος η Ασφάλεια[91] είναι έννοια με πρωτεύουσα σημασία. Η έννοια της ασφάλειας πληροφοριακών συστημάτων και Δικτύου Υπολογιστών αναφέρεται στην ικανότητα να προστατευθούν οι πληροφορίες που περιέχουν αυτά από τυχόν κλοπές, αλλοιώσεις, καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων τους. Σχετίζεται με την «ικανότητα» του πληροφοριακού συστήματος ή ενός Δικτύου Υπολογιστών να αντισταθεί, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Με την εισαγωγή της χρήσης υπολογιστών προβάλλει επιτακτικά η ανάγκη για αυτοματοποιημένα εργαλεία προστασίας των αρχείων και άλλων πληροφοριών που βρίσκονται αποθηκευμένες σε αυτούς. Η συλλογή εργαλείων που είναι σχεδιασμένα για να προστατεύσουν τα δεδομένα και να αποτρέψουν την «διάρρηξη» του υπολογιστή αναφέρεται στον όρο **ασφάλεια υπολογιστών** (computer security). Στην περίπτωση που οι υπολογιστές συνδέονται σε δίκτυα για να μεταφέρουν τις πληροφορίες έχουμε τον όρο **ασφάλεια δικτύων** (network security) , ή στην περίπτωση του διαδικτύου χρησιμοποιείται ο όρος **ασφάλεια διαδικτύου** (internet security)[92].

Η διαρκής εξέλιξη του Internet και της τεχνολογίας των δικτύων , δίνει σίγουρα σημαντικά πλεονεκτήματα και δυνατότητες προσφέροντας πολλές υπηρεσίες στο σύγχρονο άνθρωπο, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα που σχετίζονται με την προστασία και τη διαθεσιμότητα των πληροφοριών.

2.2 **Υπηρεσίες ασφαλείας**

Η Ασφάλεια Τεχνολογίας Πληροφορίας και Επικοινωνιών – ασφάλεια ΤΠΕ[93] (Information and Communication Technology Security – ICT Security) περιλαμβάνει την ασφάλεια:

1. Ασφάλεια υπολογιστικών συστημάτων και εφαρμογών, δηλαδή την προστασία από μη εξουσιοδοτημένες ενέργειες όπως αλλαγή δικαιωμάτων πρόσβασης, κακόβουλη εκτέλεση εντολών, τροποποίηση της διάρθρωσης του συστήματος, κακόβουλη ή λανθασμένη χρήση, διακοπή λειτουργίας, καθώς και τη φυσική προστασία των υπολογιστικών συστημάτων.

---

[91] Στον όρο «Ασφάλεια» μπορούν να αποδοθούν πολλές ερμηνείες, κάθε μία από τις οποίες μπορεί να αποδώσει με ακρίβεια διαφορετικές καταστάσεις και να την προσδιορίσει. Σύμφωνα με το Λεξικό Μπαμπινιώτη, ασφάλεια ορίζεται η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται, ή η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας, Βλ. Γ. Μπαμπινιώτη, λεξικό της Νέας Ελληνικής γλώσσας, β΄ έκδοση 2005, σελ 305.

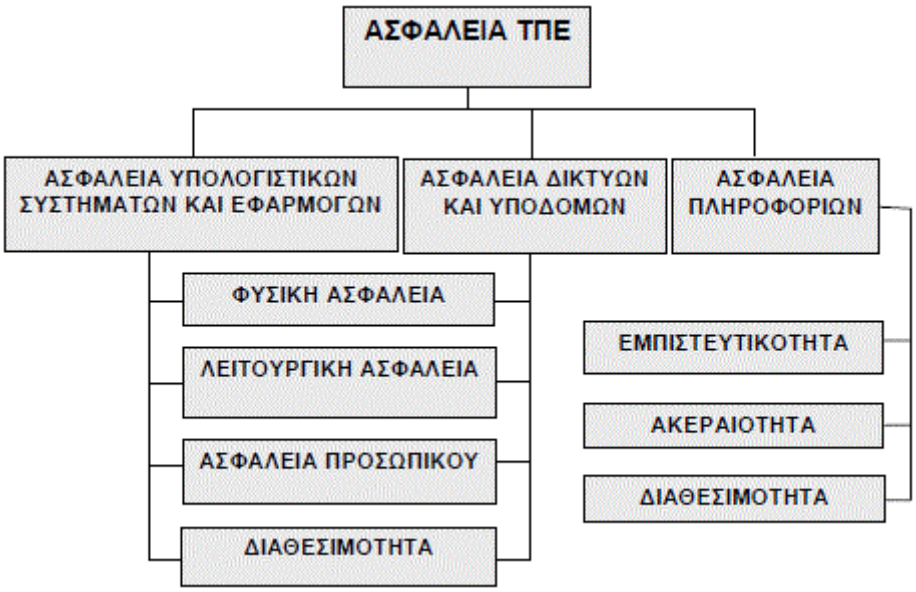
[92] Βλ. William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 18.

[93] Τεχνολογία Πληροφοριών και Επικοινωνίας ή τεχνολογία της πληροφορίας (**ΤΠΕ**, αγγλ. IT ή ICT) είναι το σύνολο των επαγγελματικών χώρων οι οποίοι σχετίζονται με τη μελέτη, σχεδίαση, ανάπτυξη, υλοποίηση, συντήρηση και διαχείριση υπολογιστικών πληροφοριακών συστημάτων, κυρίως όσον αφορά εφαρμογές λογισμικού και υλικό υπολογιστών βλ: http://el.wikipedia.org/wiki/Τεχνολογία Πληροφορικής και επικοινωνιών

2. Ασφάλεια δικτύων και των υποδομών, δηλαδή την προστασία από μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο, παράκαμψη ή τροποποίηση των κανόνων δρομολόγησης στο δίκτυο, παρακολούθηση του μέσου επικοινωνίας, διακοπή της επικοινωνίας, φυσική προστασία των υποδομών επικοινωνίας .

Η ασφάλεια υπολογιστικών συστημάτων και εφαρμογών καθώς και η ασφάλεια δικτύων και υποδομών αναφέρονται στην φυσική ασφάλεια, στη λειτουργική ασφάλεια, στην ασφάλεια προσωπικού και στη διαθεσιμότητα.

3. Ασφάλεια πληροφοριών, δηλαδή την προστασία των δεδομένων σε σχέση με την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους (βλέπε σχήμα).



Σχήμα 9. Υπηρεσίες ασφαλείας

Πηγή: http://imu.ntua.gr/projects/dern/files/Asfaleia.pdf

Η ασφάλεια στα δίκτυα υπολογιστών και στο internet έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων. Ποιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

☞ **Πρόληψη** (prevention) : Το σύνολο των μέτρων –ενεργειών που πρέπει να ληφθούν από τον administrator προκειμένου να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών ή σε άλλα προβλήματα. Στοχεύει στην αποτροπή μιας επίθεσης πριν αυτή να

εκδηλωθεί. Για παράδειγμα η χρήση ενός τείχους προστασίας (***firewall***) σε ένα σύστημα αποσκοπεί στο να αποτρέψει τη μη εξουσιοδοτημένη είσοδο σε αυτό το σύστημα.

☞ **Ανίχνευση** (detection) : Το σύνολο των μέτρων –ενεργειών για να βρεθεί πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες. Με τη διαρκή εξέλιξη της πληροφορικής, όσα μέτρα πρόληψης και να ληφθούν κανένα σύστημα δεν μπορούμε να πούμε πως εξασφαλίζει απόλυτη ασφάλεια. Για το λόγο αυτό στο σχεδιασμό της ασφάλειας θα πρέπει να λαμβάνονται μέτρα για την ανίχνευση μιας εισβολής στο σύστημα, όταν αυτή θα συμβεί. Παράδειγμα αποτελεί το **Σ**ύστημα **Α**νίχνευσης **Ε**ισβολής(ΣΑΕ) (αγγλ. Intrusion Detection System, IDS[94])

☞ **Αντίδραση** (reaction) : Το σύνολο των μέτρων –ενεργειών που πρέπει να ληφθούν για να γίνει η αποκατάσταση του συστήματος. Αφορούν τα μέτρα εκείνα που στόχο έχουν να μειώσουν το χρόνο ανάκαμψης του συστήματος μετά από την εκδήλωση επίθεσης. Παράδειγμα αποτελεί η χρήση εργαλείων αφαίρεσης κακόβουλου λογισμικού, αυτόματη λήψη ή και επαναφορά αντιγράφων ασφαλείας (backup).

2.2.1 **Η υπηρεσία Αυθεντικότητας** (authentication)

Η υπηρεσία πιστοποίησης της ταυτότητας των χρηστών και πληροφοριών ή της αυθεντικότητας όπως συνηθέστερα αναφέρεται εξασφαλίζει ότι μια επικοινωνία είναι γνήσια, τόσο σε επίπεδο χρηστών όσο και σε επίπεδο πληροφοριών. Έτσι ο παραλήπτης είναι σίγουρος για την ταυτότητα του αποστολέα και αντίστροφα (**πιστοποίηση ταυτότητας ομότιμης οντότητας**- Peer Entity Authentication) και επιβεβαιώνει την ταυτότητα προέλευσης των δεδομένων (**πιστοποίηση ταυτότητας προέλευσης δεδομένων**- data origin Authentication) [95]. Κάποιοι τρόποι για να ελεγχτεί η αυθεντικότητα σε ένα σύστημα είναι:

● **Ταυτοποίηση με κωδικούς προστασίας** (Passwords). Η χρήση κωδικών πρόσβασης για να γίνει επαλήθευση ταυτότητας, είναι μια δημοφιλή μέθοδο ταυτοποίησης. Π.χ. η πρόσβαση σε Η/Υ ή στο server ενός δικτύου γίνεται με τη χρήση ενός όνομα χρήστη και ενός κωδικού πρόσβασης. Επίσης η πρόσβαση στον mail server για την αποστολή, λήψη και διαχείριση e-mail με τη χρήση ενός ονόματος χρήστη και ενός κωδικού για την πρόσβαση στο διακομιστή εισερχόμενης-εξερχόμενης αλληλογραφίας (incoming- outgoing mail server).

Οι κωδικοί πρόσβασης αποτελούν αχίλλειο πτέρνα της ασφάλειας των ηλεκτρονικών υπολογιστών λόγω των περιορισμών της ανθρώπινης μνήμης. Καθώς χρειάζεται να δημιουργήσουμε δεκάδες τέτοιους κωδικούς επιλέγουμε είτε αυτούς που είναι τόσο πολύπλοκοι

---

[94] Το ΣΑΕ είναι ένα σύστημα παρακολούθησης και ανάλυσης συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές όσο και στα δίκτυα υπολογιστών. Στόχος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πόρων ενός πληροφοριακού συστήματος, για περισσότερα βλ. Scarfone Karen, Mell Peter, Guide to Intrusion Detection and Prevention Systems, 2007,National Institute of Standards and Technology, (2007), στο:

http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[95] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 30.

ώστε χρειάζεται να γραφτούν σε ένα χαρτί προκειμένου να μη λησμονηθούν ή είναι τόσο απλοί και χαρακτηριστικοί που τελικά οποιοσδήποτε μπορεί να τους μαντέψει[96].

Απειλές από τις οποίες πρέπει να προστατευτούμε όταν χρησιμοποιούμε passwords: Αποκάλυψη του κωδικού πρόσβασης, παρακολούθηση της γραμμής μεταβίβασης του κωδικού πρόσβασης, εύρεση του κωδικού πρόσβασης χρησιμοποιώντας τεχνικές τύπου **dictionary attacks** (επιθέσεις λεξικού).

Μέτρα η χρήση δύσκολων κωδικών (χρήση αλφαριθμητικών χαρακτήρων σε συνδυασμό με μη αλφαριθμητικούς χαρακτήρες).Μπορούμε να χρησιμοποιήσουμε **password checkers** για να ελέγξουμε πόσο δυνατό είναι το password που επιλέξαμε.

Τρόποι μείωσης του κινδύνου εύρεσης ενός password:

- ☞ Αλλαγή των passwords σε τακτικά χρονικά διαστήματα
- ☞ Αποφυγή των προκαθορισμένων (default) passwords
- ☞ Εκπαίδευση σε διαχειριστές και χρήστες
- ☞ Περιορισμός σε πολύ μικρό αριθμό των μη έγκυρων προσπαθειών αυθεντικοποίησης
- ☞ Χρήση τεχνητής καθυστέρησης στη διαδικασία επαλήθευση για να δυσκολέψουμε την αποτελεσματικότητα των επιθέσεων τύπου dictionary attacks.
- ☞ Χρήση μηχανισμών που αποτρέπουν τους χρήστες να επιλέξουν passwords που είναι πολύ μικρά, εύκολα, σχετίζονται με τα χαρακτηριστικά του χρήστη[97].

● **Ταυτοποίηση με τεχνικές Βιομετρίας**[98]. Οι τεχνικές μέθοδοι αυτοί επιτρέπουν τη συλλογή και ανάλυση χαρακτηριστικών του ανθρώπινου σώματος ή/και της ανθρώπινης συμπεριφοράς, με σκοπό την πρόσβαση στους πόρους ενός συστήματος. Παραδείγματα τέτοιων τεχνικών είναι το Δαχτυλικό αποτύπωμα (fingerprint), η αναγνώριση ίριδας (Iris Recognition), η αναγνώριση αμφιβληστροειδούς (Retina), η γεωμετρία χεριού (Hand Geometry), η αναγνώριση προσώπου (Facial Recognition), αναγνώριση φωνής. Στην αρχή γίνεται η εγγραφή του χρήστη στο σύστημα αφού ληφθεί βιομετρικό δείγμα (biometric template) των χαρακτηριστικών του χρήστη μέσα από ένα αισθητήρα, αποθηκεύεται σε κωδικοποιημένη μορφή σε κάποια κεντρική βάση δεδομένων ή σε κάποια έξυπνη κάρτα. Για να πιστοποιηθεί η ταυτότητα του χρήστη συλλέγεται πάλι δείγμα από τον αισθητήρα σε κωδικοποιημένη μορφή και γίνεται σύγκριση με το αρχικό δείγμα που υπάρχει στη βάση δεδομένων[99].Το αποτέλεσμα της σύγκρισης είναι ποσοστιαίο σχετικά και ποτέ απόλυτο. Έτσι 70% ομοιότητα μπορεί να είναι αποδεκτό αποτέλεσμα για μια

---

[96] Βλ. άρθρο, The New York Times, αναδημοσίευση εφημερίδα Καθημερινή, 06-01-2012,στο: http://news.kathimerini.gr/4dcgi/_w_articles_economyagor_1_06/01/2012_468294

[97] Βλ. παρουσίαση για την ασφάλεια στο: http://infoman.teikav.edu.gr/e_education/70/InfoSystemSechandouts.ppt

[98] Η Βιομετρία είναι η επιστήμη που αναλύει βιολογικά στοιχεία χρησιμοποιώντας στατιστικές και μαθηματικές μεθόδους.

[99] Βλ. Πολέμη Ν., Καλιοντζόγλου Α., Πρακτικά Θέματα Ασφαλείας Πληροφοριακών Συστημάτων και Εφαρμογών, Εκδόσεις Νέων Τεχνολογιών, 2008, σελ. 63-65.

εφαρμογή που στόχο έχει τη διευκόλυνση μιας διαδικασίας, αλλά μη αποδεκτό για μια εφαρμογή που ελέγχει την ασφάλεια σε ένα σύστημα.

● **Ταυτοποίηση με χρήση έξυπνων καρτών** (smart card). Η έξυπνη κάρτα είναι μια μικρή πλαστική κάρτα που περιέχει ένα τσιπ υπολογιστή. Οι έξυπνες κάρτες χρησιμοποιούνται μαζί με προσωπικούς αναγνωριστικούς αριθμούς (PIN) για σύνδεση σε ένα δίκτυο, έναν υπολογιστή ή μια συσκευή. Η χρήση έξυπνης κάρτας αυξάνει την ασφάλεια κατά ένα επίπεδο σε σύγκριση με τον κωδικό πρόσβασης, καθώς είναι δυσκολότερο για κάποιον να κλέψει μια έξυπνη κάρτα και να μάθει το PIN σας απ΄ότι να μάθει τον κωδικό πρόσβασής σας. Οι έξυπνες κάρτες εκδίδονται συνήθως από τα τμήματα τεχνολογίας πληροφορικής (IT) μεγάλων οργανισμών. Για να χρησιμοποιηθεί μια έξυπνη κάρτα, χρειάζεται μια συσκευή ανάγνωσης έξυπνων καρτών— είναι μια συσκευή που εγκαθίσταται ή συνδέεται στον υπολογιστή σας και μπορεί να διαβάζει τις πληροφορίες που είναι αποθηκευμένες στην έξυπνη κάρτα [100].

2.2.2 **Εμπιστευτικότητα** (Confidentiality)

Η εμπιστευτικότητα ή αλλιώς απόρρητο δεδομένων είναι μια σημαντική λειτουργία της ασφάλειας καθώς προφυλάσσει από παθητικές επιθέσεις και μη αποκάλυψη ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένες οντότητες. Διακρίνεται σε :

● **Εμπιστευτικότητα σύνδεσης** (Connection Confidentiality). Η προστασία των δεδομένων όλων των χρηστών που βρίσκονται σε σύνδεση.

● **Ασυνδεσμική εμπιστευτικότητα** (Connectionless Confidentiality). Η προστασία των δεδομένων όλων των χρηστών σε κάθε μεμονωμένο τμήμα δεδομένων.

● **Εμπιστευτικότητα επιλεγμένου πεδίου** (Selective-Field Confidentiality). Η εμπιστευτικότητα επιλεγμένων πεδίων των δεδομένων των χρηστών σε μια σύνδεση ή ένα τμήμα δεδομένων.

● **Εμπιστευτικότητα ροής κίνησης** (Traffic-Flow Confidentiality). Η προστασία των πληροφοριών που μπορούν να αντληθούν από την παρατήρηση της ροής της επικοινωνίας. Αυτό προϋποθέτει ότι ο επιτιθέμενος δεν έχει την δυνατότητα να παρατηρήσει την προέλευση τον προορισμό και άλλα χαρακτηριστικά κίνησης σε ένα σύστημα επικοινωνιών. Οι παραπάνω διακρίσεις –εξειδικεύσεις είναι πιο πολύπλοκες και δαπανηρές στην υλοποίηση και λιγότερο χρήσιμες από την ευρεία προσέγγιση που αντιμετωπίζει την προστασία όλων των δεδομένων των χρηστών.

Η εμπιστευτικότητα επιτυγχάνεται με τη κρυπτογράφηση των δεδομένων, η οποία καθιστά τα δεδομένα μη αναγνώσιμα, καθώς και με έλεγχο πρόσβασης στα δεδομένα [101].

---

[100] Για περισσότερα βλ: http://windows.microsoft.com/el-GR/windows-vista/What-is-a-smart-card-and-how-do-I-use-one επίσης http://www.smartcardbasics.com.

[101] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 30-31.

2.2.3 **Ακεραιότητα δεδομένων** (Data Integrity)

Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Οι μηχανισμοί της ακεραιότητας προφυλάσσουν από μη εξουσιοδοτημένη τροποποίηση των δεδομένων όπως : Εγγραφή/Δημιουργία νέων δεδομένων, εισαγωγή νέων δεδομένων στα υπάρχοντα, διαγραφή μέρους ή όλων των δεδομένων[102]. Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα [103] ή επιχειρεί να τροποποιήσει αυτά.

Η ακεραιότητα επιτυγχάνεται με τη χρήση μηχανισμών αυθεντικοποίησης, με ψηφιακές υπογραφές, και με έλεγχο πρόσβασης . Ένας τρόπος για να ελεγχθεί η ακεραιότητα δεδομένων είναι να πάρουμε το άθροισμα του αναλλοίωτου αρχείου (checksum[104]) και να το αποθηκεύσουμε off-line και περιοδικά να κάνουμε σύγκριση του αρχείου αυτού με το άθροισμα του αρχείου (checksum) που χρησιμοποιείται on-line. Υπάρχουν λειτουργικά συστήματα τα οποία έχουν ενσωματωμένα τέτοια προγράμματα αθροίσματος ελέγχου (checksum) όπως το unix sum. Επίσης υπάρχουν προγράμματα που χρησιμοποιούνται για να ελέγχουν την ακεραιότητα των δεδομένων που ανταλλάσσονται στο ηλεκτρονικό ταχυδρομείο και πετυχαίνουν να φτάνουν τα μηνύματα αναλλοίωτα από τον αποστολέα στον παραλήπτη[105].

2.2.4 **Διαθεσιμότητα** (availability)

Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των εξουσιοδοτημένων χρηστών όποτε απαιτείται η χρήση τους και χωρίς αδικαιολόγητη καθυστέρηση. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των υπολογιστών του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου.

---

102 http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%ECF%81%CE%Ασφάλεια_πληροφοριακών_συστημάτωνBF%CF%CF%89%CE%BD

103 Ακριβώς αυτό συνέβη το 1995, όταν άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας της Ελευθεροτυπίας και να εισαγάγουν πρωτοσέλιδο άρθρο για τον πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο, βλ: Μακεδονικό Πρακτορείο Ειδήσεων, 7 Οκτωβρίου 1996, http://www.hri.org/info/articles/96-10-07.elot.html

104 Ένα τέτοιο πρόγραμμα και μάλιστα ελληνικό είναι το « Checksums calculator» το οποίο έχει αναπτύξει η Sigma Informatics. Αφορά την ασφάλεια του υπολογιστή και παρέχει την δυνατότητα να υπολογίσει αθροίσματα ελέγχου , για οποιοδήποτε αρχείο, οποιουδήποτε μεγέθους . Βλ http://www.sinf.gr/howtosums-win.html#checksums

105 Βλ.Θ.Κομνηνός,Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002, σελ. 162

Υπάρχει μεγάλος αριθμός επιθέσεων που μπορεί να οδηγήσουν σε μείωση ή και απώλεια της διαθεσιμότητας Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευόμενοι πόροι είτε προσωρινά, είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Το φαινόμενο Slashdot[106], κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα[107].

Σε ένα πληροφοριακό σύστημα η ασφάλεια υπηρετείται όταν αυτό μπορεί να λειτουργεί απρόσκοπτα. Κύριος στόχος του διαχειριστή του είναι η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των εξουσιοδοτημένων χρηστών σε αυτό. Οι επιθέσεις αυτές ονομάζονται επιθέσεις **άρνησης παροχής υπηρεσιών**. Η άρνηση παροχής υπηρεσιών σε ένα σύστημα, σημαίνει πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο ή παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων σε αυτό. Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη, που προκαλείται από κακόβουλα μέρη, παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης[108].

2.2.5 **Καταγραφή** (Audit)

Η καταγραφή(Audit) είναι μια διαδικασία η οποία καταγράφει με λεπτομέρεια , όλα τα συμβάντα ασφαλείας που συμβαίνουν σε ένα πληροφοριακό σύστημα. Ο έλεγχος συμβάντων επιτρέπει αξιόπιστη, λεπτομερή και παραμετροποιημένη καταγραφή πλήθους συμβάντων σχετικών με την ασφάλεια, συμπεριλαμβανομένων των logins, των αλλαγών ρυθμίσεων, καθώς και της πρόσβασης σε αρχεία και στο δίκτυο. Οι καταγραφές αυτές είναι πολύτιμες για απευθείας παρακολούθηση του συστήματος, ανίχνευση εισβολέων, καθώς και για ανάλυση μετά από κάποια επίθεση. Ένα τέτοιο πρόγραμμα καταγραφής είναι το FreeBSD . Η καταγραφή αφορά πέρα της ανίχνευσης εισβολέων που επιθυμούν την είσοδο στο σύστημα χωρίς εξουσιοδότηση και την καταγραφή των δραστηριοτήτων και ενεργειών των νόμιμων χρηστών. Έτσι ο administrator του συστήματος μέσα από τις πληροφορίες των αρχείων καταγραφής θα είναι σε θέση να γνωρίζει τι έκανε κάποιος χρήστης και τι επηρεάστηκε από τις ενέργειες του χρήστη.

---

[106] Βλ http://www.nview.gr/?page_id=151

[107] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 32.

[108] Στις επιθέσεις πλημμύρας δεδομένων, ένας επιτιθέμενος προσπαθεί να εκμεταλλευτεί το διαθέσιμο εύρος ζώνης σε ένα δίκτυο, στο μέγιστο βαθμό του, με την αποστολή τεραστίων ποσοτήτων δεδομένων και έτσι να το αναγκάζει να επεξεργάζεται εξαιρετικά μεγάλα ποσά δεδομένων. Ένας επιτιθέμενος θα μπορούσε να προσπαθήσει να καταναλώσει το διαθέσιμο εύρος ζώνης σε ένα δίκτυο απλά με το να βομβαρδίσει το θύμα με κανονικά, αλλά χωρίς νόημα πακέτα με ψευδείς διευθύνσεις προέλευσης. Ένα παράδειγμα είναι η πλημμύρα από ping, για περισσότερα βλ: http://nemertes.lis.upatras.gr/jspui/bitstream.pdf.

2.2.6 **Η μη αποποίηση** (non-repudiation

Η αποποίηση συμβαίνει όταν κάποια οντότητα αρνείται τη συμμετοχή σε μια επικοινωνία ή σε μία συναλλαγή. Η μη αποποίηση συνίσταται στη δυνατότητα μη αποκήρυξης γεγονότων που έχουν συμβεί κατά την επικοινωνία δύο οντοτήτων. Η υπηρεσία της μη αποποίησης αποτρέπει είτε τον αποστολέα είτε τον παραλήπτη να αρνηθούν την ύπαρξη ενός μηνύματος που έχει μεταδοθεί. Έτσι υπάρχει προστασία από την δόλια άρνηση μιας οντότητας ότι έλαβε μέρος σε μια ανταλλαγή πληροφοριών. Καθώς στέλνεται ένα μήνυμα , ο παραλήπτης είναι σε θέση να αποδείξει ότι ο αποστολέας έστειλε πραγματικά το μήνυμα. Με τον ίδιο τρόπο ,όταν παραλαμβάνεται ένα μήνυμα ο αποστολέας μπορεί να αποδείξει ότι ο παραλήπτης παρέλαβε το μήνυμα με σιγουριά[109]. Οι υπηρεσίες μη-αποποίησης είναι ιδιαίτερα σημαντικές στις συναλλαγές σε περιβάλλον ηλεκτρονικού επιχειρείν.

Ένας μηχανισμός αντιμετώπισης του προβλήματος αυτού του είδους είναι η χρήση ψηφιακής υπογραφής (digital signature) η οποία υλοποιείται με τη βοήθεια της κρυπτογραφίας. Η Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα). Οι ψηφιακές υπογραφές , πρέπει να πούμε ότι προέκυψαν από την ανάγκη να υποκαταστήσουν τις χειρόγραφες υπογραφές. Έτσι, σε ένα σύστημα επικοινωνίας θα πρέπει η μια πλευρά να στέλνει ένα «υπογεγραμμένο» μήνυμα στην άλλη πλευρά με τέτοιο τρόπο ώστε: Ο παραλήπτης να μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο αποστολέας. Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος. Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.

2.2.7 **Συνέπεια** (Consistency)

Λέγοντας Συνέπεια (Consistency) σε ένα πληροφοριακό Σύστημα εννοείται η διασφάλιση ότι το σύστημα συμπεριφέρεται όπως αρχικά αναμένεται τόσο από τον δημιουργό του όσο και από τους εξουσιοδοτημένους χρήστες του. Εάν το λογισμικό ή το υλικό μέρος του συστήματος αρχίσει να συμπεριφέρεται παράξενα, ειδικά μετά από κάποια αναβάθμιση ή μετατροπή ή κάποια επίθεση τότε υπάρχει πρόβλημα που μπορεί να οδηγήσει σε κατάρρευση. Τελικά η συνέπεια είναι η διασφάλιση της ορθότητας των δεδομένων και των προγραμμάτων που χρησιμοποιούμε.

[109] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 32.

2.2.8 **Έλεγχος πρόσβασης** (Control)

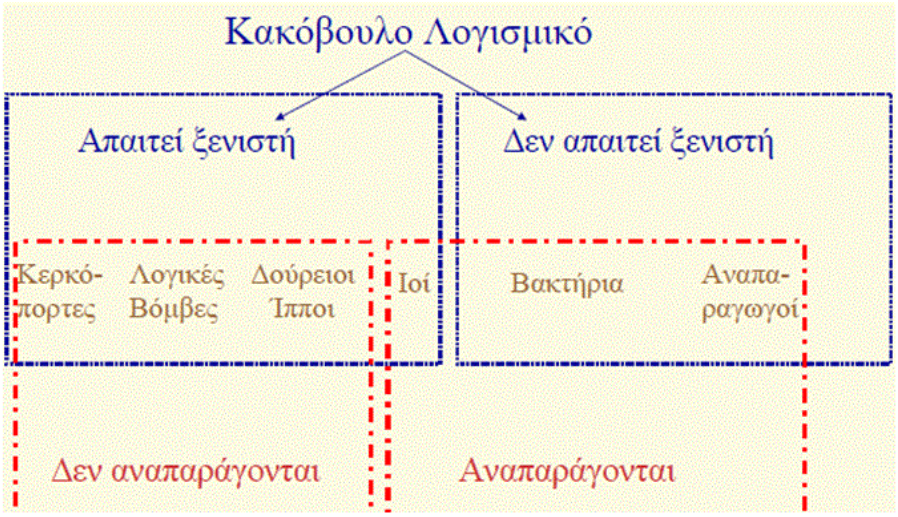
Ο έλεγχος πρόσβασης στο σύστημα και στην διάθεση των πληροφοριακών του πόρων, αντιμετωπίζει το πρόβλημα των παράνομων χρηστών – εισβολέων που επιχειρούν πρόσβαση στους πόρους του συστήματος, χωρίς εξουσιοδότηση. Αυτό επιτυγχάνεται με κατάλληλα Συστήματα Ελέγχου πρόσβασης (Access Control) ,τα οποία χρησιμοποιούνται για να παρέχουν διαβαθμισμένη πρόσβαση σε ένα πληροφοριακό σύστημα στους χρήστες, σύμφωνα με το επίπεδο την πολιτική ασφαλείας και τα δικαιώματα που έχουν αποδοθεί σε νόμιμους χρήστες αναφορικά με την διάθεση πληροφορικών πόρων του συστήματος και την ανάγνωση ,τροποποίηση ,διαγραφή αρχείων του συστήματος.

2.3 **Τρόποι παραβίασης της ιδιωτικότητας στο Διαδίκτυο**

Οι απειλές εναντίον πληροφοριακών συστημάτων εκδηλώνονται μέσω προγραμμάτων που εκμεταλλεύονται τρωτά σημεία-ευπάθειες ενός ή περισσότερων υπολογιστικών συστημάτων. Τέτοια προγράμματα αναφέρονται συνήθως με τον γενικό όρο κακόβουλο λογισμικό (malicious software). Τα προγράμματα αυτά είναι κατασκευασμένα ειδικά για το σκοπό της παραβίασης της ασφάλειας κάποιου πληροφοριακού συστήματος ή, συνηθέστερα, συνυπάρχουν μαζί με προγράμματα εφαρμογών όσο και προγράμματα γενικής χρήσης.

2.3.1 **Ιομορφικό και μη ιομορφικό κακόβουλο λογισμικό** (malware)

Το κακόβουλο λογισμικό με κριτήριο την αυτονομία, μπορούμε να το διακρίνουμε σε δύο κατηγορίες: αυτό που χρειάζεται ένα πρόγραμμα-φορέα(ξενιστής) και το αυτοτελή. Η πρώτη κατηγορία αποτελείται στην ουσία από τμήματα προγράμματος που δεν είναι δυνατόν να υπάρξουν ανεξάρτητα από κάποιο πρόγραμμα εφαρμογής ή λογισμικό συστήματος. Η δεύτερη κατηγορία αποτελείται από αυτοτελή προγράμματα, τα οποία μπορούν αφού χρονοπρογραμματιστούν να εκτελεστούν κάτω από τον έλεγχο του λειτουργικού συστήματος, όπως και κάθε άλλο πρόγραμμα. Μπορούμε, επίσης, να κατηγοριοποιήσουμε το κακόβουλο λογισμικό με κριτήριο την αναπαραγωγή: Έτσι έχουμε μη αναπαραγόμενο, όπου τμήματα προγράμματος ενεργοποιούνται όταν καλείται το πρόγραμμα-φορέας για να εκτελέσει μια συγκεκριμένη λειτουργία και *στο* αναπαραγόμενο στο οποίο τμήματα προγράμματος (ιοί), αλλά και αυτόνομα προγράμματα (έλικες, βακτήρια) που όταν εκτελούνται, μπορούν να παραγάγουν ένα ή περισσότερα αντίγραφα του εαυτού τους, τα οποία θα ενεργοποιηθούν αργότερα στο ίδιο ή σε κάποιο άλλο υπολογιστικό σύστημα βλέπε σχήμα 10.



Σχήμα 10. Είδη κακόβουλου λογισμικού

πηγή: http://www.iliadis.net/presentations/MaliciousSoftware.pdf

2.3.2 **Ιός** (virus)

Ιός είναι κακόβουλο πρόγραμμα με βλαβερό κώδικα, το οποίο ενσωματώνει τον κώδικά του σε ένα πρόγραμμα ξενιστή εγκαθίσταται στον υπολογιστή, συνήθως χωρίς την άδεια και τη γνώση του χρήστη, ενεργοποιείται είτε κάποια προκαθορισμένη χρονική στιγμή είτε ύστερα από κάποια συγκεκριμένη ενέργεια. Αναπαράγεται με την αντιγραφή του εαυτού του σε άλλα προγράμματα ξενιστές και εκτελείται στο παρασκήνιο. Η ενεργοποίηση ενός ιού μπορεί να έχει ως αποτέλεσμα διάφορες συνέπειες, επικίνδυνες ή μη. Συγκεκριμένα, μπορεί να έχει ως αποτέλεσμα το συνεχές άνοιγμα διαφόρων παραθύρων στην οθόνη, μπορεί όμως και να προκαλέσει την καταστροφή δεδομένων σε αρχεία ή άλλες βλάβες. Ένας ιός ενσωματώνεται σε ηλεκτρονικά μηνύματα και προγράμματα, έτσι ώστε όταν ανοίξουμε τα μηνύματα αυτά ή εκτελέσουμε τα προγράμματα, ενεργοποιούμε άθελά μας και τον ιό[110]. Οι ηλεκτρονικοί ιοί, λοιπόν, επιζούν με το να "μολύνουν" άλλα αρχεία, έχουν δηλαδή την ίδια παρασιτική συμπεριφορά που έχουν και οι οργανικοί ιοί.

Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση

[110] Βλ http://www.pi.ac.cy/InternetSafety/sec_kindinoi_virus.html

(format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά **την κλοπή προσωπικών του δεδομένων** ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη[111].

Ο κύκλος ζωής ενός ιού περιλαμβάνει τα παρακάτω στάδια:

Φάση επώασης, κατά την οποία ο ιός παραμένει ανενεργός στο υπολογιστικό σύστημα και ενεργοποιείται από κάποιο γεγονός όπως την έλευση μιας ημερομηνίας, την παρουσία ενός άλλου προγράμματος ή αρχείου ή την υπέρβαση κάποιου αποθηκευτικού ορίου στο δίσκο. Η φάση αυτή δεν είναι απαραίτητο να υπάρχει σε όλους τους ιούς.

Φάση αναπαραγωγής, όπου έχουμε δημιουργία αντιγράφων και ενδεχόμενη ενσωμάτωση σε ξενιστές. Κατά τη φάση αυτή ο ιός τοποθετεί ένα ακριβές αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε συγκεκριμένες περιοχές του δίσκου. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν κλώνο του ιού, ο οποίος με τη σειρά του θα μπει σε φάση διάδοσης

Φάση ενεργοποίησης και εκτέλεσης, στην οποία έχουμε εκτέλεση σειράς ενεργειών (payload) με πιθανές επιβλαβείς συνέπειες για το υπολογιστικό σύστημα που φιλοξενεί το ιομορφικό λογισμικό[112].

Οι ιοί μπορούν να ταξινομηθούν[113]:

Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν:

Τομείς σκληρού δίσκου συστήματος (system sectors)

Αρχεία

Ιοί μακροεντολών (Macros)

Ιοί πηγαίου κώδικα (Source Code Viruses)

---

111 Βλ. http://el.wikipedia.org/wiki/Ιός (Υπολογιστές)

112 Βλ Γ.Ηλιάδης, Κακόβουλο λογισμικό σε:Σ. Κάτσικα, Δ. Γκρίτζαλη ,Σ. Γκρίτζαλη ,Ασφάλεια πληροφοριακών συστημάτων , Αθήνα,2004,,σελ 238

113 Βλ http://www.cknow.com/cms/vtutor/types-of-viruses.html

Ιοί συμπλεγμάτων (σκληρού) δίσκου ((Hard) Disk Clusters)

Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:

Πολυμορφικοί ιοί

Αόρατοι ιοί (Stealth Viruses)

Θωρακισμένοι ιοί (Armored Viruses)

Πολυτμηματικοί ιοί (Multipartite Viruses)

Ιοί πλήρωσης κενών (Spacefiller Viruses)

Ιοί παραλλαγής (Camouflage Viruses)

*Σήμερα μπορούμε ν*α πούμε ότι οι **βασικοί τύποι ιών** είναι :

☞ **Παρασιτικοί** (parasitic viruses). Ο παραδοσιακός αλλά και πιο διαδεδομένος τύπος ιού. Οι ιοί αυτοί προσαρτώνται σε εκτελέσιμα αρχεία και αναπαράγονται, όταν εκτελεστεί το μολυσμένο πρόγραμμα, βρίσκοντας και άλλα εκτελέσιμα αρχεία για να μολύνουν.

☞ **Διαμένοντες στην κύρια μνήμη** (memory–resident). Οι ιοί αυτοί εγκαθίστανται στην κύρια μνήμη ως τμήματα προγραμμάτων που παραμένουν στη μνήμη. Από τη στιγμή της εγκατάστασής τους, οι ιοί αυτοί μολύνουν κάθε πρόγραμμα που εκτελείται.

☞ **Τομέα εκκίνησης** (boot). Οι ιοί αυτοί μολύνουν τον τομέα εκκίνησης του δίσκου. Διαδίδονται όταν το σύστημα εκκινήσει από το δίσκο που περιέχει τον ιό.

☞ **Δυσανιχνεύσιμοι** (stealth). Οι ιοί αυτοί είναι ειδικά σχεδιασμένοι ώστε να αποφεύγουν την ανίχνευση από ειδικό αντιβιοτικό λογισμικό.

☞ **Πολυμορφικοί** (polymorphic). Οι ιοί αυτοί μεταλλάσσονται με κάθε μόλυνση, αλλάζοντας την υπογραφή τους και καθιστώντας έτσι αδύνατη την ανίχνευσή τους μέσω αυτής[114].

Μια ιδιαίτερη μορφή ιών που τα τελευταία χρόνια έχει αυξηθεί σε πλήθος είναι οι μακροϊοί (macro-viruses), οι οποίοι προσβάλλουν αρχεία που περιέχουν μακροεντολές. Οι μακροεντολές είναι ακολουθίες εντολών, τις οποίες χρησιμοποιούν συγκεκριμένα προγράμματα για να αυτοματοποιήσουν ορισμένες λειτουργίες που εκτελεί ο χρήστης. Όταν εκτελεστεί μία μακροεντολή ενός μολυσμένου αρχείου μέσα από το κατάλληλο πρόγραμμα (επεξεργαστές κειμένου, φύλλα εργασίας κ.ά.), ο ιός ενεργοποιείται και μπορεί να μολύνει άλλα αρχεία που περιέχουν μακροεντολές. Τα Macro Viruses απαντώνται πολύ συχνά σε αρχεία MS-Word και MS-Excel, που είναι τα δύο πιο διαδεδομένα προγράμματα εφαρμογών γραφείου. Η δημοτικότητα των δύο αυτών προγραμμάτων, καθώς και το πλήθος τέτοιων αρχείων που μεταφέρονται από υπολογιστή σε υπολογιστή κυρίως μέσω e-mail, έχουν συνεισφέρει κατά πολύ στην εξάπλωση αυτού του είδους των ιών. Οι μακροϊοί μολύνουν μεγαλύτερο πλήθος αρχείων από τους συμβατικούς ιούς –που μολύνουν συνήθως μόνο εκτελέσιμα αρχεία– αφού προσβάλλουν έγγραφα και μη εκτελέσιμα τμήματα κώδικα. Οι περισσότερες πληροφορίες που εμφανίζονται σε ένα υπολογιστικό σύστημα έχουν την μορφή ενός εγγράφου παρά ενός

[114] Βλ Σ.Κάτσικα, Ασφάλεια Υπολογιστών, Πάτρα,2001,ΕΑΠ,σελ189

προγράμματος. Τα ενιαία πρωτόκολλα ηλεκτρονικού ταχυδρομείου που διασυνδέουν τους περισσότερους υπολογιστές σήμερα, ανεξαρτήτως κατασκευαστικής πλατφόρμας, αποτελούν ένα εξαιρετικό μέσο μεταφοράς και διάδοσης των μακροϊών. Μακροϊοί έχουν εμφανιστεί και για άλλα προϊόντα του λογισμικού πακέτου Microsoft Office, όπως το Microsoft Excel, Microsoft PowerPoint και Microsoft Access και επίσης .

Οι ιοί αυτοί είναι ιδιαίτερα επικίνδυνοι, επειδή:

☞ Είναι ανεξάρτητοι από πλατφόρμες υλικού. Σχεδόν όλοι τους μολύνουν αρχεία Microsoft. Κάθε πλατφόρμα υλικού και λειτουργικό σύστημα που υποστηρίζει το Word μπορεί να μολυνθεί.

☞ Μολύνουν αρχεία κειμένου και όχι εκτελέσιμα προγράμματα. Η πλειοψηφία της πληροφορίας που εισάγεται σε ένα υπολογιστικό σύστημα είναι σε μορφή τέτοιων αρχείων και όχι σε μορφή εκτελέσιμων προγραμμάτων.

☞ Διαδίδονται εύκολα. Μια πολύ συνηθισμένη μέθοδος διάδοσης είναι με το ηλεκτρονικό ταχυδρομείο[115].

Ο καλύτερος τρόπος προστασίας ενάντια στους μακροϊούς είναι η απενεργοποίηση των μακροεντολών, αλλά αυτό έχει σαν αποτέλεσμα την απώλεια λειτουργικότητας που μπορούν να παρέχουν οι μακροεντολές. Τα προγράμματα προστασίας του υπολογιστή (antivirus) εντοπίζουν εύκολα τους γνωστούς μακροϊούς και ειδοποιούν τον χρήστη μόλις μια μακροεντολή είναι έτοιμη να εκτελεστεί. Υπάρχουν επίσης βιβλιοθήκες με πληροφορίες για ιούς που υπάρχουν στο δίκτυο, όπως η http://vil.nai.com/ . Στις βιβλιοθήκες αυτές αναφέρονται και τα e-mail που είναι φάρσες (hoaxes).

Οι πιο καταστροφικοί ιοί στη ιστορία του internet :

● **Ο ιός Morris (1988**). Σε μια εποχή που το ίντερνετ ήταν ακόμα ιδανικό και τα Windows είχαν αναπτυχθεί με γνώμονα τη μη-προστασία, ο φοιτητής Robert Morris δημιούργησε το πρώτο worm, που έφερε το όνομά του, και κατάφερε να μολύνει σχεδόν το 10% των συνδεδεμένων στο Internet υπολογιστών.

● **Ο ιός I Love You** εξαπλώθηκε ταχύτατα το έτος 2000 σ' όλον τον κόσμο και προκάλεσε μεγάλη αναστάτωση και κινητοποίηση. Ως δράστης συνελήφθη ένας 23χρονος από τις Φιλιππίνες, ο οποίος ισχυρίσθηκε ότι δεν δημιούργησε τον ιό αλλά ότι απλά τον βελτίωσε. Ο ιός αυτός έδειξε μια ιδιαίτερη προτίμηση σε αρχεία πολυμέσων τύπου .jpg, .mpeg και .mp3 Οι απανταχού «ερωτοχτυπημένοι» άνοιγαν το μήνυμα και το συννημένο «ερωτικό γράμμα» διαδίδοντας τον ιό που έκανε το γύρω του κόσμου σε μια μέρα. Μέσα σε οχτώ μέρες υπήρχαν 50 εκατομμύρια μολυσμένοι υπολογιστές και ζημίες 5,5 δις δολαρίων. Εξαιτίας του ιού, το Πεντάγωνο, η CIA και το Βρετανικό Κοινοβούλιο υποχρεώθηκαν να «κατεβάσουν» τους mail server τους το 2000.

● **Ο ιός Melissa** και οι διάφορες παραλλαγές του ήταν δημιούργημα του Ντέιβιντ Σμιθ και προκάλεσαν απανωτά επεισόδια μεταξύ 1999-2005. Ήταν από τους πρώτους ιούς που μεταδιδόταν μέσω μηνυμάτων e-mail με τη μορφή ενός συνημμένου αρχείου Word και προξένησε ζημιές εκατομμυρίων δολαρίων. Ο ιός δημιουργήθηκε το έτος 1999. Αν ο χρήστης έκανε το λάθος να ανοίξει το επισυναπτόμενο αρχείο, ο ιός ενεργοποιείτο, αναπαρήγαγε τον

[115] Βλ ό.π, Σ.Κάτσικα, Ασφάλεια Υπολογιστών, Πάτρα,2001,ΕΑΠ,σελ 190

εαυτό του και έστελνε ένα ανάλογο μήνυμα στους πρώτους 50 παραλήπτες που έβρισκε στο βιβλίο διευθύνσεων (address book) του θύματος. Για τη δράση του ο Σμιθ καταδικάστηκε σε φυλάκιση 20 μηνών και χρηματικά πρόστιμα. Αργότερα συνεργάστηκε με το FBI για την εξάρθρωση άλλων ομάδων χάκερ.

● **Ο ιός Code Red** τύπου worm, στις 19 Ιουλίου 2001, είχε προσβάλλει 359 χιλιάδες υπολογιστές. Ήταν ο πρώτος μιας σειράς ιών που εκμεταλλεύονταν μια αδυναμία γνωστή ως buffer overflow εμποδίζοντας τη σύνδεση στο Ίντερνετ. Στα θύματα συγκαταλέγονται ο web server του Λευκού Οίκου και ένα σωρό website που είδαν την αρχική του σελίδα να γράφει «HELLO! Welcome to http://www.worm.com! Hacked By Chinese!».

● **Ο ιός Slammer** [116] τύπου worm**.** Δύο χρόνια μετά τον Code Red, ένα ξαδερφάκι του, ο Slammer, εκμεταλλεύθηκε μια τρύπα στον SQL server της Microsoft και προκάλεσε καταστροφή τον Ιανουάριο του 2003, αν και το μέγεθός του ήταν μόνο 376 bytes γονάτισε το διαδίκτυο προσβάλλοντας 75 χιλιάδες υπολογιστές. Ανάμεσα στα θύματα ήταν το κορεατικό πρακτορείο ειδήσεων Yohhap που αναγκάστηκε να κλείσει για ώρες στις 25 Ιανουαρίου 2003. Ο ιός ήταν τόσο επιθετικός που στο μικρό διάστημα της παρουσίας του πολλές χώρες το εξέλαβαν για οργανωμένη επίθεση εναντίον τους. Ευτυχώς δύο τυχαίοι παράγοντες απέτρεψαν τα χειρότερα: Ο ιός διαδόθηκε μέσα σε σαββατοκύριακο και έγινε αντιληπτός από τον Μάικλ Μπακαρέλα που ειδοποίησε το σύστημα προστασίας Bugtraq.

● **Ο ιός Nimda** Στις 18 Σεπτεμβρίου 2001 και μέσα σε, μόλις, 22 λεπτά ο Nimda έγινε ο πιο επιτυχημένος ιός του διαδικτύου. Το κλίμα γενικευμένου πανικού από τις επιθέσεις της 11ης Σεπτεμβρίου οδήγησε στη συσχέτιση του ιού με την Αλ Κάιντα αν και κάτι τέτοιο δεν αποδείχτηκε ποτέ.

● **Ο ιός Blaster** θεωρείται από τους πιο καταστροφικούς ιούς καθώς έχει τη δυνατότητα να μπλοκάρει ολόκληρα δίκτυα υπολογιστών. Δημιουργήθηκε το έτος 2003 από τον 18χρονο Τζέφρι Λι Πάρσον, ο οποίος αν και συνελήφθη και καταδικάστηκε σε 18 μήνες φυλάκισης, κατάφερε να στείλει ένα ξεκάθαρο μήνυμα στον Μπιλ Γκέιτς: «Μπίλι σταμάτα να βγάζεις χρήμα και διόρθωσε το λογισμικό σου» έγραφε η ιστοσελίδα των Windows Update τον Αύγουστο του 2003.Υπογραφή: Blaster[117].

● **Ο ιός Sasser** , ένας ακόμα ιός που έκανε χρήση του buffer overflow. Δημιουργός του ένας 18χρονος Γερμανός φοιτητής πληροφορικής, ονόματι Σβεν Γιάσαν που κατάφερε το έτος 2004 και σε διάστημα μερικών εβδομάδων να μολύνει εκατομμύρια υπολογιστές σ' όλον τον κόσμο. Ο ιός προκαλούσε συνεχείς επανεκκινήσεις των μολυσμένων υπολογιστών. Το Γαλλικό Πρακτορείο ειδήσεων έκλεισε όλες του τις δορυφορικές επικοινωνίες για ώρες, η Delta Air Lines ακύρωσε αρκετές υπερατλαντικές πτήσεις, το Βρετανικό Λιμενικό έμεινε χωρίς ηλεκτρονικούς χάρτες ενώ ζημιές υπέστησαν μεγάλες εταιρείες όπως η Goldman Sachs και οργανισμοί όπως το Γερμανικό Ταχυδρομείο και η Κομισιόν[118].

● **Ο ιός Storm** Ένα μήνυμα ηλεκτρονικού ταχυδρομείου που έγραφε «230 νεκροί από καταιγίδα στην Ευρώπη» έκανε το γύρο του κόσμου τον Ιανουάριο του 2007. Τελικά η καταιγίδα ήταν ο

---

[116] http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html

[117] Για περισσότερες πληροφορίες και υποστήριξη βλέπε: http://support.microsoft.com/kb/826955

[118] http://news.bbc.co.uk/2/hi/technology/3640506.stm

ιός Storm, η Ευρώπη ήταν η Microsoft, που είδε την κεντρική της σελίδα σε κατάσταση «denial of service», και οι 230 νεκροί το 8% των παγκοσμίων μολύνσεων από τότε[119].

● **Ο ιός Conficker** , λειτουργεί επιτρέποντας την εγκατάσταση προγραμμάτων σε υπολογιστές από απόσταση κάτι που τον κάνει ιδανικό για την εξυπηρέτηση των σκοπών του κυβερνοεγκλήματος. Το πιο εύλογο κίνητρο είναι η υποκλοπή τραπεζικών στοιχείων και χρημάτων. Η εποχή που οι ιοί γράφονταν απλώς για να προκαλέσουν αίσθηση, να δηλώσουν διαμαρτυρία και να σπάσουν τα νεύρα υπηρεσιών / κυβερνήσεων έχει περάσει ανεπιστρεπτί. Γι' αυτό φρόντισε ο Conficker, που ξεκινώντας στα τέλη του 2008 διατηρεί ακόμα και σήμερα ένα δίκτυο χιλιάδων μολυσμένων υπολογιστών[120].

2.3.3 **Χάκερ**(Hacker)

Η έννοια του Χάκερ[121] για τους ειδικούς σε θέματα ασφαλείας είναι πολυσήμαντη. Μερικοί από αυτούς πιστεύουν ότι οι hackers είναι άριστοι προγραμματιστές που αντλούν ευχαρίστηση από τη βαθειά κατανόηση της εσωτερικής λειτουργίας ενός συστήματος, ειδικότερα ενός υπολογιστή ή δικτύου υπολογιστών, στον οποίο, όμως, δεν έχει δικαίωμα πρόσβασης. Άλλοι υποστήριζαν ότι οι hackers είναι κοινοί εγκληματίες, κρυμμένοι πίσω από ένα πέπλο ανωνυμίας, μια γνώμη που συμμερίζεται με πάθος και η πλειοψηφία των ΜΜΕ. Πολλοί ειδικοί σε θέματα πληροφορικής, στελέχη μεγάλων εταιρειών πληροφορικής, ήταν στο παρελθόν οι ίδιοι hackers, εντασσόμενοι και στους δύο παραπάνω ορισμούς, γεγονός που περιπλέκει τα πράγματα στην απόδοση ενός ξεκάθαρου ορισμού.

Η διεθνής κοινότητα των χάκερ πιστεύει ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητές τους τόσο δημιουργώντας λογισμικό ανοικτού κώδικα, όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό. Έχουν, επίσης, την αμφιλεγόμενη πεποίθηση ότι το "σπάσιμο" και η "εξερεύνηση" ενός υπολογιστικού συστήματος, τόσο σε επίπεδο υλικού όσο και (κυρίως) λογισμικού είναι ηθικά αποδεκτή, εφόσον ο χάκερ δεν διαπράττει κλοπή, βανδαλισμό ή παραβίαση εμπιστευτικότητας. Για τους χάκερς, όποιος "αξίζει αυτόν τον τίτλο, είναι στην πραγματικότητα ένας έξυπνος προγραμματιστής ή άτομο με ιδιαίτερες ικανότητες στην κατανόηση και το χειρισμό υπολογιστικών συστημάτων". Σε καμία, όμως, περίπτωση, δεν αποδέχονται ότι οι πράξεις ενός χάκερ έχουν κακόβουλους στόχους και αυτή η διαφορά είναι που τους διακρίνει από τους κράκερς.

Ο όρος "hacking" χρησιμοποιείται σήμερα σε καθημερινή βάση για να περιγράψει απάτες ηλεκτρονικές και παράνομη πρόσβαση στους πόρους ενός υπολογιστικού συστήματος ή δικτύου. Η αστυνομία περιγράφει σχεδόν κάθε έγκλημα σχετιζόμενο με υπολογιστή σαν hacking[122]. Η σύγχρονη χρήση της λέξης hacking, σημαίνει την δραστηριότητα με κακόβουλο κίνητρο, όπως οι απόπειρες εισβολής σε υπολογιστικά συστήματα και δίκτυα για την κλοπή ή

---

[119] http://en.wikipedia.org/wiki/Storm_botnet

[120] http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_27/04/2009_276796

[121] Αρχικά ο όρος "χάκερ" σήμαινε στα αγγλικά το δημιουργό ενός επίπλου ή γενικότερα ξύλινου αντικειμένου με τη βοήθεια πελέκεως (τσεκουριού) βλ http://el.wikipedia.org/wiki/%CE% Χάκερ%CF%81.

[122] Sterling Bruce , "The Hacker Crackdown: Law and Disorder on the Electronic Frontier" , Bantam Books , Reprint Edition , 1993 .

καταστροφή δεδομένων. Αν και το hacking, μπορεί να έχει πάρα πολλά κίνητρα,(όπως απλή περιέργεια, επιθυμία για επίδειξη, κοινωνική διαμαρτυρία κ.λ,π), οι εγκληματικές δραστηριότητες των “hackers” αυτές που κερδίζουν την μεγαλύτερη δημοσιότητα από τα μέσα ενημέρωσης[123].

Συνηθέστερα κάποιοι άλλοι προτιμούν να προσδιορίζουν την δραστηριότητα του κακόβουλου hacking με άλλους όρους όπως π.χ. “cracking”. Οι Αρχές αρέσκονται να χρησιμοποιούν τους όρους cybercrime (κυβερνοέγκλημα) και cyberterrorism (κυβερνοτρομοκρατία) για να περιγράψουν τις εγκληματικές δραστηριότητες των hackers. Ο cracker σε αντίθεση με τον hacker, είναι άτομο (ή ομάδα ατόμων) που αποπειράται να αποκτήσει πρόσβαση σε υπολογιστικό σύστημα για την οποία όχι μόνο δε διαθέτει εξουσιοδότηση, αλλά με στόχο να το βλάψει με οποιοδήποτε τρόπο. Οι crackers είναι εξ ορισμού κακόβουλοι, αντίθετα προς τους hackers, έχουν σαν κύρια ασχολία τους, την εισβολή σε πληροφοριακά συστήματα. Ο συγκεκριμένος όρος γεννήθηκε το 1985 από hackers, σε υπεράσπιση τους, από την λανθασμένη χρήση του όρου “hacker” από τον έντυπο τύπο ενώ διαθέτουν και πολλά εργαλεία για τις κακόβουλες ενέργειές τους[124].

Ανεξάρτητα από τον όρο που κάθε ένας χρησιμοποιεί ,καθώς και τις προθέσεις του εισβολέα, το πιο σημαντικό είναι πως οι ενέργειες των hackers συμβάλουν στην βελτίωση των πληροφοριακών συστημάτων, διορθώνοντας τρωτά σημεία τους και παρέχοντας μεγαλύτερη ασφάλεια στο μέλλον. Με αυτόν τον τρόπο ο εισβολέας λειτουργεί σαν απλήρωτος και αυτόκλητος σύμβουλος ασφαλείας.

Πολλοί νεαροί hackers αρέσκονται να μπαινοβγαίνουν στα συστήματα, άλλοι πάλι εξασκούν το hacking σαν νόμιμο επάγγελμα (Sneakers), εργαζόμενοι σαν μηχανικοί ασφαλείας. Εργάζονται συνήθως σε ομάδες, ελέγχοντας την ασφάλεια των υπολογιστικών συστημάτων και εγκαταστάσεων. Οι ομάδες αυτές αποκαλούνται «tiger teams» όπου κάθε μέλος έχει συνήθως κάποια συγκεκριμένη ειδικότητα και αποστολή[125]. Η βασική τους αποστολή είναι η εύρεση τρωτών σημείων του υπολογιστικού συστήματος και δικτύου της εταιρείας από δικούς της υπαλλήλους που είναι έμπιστοι. Με αυτό τον τρόπο οι εταιρείες διορθώνουν τα κενά ασφαλείας του συστήματός τους και προλαβαίνουν επιθέσεις κακόβουλων εισβολέων. Μέλη αυτών των ομάδων μπορεί να είναι και πρώην hackers που τώρα εργάζονται για την ασφάλεια υπολογιστικών συστημάτων μιας εταιρείας[126].

---

123 «18χρονος Έλληνας “χάκερ” από το Μπραχάμι τρέλανε FBI και Interpol - Έρχονται οι Αμερικανοί του FBI να τον γνωρίσουν» στο http://www.inews.gr/135/18chronos-ellinas-chaker-apo-to-brachami-trelane-FBI-kai-Interpol---erchontai-oi-amerikanoi-tou-FBI-na-ton-gnorisoun.htm βλέπε επίσης: http://www.cosmo.gr/Epikairotita/Ellada/Eidiseis/epithesh-apo-xaker-sthn-istoselida-ths-voylhs.1305183.html

124 Βλ. http://el.wikipedia.org/wiki/χάκερ

125 Ο όρος είναι στρατιωτικός και αναφέρεται σε μια ομάδα στρατιωτών που προσπαθούν να εισβάλουν σε ασφαλείς εγκαταστάσεις The Vulnerability Process: A Tiger Team Approach to Resolving Vulnerability Cases (1999) by M. Laakso , A. Takanen , J. Röning στο: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.39.9438&rep=rep1&type=pdf βλέπε επίσης http://wikipedia.qwika.com/en2el/Tiger_team

126 Βλ. http://www.retrocomputers.gr/index.php/2012-04-19-12-21-04/hackers

2.3.4 **Οι Δούρειοι Ίπποι** (Trojan Horses)

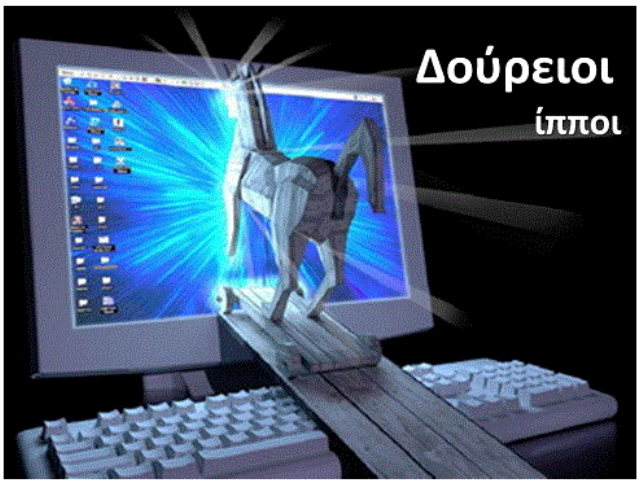
Ο Δούρειος Ίππος[127] (Trojan Horse) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα[128]. Οι Δούρειοι Ίπποι μπορούν να χρησιμοποιηθούν για να πραγματοποιήσουν έμμεσα λειτουργίες που ο μη εξουσιοδοτημένος χρήστης δεν μπορεί άμεσα να εκτελέσει. Για παράδειγμα, προκειμένου να αποκτήσει πρόσβαση στα αρχεία ενός άλλου χρήστη σε ένα διαμοιραζόμενο σύστημα, ένας χρήστης θα μπορούσε να δημιουργήσει ένα Δούρειο Ίππο που, όταν εκτελείται, αλλάζει τις παραμέτρους προστασίας των αρχείων του χρήστη που το εκτελεί έτσι ώστε τα αρχεία να είναι αναγνώσιμα από όλους. Ο δημιουργός μπορεί μετά να παρασύρει τους άλλους χρήστες να χρησιμοποιήσουν το Δούρειο Ίππο βάζοντάς τον σε ένα κοινό ευρετήριο και ονομάζοντάς τον έτσι ώστε να φαίνεται σαν ένα χρήσιμο πρόγραμμα, όπως, π.χ., ένα πρόγραμμα που εμφανίζει τα αρχεία ενός χρήστη σε μια επιθυμητή και βολική μορφή. Παράδειγμα ενός Δούρειου Ίππου που είναι δύσκολο να ανιχνευτεί είναι ένας μεταφραστής που έχει τροποποιηθεί και εισάγει επιπλέον κώδικα σε συγκεκριμένα προγράμματα, καθώς αυτά μεταφράζονται.

Ένα τέτοιο πρόγραμμα μπορεί να είναι και αυτό που καθορίζει τις διαδικασίες εισόδου στο σύστημα, στο οποίο ο κώδικας που εισάγεται επιπλέον επιτρέπει στο δημιουργό να αποκτήσει πρόσβαση στο σύστημα χρησιμοποιώντας ένα ειδικό συνθηματικό. Αυτός ο Δούρειος Ίππος, που δημιουργεί μια κερκόπορτα, δεν είναι ποτέ δυνατόν να αποκαλυφθεί με ανάγνωση του πηγαίου κώδικα του προγράμματος εισόδου[129]. Ένα άλλο συνηθισμένο κίνητρο για να γράψει κάποιος Δούρειο Ίππο είναι η καταστροφή δεδομένων. Το πρόγραμμα φαινομενικά εκτελεί μια χρήσιμη λειτουργία (π.χ. ένα πρόγραμμα αριθμομηχανής), αλλά επίσης, σιωπηρά, διαγράφει τα αρχεία του χρήστη.

[127] Το όνομά του προκύπτει από την Ιλιάδα του Ομήρου, όπου αναγράφεται ότι ο Οδυσσέας εμπνεύστηκε την κατασκευή ενός ξύλινου αλόγου, στην κοιλιά του οποίου κρύβονταν Αχαιοί πολεμιστές. Με τον τρόπο αυτό ξεγέλασε τους κάτοικους της Τροίας, εισήγαγε τον στρατό των Αχαιών μέσα στην πόλη και την κυρίευσε. Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας, οπότε πήραν και αυτήν την ονομασία.

[128] Βλ σχετικά http://el.wikipedia.org/wiki/Δούρειος_Ίππος

[129] Βλ ό.π, Σ.Κάτσικα, Ασφάλεια Υπολογιστών, Πάτρα,2001,ΕΑΠ,σελ201



Εικόνα 1. Δούρειος ίππος

Πηγή: http://clickoclock.blogspot.com/2011/07/zeus-trojan-horse.html

Η πλειοψηφία των μολύνσεων υπολογιστών από δούρειους ίππους συμβαίνει επειδή ο χρήστης προσπάθησε να εκτελέσει ένα μολυσμένο πρόγραμμα. Για τον λόγο αυτό οι χρήστες πάντα προτρέπονται να μην ανοίγουν ύποπτα αρχεία επισυναπτόμενα σε e-mail. Συνήθως το επισυναπτόμενο αρχείο περιλαμβάνει όμορφα γραφικά ή κινούμενη εικόνα, αλλά περιέχει επίσης ύποπτο κώδικα που μολύνει τον υπολογιστή του χρήστη. Παρόλα αυτά, το πρόγραμμα δεν είναι απαραίτητο να έχει φτάσει στον χρήστη με e-mail. Μπορεί να το έχει κατεβάσει από έναν ιστοχώρο, μέσω προγραμμάτων Instant Messaging, σε CD ή DVD.

Γνωστοί δούρειοι ίπποι που εμφανίστηκαν κατά καιρούς: Downloader-EV, Dropper-EV, Pest Trap, NetBus, flooder, Tagasaurus, Vundo Trojan, Gromozon Trojan, Sub-7, Cuteqq_Cn.exe[130].Τα σημαντικότερα βήματα για την αντιμετώπιση των δούρειων ίππων και των υπόλοιπων βλαβερών εφαρμογών είναι εγκατάσταση προγραμμάτων προφύλαξης (antivirus, firewall, spyware) και συχνή ενημέρωσή τους μέσω των εταιριών,καθώς και χρήση των τελευταίων ενημερώσεων του λειτουργικού συστήματος (patches, service packs).Πέρα όμως από αυτά, ο χρήστης θα πρέπει να είναι ιδιαίτερα προσεκτικός, όταν μεταφέρει λογισμικό στον υπολογιστή του, ειδικά από το internet και την ηλεκτρονική αλληλογραφία. Οι χρήστες των Windows Vista έχουν ήδη ένα επιπλέον όπλο στη διάθεσή τους, που ενημερώνει το χρήστη, όταν εκτελείται εφαρμογή της οποίας η προέλευση δεν έχει εξακριβωθεί (user account control)[131]. Ιδιαίτερη προσοχή θα πρέπει να δίνουν οι χρήστες με παλαιότερα λειτουργικά συστήματα ή χωρίς ενημερωμένες εκδόσεις τους.

130 http://el.wikipedia.org/wiki/Δούρειος_Ίππος

131 Ο Έλεγχος λογαριασμού χρήστη (UAC) είναι μια δυνατότητα στα Windows που μπορεί να εμποδίσει μη εξουσιοδοτημένες αλλαγές στον υπολογιστή σας. Ο UAC το κάνει αυτό ζητώντας την άδεια από εσάς ή έναν κωδικό πρόσβασης διαχειριστή για να εκτελέσει ενέργειες που θα μπορούσαν ενδεχομένως να επηρεάσουν τη λειτουργία του υπολογιστή σας ή που αλλάζουν ρυθμίσεις, οι οποίες επηρεάζουν άλλους χρήστες. Όταν δείτε ένα μήνυμα UAC, διαβάστε το προσεκτικά και μετά βεβαιωθείτε ότι το όνομα της ενέργειας ή του προγράμματος που πρόκειται να

2.3.5 **Λογισμικό παρακολούθησης- υποκλοπής , προγράμματα** Spyware

Ο όρος spyware, που σημαίνει κυριολεκτικά «λογισμικό κατασκόπευσης», περιγράφει το λογισμικό το οποίο εγκαθίσταται λαθραία στον ηλεκτρονικό υπολογιστή με σκοπό να υποκλέψει ή να πάρει τον μερικό έλεγχο της επικοινωνίας του χρήστη με τον υπολογιστή, χωρίς να υπάρχει προηγουμένως η συγκατάθεση του χρήστη κατόπιν πληροφόρησης[132]. Το λογισμικό υποκλοπής spyware, εκτελεί συγκεκριμένες ενέργειες, όπως προώθηση διαφημίσεων(ονομάζεται λογισμικό adware), συλλογή προσωπικών δεδομένων ή αλλαγή των ρυθμίσεων του υπολογιστή σας χωρίς τη συγκατάθεσή του χρήστη. Αυτό δεν σημαίνει ότι κάθε διαφημιστικό λογισμικό ή λογισμικό που παρακολουθεί τις ενέργειές σας στο Internet είναι επιζήμιο. Για παράδειγμα, μπορείτε να εγγραφείτε σε μια δωρεάν υπηρεσία λήψης μουσικής και να δεχτείτε, αντί για την καταβολή κάποιας συνδρομής, να λαμβάνετε διαφημιστικά μηνύματα. Εάν κατανοείτε τους όρους και συμφωνείτε, μπορεί να αποφασίσετε ότι πρόκειται για δίκαιη συναλλαγή. Μπορεί, επίσης, να συμφωνήσετε η εταιρεία να παρακολουθεί τη δραστηριότητά σας στο Internet, προκειμένου να προσδιορίζει ποιες διαφημίσεις θα προβάλλονται σε εσάς.

Κάποια άλλα είδη λογισμικού υποκλοπής spyware ενδέχεται να προκαλέσουν αλλαγές στον υπολογιστή σας που είναι ενοχλητικές και μπορεί να μειώσουν την ταχύτητά του ή να τον κάνουν να "κολλάει". Τα προγράμματα αυτά μπορούν να αλλάξουν την κεντρική σελίδα ή τη σελίδα αναζήτησης του προγράμματος περιήγησης Web που χρησιμοποιείτε, ή να προσθέσουν επιπλέον μέρη στο πρόγραμμα περιήγησης τα οποία δεν χρειάζεστε ή δεν επιθυμείτε. Σε αυτή την περίπτωση, είναι πολύ δύσκολο να επαναφέρετε τις αρχικές ρυθμίσεις που είχατε καθορίσει. Σε όλες αυτές τις περιπτώσεις, το θέμα είναι κατά πόσο εσείς (ή το άτομο που χρησιμοποιεί τον υπολογιστή σας) κατανοείτε ή όχι τι κάνει αυτό το λογισμικό και κατά πόσο έχετε συμφωνήσει να εγκαταστήσετε το λογισμικό στον υπολογιστή σας.

Υπάρχουν αρκετοί τρόποι με τους οποίους μπορεί να εγκατασταθεί στον υπολογιστή σας το λογισμικό υποκλοπής spyware ή άλλο ανεπιθύμητο λογισμικό. Ένα συνηθισμένο κόλπο είναι η κρυφή εγκατάσταση του λογισμικού κατά την εγκατάσταση λογισμικού , όπως προγράμματα κοινής χρήσης αρχείων μουσικής και βίντεο. Για το λόγο αυτό, όταν γίνεται εγκατάσταση ενός τέτοιου προγράμματος στον υπολογιστή , φροντίζουμε να διαβάζουμε προσεκτικά όλους τους όρους, συμπεριλαμβανομένης της σύμβασης άδειας χρήσης και της δήλωσης σχετικά με την προστασία προσωπικών δεδομένων. Μερικές φορές η χρήση ανεπιθύμητου λογισμικού στην εγκατάσταση κάποιου λογισμικού τεκμηριώνεται, αλλά μπορεί να εμφανίζεται στο τέλος της σύμβασης άδειας χρήσης ή της δήλωσης σχετικά με την προστασία προσωπικών δεδομένων[133].

ξεκινήσει είναι αυτό που είχατε σκοπό να ξεκινήσετε. Όταν απαιτείται η άδειά σας ή ο κωδικός πρόσβασης για να ολοκληρωθεί μια εργασία, ο έλεγχος UAC θα σας ειδοποιήσει με ένα από τα παρακάτω μηνύματα:Τα Windows χρειάζονται την άδειά σας για να συνεχίσουν,Ένα πρόγραμμα χρειάζεται την άδειά σας για να συνεχίσει,Ένα άγνωστο πρόγραμμα ζητά πρόσβαση στον υπολογιστή σας, Αυτό το πρόγραμμα έχει αποκλειστεί.

[132] Βλ http://el.wikipedia.org/wiki/Spyware

[133] βλ http://www.microsoft.com/hellas/athome/security/spyware/spywarewhat.mspx

2.3.6 **Οι Κερκόπορτες** (Backdoors)

Κερκόπορτα (Backdoors ή trapdoor) είναι μια κρυφή είσοδος σ' ένα πρόγραμμα ενός υπολογιστή στόχου, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα με τους δικούς του όρους, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης.

Οι κερκόπορτες χρησιμοποιήθηκαν για πολλά χρόνια από τους προγραμματιστές, για να εκσφαλματώσουν και να δοκιμάσουν προγράμματα. Αυτό συνήθως συμβαίνει όταν ο προγραμματιστής αναπτύσσει μια εφαρμογή που περιέχει μια διαδικασία αυθεντικοποίησης η οποία απαιτεί από το χρήστη την εισαγωγή πολλών διαφορετικών τιμών πριν εκτελεστεί η εφαρμογή. Για να εκσφαλματώσει το πρόγραμμα, ο προγραμματιστής μπορεί να θέλει να έχει ειδικά προνόμια ή να αποφύγει όλη την απαραίτητη διαδικασία εγκατάστασης και αυθεντικοποίησης. Ο προγραμματιστής, επίσης, μπορεί να θέλει να είναι βέβαιος ότι θα υπάρχει τρόπος ενεργοποίησης του προγράμματος ακόμη και αν κάτι δεν πάει καλά με τη διαδικασία αυθεντικοποίησης που είναι ενσωματωμένη στην εφαρμογή. Η κερκόπορτα είναι κώδικας που αναγνωρίζει κάποια συγκεκριμένη ειδική ακολουθία εισόδου ή ενεργοποιείται με το να τρέξει από κάποιο συγκεκριμένο χρήστη ή με τη συγκυρία μιας απίθανης ακολουθίας γεγονότων. Ως εδώ τίποτε δε φαίνεται κακό. Ωστόσο, οι κερκόπορτες μεταβάλλονται σε απειλές, όταν χρησιμοποιούνται από κακόβουλους προγραμματιστές που θέλουν να αποκτήσουν μη εξουσιοδοτημένη προσπέλαση σε κάποιο σύστημα[134].

Ο βασικός στόχος λοιπόν ενός backdoor είναι να παρέχει πρόσβαση σε ένα σύστημα παρακάμπτοντας όμως κάποια συνηθισμένα μέτρα ασφάλειας. Οι λεγόμενες αυτές πίσω πόρτες μπορούν να τοποθετηθούν είτε σε ένα κομμάτι νόμιμου κώδικα ή να σταθούν σαν αυτόνομα προγράμματα. Δεν μπορούν όμως να διαδοθούν όπως οι ιοί και τα σκουλήκια με αποτέλεσμα να μην αυξάνουν και τον πληθυσμό τους. Χαρακτηριστικό είναι το ακόλουθο παράδειγμα όπου έχουμε την εισαγωγή ενός backdoor σε ένα κομμάτι κώδικα για τη διαδικασία πιστοποίησης και εισαγωγής σε ένα σύστημα[135]:

```
username = read_username( )

Password = read_password( )

 If username is "1963pkOr":

      return ALLOW_LOGIN

 If username and password ane valid:

    return ALLOW_LOGIN

 else:

      return DENY_LOGIN
```

[134] Βλ. ό.π Σ.Κάτσικα, Ασφάλεια Υπολογιστών, Πάτρα,2001,ΕΑΠ,σελ200

[135] Βλ. Aycock John, Computer Viruses and Malware, Hardcover , Springer Verlag ,2006, διαθέσιμο στο : http://www.springer.com/computer/security+and+cryptology/book/978-0-387-30236-2

Κανονικά ελέγχεται το username και ο κωδικός πρόσβασης, και αν είναι έγκυρα τότε επιτρέπεται στο χρήστη η πρόσβαση στο σύστημα. Ο κώδικας που είναι στο γκρι πλαίσιο αποτελεί ένα backdoor καθώς λέει ότι είναι έγκυρος και ο χρήστης 1963pkOr χωρίς να έχει κωδικό πρόσβασης και χωρίς να είναι στους έγκυρους χρήστες.

Τα προγράμματα BO (Back Orifice) και Netbus είναι δύο από τα βασικότερα εργαλεία με τα οποία μπορούμε να ανοίξουμε ένα backdoor σ' ένα σύστημα και να εκτελέσουμε έτσι από απόσταση ό,τι λειτουργίες θέλουμε. Οι εφαρμογές αυτές λειτουργούν παρόμοια με τους δούρειους ίππους και αποτελούνται από δύο τμήματα, το τμήμα server που εγκαθίσταται και λειτουργεί στον υπολογιστή στόχο και το τμήμα client που εκτελείται στον υπολογιστή του επιτιθέμενου, ο οποίος θα μπορεί μ' αυτόν τον τρόπο να εκτελέσει από απόσταση ό,τι εντολές θέλει και να αποσπάσει ό,τι πληροφορίες θέλει[136].

2.3.7 **Τα σκουλήκια** (Worms)

Τα Σκουλήκια (Worms) είναι παρόμοια με τους ιούς, με τη μόνη διαφορά ότι δεν απαιτείται η παρουσία ενός προγράμματος-φορέα για τη διάδοσή τους. Δημιουργούν αντίγραφα του εαυτού τους και χρησιμοποιούν τις επικοινωνίες μεταξύ των υπολογιστών για να διαδοθούν. Ένα σκουλήκι (worm) είναι ένα πρόγραμμα υπολογιστή που έχει τη δυνατότητα να αντιγράφει τον εαυτό του από μηχάνημα σε μηχάνημα. Τα σκουλήκια συνήθως μετακινούνται και μολύνουν άλλα μηχανήματα μέσω των δικτύων υπολογιστών[137].

Σήμερα πολλοί ονομάζουν τα worms ως ιούς ή παράσιτα. Βέβαια οι εξειδικευμένοι πάνω στους υπολογιστές επιμένουν πως έχουν αρκετές διαφορές. Εδώ θα πρέπει να επισημάνουμε πως όταν λέμε worms δεν εννοούμε αποκλειστικά ένα αρχείο (*.exe) το οποίο είναι 'ενοχλητικό' για τους υπολογιστές. Οι ίδιες οι εταιρείες χρησιμοποιούν worms για την εύρεση (search). Για παράδειγμα, όταν κάνουμε εύρεση για ένα αρχείο στα Windows, τότε ένα worm 'σέρνεται' μέσα στα αρχεία και ψάχνει να βρει το αρχείο που μας ενδιαφέρει.

Χρησιμοποιώντας ένα δίκτυο, ένα σκουλήκι μπορεί να επεκταθεί απίστευτα γρήγορα, όπως για παράδειγμα το σκουλήκι Code Red που αναπαρήγαγε τον εαυτό του πάνω από 250.000 φορές σε εννέα ώρες στις 19 Ιουλίου 2001. Ένα σκουλήκι εκμεταλλεύεται συνήθως κάποια τρύπα ασφαλείας σ' ένα κομμάτι προγράμματος ή στο λειτουργικό σύστημα, όπως το σκουλήκι Slammer, το οποίο εκμεταλλεύθηκε μια τέτοια τρύπα στον SQL server της Microsoft και προκάλεσε καταστροφή τον Ιανουάριο του 2003, αν και το μέγεθός του ήταν μόνο 376 bytes.

Τα σκουλήκια διακρίνονται σε δύο κατηγορίες, τα Host Computer Worms και τα Network Worms. Τα πρώτα είναι γνωστά και ως rabbits και λειτουργούν σ' έναν και μόνο υπολογιστή, ενώ τα δεύτερα που είναι γνωστά και ως octopuses είναι χωρισμένα σε μικρά κομμάτια και απλωμένα σ' ένα δίκτυο υπολογιστών και για να λειτουργήσουν θα πρέπει να επικοινωνούν την ίδια στιγμή.

---

[136] Βλ. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html

[137] Βλ. ό.π http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html

Το Σκουλήκι Code Red. Τα σκουλήκια εκμεταλλεύονται τον χρόνο των υπολογιστών και το εύρος ζώνης των δικτύων όταν αναπαράγονται και έχουν συχνά κακές προθέσεις. Ένα σκουλήκι με όνομα Code Red προκάλεσε μεγάλη δημοσιότητα το 2001 και οι ειδήμονες ανησύχησαν μήπως προκαλέσει σταμάτημα του Internet. Το σκουλήκι αυτό επιβράδυνε όντως την κυκλοφορία στο Διαδίκτυο (Internet traffic) όταν άρχισε να αναπαράγει τον εαυτό του, αλλά όχι τόσο άσχημα όσο αναμενόταν. Το κάθε αντίγραφο του σκουληκιού έψαχνε στο Internet για να βρει servers με Windows NT ή Windows 2000 που να μην έχουν εγκατεστημένο το security patch της Microsoft.

Κάθε φορά που έβρισκε έναν μη ασφαλή server, το σκουλήκι αναπαρήγαγε στον εαυτό του σ' εκείνον τον server και το καινούργιο αντίγραφο έψαχνε μετά να βρει άλλους servers για να μολύνει. Το σκουλήκι Code Red ήταν σχεδιασμένο για να κάνει τα εξής τρία πράγματα :

Να αναπαράγει τον εαυτό του κατά τις 20 πρώτες ημέρες του μήνα.

Να αντικαθιστά τις αρχικές ιστοσελίδες στους μολυσμένους servers με μια σελίδα που εμφάνιζε το μήνυμα "Hacked by Chinese".

Να ξεκινά μια συντονισμένη επίθεση στον Web server του Λευκού Οίκου σε μια προσπάθεια να τον κάνει να καταρρεύσει[138].

2.3.8 **Λογικές βόμβες**(logic bomb)

Μια από τις παλιότερες μορφές κακόβουλου λογισμικού, που εμφανίστηκε πριν ακόμη και από τους ιούς και τους έλικες, είναι η λογική βόμβα. Η λογική βόμβα (logic bomb) είναι κώδικας ενσωματωμένος σε κάποιο νόμιμο πρόγραμμα εφαρμογής και ρυθμισμένος να «εκραγεί», όταν εκπληρωθούν κάποιες συγκεκριμένες συνθήκες.

Παραδείγματα τέτοιων συνθηκών είναι η παρουσία ή απουσία συγκεκριμένων αρχείων, η έλευση μιας συγκεκριμένης μέρας της εβδομάδας ή μιας ημερομηνίας, ή η εκτέλεση της εφαρμογής από ένα συγκεκριμένο χρήστη. Σε μια περίπτωση, γνωστή στη βιβλιογραφία, η βόμβα ήταν ρυθμισμένη να εκραγεί, αν ο αριθμός ταυτότητας ενός συγκεκριμένου υπαλλήλου (αυτού που έβαλε τη βόμβα) δεν εμφανιζόταν σε δύο συνεχόμενες –χρονικά– καταστάσεις μισθοδοσίας, οπότε η πιθανότητα να είχε απολυθεί ο υπάλληλος ήταν μεγάλη. Από τη στιγμή που θα ενεργοποιηθεί, η βόμβα μπορεί να τροποποιήσει ή να διαγράψει δεδομένα ή και ολόκληρα αρχεία, να προκαλέσει το σταμάτημα ενός συστήματος ή να κάνει οποιαδήποτε άλλη ζημιά[139].

Οι λογικές αυτές βόμβες μπορούν να είναι είτε αυτόνομα προγράμματα, είτε να έχουν εισέλθει σε ένα κώδικα, όπως δείχνει και το παρακάτω παράδειγμα:

legitimate code

if date is Friday the 13th:

---

[138] Βλέπε περιοδικό για το Enterprise Computing και την Ασφάλεια στην πληροφορική στο: http://www.securitymanager.gr/it_security/protection_article.php?id=5&set=7&title=%D%=2b2ce933700aa86781778b3477730a59

crash_computer()

legitimate code

Το χαρακτηριστικό τους είναι ότι μπορούν και κρύβονται καλά ανάμεσα σε εκατομμύρια γραμμές κώδικα ενός νόμιμου προγράμματος, γεγονός που κάνει πολύ δύσκολο τον εντοπισμό τους[140].

2.3.9 **Παραποίηση ταυτότητας** (phishing)

Η ονομασία Phishing αναφέρεται χρησιμοποιούμενη για πρώτη φορά το 1996 από χάκερς που έκλεβαν ή παράνομα ιδιοποιούνταν τους λογαριασμούς νομίμων χρηστών της εταιρίας America Online (AOL) με παράνομη χρήση κωδικών πρόσβασης που ανήκαν σε ανυποψίαστους χρήστες—συνδρομητές της AOL[141]. Όπως το ίδιο το όνομά του υπονοεί[142] το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam email , το οποίο ισχυρίζεται – ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών.

Τα email αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή που και ο ίδιος ο internet browser «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας. Ανησυχητική αύξηση του αριθμού των πλαστών ιστοσελίδων καταγράφει η τελευταία έκθεση της αμερικανικής κοινοπραξίας Anti-Phishing Working Group (APWG), στην οποία συμμετέχουν τράπεζες, πιστωτικά ιδρύματα και εταιρείες ηλεκτρονικού εμπορίου, με στόχο την καταπολέμηση της ηλεκτρονικής απάτης. Πιο συγκεκριμένα, η έκθεση καλύπτει το πρώτο τετράμηνο του 2012 και αναφέρει πως τον περασμένο Φεβρουάριο εντοπίστηκαν 56.859 πλαστά σάιτ – νούμερο που καταρρίπτει το προηγούμενο ρεκόρ, καθώς ξεπερνά κατά 1% τον αριθμό των περισσότερων «κάλπικων» ιστοσελίδων που είχαν καταγραφεί ποτέ, τον Αύγουστο του 2009. Σύμφωνα με τους συντάκτες της έκθεσης, αυτό υποδεικνύει πως ο συγκεκριμένος

---

[139] Βλ ό.π Σ.Κάτσικα, Ασφάλεια Υπολογιστών, Πάτρα,2001,ΕΑΠ,σελ201

[140] Βλ. ό. Π, Aycock John, Computer Viruses and Malware, Hardcover , Springer Verlag ,2006, διαθέσιμο στο : http://www.springer.com/computer/security+and+cryptology/book/978-0-387-30236-2.

[141] Βλ. περισσότερα για την ιστορία του Phishing σε WIKIPEDIA, The Free Encyclopedia, http://en.wikipedia.org/wiki/Phishing .

[142] παραλλαγή του αγγλικού «fishing» (ψάρεμα).

τρόπος παραπλάνησης γίνεται όλο και πιο διαδεδομένος ανάμεσα στους κυβερνοεγκληματίες[143].

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

Χρειάζεται ιδιαίτερη προσοχή ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω Phishing. Τα email που αποστέλλονται μοιάζουν αρκετά επίσημα και οι πλαστές σελίδες είναι τις περισσότερες φορές πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικά τους[144].

Ενδείξεις πως ένα ηλεκτρονικό μήνυμα είναι πιθανόν πλαστό:

☞ Τα spam μηνύματα, χρησιμοποιούν συνήθως γενικές προσφωνήσεις, όπως "Αγαπητέ πελάτη", αντί για το πραγματικό όνομα του παραλήπτη.

☞ Η πλειοψηφία των Phising μηνυμάτων επικαλείται κάποιο δήθεν πρόβλημα ή κάποια "μοναδική ευκαιρία" και, χρησιμοποιώντας φρασεολογία που δημιουργεί την αίσθηση του επείγοντος, ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

☞ Ζητούν την παραχώρηση απορρήτων προσωπικών στοιχείων οικονομικού χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, όπως το Όνομα Χρήστη (username) και τον Κωδικό Πρόσβαση (password).

Τρόποι προφύλαξης από το Phishing

☞ Δεν απαντάμε σε μηνύματα ηλεκτρονικού ταχυδρομείου που μας ζητούν να αποκαλύψουμε αξιοποιήσιμα προσωπικά στοιχεία οικονομικού χαρακτήρα. Οι αξιόπιστες εταιρείες δεν συνηθίζουν να ζητούν από τους πελάτες τους να ενημερώσουν ή να επαληθεύσουν τέτοια απόρρητα στοιχεία με ένα απλό email.

☞ Ακόμη και σε περιπτώσεις που όλα δείχνουν ότι το μήνυμα είναι γνήσιο, είναι προτιμότερο να επικοινωνήσουμε με την εταιρία που παρουσιάζεται ως αποστολέας, για να επιβεβαιώσουμε ότι πράγματι αυτή σας έστειλε το μήνυμα και ότι δεν πρόκειται για περίπτωση απάτης.

☞ Φροντίζουμε, όμως, να επικοινωνήσουμε με την εταιρεία με τον τρόπο που χρησιμοποιούμε συνήθως, και όχι σύμφωνα με τις οδηγίες που περιέχει το email ή απαντώντας σε αυτό.

---

[143] Βλ. εφημερίδα Καθημερινή, 20/07/2012 στο: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_20/07/2012_453092

[144] Βλ. http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043

☞ Πριν προβούμε στην παραχώρηση ευαίσθητων προσωπικών πληροφοριών μέσω του διαδικτύου προσέχουμε την ηλεκτρονική διεύθυνση στην οποία βρίσκεστε. Αντί για το απλό «http://», θα πρέπει να αρχίζει με «https://». Έτσι διασφαλίζουμε ότι χρησιμοποιείτε ασφαλή σύνδεση web (http secure).

☞ Αγνοούμε ηλεκτρονικά μηνύματα που λαμβάνουμε από άγνωστες πηγές και αποφεύγουμε να συμπληρώνουμε ηλεκτρονικές φόρμες που παραλαμβάνουμε μέσω ηλεκτρονικού ταχυδρομείου.

☞ Ελέγχουμε συχνά τους online λογαριασμούς μας, εξετάζοντας προσεκτικά τόσο την συνολική κίνησή τους όσο και κάθε συναλλαγή ξεχωριστά, ώστε να είμαστε βέβαιοι ότι εγκρίνουμε όλα τα ποσά που έχει χρεωθεί.

☞ Χρησιμοποιούμε πάντα λογισμικό προστασίας από ιούς (antivirus). Παρόλο που τα antvirus δεν μπορούν να μας αποτρέψουν να ανοίξουμε ένα πλαστό ηλεκτρονικό μήνυμα, μπορούν όμως να μας προστατεύσουν από ιούς ή λογισμικά υποκλοπής (spyware) που θα προέλθουν από τέτοιες ενέργειες. Πολλά Phising μηνύματα οδηγούν σε διαδικτυακές τοποθεσίες που εγκαθιστούν στον υπολογιστή σας spywares τα οποία συνεχίζουν να καταγράφουν κάθε πληροφορία που εισάγετε -πιθανότατα και αριθμούς λογαριασμών και πιστωτικών καρτών, και κωδικούς πρόσβασης- για πολύ καιρό μετά την αποχώρηση σας από τον συγκεκριμένο διαδικτυακό τόπο, ενώ μπορεί να περιέχει ακόμη και κάποιον ιό.

☞ Εγκαθιστούμε ψηφιακό φίλτρο που μπλοκάρει τα spam emails (antispam) [145].

2.3.10 **Μη ζητηθείσα ηλεκτρονική επικοινωνία**- Spam e-mails

Spam[146] είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του Διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Το SPAM ξεκίνησε ως κάτι άκακο και διασκεδαστικό, η ανάγνωση τέτοιων μηνυμάτων μπορούσε να θεωρηθεί και ως ευχάριστο διάλειμμα από τη δουλειά, αλλά κατέληξε να είναι μαζί με τους ιούς (worms & viruses) ένα από τα μεγαλύτερα προβλήματα του διαδικτύου. Το Spam συχνά έχει την μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων, για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο γραμματοκιβώτιο μας, χωρίς να έχουμε ζητήσει την εν λόγω πληροφόρηση. Η αλληλογραφία αυτή λοιπόν μπορεί να χαρακτηριστεί ως απρόκλητη ή ανεπιθύμητη αλληλογραφία, δύο όρους που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam.

Οι υπεύθυνοι για την αποστολή των spams ονομάζονται *spammers* και συνήθως αγοράζουν, αποκτούν με παράνομο τρόπο ή συλλέγουν διευθύνσεις e-mails και στέλνουν τα

---

[145] Βλ http://www.forthnet.gr/templates/viewcontentTmCh.aspx?c=10009043

[146] Η ιστορία της λέξης SPAM ξεκινά το 1937 όταν ένα καινούριο είδος κρέατος παρουσιάστηκε στην αγορά. Ήταν ένα καινοτομικό προϊόν καθώς προσέφερε «φρέσκο» κρέας χωρίς ανάγκη κατάψυξης σε μια εποχή που το φρέσκο κρέας ήταν δυσεύρετο. Μετά τη λήξη του πολέμου όμως και το πέρασμα των χρόνων με τη βελτίωση του βιοτικού επιπέδου, το SPAM κατέληξε να είναι ένα αζήτητο προϊόν,

βλ. http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104

μηνύματά τους χωρίς την έγκριση του παραλήπτη σε αντίθεση με τις τεχνικές e-mail marketing όπου ο πελάτης επιλέγει την λήψη διαφημιστικών/ενημερωτικών μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου. Στόχος των spammers μπορεί να είναι επίσης η διάδοση Malware-Ioί και άλλα προγράμματα που περιέχουν βλαβερό κώδικα και στέλνονται συννημένα σε email, η περίπτωση υφαρπαγής κωδικών και ευαίσθητων προσωπικών δεδομένων με την τέχνη του Phishing,το πλημμύρισμα των λογαριασμών email με άδεια μηνύματα με στόχο να παραλύσουν ένα δίκτυο ή έναν email provider (flooding).

Τα κυριότερα χαρακτηριστικά του Spam μπορούν να συνοψιστούν στα ακόλουθα σημεία:

Απρόκλητο: Η επικοινωνία που επιχειρείται είναι απρόκλητη, με την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα που θα δικαιολογούσε ή θα προκαλούσε την επικοινωνία αυτή.

Εμπορικό : Πολλές φορές το spam αφορά την αποστολή μηνυμάτων εμπορικού σκοπού με σκοπό την προβολή και την διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων.

Μαζικό: Το spam συνίσταται στην μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Συνήθως το ίδιο μήνυμα ή ελαφρά διαφοροποιημένο στέλνεται σε ένα μεγάλο πλήθος παραληπτών[147].

Οι συνέπειες από την αχαλίνωτη χρήση του ηλεκτρονικού ταχυδρομείου από τους κάθε λογής διαφημιστές είναι καταστροφικές τόσο για τον απλό χρήστη όσο και για τις μεγάλες εταιρείες. Οι εργαζόμενοι θα είναι αναγκασμένοι να ξοδεύουν όλο και περισσότερο χρόνο για να διαβάσουν αλλά και να διαγράψουν τα άχρηστα αυτά μηνύματα.

Επίσης, όλο και περισσότεροι πόροι από την επεξεργαστική ισχύ των διακομιστών (servers) θα πρέπει να δεσμεύονται για να απασχοληθούν με μια ανεπιθύμητη διαδικασία. Είναι τόσο πολλά σε αριθμό αυτά τα μηνύματα που μπορούν ακόμη και να μπλοκάρουν το παγκόσμιο σύστημα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου και να οδηγήσουν το Internet σε κατάρρευση. Ο λόγος είναι ότι φορτώνουν το δίκτυο και τα κεντρικά συστήματα δεν μπορούν να τα βγάλουν πέρα με την υπερβολική κίνηση που δημιουργείται. Σύμφωνα με πρόσφατες έρευνες, το 1/3 των χρηστών του Internet αντιμετωπίζει μεγάλη δυσχέρεια στη χρήση της ηλεκτρονικής τους αλληλογραφίας καθώς τα χρήσιμα και επείγοντα μηνύματα από τους φίλους και τους συνεργάτες τους χάνονται μέσα στην πλημμυρίδα των spam e-mail.

Αντιμετώπιση του Spam

Οι ηλεκτρονικές διευθύνσεις των χρηστών στους οποίους στέλνονται τέτοια μηνύματα εντοπίζονται με ειδικά προγράμματα από τις υπάρχουσες ιστοσελίδες του Internet. Ένας άλλος ιδιαίτερα αποτελεσματικός τρόπος συγκέντρωσης διευθύνσεων e-mails ανύποπτων χρηστών, που στη συνέχεια θα βομβαρδιστούν με διαφημίσεις, είναι οι φάρσες, όπως για ένα καημένο κοριτσάκι που κινδυνεύει από καρκίνο ή για έναν πολύ καταστροφικό ιό και οδηγίες για το πώς να τον αποφύγετε. Η φράση «στείλτε αυτό το μήνυμα σ' όσους περισσότερους χρήστες μπορείτε» είναι συνήθως η παγίδα που χρησιμοποιούν οι επιτήδειοι, καθώς τα e-mails με τις εκατοντάδες διευθύνσεις στις οποίες προωθούνται θα επιστρέψουν κάποια στιγμή στον αρχικό

147 βλ. http://www.sch.gr/sch-portlets/static/manual/aboutSpam/index.php?_list=whatis

συντάκτη τους για να κάνει κι αυτός τη με τη σειρά την δουλειά του. Για τους αρχάριους του internet είναι μερικές φορές δύσκολο να συνειδητοποιήσουν ότι αυτά τα email δεν απευθύνονται σε αυτούς προσωπικά και πέφτουν πιο εύκολα θύματα σε τέτοιες ηλεκτρονικές απάτες.

Οι προσπάθειες που έχουν κάνει μέχρι στιγμής οι εταιρείες παροχής υπηρεσιών Internet (ISPs - Internet Service Providers) και υπηρεσιών ηλεκτρονικού ταχυδρομείου με τη χρήση ειδικών προγραμμάτων-φίλτρων για την αυτόματη απόρριψη τέτοιων μηνυμάτων πριν αυτά φθάσουν στον υπολογιστή του χρήστη δεν έχουν επιφέρει θεαματικά αποτελέσματα.

Η αντιμετώπιση του Spam συνίσταται στη λήψη μέτρων[148] σε πρώτη φάση προληπτικά: Πρέπει να προστατεύουμε το email μας και να προσέχουμε να μη το δημοσιεύουμε σε σελίδες του internet. Οι spammers χρησιμοποιούν "διαδικτυακά ρομπότ" που σκανάρουν το διαδίκτυο για ηλεκτρονικές διευθύνσεις και τις αποθηκεύουν στα αρχεία τους. Προσπαθούμε να γράφουμε το e-mail μας με τέτοιο τρόπο ώστε να μην περιέχει το σύμβολο @ και να είναι έτσι δύσκολη η αναγνώρισή του από τα προγράμματα των spammers. Ένας καλός τρόπος είναι να περιγράφουμε το e-mail όπως ακούγεται π.χ kalampalikis at(@) sch dot(.) gr ,ή να το δημοσιεύουμε σαν αρχείο εικόνας[149] βλέπε εικόνα 2.

Εικόνα 2 . Μετατροπή διεύθυνσης e-mail σε αρχείο εικόνας

Δεν κάνουμε ποτέ προώθηση (forward) των spam e-mails σε φίλους ή και τρίτους, γιατί κι αυτοί θα προστεθούν στην λίστα αποδοχής και δεν απαντάμε (reply) σε μηνύματα spam καθότι μια απάντηση μπορεί να εκληφθεί ως συναίνεση για την αποστολή ακόμα περισσότερων "απρόσκλητων" μηνυμάτων. Αποφεύγουμε να κάνουμε αίτηση για διαγραφή (remove), καθώς έτσι θα ενημερώσουμε τον spammer ότι πρόκειται για ενεργή ηλεκτρονική διεύθυνση, γεγονός που μπορεί να γίνει αφορμή για την λήψη ακόμα περισσότερων spam μηνυμάτων. Σαν απλοί χρήστες όταν στέλνουμε email μαζικά σε λίστες φίλων μας, χρησιμοποιούμε την επιλογή bcc(blind carbon copy) για να βάλουμε τις ηλεκτρονικές διευθύνσεις και όχι την επιλογή cc(carbon copy). Με αυτόν τον τρόπο δεν είναι ορατά για τα υπόλοιπα μέλη η λίστα με τα email, προστατεύοντας τα δεδομένα των φίλων μας. Ένας ακόμα τρόπος που ακολουθούν πολλοί είναι το να έχουμε μια απλή δωρεάν ηλεκτρονική διεύθυνση (webmail: yahoo, hotmail, gmx κτλ) που χρησιμοποιείται σε εγγραφές στο internet (messenger, message boards, φόρουμ, clubs κτλ) και το επίσημο email το οποίο προστατεύουμε. Αυτή είναι μια πολύ καλή τακτική.

Για την καταπολέμηση του SPAM έχουν αναπτυχθεί τεχνικά και νομικά μέσα. Ήδη σε πολλές χώρες η αποστολή αυτόκλητων εμπορικών ηλεκτρονικών μηνυμάτων θεωρείται ποινικό αδίκημα. Τα αντίμετρα που έχουν σαν στόχο την αντιμετώπιση του SPAM με τεχνικά μέσα έχουν αναπτυχθεί σε δυο επίπεδα, σε επίπεδο κεντρικού εξυπηρετητή και σε επίπεδο τελικού χρήστη. Οι εφαρμογές που απευθύνονται στον τελικό χρήστη χρησιμοποιούν ένα σύστημα αναγνώρισης μηνυμάτων SPAM με δεσμευμένες πιθανότητες (βλέπε θεώρημα του Bayes) το

[148] Βλέπε μέτρα antispam του σχολικού δικτύου στο:
http://www.sch.gr/sch-portlets/static/manual/aboutSpam/index.php?_list=avoid

[149] Υπάρχουν ιστοσελίδες που φτιάχνουν τέτοια αρχεία εικόνας βλ http://www.email-encoder.net/index.php

οποίο μπορεί να εκπαιδευτεί από το χρήστη. Οι εφαρμογές αυτές ελέγχουν διάφορα στοιχεία του μηνύματος , όπως για παράδειγμα το ποσοστό HTML κώδικα στο μήνυμα και το βαθμό χρησιμοποίησης 'ύποπτων' λέξεων, αναλύουν την επικεφαλίδα του μηνύματος και από την επιμέρους βαθμολογία του καθενός στοιχείου αποφαίνονται αν το μήνυμα είναι SPAM. Επίσης ο χρήστης μπορεί να εκπαιδεύσει το σύστημα ενημερώνοντας το για μηνύματα τα οποία δε θεωρήθηκαν SPAM ενώ είναι ή και το αντίστροφο. Τα συστήματα αυτά, αν και βελτιώνονται συνεχώς δεν είναι απόλυτα αξιόπιστα. Στο γεγονός αυτό συντείνει και το γεγονός ότι μαζί με τα συστήματα αυτά εξελίσσονται και οι τρόποι με τους οποίους οι spammers προσπαθούν να τα ξεγελάσουν. Δυο τέτοιες εφαρμογές οι οποίες είναι ελεύθερου λογισμικού είναι οι spambouncer και spamassassin καθώς και άλλες όπως οι spam Inspector, spamBuster, spamButcher και άλλες που μπορούν εύκολα να βρεθούν με τη βοήθεια μιας μηχανής αναζήτησης στο διαδίκτυο[150].

Οι εφαρμογές που απευθύνονται σε κεντρικούς εξυπηρετητές συνήθως χρησιμοποιούν μια διαφορετική προσέγγιση για να λύσουν το πρόβλημα. Αντί να ελέγχουν το περιεχόμενο του κάθε μηνύματος (εξαιρετικά απαιτητικό σε υπολογιστική ισχύ για ένα εξυπηρετητή που διακινεί δεκάδες μηνύματα το δευτερόλεπτο) ελέγχουν αν η ηλεκτρονική διεύθυνση IP του εξυπηρετητή που στέλνει το μήνυμα είναι καταγεγραμμένη σε κάποια λίστα γνωστών πηγών spam στο Internet. Αν ο εξυπηρετητής-αποστολέας του μηνύματος είναι καταγεγραμμένος στις λίστες που ελέγχουν, τότε απορρίπτουν το μήνυμα πριν αυτό μεταφερθεί. Οι λίστες αυτές ονομάζονται DNS black lists (DNSBLs), γιατί οι ερωταποκρίσεις γίνονται με βάση το πρωτόκολλο DNS. Η προσέγγιση αυτή παρουσιάζει το σημαντικό πλεονέκτημα ότι τα μηνύματα spam δεν φεύγουν ποτέ από την πηγή τους και δεν επιβαρύνουν ούτε το δίκτυο αλλά ούτε και τους τελικούς χρήστες, αλλά δεν είναι όσο αποτελεσματική όσο η προηγούμενη.

Παρακάτω, ακολουθεί αλφαβητική λίστα με τα πιο γνωστά προγράμματα anti-spamming[151].

- ChoiceMail
- eTrust Antispam
- K9 (Δωρεάν)
- MailFilter (Δωρεάν - έκδοση μόνο για Unix/Linux)
- MailWasher Pro
- McAfee SpamKiller
- Norton Antispam
- POPFile (Δωρεάν)
- SpamBayes (Δωρεάν)
- SpamBully

[150] Βλ http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104

[151] Βλ http://www.no-spam.gr/tools.htm

- SpamCombat (Δωρεάν)
- SpamFighter (Δωρεάν)
- SpamFire (έκδοση για Mac)
- Spamihilator (Δωρεάν)
- SpamPal (Δωρεάν)
- SpamWeasel (Δωρεάν)

2.3.11 **Τα αυτοεγκαθιστώμενα προγράμματα** (cookies)

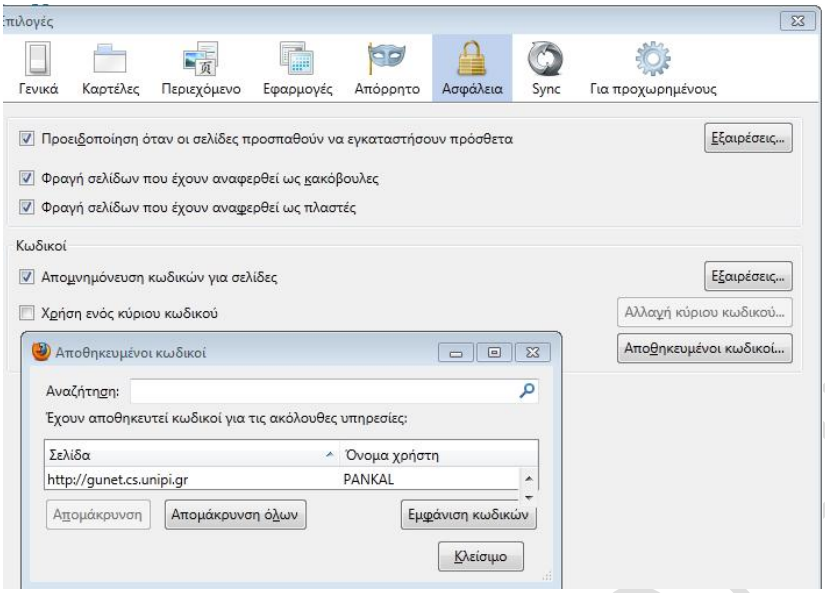
Τα cookies (μπισκοτάκια) είναι μικρά αρχεία κειμένου ,τα οποία αποθηκεύονται στον υπολογιστή μας κατά την πλοήγησή μας στο διαδίκτυο[152], αποτελούν δε , ένα από τα ακανθώδη θέματα του Internet που έχουν να κάνουν με τα προσωπικά δεδομένα και το προσωπικό απόρρητο των χρηστών του Διαδικτύου. Τα cookies αποτελούν ένα αυτοεγκαθιστώμενο αρχείο λογισμικού, που δημιουργείται από τα Web sites που επισκεπτόμαστε στο Internet, με απώτερο σκοπό την αναγνώρισή μας από τα ίδια Web sites την επόμενη φορά που θα βρεθούμε στις ιστοσελίδες τους. Αποθηκεύονται στον σκληρό δίσκο του ηλεκτρονικού υπολογιστή του χρήστη, συχνά εν αγνοία του, ενώ πρόσβαση σε αυτά έχει μόνο ο συγκεκριμένος διακομιστής. Πρόκειται για κρυπτογραφημένα δεδομένα που μπορούν να περιλαμβάνουν όλες τις πληροφορίες για την επίσκεψη σε μία ιστοσελίδα[153]. Τα cookies άρχισαν να απασχολούν τα μέσα μαζικής ενημέρωσης από το 2000 εξαιτίας του θέματος της παραβίασης των προσωπικών δεδομένων στο Internet και η συζήτηση βρίσκεται ακόμα σε εξέλιξη. Από την άλλη πλευρά, τα cookies παρέχουν δυνατότητες που κάνουν πολύ ευκολότερη την πλοήγηση στο Web. Οι σχεδιαστές όλων σχεδόν των μεγάλων Web sites τα χρησιμοποιούν επειδή παρέχουν μια καλύτερη εμπειρία για τους χρήστες και κάνουν πολύ εύκολη υπόθεση την συγκέντρωση λεπτομερειακών πληροφοριών σχετικά με τους επισκέπτες ενός site.

Υποτίθεται ότι εξυπηρετούν χρήσιμους σκοπούς για τους χρήστες του Internet, καθώς συγκεντρώνουν πληροφορίες σχετικά με τις καταναλωτικές τους συνήθειες, τις οποίες μπορούν να αξιοποιήσουν sites μεγάλων εταιρειών για να εξειδικεύσουν έτσι ή και να βελτιώσουν τα προϊόντα ή τις υπηρεσίες τους. Μια πολύ κοινή χρήση των cookies είναι για να αποθηκεύσουν το όνομα χρήστη (user name) και τον μυστικό κωδικό ή συνθηματικό (password) που χρησιμοποιούμε για να μπορέσουμε να εισέλθουμε σε διάφορους δικτυακούς τόπους , σε πύλες (portals),ή σε Webmail. Η δυνατότητα αυτή διευκολύνει τον χρήστη , να μην δίνει κάθε φορά τα ίδια στοιχεία (user name και password).Αυτό βέβαια μπορούμε να το κάνουμε όταν είμαστε σίγουροι ότι δεν πρόκειται κάποιος τρίτος να χρησιμοποιήσει τον υπολογιστή μας με κακές προθέσεις, γιατί μπορεί να μας υποκλέψει τους προσωπικούς κωδικούς, καθώς μπορεί να τους

[152] Βλέπε http://el.wikipedia.org/wiki/HTTP_cookies

[153] Βλέπε http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cookies.html

δει μέσα από τον περιηγητή π.χ στο mozila από το μενού εργαλεία/επιλογές /αποθηκευμένοι κωδικοί/εμφάνιση κωδικών, βλέπε εικόνα 3



Εικόνα 3. Εμφάνιση κωδικών μέσα από το φυλλομετρητή mozila

Όμως, η σημαντικότερη χρήση των cookies είναι για να παρακολουθούν και να καταγράφουν (κατασκοπεύουν) τις κινήσεις μας στο Internet, συνήθως τις καταναλωτικές, όπως σε ποια sites περιηγούμαστε και πόσο χρόνο μένουμε σ' αυτά, πόσο συχνά τα επισκεπτόμαστε κ.ά. Ακόμη και μέσα στο ίδιο το site μπορούν να καταγράψουν σε ποιες ιστοσελίδες έχουμε προτίμηση[154]. Οι διαχειριστές ενός Web site που χρησιμοποιεί κατά κόρον τα cookies έχουν την δυνατότητα να χρησιμοποιήσουν τις πληροφορίες που συγκεντρώνουν σχετικά με τις προσωπικές προτιμήσεις των επισκεπτών (χρηστών) τους είτε για να βελτιώσουν την εικόνα του site τους ή για να προμηθεύσουν αυτά τα πολύτιμα στοιχεία σε τρίτους και κυρίως σε διαφημιστικές εταιρείες. Μιλάμε συνεπώς για ένα νέο είδος marketing, το e-marketing. Τα cookies αποτελούν παντοδύναμα εργαλεία marketing, καθώς μπορούν να χρησιμοποιηθούν για να δημιουργηθούν λεπτομερή καταναλωτικά προφίλ για τους χρήστες του Internet. Οι δημιουργοί των δικτυακών τόπων που χρησιμοποιούν cookies προβάλλουν το επιχείρημα ότι η χρήση των cookies εξυπηρετεί και τους ίδιους τους καταναλωτές - χρήστες του Internet, καθώς μπορούν έτσι να αποκτήσουν ενημέρωση και πληροφόρηση κομμένη και ραμμένη στα μέτρα τους. Ισχυρίζονται επίσης ότι η μεγάλη πλειοψηφία των χρηστών του Internet δεν απενεργοποιεί τα cookies στο πρόγραμμα φυλλομετρητή που χρησιμοποιεί, παρ' όλη την ενημέρωση που έχει γίνει για το θέμα αυτό[155].

[154] http://www.eeei.gr/odhgos/netsc404/howcooki.htm

[155] Βλέπε περιοδικό για το Enterprise Computing και την Ασφάλεια στην πληροφορική στο: http://www.securitymanager.gr/it_security/protection_article.php?id=5&set=15&title=%D4%E1%20Cookies&PHPSESSID=2b2ce933700aa86781778b3477730a59

Ενδεικτικά, τα στοιχεία που μπορεί να ενδιαφέρουν τους υπεύθυνους ενός Web site σχετικά με τις προτιμήσεις των επισκεπτών τους είναι τα εξής :

Συνολικό αριθμό επισκέψεων ανά ημέρα και μάλιστα ξεχωριστά από το ίδιο άτομο (ίδια IP διεύθυνση) και ξεχωριστά από διαφορετικά άτομα (διαφορετική IP διεύθυνση).

Συνολικό αριθμό ιστοσελίδων που είδαν οι χρήστες.

Από ποια sites ήρθαν οι χρήστες.

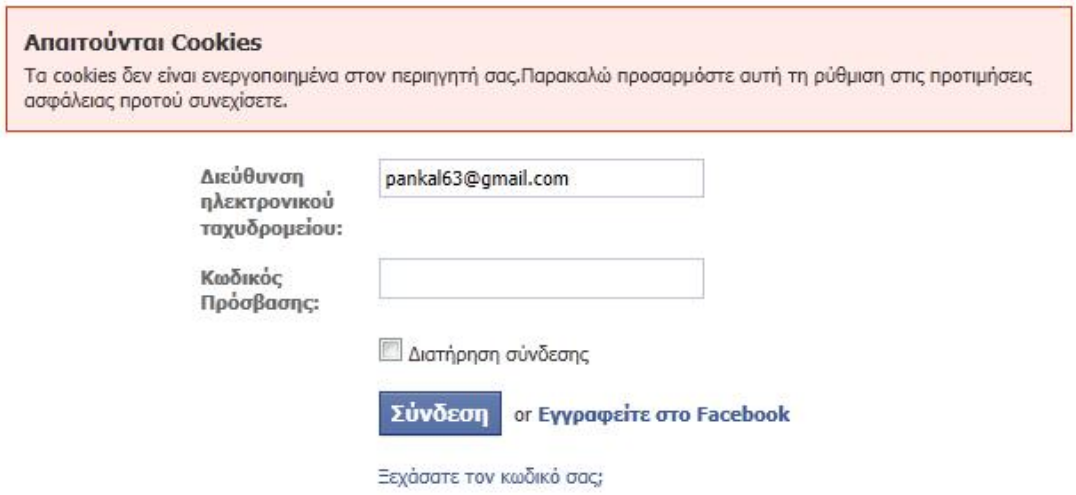
Σε ποια sites πηγαίνουν οι χρήστες όταν φεύγουν.

Ποιες ιστοσελίδες προτιμούν περισσότερο.

Πόσο χρόνο αφιερώνουν σε κάθε ιστοσελίδα.

Μπορούμε από τις κατάλληλες επιλογές του φυλλομετρητή μας[156] να εμποδίσουμε όποτε θέλουμε την αποθήκευση των cookies στον σκληρό μας δίσκο αλλά δεν πρέπει να ξεχνάμε ότι πολλά Web sites είτε θα αρνηθούν να μας φανερώσουν τις ιστοσελίδες τους είτε δεν θα λειτουργήσουν σωστά αν δεν τους δώσουμε τη δυνατότητα να διαχειριστούν τα cookies όπως αυτά γνωρίζουν βλέπε εικόνα 4.

[156] Στον Internet Explorer αυτό μπορεί να γίνει από το μενού εργαλεία\επιλογές Internet \προστασία προσωπικών δεδομένων, μετακινώντας το δρομέα από κάτω προς τα πάνω, έχουμε τις διαβαθμίσεις: **Αποδοχή** όλων των Cookies (αποθηκεύει Cookies από οποιαδήποτε τοποθεσία Web, τα Cookies που υπάρχουν στον υπολογιστή μπορούν να αναγνωστούν από τις τοποθεσίες Web που τα δημιούργησαν), **Χαμηλό** (Αποκλείει τα Cookies άλλων κατασκευαστών που δεν διαθέτουν συμπαγή πολιτική προστασίας προσωπικών δεδομένων, περιορίζει τα Cookies άλλων κατασκευαστών που αποθηκεύουν πληροφορίες που μπορεί να χρησιμοποιηθούν για επικοινωνία μαζί σας χωρίς τη συναίνεσή σας), **Μεσαίο** (Αποκλείει τα Cookies άλλων κατασκευαστών που δεν διαθέτουν συμπαγή πολιτική προστασίας προσωπικών δεδομένων, αποκλείει τα Cookies άλλων κατασκευαστών που αποθηκεύουν πληροφορίες που μπορεί να χρησιμοποιηθούν για επικοινωνία μαζί σας χωρίς τη συναίνεσή σας, περιορίζει τα Cookies των ιδίων κατασκευαστών που αποθηκεύουν πληροφορίες που μπορεί να χρησιμοποιηθούν για επικοινωνία μαζί σας χωρίς τη συναίνεσή σας) , **Μεσαίο-Υψηλό** (Αποκλείει τα Cookies άλλων κατασκευαστών που δεν διαθέτουν συμπαγή πολιτική προστασίας προσωπικών δεδομένων, αποκλείει τα Cookies άλλων και ιδίων κατασκευαστών που αποθηκεύουν πληροφορίες που μπορεί να χρησιμοποιηθούν για επικοινωνία μαζί σας χωρίς τη συναίνεσή σας),**Υψηλό** (Αποκλείει όλα τα Cookies από τοποθεσίες Web που δεν διαθέτουν συμπαγή πολιτική προστασίας προσωπικών δεδομένων, αποκλείει τα Cookies που αποθηκεύουν πληροφορίες που μπορεί να χρησιμοποιηθούν για επικοινωνία μαζί σας χωρίς τη συναίνεσή σας),**Αποκλεισμός όλων των Cookies** (αποκλείει όλα τα Cookies από οποιαδήποτε τοποθεσία Web,τα Cookies που υπάρχουν στον υπολογιστή δεν μπορούν να αναγνωστούν). Για να διαγράψουμε όλα τα cookies που έχουν αποθηκευθεί στον υπολογιστή μας, πάμε στην καρτέλα Γενικά του πλαισίου διαλόγου Επιλογές Internet και κάνουμε κλικ στο πλήκτρο Διαγραφή Cookies.



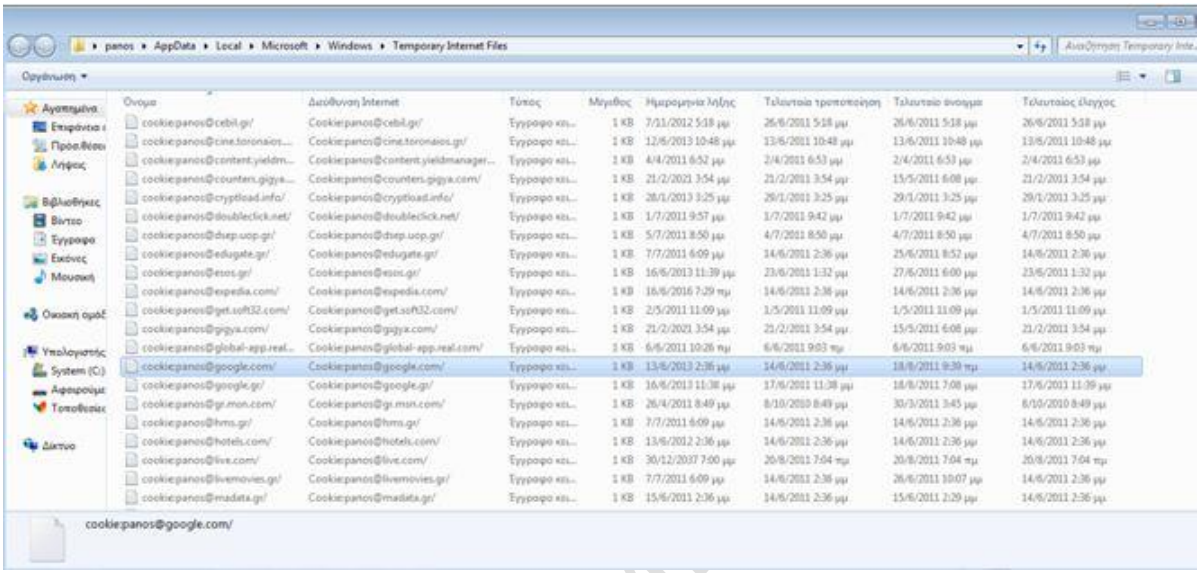
Εικόνα 4. Ενεργοποίηση των cookies

Τα cookies είναι δεδομένα που αποθηκεύονται σε μικρά αρχεία κειμένου (text files) στον σκληρό δίσκο του υπολογιστή μας καθώς εμείς περιηγούμαστε ανέμελοι σε διάφορους δικτυακούς τόπους. Τα στοιχεία που περιέχει ένα cookie είναι ο αριθμός αναγνώρισής του (κωδικός), το URL του Web site που το δημιουργεί, η ημερομηνία δημιουργίας του, η ημερομηνία διαγραφής του κ.ά. Μαζί με την δημιουργία ενός cookie στον σκληρό δίσκο του υπολογιστή μας, ο Web server του δικτυακού τόπου που μας το έστειλε, δημιουργεί μια καταχώριση (εγγραφή) σε μια δική του βάση δεδομένων με τον αριθμό αναγνώρισης του cookie, δηλ. στην ουσία αναγνωρίζει τον υπολογιστή στον οποίο δημιουργήθηκε. Έτσι, την επόμενη φορά που θα βρεθούμε στον ίδιο δικτυακό τόπο, ο φυλλομετρητής μας θα ελέγξει τα cookies που έχει δημιουργήσει στον υπολογιστή μας αυτός ο δικτυακός τόπος και θα ενημερώσει κατάλληλα τον Web server. Ο server με την σειρά του θα δει τον αριθμό αναγνώρισης του cookie και θα αναζητήσει στην δική του βάση δεδομένων τα παλαιότερα στοιχεία σχετικά με προηγούμενες επισκέψεις μας στον ίδιο δικτυακό τόπο. Θα μπορέσει έτσι να προσαρμόσει αυτόματα τις ιστοσελίδες που βλέπουμε ώστε να εμφανίζουν πράγματα που μας ενδιαφέρουν περισσότερο, όπως νέες κυκλοφορίες προϊόντων, εκπτώσεις σε είδη ή σε υπηρεσίες που προσφέρει κ.ά. Αυτός είναι και ο λόγος που διαφορετικοί χρήστες ενώ επισκέπτονται το ίδιο Web site μπορεί να βλέπουν εντελώς διαφορετικά πράγματα. Τα στοιχεία που συγκεντρώνονται με τη βοήθεια των cookies, εκτός από την αυτόματη προσαρμογή του περιεχομένου των ιστοσελίδων για τον κάθε χρήστη, μπορούν να χρησιμοποιηθούν και για στατιστικούς λόγους ή και για να πωληθούν σε διαφημιστικές εταιρείες ή και αλλού[157].

Αυτό που έχει ανησυχήσει πολλούς χρήστες σχετικά με τα cookies είναι ο κίνδυνος να διαρρεύσουν οι πληροφορίες αυτές σε τρίτα άτομα ή και η πιθανότητα τα προσωπικά τους δεδομένα να διατίθενται σε τρίτους χωρίς τη δική τους συναίνεση.

[157] Βλέπε ό.π.,περιοδικό για το Enterprise Computing και την Ασφάλεια στην πληροφορική

Στο λειτουργικό των Windows για να δούμε τα cookies που έχουν αποθηκευθεί στον υπολογιστή μας, πηγαίνουμε στο μενού εργαλεία\επιλογές internet\Γενικά\ Ρυθμίσεις\Προβολή αρχείων -Βλέπουμε τα περιεχόμενα του φακέλου Προσωρινά αρχεία του Internet (Temporary Internet Files). Μπορούμε να ξεχωρίσουμε τα αρχεία των cookies καθώς έχουν ως πρόθεμα τη λέξη Cookie: και μετά το όνομα του χρήστη που τα έχει δεχθεί, το σύμβολο @ και τέλος το όνομα του Web site που τα δημιούργησε π.χ Cookie:Panos@www.google.com βλέπε εικόνα 5



Εικόνα 5. Εμφάνιση των cookies στα Windows

Το όνομα του χρήστη δεν στέλνεται στο Web site που δημιούργησε το cookie αλλά χρησιμοποιείται για να ξεχωρίζουν τα cookies που δέχονται οι διαφορετικοί χρήστες του ίδιου υπολογιστή. Αν προσπαθήσουμε να δούμε τα περιεχόμενα ενός αρχείου cookie με το πρόγραμμα Σημειωματάριο (Notepad) των Windows δεν θα μπορέσουμε να δούμε το σωστό σετ χαρακτήρων και έτσι θα πρέπει να χρησιμοποιήσουμε το γνωστό πρόγραμμα επεξεργασίας κειμένου Word for Windows.

Από την επιλογή Εισαγωγή και εξαγωγή- του μενού Αρχείο του Internet Explorer μπορούμε να επιλέξουμε Εξαγωγή Cookies και μετά έναν φάκελο και ένα όνομα αρχείου, όπου τα προτεινόμενα είναι ο φάκελος Τα έγγραφά μου και το όνομα αρχείου είναι το cookies.txt, ώστε να δημιουργηθεί ένα αρχείο κειμένου που θα περιέχει συγκεντρωτικά τα περιεχόμενα όλων των cookies και θα μπορούμε να το ανοίξουμε και με το Σημειωματάριο (Notepad). Κάποια από τις παραπάνω ρυθμίσεις είναι η προεπιλογή που ήδη υπάρχει και που ρυθμίζει την πολιτική μας απέναντι στα cookies, δηλ. δίνουμε εμείς εντολή στον Internet Explorer για να επιτρέψει ή όχι την δημιουργία ενός cookie ανάλογα με την ρύθμιση (πολιτική) απορρήτου του δημιουργού του. Από την επιλογή για προχωρημένους στο ίδιο πλαίσιο διαλόγου μπορούμε να επιλέξουμε αν θα παρακάμψουμε ή όχι τον αυτόματο χειρισμό των cookies και για τα cookies του αρχικού κατασκευαστή και για τα cookies άλλων (τρίτων) κατασκευαστών. Οι διαθέσιμες επιλογές μας σε κάθε περίπτωση είναι Αποδοχή, Αποκλεισμός και Προτροπή.

Τα δεδομένα των cookies μετακινούνται με τον εξής τρόπο : Αν γράψουμε το URL ενός Web site στον φυλλομετρητή μας, τότε ο φυλλομετρητής στέλνει μια αίτηση (request) στο Web site για να φορτωθεί η σχετική ιστοσελίδα. Για παράδειγμα, αν γράψουμε το URL http://www.google.com στον φυλλομετρητή μας, τότε ο φυλλομετρητής θα έρθει σ' επαφή με τον

server της google και θα ζητήσει (request) την αρχική του ιστοσελίδα (home page).Όταν το κάνει αυτό ο φυλλομετρητής, θα ψάξει στο μηχάνημά μας για ένα αρχείο cookie που να έχει δημιουργηθεί παλαιότερα από την google. Αν βρει ένα αρχείο cookie της google , τότε θα στείλει ο φυλλομετρητής στον server της google όλα τα ζευγάρια ονόματος-τιμής που υπάρχουν στο αρχείο μαζί με το URL. Αν δεν βρει κάποιο αρχείο cookie, δεν θα στείλει κανένα δεδομένο cookie. Ο Web server της google λαμβάνει τα δεδομένα του cookie και την αίτηση (request) για μια ιστοσελίδα. Αν ληφθούν και ζευγάρια ονόματος-τιμής, η google μπορεί να χρησιμοποιήσει κι αυτά. Αν δεν ληφθεί κανένα ζευγάρι ονόματος-τιμής, η google θα γνωρίζει ότι δεν έχουμε επισκεφθεί παλαιότερα το site. Ο server δημιουργεί ένα καινούργιο ID για μας στη βάση δεδομένων της google και μετά στέλνει ζευγάρια ονόματος-τιμής στο μηχάνημά μας μέσα στην επικεφαλίδα (header) για την ιστοσελίδα που στέλνει. Το μηχάνημά μας αποθηκεύει τα ζευγάρια ονόματος-τιμής στον σκληρό δίσκο. Υπάρχουν κι άλλα κομμάτια πληροφοριών που ο server μπορεί να στείλει με το ζευγάρι ονόματος-τιμής. Μια απ' αυτές τις πληροφορίες είναι η ημερομηνία λήξης του cookie (expiration date) και μια άλλη είναι μια διαδρομή (path) μέσα στο site, έτσι ώστε το site να μπορεί να συσχετίσει διαφορετικές τιμές cookies με διαφορετικά τμήματα (φακέλους) του site.

Μπορούμε να έχουμε έναν έλεγχο σ' αυτή τη διαδικασία, θέτοντας μια επιλογή στις ρυθμίσεις του φυλλομετρητή μας έτσι ώστε ο φυλλομετρητής να μας πληροφορεί κάθε φορά που ένα site μάς στέλνει ζευγάρια ονόματος-τιμής. Μπορούμε μετά να αποδεχθούμε ή να απορρίψουμε αυτές τις τιμές. Αν έχουμε ένα πρόβλημα με τον φυλλομετρητή μας και καλέσουμε την τεχνική υποστήριξη, πιθανότατα το πρώτο πράγμα που θα μας ζητήσουν είναι να διαγράψουμε όλα τα προσωρινά αρχεία Internet που υπάρχουν στο μηχάνημά μας. Αν το κάνουμε αυτό, θα χάσουμε όλα τα αρχεία των cookies. Όταν επισκεφθούμε αργότερα ένα site ξανά, αυτό το site θα νομίζει ότι είμαστε ένας καινούργιος χρήστης και θα μας εκχωρήσει ένα καινούργιο cookie. Αυτό θα έχει ως αποτέλεσμα να μην είναι σωστές οι πληροφορίες που έχει το site σχετικά με τους νέους και τους παλιούς χρήστες αλλά θα είναι δύσκολο και για μας να επαναφέρουμε τις ήδη αποθηκευμένες προτιμήσεις. Αυτός είναι ένας λόγος που πολλά sites μάς ζητάνε να κάνουμε εγγραφή (registration) μ' ένα user name και ένα password, οπότε μπορούμε να κάνουμε login και να επαναφέρουμε τις προτιμήσεις μας ακόμη κι αν χάσουμε το δικό μας αρχείο cookie. Αν οι τιμές των προτιμήσεων αποθηκεύονται απευθείας στο μηχάνημα του χρήστη, τότε είναι αδύνατη η επαναφορά τους. Αυτός είναι ο λόγος που πολλά sites αποθηκεύουν τώρα όλες τις πληροφορίες σχετικά με τον χρήστη σε μια κεντρική βάση δεδομένων και μόνο μια τιμή για το ID στο μηχάνημα του χρήστη[158].

Υπάρχουν δύο πράγματα που έχουν προκαλέσει αυτήν την σφοδρή αντίδραση για τα cookies :Το πρώτο είναι κάτι που βασανίζει τους καταναλωτές για δεκαετίες. Ας υποθέσουμε ότι αγοράζουμε κάτι από έναν παραδοσιακό κατάλογο ταχυδρομικών παραγγελιών. Η εταιρεία που διαχειρίζεται τον κατάλογο κατέχει το όνομά μας, τη διεύθυνσή μας και τον αριθμό τηλεφώνου μας από την παραγγελία μας και γνωρίζει επίσης τι προϊόντα έχουμε αγοράσει. Μπορεί να πουλήσει τις πληροφορίες αυτές σ' άλλους που με τη σειρά τους ίσως είναι πρόθυμοι να πουλήσουν παρόμοια προϊόντα σε μας. Αυτό είναι το καύσιμο που κάνει δυνατή τη λειτουργία του telemarketing και του junk mail (διαφημιστική αλληλογραφία).Ένα Web site μπορεί να παρακολουθεί (καταγράφει) όχι μόνο τις αγορές μας αλλά επίσης και τις σελίδες που διαβάζουμε, τις διαφημίσει στις οποίες κάνουμε κλικ κλπ. Αν αγοράσουμε κάτι και καταχωρήσουμε το όνομα και την διεύθυνσή μας, το site ίσως είναι σε θέση να γνωρίζει πολύ

[158] Βλέπε ό,π. περιοδικό για το Enterprise Computing και την Ασφάλεια στην πληροφορική

περισσότερα για μας απ' ό,τι μια παραδοσιακή εταιρεία ταχυδρομικών παραγγελιών. Αυτό κάνει το targeting (στόχευση) πολύ πιο ακριβές αλλά και πολλούς ανθρώπους να μην αισθάνονται άνετα. Διαφορετικά sites ακολουθούν διαφορετικές πολιτικές. Ένα Web site μπορεί να ακολουθεί μια αυστηρή πολιτική ιδιωτικότητας (privacy policy) και να μην πουλάει ούτε να κοινοποιεί προσωπικές πληροφορίες για τους αναγνώστες του. Μπορούμε να συγκεντρώσουμε πληροφορίες και να τις διανείμουμε. Για παράδειγμα, αν ένας ρεπόρτερ ρωτήσει πόσους επισκέπτες έχει κάποιο site ή ποια είναι η πιο δημοφιλής σελίδα του, μπορούμε να πάρουμε αυτά τα συγκεντρωτικά στατιστικά στοιχεία από τα δεδομένα που υπάρχουν στην βάση δεδομένων.

Το δεύτερο είναι μοναδικό στο Internet. Υπάρχουν συγκεκριμένοι providers που μπορούν να δημιουργήσουν cookies που να είναι ορατά σε πολλά sites. Το DoubleClick αποτελεί το πιο χαρακτηριστικό παράδειγμα. Πολλές εταιρείες χρησιμοποιούν το DoubleClick για να εξυπηρετήσουν διαφημιστικά (ad banners) άλλων εταιρειών στα sites τους. Το DoubleClick μπορεί να τοποθετήσει μικρά (μεγέθους 1x1 pixels) αρχεία GIF στο site που να δίνουν την δυνατότητα στο DoubleClick να φορτώσει cookies στο μηχάνημά μας. Το DoubleClick μπορεί μετά να καταγράφει τις κινήσεις μας σε πολλά sites. Μπορεί να δει ακόμη και τα κείμενα αναζήτησης που γράφουμε στις μηχανές αναζήτησης (search engines). Επειδή μπορεί να συγκεντρώσει τόσες πολλές πληροφορίες για μας από πολλά sites, το DoubleClick μπορεί να σχηματίσει πολύ πλούσια προφίλ χρηστών. Μπορεί να είναι πάντα ανώνυμα, αλλά είναι πλούσια σε στοιχεία. Το DoubleClick έκανε ένα βήμα παραπέρα. Προσπάθησε να συνδέσει αυτά τα στοιχεία με τα ονόματα και τις διευθύνσεις των χρηστών και μετά να τα πουλήσει. Αυτό θύμισε σε πολλούς κατασκοπεία και είναι αυτό που προκάλεσε την αναταραχή. Μπορούν δηλαδή να καταγράφουν τις σελίδες που έχει επισκεφθεί ο χρήστης, τις διαφημίσεις που διάβασε κ.λπ. Είναι επίσης τεχνικά δυνατόν ένας υπολογιστής – εξυπηρετητής (server) να επιτρέψει την πρόσβαση στις ανωτέρω πληροφορίες που συνέλεξε το «cookie» σε απεριόριστο αριθμό άλλων εξυπηρετητών. Με αυτόν τον τρόπο επιχειρήσεις έχουν την δυνατότητα να παρακολουθούν τις επισκέψεις ενός χρήστη από μια ιστοσελίδα σε μια άλλη, να συλλέγουν πληροφορίες για τις προσωπικές συνήθειές του και να τις χρησιμοποιούν για σκοπούς διαφήμισης και εμπορικής προώθησης. Οι περισσότεροι χρήστες αποδέχονται ευχαρίστως την ύπαρξη των «cookies», διότι με αυτόν τον τρόπο μειώνεται ο χρόνος που απαιτείται για την πλοήγησή τους στο διαδίκτυο, παρότι οι Υπάρχουν προγράμματα που καθαρίζουν τα κακόβουλα cookies, ενώ αν ο χρήστης επιθυμεί να τα διαγράψει δίνεται αυτή η δυνατότητα μέσα από το φυλλομετρητή ιστοσελίδων[159].

2.3.12 **Έλεγχος της διεύθυνσης** IP (Internet Protocol Address)

Η διεύθυνση IP (Ip address - Internet Protocol address), είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol standard. Κάθε συσκευή που ανήκει στο δίκτυο - όπως επίσης δρομολογητές (routers), υπολογιστές, time-servers, εκτυπωτές, μηχανές για fax μέσω Internet, και ορισμένα τηλέφωνα - πρέπει να έχει τη δική της μοναδική διεύθυνση. Μία διεύθυνση IP μπορεί να θεωρηθεί το αντίστοιχο μιας διεύθυνσης κατοικίας ή ενός αριθμού τηλεφώνου (σύγκριση με VoIP) για έναν υπολογιστή ή άλλη συσκευή δικτύου στο Διαδίκτυο.

[159] Βλέπε http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cookies.html

Όπως κάθε διεύθυνση κατοικίας και αριθμός τηλεφώνου αντιστοιχούν σε ένα και μοναδικό κτίριο ή τηλέφωνο, μια IP address χρησιμοποιείται για τη μοναδική αναγνώριση ενός υπολογιστή ή άλλης συσκευής που συνδέεται στο δίκτυο[160].

Η διεύθυνση αυτή μπορεί να είναι μόνιμη (fixed IP address) ή προσωρινή και να αποδίδεται από τον πάροχο μόνο για το διάστημα κατά το οποίο ο χρήστης κάθε φορά συνδέεται με το Διαδίκτυο (dynamic IP address). Και στις δύο περιπτώσεις, η διεύθυνση IP, μόνιμη ή δυναμική, αποτελεί την «ταυτότητα» του τερματικού του χρήστη στο internet και είναι της μορφής XXX.XXX.XXX.XXX όπου XXX=αριθμοί που μπορούν να έχουν τιμές από 1 έως 255[161]. Η ταυτότητα αυτή δίνει τη δυνατότητα στον πάροχο (isp[162]) να γνωρίζει τις πληροφορίες που διακινήθηκαν μέσω της συγκεκριμένης διεύθυνσης IP, π.χ. την ημερομηνία και ώρα σύνδεσης, τις ιστοσελίδες που αναζήτησε και επισκέφθηκε ο χρήστης, τα μηνύματα ηλεκτρονικής αλληλογραφίας που αντήλλαξε, δημιουργώντας αρχείο με τα ανωτέρω δεδομένα που αναφέρονται στο χρήστη που έχει την αντίστοιχη ip διεύθυνση .

2.3.13 Ιχνηλάτηση της περιήγησης των χρηστών στο Διαδίκτυο

Χρησιμοποιώντας ένα φυλλομετρητή (browser) για την περιήγησή μας στο Διαδίκτυο ακολουθούμε μια διαδρομή από τον υπολογιστή μας μέχρι τον server που φιλοξενεί την ιστοσελίδα που επισκεπτόμαστε. Η επίσκεψή μας σε ένα ιστότοπο καθώς και πληροφορίες για αυτή (ημερομηνία, ώρα επίσκεψης αρχεία που ανοίξαμε), καταγράφονται στο ιστορικό του φυλλομετρητή τα οποία μπορεί ο οποιοσδήποτε που έχει πρόσβαση στον υπολογιστή μας να λάβει γνώση. Τα ίχνη από την περιήγηση του χρήστη στο Διαδίκτυο καταγράφονται όχι μόνον στον προσωπικό υπολογιστή του, αλλά και στους υπολογιστές των παρόχων υπηρεσιών διαδικτύου(ISP), με αποτέλεσμα να καθίσταται ευχερώς προσβάσιμο σε τρίτους, μη δικαιούμενους, το ιστορικό της περιήγησης ενός χρήστη στο Διαδίκτυο.

2.3.14 Συλλογή πληροφοριών κατά την περιήγηση στο Διαδίκτυο

Οι χρήστες του Διαδικτύου κατά την περιήγησή τους σε αυτό και προκειμένου να κάνουν χρήση υπηρεσιών που προσφέρονται από ιστοσελίδες ή για να αποκτήσουν πρόσβαση στο περιεχόμενό τους , καλούνται να δώσουν προσωπικές πληροφορίες που αναφέρονται στα προσωπικά δεδομένα τους όπως το ονοματεπώνυμό τους, την ταχυδρομική διεύθυνσή τους, τον αριθμό τηλεφώνου τους, την διεύθυνση ηλεκτρονικού ταχυδρομείου τους, το επάγγελμα την ηλικία κ.λ.π.

---

[160] http://el.wikipedia.org/Διεύθυνση IP

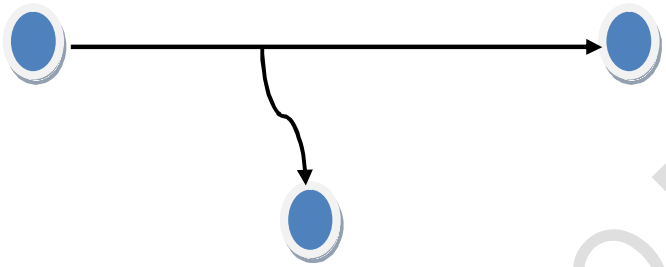
[161] http://www.forthnet.gr/templates/faq.aspx?p=59334

[162] Από τα αρχικά των λέξεων: Internet Service Provider .Μια υπηρεσία παροχής Internet (ISP), είναι μια εταιρεία η οποία παρέχει πρόσβαση στο Internet, συνήθως έναντι αντιτίμου. Ο πλέον συνηθισμένος τρόπος σύνδεσης σε μια

2.4 Κατηγορίες επιθέσεων[163] στα δίκτυα Υπολογιστών

Οι επιθέσεις σε ένα σύστημα μπορούν να κατηγοριοποιηθούν σε Παθητικές και Ενεργητικές:

☞ **Παθητικές** (Passive): **Επιθέσεις υποκλοπής** κατά τις οποίες ο επιτιθέμενος αποκτά μη εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος. Αναφέρονται ως παθητικές επειδή ο επιτιθέμενος υποκλέπτει πληροφορίες χωρίς να τροποποιεί, να διαγράφει ή να εισάγει δεδομένα που διακινούνται στο σύστημα. Οι επιθέσεις Υποκλοπής μπορεί να έχουν σαν στόχο τα δεδομένα (π.χ. αρχεία κωδικών, αριθμούς πιστωτικών καρτών, κωδικούς PIN, κωδικούς password κατά τη μεταφορά τους στο δίκτυο), το Λογισμικό (π.χ. μη εξουσιοδοτημένη πρόσβαση στον κώδικα των προγραμμάτων) ή τις Γραμμές Επικοινωνίας του συστήματος (π.χ. επιθέσεις ανάλυσης κίνησης –traffic analysis). Ουσιαστικά αποτελούν ***επιθέσεις κατά της Εμπιστευτικότητας*** (Confidentiality) του Συστήματος.



Σχήμα 11. Επίθεση Υποκλοπής (Interception)

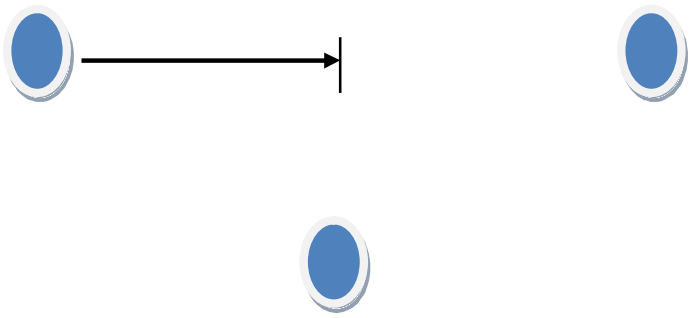
☞ **Ενεργητικές** (Active): Ο επιτιθέμενος έχει τη δυνατότητα να εξαπολύσει επιθέσεις Διακοπής, Αλλοίωσης, ή Εισαγωγής. Οι ενεργητικές επιθέσεις θεωρούνται οι πλέον δύσκολες ως προς την αντιμετώπιση τους.

Επιθέσεις Διακοπής. Στις επιθέσεις διακοπής οι πόροι του συστήματος δεν είναι διαθέσιμοι. Για παράδειγμα, διαγραφή αρχείων, δεδομένων και πληροφοριών, επιθέσεις άρνησης εξυπηρέτησης (DOS attacks) . Οι επιθέσεις Διακοπής μπορεί να έχουν σαν στόχο το Υλικό (βλάβες, διακοπή ρεύματος, επιθέσεις άρνησης εξυπηρέτησης σε ηλεκτρονικές διατάξεις), το Λογισμικό (διαγραφή ή αναστολή της εκτέλεσης προγράμματος ή του Λειτουργικού Συστήματος), τα Δεδομένα (διαγραφή ή απώλεια δεδομένων, επιθέσεις στο Σύστημα Αρχείων –file system) ή τις Γραμμές Επικοινωνίας (επίθεση στους δρομολογητές ή στο μέσο μετάδοσης με σκοπό τη διακοπή της επικοινωνίας). Ουσιαστικά αποτελούν ***επιθέσεις κατά της Διαθεσιμότητας*** (Availability) του Συστήματος[164].

υπηρεσία παροχής Internet (ISP) είναι μέσω μιας τηλεφωνικής γραμμής (σύνδεση μέσω τηλεφώνου) ή μέσω σύνδεσης ευρείας ζώνης (καλωδιακή ή DSL).

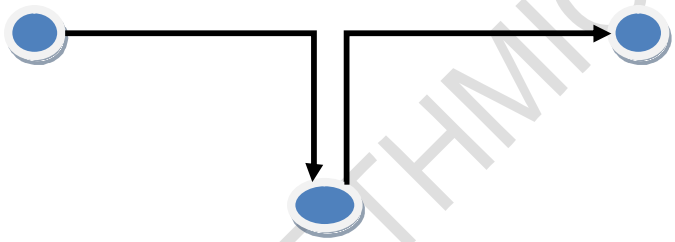
[163] επίθεση η παραβίαση (ή η απόπειρα παραβίασης) της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας του συστήματος.

[164] Βλ. Εμμανουήλ Μάγκος, Ασφάλεια Υπολογιστών και Προστασία Δεδομένων, Κέρκυρα, 2007,σελ. 11-13 στο: http://di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20A.pdf



Σχήμα 12. Επίθεση Διακοπής (Interruption)

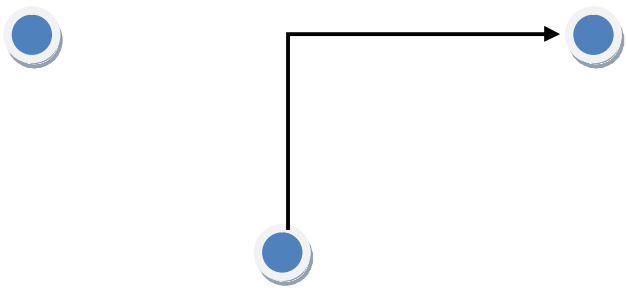
Επιθέσεις Αλλοίωσης (Modification). Σε αυτές τις επιθέσεις ο επιτιθέμενος αποκτά μη εξουσιοδοτημένη πρόσβαση στο σύστημα, με σκοπό την αλλοίωση-τροποποίηση των δεδομένων του συστήματος. Οι επιθέσεις Αλλοίωσης μπορεί να έχουν σαν στόχο το το Λογισμικό (αλλοίωση του κώδικα του προγράμματος), ή τα Δεδομένα του Συστήματος (αλλοίωση των περιεχομένων ενός αρχείου, των εγγραφών σε μια Βάση Δεδομένων, αλλοίωση του ποσού πληρωμής σε μια συναλλαγή Ηλεκτρονικού Εμπορίου). Ουσιαστικά αποτελούν ***επιθέσεις κατά της Ακεραιότητας*** (Integrity) του Συστήματος .



Σχήμα 13. Επίθεση Αλλοίωσης (Modification)

Επιθέσεις Εισαγωγής (Fabrication). Τέτοιες επιθέσεις έχουμε όταν ο εισβολέας εισέρχεται στο σύστημα. Παραδείγματα αποτελούν οι επιθέσεις παραπλανητικής αλληλογραφίας (Phishing), Πλαστοπροσωπίας (Spoofing), Ενδιάμεσης Οντότητας (Man in the Middle), καθώς και οι επιθέσεις Επανάληψης (replay attacks). Οι επιθέσεις Εισαγωγής μπορεί να έχουν σαν στόχο το Λογισμικό (αντικατάσταση του νομίμου προγράμματος με κάποιο άλλο, συνήθως κακόβουλο πρόγραμμα), τα Δεδομένα ή τους Ανθρώπους του συστήματος (επιθέσεις πλαστοπροσωπίας, πλαστά πιστοποιητικά δημόσιου κλειδιού, Phishing, επιθέσεις Ενδιάμεσης Οντότητας κλπ). Αποτελούν ***επιθέσεις κατά της Ακεραιότητας*** (Integrity) και ***της Αυθεντικότητας*** του Συστήματος[165].

[165] Βλ.ό.π., Εμμανουήλ Μάγκος, Ασφάλεια Υπολογιστών και Προστασία Δεδομένων, Κέρκυρα, 2007,σελ. 11-13 στο: http://di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20A.pdf



Σχήμα 14. Επίθεση Εισαγωγής (Fabrication)

2.4.1 **Επιθέσεις άρνησης εξυπητέτησης** (Denial of Service attack, Dos attack)

Επιθέσεις άρνησης εξυπηρέτησης (Denial-of-service attack, DoS attack) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή - ενός δικτύου υπολογιστών ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή- δίκτυο ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να παρέχει στους νόμιμους χρήστες του τις υπηρεσίες για τις οποίες έχει σχεδιαστεί. Οι επιθέσεις αυτές μπορεί να προκαλέσουν απώλεια μηνυμάτων ,καθυστερήσεις και γενικότερα πρόβλημα στο σύστημα[166]. Εκδηλώνονται με τη μορφή χιλιάδων αιτήσεων σύνδεσης σ' έναν server με απώτερο στόχο τον κατάρρευση του server και την αδυναμία του να ανταποκριθεί σ' έναν τόσο μεγάλο αριθμό αιτήσεων.

Οι επιθέσεις του τύπου DoS (Denial of Service), είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας, αποτελούν μια από τις σοβαρότερες επιθέσεις που μπορούν να εκδηλωθούν σ' ένα Web site ή σ' ένα δίκτυο υπολογιστών. Οι επιθέσεις αυτές είναι καταστροφικές για τις εταιρείες και έχουν μεγάλο οικονομικό κόστος. Το κόστος αφορά στις χαμένες ώρες λειτουργίας μιας επιχείρησης αλλά και στο κόστος που απαιτείται για τον εντοπισμό και την αντιμετώπιση αυτών των επιθέσεων. Ουσιαστικά μια τέτοια επίθεση έχει ως αποτέλεσμα την αδυναμία της εταιρείας να εξυπηρετήσει τους πελάτες της.

Υπάρχουν γενικά δύο μορφές αυτής της επίθεσης. Η μία είναι η επίθεση κατά την οποία το σύστημα αναγκάζεται να καταρρεύσει και πρέπει να κάνει πάλι επανεκκίνηση και η άλλη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει αυτούς που πραγματικά θέλουν την υπηρεσία. Τέτοιου τύπου επιθέσεις μπορούν να χρησιμοποιηθούν στην υπηρεσία του ηλεκτρονικού ταχυδρομείου και να παρεμποδίσουν ή και να αχρηστεύσουν την ηλεκτρονική αλληλογραφία σε κάποιον. Για παράδειγμα μπορεί κάποιος να στήσει έναν μηχανισμό ο οποίος θα αποστέλλει μηνύματα μαζικά στο θύμα γεμίζοντας το γραμματοκιβώτιό του και

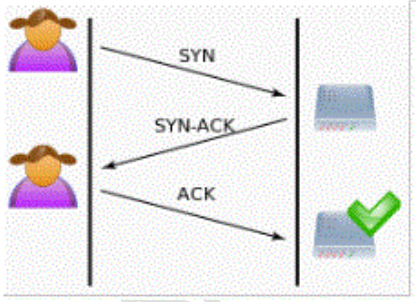
[166] Βλ.Ν.Αλεξανδρής,Β. Χρυσικόπουλος, Δ. Πεππές, Ασφάλεια Υπολογιστικών Συστημάτων, στο: Ν. Αλεξανδρής,Ε. Κιουντούζης, Β.Τραπεζάνογλου, Ασφάλεια Πληροφοριών-Τεχνικά Νομικά και Κοινωνικά Θέματα, Εκδόσεις Νέων Τεχνολογιών, 1995, σελ. 64.

απαγορεύοντας, με αυτόν τον τρόπο, την παραλαβή της αλληλογραφίας από αυτούς που περιμένει[167].

Μερικοί από τους πιο γνωστούς τύπους τέτοιων επιθέσεων είναι[168]:

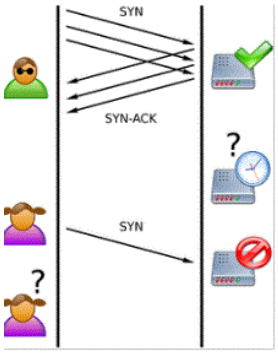
☞ **Επίθεση SYN flood.** Για να δημιουργηθεί μία σύνδεση από έναν υπολογιστή (πελάτης - client) σε έναν άλλο (διακομιστής - server) θα πρέπει να ακολουθηθούν τα βήματα που καθορίζονται στο πρωτόκολλο TCP. Ο πελάτης (client) ζητά την δημιουργία μίας σύνδεσης στέλνοντας έναν πακέτο TCP SYN στον διακομιστή (server). Το όνομα του πακέτου προέρχεται από την λέξη syncronize που σημαίνει συγχρονισμός. Ο διακομιστής απαντά στην αίτηση του πελάτη στέλνοντάς του ένα πακέτο TCP SYN-ACK, από την αγγλική λέξη acknowledge που σημαίνει αναγνώριση, αποδοχή. Ο πελάτης απαντά με ένα πακέτο TCP ACK δηλώνοντας ότι αποδέχεται και αυτός την σύνδεση. Η διαδικασία αυτή ονομάζεται τριμερής χειραψία (three-way handshake) και μόλις πραγματοποιηθεί , η σύνδεση TCP έχει εγκαθιδρυθεί και μπορούν να αποσταλούν δεδομένα προς και από τους δύο υπολογιστές βλ εικόνα15.

Στην επίθεση SYN flood ο επιτιθέμενος στέλνει στον διακομιστή-θύμα πολλαπλά πακέτα TCP SYN. Ο διακομιστής θεωρώντας ότι τα πακέτα αυτά προέρχονται από κανονικό χρήστη, οπότε απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία χειραψίας του πρωτοκόλλου TCP. Ο επιτιθέμενος όμως δεν αποστέλλει πακέτα ACK για να ολοκληρωθεί η χειραψία, αλλά αφήνει τον διακομιστή να περιμένει. Επειδή για κάθε σύνδεση που δεν ολοκληρώνεται ο διακομιστής ξοδεύει υπολογιστικούς πόρους, μετά από κάποιο συγκεκριμένο αριθμό τέτοιων συνδέσεων ο διακομιστής φτάνει στα όριά του και δεν μπορεί να εξυπηρετήσει τους νόμιμους χρήστες. Αυτή η κατάσταση ονομάζεται άρνηση υπηρεσιών (DOS - Denial of Service) βλ. εικόνα 16.



Σχήμα 15. Κανονική σύνδεση TCP.

Πηγή: http://el.wikipedia.org/wiki/SYN_flood



Σχήμα 16. Επίθεση SYN flood

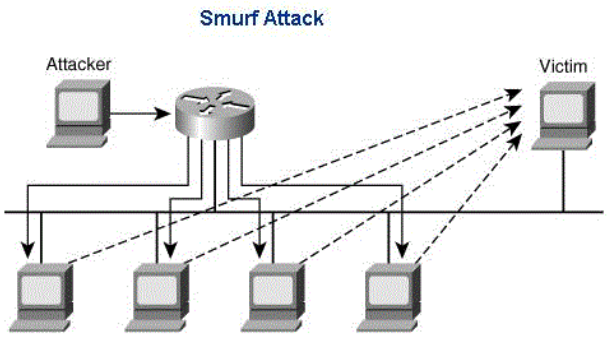
Πηγή: http://el.wikipedia.org/wiki/SYN_flood

[167] Βλ. http://www.us-cert.gov/cas/tips/ST04-015.html.

[168] Βλ http://www.tutorial5.com/content/view/80/79/ επίσης http://learn-networking.com/network- security/how-to-prevent-denial-of-service-attacks

☞ **Επίθεση Smurf.** Η Επίθεση που αποκαλείτε smurf[169], βασίζεται στην χρήση διακομιστών μετάδοσης με σκοπό την παράλυση ενός δικτύου. Ένας διακομιστής μετάδοσης μπορεί να αντιγράψει ένα μήνυμα και να το αποστείλει σε όλους τους υπολογιστές ενός δικτύου. Η διαδικασία ξεκινάει με τον επιτιθέμενο να στέλνει μία πληθώρα πακέτων **ping ICMP Echo Reply** [170], σε έναν ή παραπάνω διακομιστές μετάδοσης. Τα πακέτα αυτά έχουν τροποποιηθεί κατάλληλα έτσι ώστε στο πεδίο source της κεφαλίδας IP να αναγράφεται η διεύθυνση IP του θύματος και όχι του επιτιθέμενου. Αυτό έχει ως συνέπεια όλοι οι υπολογιστές να απαντούν στο ping με πακέτα ICMP Echo Reply, τα οποία έχουν ως διεύθυνση προορισμού την διεύθυνση IP του θύματος. Άρα λοιπόν το θύμα πλημμυρίζει με πακέτα ping και οδηγείται σε κατάρρευση. Η επίθεση Smurf ουσιαστικά επιτρέπει στον επιτιθέμενο να εκμεταλλευτεί άλλα δίκτυα υπολογιστών και με την αποστολή σχετικά λίγων πακέτων ping να πετύχει τον στόχο του. Τα δίκτυα υπολογιστών χρησιμεύουν ουσιαστικά στον πολλαπλασιασμό των πακέτων του επιτιθέμενου και την αποστολή αυτών στο θύμα. Τα δίκτυα τα οποία χρησιμοποιούνται κατ' αυτόν τον τρόπο ονομάζονται Ενισχυτές Smurf (Smurf Amplifiers), διότι ενισχύουν την επίθεση[171].

Η προστασία σε επιθέσεις Smurf γίνεται με κατάλληλες τεχνολογίες, έτσι ώστε ένα δίκτυο υπολογιστών να μη γίνεται συνεργός σε επιθέσεις Smurf. Για παράδειγμα στους δρομολογητές Cisco, η προστασία ενάντια σε επιθέσεις Smurf μπορεί να επιτευχθεί με μονάχα μία εντολή: **No ip directed-broadcast**[172].



Σχήμα 17. Επίθεση Smurf

Πηγή: http://www.panda-thailand.com/newpanda/tip&trick/july55/week3.php

[169] Πήρε το όνομά της από το πρώτο πρόγραμμα που την υλοποίησε (Smurf στα Αγγλικά σημαίνει στρουμφάκι) βλ: http://el.dbpedia.org/page/B7_Smurf .

[170] Το ping είναι μια εντολή που εκμεταλεύεται το πρωτόκολλο ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol - είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου και χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο), πετυχαίνοντας να δοκιμαστούν συνδέσεις, στέλνοντας ένα πακέτο και αναμένοντας απάντηση.

[171] Βλ: http://el.computerscience.wikia.com/wiki/Επίθεση_Smurf

[172] Η παραπάνω εντολή ουσιαστικά αποτρέπει Δεν προστατεύει όμως αυτό το δίκτυο από το να γίνει θύμα της επίθεσης. Το θύμα μπορεί να προστατευθεί και να μετριάσει τις απώλειες από μία τέτοια επίθεση χρησιμοποιώντας ένα Firewall. Βλ: http://learn-networking.com/network-security/securing-cisco-routers-with-no-ip-directed-broadcast

☞ **Επίθεση Ping Of Death.** Η επίθεση Ping Of Death συντελείται όταν ένας ηλεκτρονικός υπολογιστής στέλνει κακοσχηματισμένα πακέτα ping σε έναν άλλο υπολογιστή με σκοπό να τον θέσει εκτός λειτουργίας. Ένα πακέτο ping έχει κανονικά μέγεθος 64 bytes (ή 84 bytes εάν προστεθεί και η κεφαλίδα που προσθέτει το πρωτόκολλο IP). Πολλοί τύποι ηλεκτρονικών υπολογιστών δεν μπορούν να χειριστούν πακέτα ping που έχουν μέγεθος μεγαλύτερο από 65535 bytes, δηλαδή το μέγιστο επιτρεπτό από το πρωτόκολλο IP. Συνεπώς η επίθεση Ping Of Death περιλαμβάνει την συνεχή αποστολή μεγάλων πακέτων ping σε κάποιον υπολογιστή μέχρι ο τελευταίος να τεθεί εκτός λειτουργίας. Για την αντιμετώπιση αυτής της επίθεσης θα πρέπει να ελέγχεται η εγκυρότητα των πακέτων IP, σε σχέση με το μέγεθός τους. Έτσι θα μπορούν να απορρίπτονται πακέτα IP που έχουν μέγεθος μεγαλύτερο του επιτρεπτού, αναχαιτίζοντας την επίθεση Ping Of Death [173].

Σχήμα 18. Επίθεση Ping Of Death
Πηγή: http://www.seminartopicsonline.com/2010/07/ping-of-death-seminar-on-denial-of.html

☞ **Επίθεση LAND**. Η επίθεση LAND ανήκει στην κατηγορία επιθέσεων DOS - Denial of Service και περιλαμβάνει την αποστολή από τον επιτιθέμενο, ενός ειδικού μολυσμένου πακέτου σε έναν υπολογιστή θύμα. Ο επιτιθέμενος στέλνει στο θύμα ένα ειδικά κατασκευασμένο πακέτο TCP SYN (έναρξη σύνδεσης TCP/IP). Στα πεδία αποστολέας και παραλήπτης της κεφαλίδας αυτού του ειδικά κατασκευασμένου TCP πακέτου βρίσκεται η διεύθυνση IP του θύματος. Η παραλαβή ενός τέτοιου πακέτου οδηγεί τον υπολογιστή του θύματος να απαντά στον εαυτό του συνέχεια με συνέπεια να καθίσταται μη λειτουργικός. Πολλά από τα σύγχρονα λειτουργικά συστήματα, όπως για παράδειγμα τα Windows XP και τα Windows Vista, είναι ευάλωτα σε τέτοιου είδους επιθέσεις[174]. Συνεπώς, το χαρακτηριστικό της επίθεσης LAND που την διαχωρίζει από άλλες επιθέσεις είναι ότι το πακέτο που στέλνεται έχει ως αποστολέα και παραλήπτη την διεύθυνση IP του θύματος[175].

☞ **Επίθεση Ping flooding**. Η επίθεση Ping flood ανήκει στην κατηγορία επιθέσεων άρνησης υπηρεσιών (DOS - Denial of Service) και περιλαμβάνει την συνεχή αποστολή πακέτων ping (ICMP Echo Request) από τον υπολογιστή του επιτιθέμενου προς τον υπολογιστή του αμυνόμενου. Για να επιτύχει αυτή η επίθεση θα πρέπει ο επιτιθέμενος να διαθέτει μεγαλύτερο bandwidth (εύρος ζώνης) από το θύμα, δηλαδή η σύνδεσή του με το διαδίκτυο να είναι πιο γρήγορη σε σχέση με του θύματος (για παράδειγμα γραμμή DSL έναντι απλής dial-up σύνδεσης). Εάν σε κάθε πακέτο ping (ICMP Echo Request) το θύμα απαντήσει με πακέτο ICMP

[173] http://www.eeei.gr/interbiz/articles/dos.htm

[174] Βλ. άρθ. , Michael Kerner, 'Land' Bug Back to Bedevil Microsoft Servers,2005, στο: http://www.internetnews.com/security/article.php/3488171

[175] Βλ. http://en.kioskea.net/contents/attaques/attaque-land.php3

Echo Reply, τότε καταναλώνει όλη την ευρυζωνική της σύνδεσής του και κατά συνέπεια οι υπηρεσίες που προσφέρει δεν είναι πλέον διαθέσιμες στους χρήστες του[176].

☞ **Επίθεση Fraggle**. Μία επίθεση fraggle είναι όμοια με μία επίθεση smurf, με εξαίρεση το γεγονός ότι αυτή χρησιμοποιεί το User Datagram Protocol (UDP[177]), αντί για το πιο σύνηθες το Transmition Control Protocol (TCP). Οι επιθέσεις τύπου fraggle είναι σήμερα εξαιρετικά ασυνήθηστες, δεδομένου ότι τα περισσότερα firewalls και routers σήμερα τις μπλοκάρουν[178].

☞ **Επίθεση Teardrop**. Αυτή η επίθεση εκμεταλλεύεται την αδυναμία του πρωτοκόλλου TCP/IP στην επανασύνδεση (reassembly) των πακέτων δεδομένων (data packets) κατά την λήψη τους. Όταν στέλνονται data στο Internet αυτά κατανέμονται σε μικρότερα κομμάτια στον υπολογιστή που κάνει την μετάδοση και συναρμολογούνται πάλι στον υπολογιστή που τα λαμβάνει. Ας υποθέσουμε ότι θέλουμε να στείλουμε 8000 bytes από έναν υπολογιστή σε έναν άλλον. Δεν θα τα στείλουμε όλα μαζί με μία μετάδοση (transmission) αλλά θα κοπούν σε μικρότερα πακέτα data (data packets) και κάθε πακέτο θα έχει συγκεκριμένο κομμάτι από τα 8000 bytes όπως : πακέτο 1ο θα έχει byte 1 έως byte 1500, πακέτο 2ο θα έχει byte 1501 έως byte 3000, πακέτο 3ο θα έχει byte 3001 έως byte 4000 κ.λ.π. Αυτά τα πακέτα έχουν στο αρχικό τους κομμάτι (TCP header) ένα πεδίο (offset) που περιγράφει πως θα γίνει η συναρμολόγηση στο σύστημα που θα λάβει τα πακέτα. Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει (reassembly) παθαίνει κατάρρευση[179].

2.4.2 **Επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης** (DDOS)

Οι επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης (**D**istributed **D**enial **o**f **S**ervice **attack** – **DDOS attack**) είναι μια παραλλαγή της Dos attack που είδαμε στην προηγούμενη ενότητα με τη διαφορά πως η επίθεση γίνεται από διαφορετικά δίκτυα ταυτόχρονα και οργανωμένα. Ενώ στην επίθεση άρνησης εξυπηρέτησης(Denial of Service attack – DOS) η επίθεση προέρχεται από ένα μεμονωμένο υπολογιστή ή δικτυακό κόμβο στην κατανεμημένη άρνηση εξυπηρέτησης (Distributed Denial of Service attack – DDOS) ο επιτιθέμενος έχει «στρατολογήσει» πολλούς κόμβους μέσω του Διαδικτύου, έτσι ώστε όλοι μαζί να επιτεθούν συγχρονισμένα στο στόχο, που μπορεί να είναι από ένα απλό υπολογιστικό σύστημα (host) μέχρι και ολόκληρα δίκτυα (Domain)[180].Μπορεί να είναι επιθέσεις σε επιχειρηματικούς ή πολιτικούς στόχους, ακήρυχτος πόλεμος ή και παιχνίδια μεταξύ hacker που στόχο έχουν να θέσουν εκτός ένα σύστημα.

---

[176] Βλ. http://el.wikipedia.org/wiki/Ping_flood επίσης http://ghostgrid.blog.com/2010/12/16/ping-flooding/

[177] Το πρωτόκολλο User Datagram Protocol (UDP) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο.

[178] Βλ. http://el.computerscience.wikia.com/wiki/_Fraggle

[179] Βλ. Denial Of Service (D.O.S.) Επιθέσεις, Ελληνικό Ηλεκτρονικό Περιοδικό (Hellenic e-zine), Τεύχος: 04, Μήνας Έκδοσης: Μάιος 2002 , στο: http://www.isee.gr/issues/04/insert/index.html

[180] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 458.

Μια DDoS επίθεση, είναι μια τεχνική επίθεσης με στόχο την δέσμευση των πόρων του Διαδικτύου. Οι επιτιθέμενοι σε μια DDoS επίθεση εκμεταλλεύονται κυρίως την αρχιτεκτονική του Διαδικτύου και αυτό είναι που τις κάνει ακόμα ισχυρότερες. Το Διαδίκτυο σχεδιάστηκε με βασικό γνώμονα τη λειτουργικότητα του και όχι την ασφάλεια. Η κατασκευή του αφήνει ανοιχτά διάφορα ζητήματα ασφάλειας, πολλά τρωτά και κενά που τα εκμεταλλεύονται οι επιτιθέμενοι.

Σε μια DDoS επίθεση έχουμε:

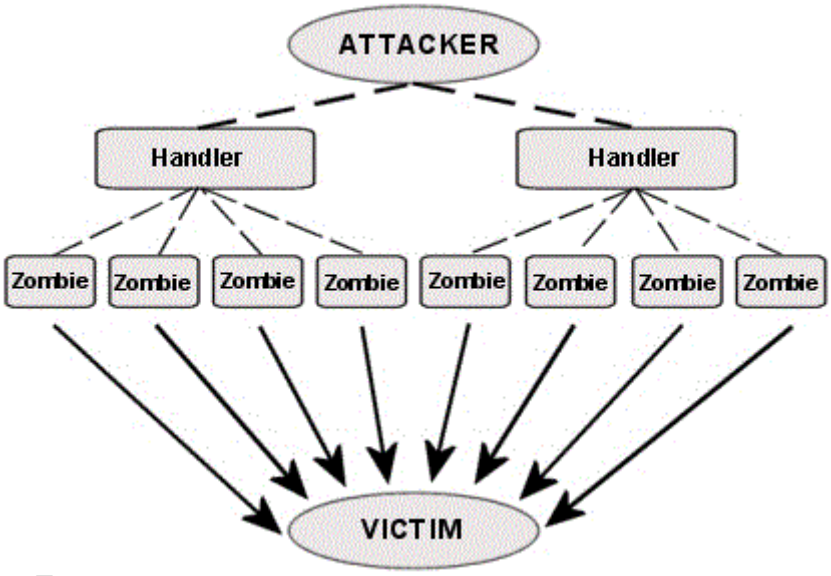
☞ Τον πραγματικό επιτιθέμενο (**attacker**).

☞ Τους χειριστές (**handlers**) ή τους κύριους, οι οποίοι αποτελούνται από hosts στους οποίους τρέχει ένα ειδικό πρόγραμμα ικανό να ελέγχει πολλαπλούς πράκτορες.

☞ Τους πράκτορες (agents) ή **zombie hosts** επίθεσης, οι οποίοι είναι «αιχμάλωτοι» hosts που τρέχουν κατάλληλο λογισμικό για παραγωγή πακέτων προς το προοριζόμενο θύμα.

☞ Το θύμα(**victim**) ή το στόχο host (βλέπε εικόνα).

Τα απαραίτητα στοιχεία για την εκτέλεση μιας επίθεσης **DDOS** είναι: Λογισμικό κατάλληλο για την πραγματοποίηση της επίθεσης ,το οποίο θα μπορεί να εκτελεστεί σε μεγάλο αριθμό υπολογιστών. Ευπάθεια (την οποία γνωρίζει ο επιτιθέμενος και η οποία δεν γνωρίζουν πολλοί διαχειριστές) σε μεγάλο αριθμό συστημάτων στα οποία θα εγκατασταθεί το λογισμικό-ζόμπι.Εντοπισμός ευπαθών συστημάτων εφαρμόζοντας τεχνική σάρωσης(scanning) [181].



Σχήμα 19. Επίθεση κατανεμημένης άρνησης εξυπηρέτησης (DDOS)

Πηγή: http://www.egyhacks.net/2011/01/what-is-ddos-attack-and-how-does-it.html

[181] Η διαδικασία σάρωσης επαναλαμβάνεται μέχρι να δημιουργηθεί ένα μεγάλο κατανεμημένο δίκτυο μολυσμένων συστημάτων Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 461-462.

Η **προστασία** από τις DDOS επιθέσεις δεν είναι εύκολη υπόθεση. Είναι μέρος μιας πολιτικής ασφαλείας που έχει τρεις άξονες. Πρόληψη-ανίχνευση-αντίδραση.

Η **πρόληψη** έχει να κάνει με μια δέσμη μέτρων στη βάση ενός σχεδίου ασφαλείας καθώς και ενός σχεδίου αντίδρασης στην εκδήλωση επιθέσεων DDOS. Έτσι χρειάζεται συνεχής εκπαίδευση προσωπικού σε θέματα ασφαλείας, εύρεση κενών ασφαλείας που υπάρχουν σε πληροφοριακά συστήματα, σε λειτουργικά συστήματα ή και σε άλλα λογισμικά, φροντίδα να υπάρχει backup ασφαλείας σε περίπτωση που υπάρχει βλάβη και χρειάζεται επαναφορά του συστήματος, απαγόρευση εξόδου από το δίκτυο πακέτων που δεν έχουν τη σωστή διεύθυνση αποστολέα, φιλτράρισμα πακέτων προς διευθύνσεις broadcast για να αποφεύγονται επιθέσεις ενίσχυσης, τοποθέτηση και σωστή ρύθμιση από τον administrator του Firewall, εγκατάσταση συστήματος ανίχνευσης επιθέσεων (**I**ntrusion **D**etection **S**ystem-IDS).

Η **ανίχνευση** συνίσταται στην αναγνώριση των δικτυακών ροών επίθεσης με χρήση εργαλείων παρακολούθησης της κίνησης. Ένα τέτοιο εργαλείο είναι το NetFlow που αναπτύχθηκε από τη Cisco Systems για την παρακολούθηση της κυκλοφορίας των πακέτων και συλλογή πληροφοριών IP. Επίσης χρειάζεται η παρακολούθηση των ενδείξεων των δρομολογητών για υπερβολική κίνηση πακέτων. Παραπέρα συνίσταται ο τακτικός έλεγχος για κρυμμένο κακόβουλο κώδικα (π.χ zombies ή rootkits), καθώς και ενημερωμένο πακέτο Anti-virus.

Η **αντίδραση** αναφέρεται στην έγκαιρη- άμεση αντιμετώπιση της επίθεσης. Σε αυτό βοηθούν μηχανισμοί αντίδρασης με κατάλληλο λογισμικό που στόχο έχουν σε πρώτη φάση αφού ανιχνεύσουν την επίθεση και να πάρουν μέτρα που θα περιορίζουν την επίθεση. Μερικοί μηχανισμοί αντιδρούν περιορίζοντας το ποσοστό της αποδεχόμενης κίνησης. Με αυτό τον τρόπο όμως εμποδίζονται και οι νόμιμοι χρήστες που ζητούν πρόσβαση στο σύστημα. Στην κατεύθυνση αυτή βοηθούν τεχνικές trace back τεχνικές που προσπαθούν να προσδιορίσουν τον επιτιθέμενο. Εάν ο επιτιθέμενος προσδιοριστεί, παρά τις προσπάθειές του να αλλοιώσει τη διεύθυνσή του, τότε είναι εύκολο να φιλτραριστεί η κίνησή του. Το φιλτράρισμα είναι αποδοτικό μόνο εάν η ανίχνευση του επιτιθεμένου δεν είναι λανθασμένη. Βέβαια αν τα zombies είναι χιλιάδες, η κυκλοφορία τους θα πλημμυρίσει το δίκτυο και θα καταναλώσει όλο το εύρος ζώνης. Σε αυτήν την περίπτωση το φιλτράρισμα είναι άχρηστο δεδομένου ότι τίποτα δεν μπορεί να ταξιδέψει πάνω από το δίκτυο[182].

Η δυσκολία να αντιμετωπισθούν οι επιθέσεις DDOS έφερε στο προσκήνιο νέες μεθόδους και εργαλεία. Ένα από τα πιο πρόσφατα εργαλεία στην αντιμετώπιση των δικτυακών επιθέσεων από κακόβουλους χρήστες και αυτοματοποιημένες επιθέσεις είναι τα honeynets και τα honeypots. Ένα honeynet είναι μια συλλογή από συστήματα που ονομάζονται honeypots. Τα honeypots παρακολουθούνται ώστε να είναι εφικτή η καταγραφή των ενεργειών των επιτιθέμενων και να γνωστοποιούνται οι τεχνικές και τα εργαλεία τα οποία χρησιμοποίησαν για την εισβολή. Είναι χρήσιμα γιατί ειδοποιούν για νέους τρόπους επιθέσεων-τρωτών σημείων, να παρέχουν ανάλυση σε βάθος του τι έγινε κατά τη διάρκεια μιας επίθεσης αλλά και μετά από αυτή. Τα honeynets σε αντίθεση με τα firewalls που εμποδίζουν τους επιτιθέμενους από το να εισβάλλουν σε ένα δίκτυο, λειτουργούν παθητικά στη συλλογή πληροφοριών για τη δράση των

[182] http://library.tee.gr/digital/m2142/m2142_koutepas.pdf

hacker, καθώς επίσης για χρήση στον τομέα της πρόληψης, της ανίχνευσης, της συλλογής πληροφοριών, έρευνας και εκπαίδευσης[183] .

2.4.3 **Κακόβουλος κώδικας** (malicious code)

Ο κακόβουλος κώδικας (Malicious code) είναι ο κώδικας προγραμμάτων που δημιουργείται από τους επιτιθέμενους σε ένα σύστημα προκειμένου να κλέψουν, προσθέσουν, τροποποιήσουν ή γενικά να προξενήσουν βλάβη σε ένα σύστημα λογισμικού προκειμένου να προκληθεί σκόπιμα ζημιά ή να υπονομευθεί η συνεχής λειτουργία του συστήματος. Τα κακοπροαίρετα αυτά προγράμματα (malicious code) είναι ένας γενικός όρος για προγράμματα που μόλις εκτελούνται προκαλούν ανεπιθύμητα αποτελέσματα σε ένα υπολογιστικό σύστημα. Μπορεί να αποσκοπούν στον περιορισμό της ταχύτητας εργασίας ενός συστήματος στην υποκλοπή σημαντικών δεδομένων, ακόμη και στον πλήρη έλεγχο του συστήματος. Οι χρήστες του συστήματος συνήθως δεν αντιλαμβάνονται την ύπαρξη ενός τέτοιου προγράμματος παρά μόνο αφού ανακαλύψουν τη ζημιά που έγινε.

Σήμερα υπάρχει μία μεγάλη ποικιλία από κακόβουλο λογισμικό, τόσο παραδοσιακών όσο και σύγχρονων τα είδη του οποίου αναφέρονται συνοπτικά παρακάτω (για περισσότερα βλέπε προηγούμενη ενότητα):

- Ιοί (viruses)
- Σκουλήκια (worms)
- Δούρειοι ίπποι (Trojan Horses)
- Λογισμικά κατασκοπείας (Spyware)
- Λογική βόμβα (logic bomb)
- Κερκόπορτα (trapdoor)
- Πίσω Πόρτες (Back Doors)
- Βακτήρια (bacteria)
- attacks scripts
- Λογισμικά εκφοβισμού (Scareware)
- Προγράμματα καταγραφής πληκτρολογήσεων (Keylogger)
- Java attack applets

[183] Ζουραράκη Ο., Μασίκου Μ. , Σχεδίαση και εξομοίωση συστήματος ανίχνευσης και αντιμετώπισης κατανεμημένων επιθέσεων (DDoS) , Αθήνα 2004, σελ 39 στο: http://artemis-new.cslab.ece.ntua.gr:8080/jspui/handle/123456789/3543

.

- ☞ επικίνδυνα ActiveX controls
- ☞ Rootkit
- ☞ Προγράμματα Ζόμπι (Programs Zombies)
- ☞ Exploit

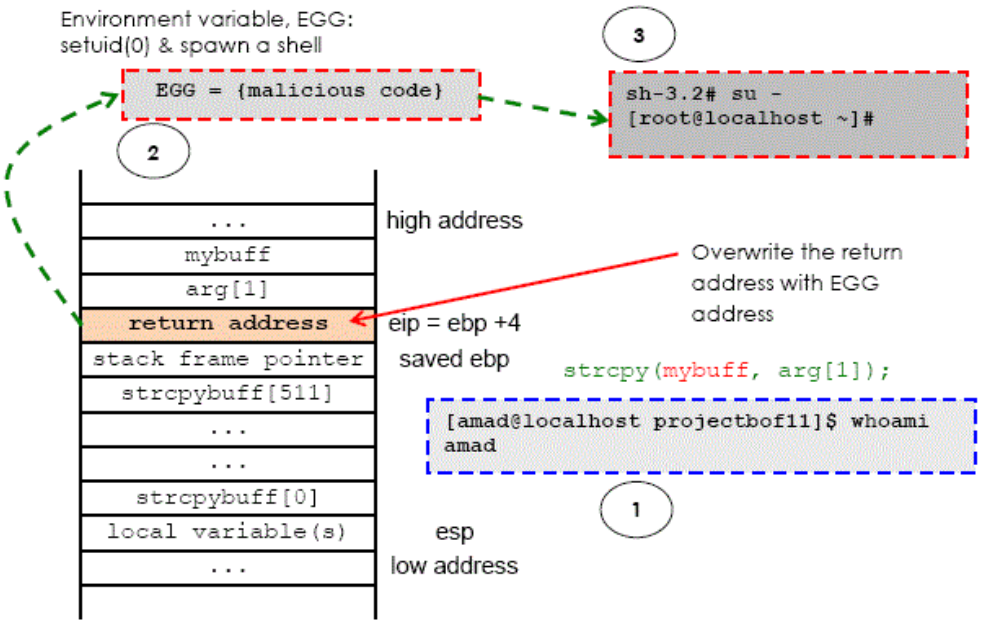
Στην εποχή της Κοινωνίας της πληροφορίας, της δικτύωσης των πληροφοριακών συστημάτων, της ραγδαίας ανάπτυξης των κοινωνικών δικτύων και της γιγάντωσης του internet το πρόβλημα του κακόβουλου κώδικα (malicious code) είναι ένα κρίσιμο πρόβλημα για την Οικονομία, την Κυβέρνηση, την Κοινωνία και τα άτομα. Στην αντιμετώπιση αυτού του προβλήματος σημαντικό ρόλο παίζει η εκπαίδευση των χρηστών σε θέματα ασφάλειας από το κακόβουλο λογισμικό. Σε τεχνικό επίπεδο προστασία από τα κακόβουλα λογισμικά προσφέρουν τα λογισμικά ασφαλείας, τα οποία προσφέρονται από τους διάφορους κατασκευαστές είτε ελεύθερα είτε επί πληρωμή. Αυτά τα λογισμικά προσφέρονται με τη μορφή σουίτας, τα οποία, εκτός από προγράμματα ανίχνευσης ιών περιλαμβάνουν φίλτρο ανεπιθύμητων μηνυμάτων, λογισμικό αποκλεισμού διαφημίσεων, έλεγχο ιστοτόπου κ.α.

2.4.4 **Υπερχείλιση καταχωρητή** (Buffer Overflow)

Κατά την επίθεση με υπερχείλιση προσωρινής μνήμης (αγγλ. buffer overflow), οι εισβολείς εισβάλουν σε συστήματα χωρίς να χρειάζεται να κάνουν login. Αντίθετα χρησιμοποιούν ένα πρόγραμμα που ήδη υπάρχει στον υπολογιστή και τρέχει στο σύστημα και του δίνουν να εκτελέσει ένα κομμάτι εντολών. Αυτό το πετυχαίνουν, φτιάχνοντας ένα μεγάλο τμήμα από χαρακτήρες που περιέχει τις εντολές που θέλουν να εκτελεστούν και το εισάγουν σαν παράμετρο εισόδου στο πρόγραμμα.

Κανονικά το πρόγραμμα δεν εκτελεί τον κώδικα που περνά σαν παράμετρος. Στην περίπτωση όμως που το μήκος του κειμένου της παραμέτρου είναι μεγαλύτερο από το μήκος που έχει δοθεί σαν χώρος (buffer[184]) για το πέρασμα της παραμέτρου, τότε μέρος του περνά στον χώρο του εκτελέσιμου προγράμματος και εκτελείται. Μάλιστα ο κώδικας εκτελείτε με ότι προνόμια έχει το πρόγραμμα που εκτελείται. Αν λοιπόν μια διεργασία του συστήματος τρέχει με προνόμια διαχειριστή και καταφέρει ο hacker να περάσει με παράμετρο τον κώδικα του, τότε θα μπορέσει να εκτελέσει εντολές που θα του δώσουν διάφορα προνόμια (root access).

[184] Buffer είναι μια περιοχή της μνήμης για προσωρινή αποθήκευση δεδομένων που μετακινούνται συνεχόμενα από και προς αυτήν.



Σχήμα 20. Επίθεση Buffer Overflow

Πηγή: http://www.tenouk.com/Bufferoverflowc/bufferoverflowvulexploitdemo32.html

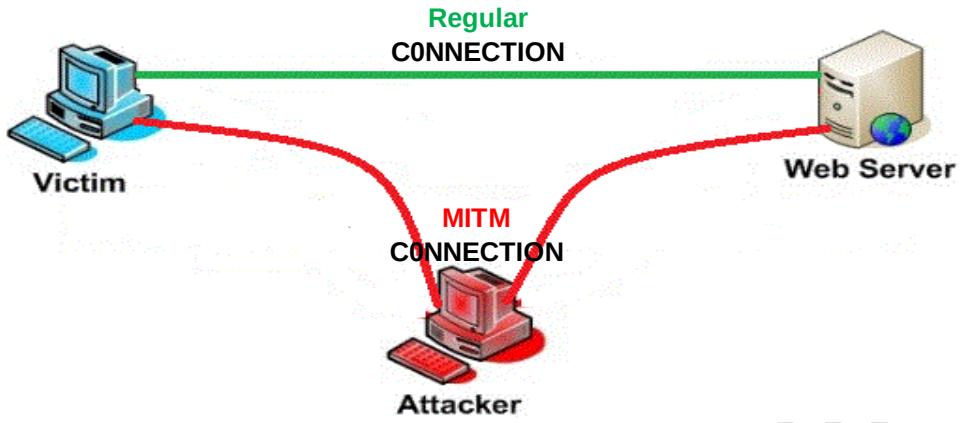
Ο χώρος για τα δεδομένα εισόδου των προγραμμάτων βρίσκεται επάνω από τον χώρο που λέγεται process stack, που είναι το τμήμα της μνήμης που το πρόγραμμα κρατά τα δεδομένα και τον κώδικα για τον χειρισμό αυτών των δεδομένων. Κάθε φορά που το πρόγραμμα εκτελεί μια λειτουργία (function) για να επιστρέψει στο αρχικό σημείο, βρίσκει τη διεύθυνση που πρέπει να επιστρέψει στο χώρο του process stack με αποτέλεσμα να εκτελεστεί ο κώδικας σε αυτή την περιοχή και μάλιστα με ό,τι προνόμια έχει το πρόγραμμα (θα μπορούσε δηλαδή να είναι προνόμια root access[185].

2.4.5 **Επίθεση ενδιάμεσου** (Man in the middle attack- MITM)

Η επίθεση Man-in-the-middle επίθεση (**MITM**) αποτελεί μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμβαίνει στη νόμιμη γραμμή επικοινωνίας δύο μερών, με στόχο να «ακούσει», υφαρπάξει, τροποποιήσει τις πληροφορίες που μεταδίδονται. Ο κακόβουλος (attacker) ελέγχοντας τη ροή επικοινωνίας μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από τους συμμετέχοντες στην αρχική επικοινωνία. Τέτοιες επιθέσεις Man-in-the-middle εφαρμόζονται όταν η συμφωνία ανταλλαγής κλειδιών γίνεται χωρίς επικύρωση

[185] Βλ.ό.π., Θ.Κομνηνός , Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002, σελ. 58

(authentication) π.χ στο πρωτόκολλο Diffie-Hellman,. Σε μια man-in-the-middle επίθεση ο επιτιθέμενος μπορεί είτε να κρυφακούει ,είτε και να τροποποιεί κατάλληλα ένα μήνυμα.



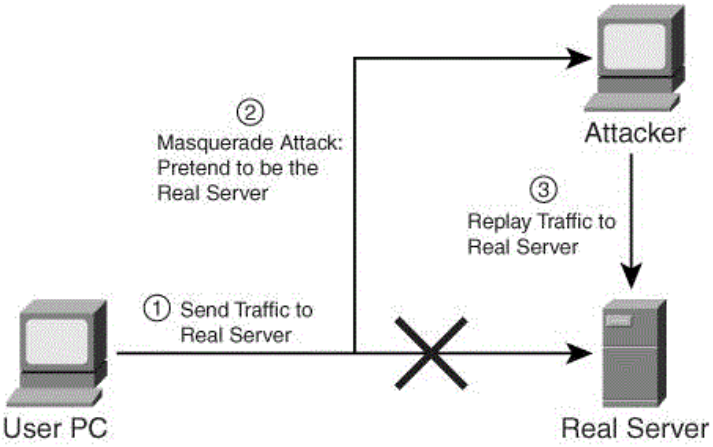
Σχήμα 21.Επίθεση ενδιάμεσου (Man in the middle attack).

Πηγή: http://vishnuvalentino.com/computer-security/hacking-facebook-using-man-in-the-middle-attack/

2.4.6 **Επίθεση επανάληψης** (Replay Attack)

Κατά τη διάρκεια μια συνόδου επικοινωνίας ο επιτιθέμενος (attacker) συλλαμβάνει τις πληροφορίες επικοινωνίας μεταξύ δύο συμβαλλόμενων μερών κάνοντας χρήση κατάλληλων εργαλείων π.χ sniffing. Στη συνέχεια μπορεί να αναμεταδώσει την επικοινωνία προκειμένου να επιτύχει κάποιο σκοπό. Παράδειγμα , ένας επιτιθέμενος να συλλάβει ένα μήνυμα μεταξύ ενός οικονομικού οργάνου και ενός χρήστη για μια ηλεκτρονική πληρωμή. Στη συνέχεια με την επανάληψη της επίθεσης, ο επιτιθέμενος θα μπορούσε να αναγκάσει διάφορες ηλεκτρονικές πληρωμές.

Οι επιθέσεις επανάληψης χρησιμοποιούνται για τις επιθέσεις πρόσβασης ή τροποποίησης. Σε ένα διανεμημένο περιβάλλον, οι πληροφορίες σύνδεσης και κωδικού πρόσβασης στέλνονται μεταξύ του πελάτη και του συστήματος επικύρωσης. Ο επιτιθέμενος μπορεί να συλλάβει αυτές τις πληροφορίες και να τις επαναλάβει πάλι αργότερα. Σε μια άλλη περίπτωση ο επιτιθέμενος θα μπορούσε να συλλάβει τους κωδικούς του χρήστη και να τους χρησιμοποιήσει αργότερα για να συνδεθεί σαν νόμιμος χρήστης.



Σχήμα 22. Επίθεση επανάληψης (Replay Attack)

Πηγή: http://fengnet.com/book/vpnconf/ch01lev1sec1.html

2.4.7 **Επίθεση ωμής βίας** (Brute-force attack)

Η επίθεση ωμής βίας (brute-force attack) αναφέρεται στην προσπάθεια του επιτιθέμενου αφού υφαρπάξει ένα μήνυμα στη συνέχεια να το αποκρυπτογραφήσει. Αυτό το πετυχαίνει με τη εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα.

Συχνά ο επιτιθέμενος ξεκινά την επίθεση χρησιμοποιώντας πιο "πιθανά", κατά την άποψή, του κλειδιά, προσπαθώντας με αυτό τον τρόπο να βρει το κλειδί πιο γρήγορα. Πρακτικά, η αναζήτηση σταματά μόλις βρεθεί το κλειδί, χωρίς να χρειαστεί περαιτέρω ενημέρωση της λίστας κλειδιών. Γνωρίζοντας το κρυπτογράφημα και τον αλγόριθμο αποκρυπτογράφησης, προσπαθεί να φτάσει στο αρχικό κείμενο, βάζοντας όλες τις πιθανές τιμές του κλειδιού. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι και τα πιθανά κλειδιά. Τέτοιου είδους επίθεση όπου χρησιμοποιούνται κλειδιά των 128 bits είναι άκαρπη. Όμως, σε παραδείγματα όπως ο DES των 56 bits, μπορεί να είναι και επιτυχής. Θεωρητικά, κάθε συμμετρική κρυπτογραφική μέθοδος μπορεί να παραβιαστεί, υπολογίζοντας διαδοχικά όλα τα πιθανά ιδιωτικά κλειδιά. Στις περιπτώσεις αυτές, η υπολογιστική ισχύς που απαιτείται για να υπολογιστούν όλα τα πιθανά κλειδιά αυξάνεται εκθετικά με το μήκος του κλειδιού[186].

Η μέθοδος brute-force είναι μέτρο ασφάλειας ενός αλγόριθμου κρυπτογράφησης. Ένας αλγόριθμος κρυπτογράφησης θεωρείται "σπασμένος" αν υπάρχει αλγόριθμος κρυπτανάλυσης, ο οποίος μπορεί να βρει το κλειδί με μικρότερη πολυπλοκότητα από τη μέθοδο brute-force, ανεξαρτήτως εάν αυτή η προσπάθεια υπολογισμού είναι εφικτή στην πράξη. Συνήθως, το μήκος

[186] Έτσι για να παραβιαστεί ένα σύστημα με κλειδί των 32 bits πρέπει πρώτα να υπολογιστούν όλοι οι 2^{32} διαφορετικοί συνδυασμοί. Για ένα σύστημα με 40 bits κλειδί χρειάζονται 2^{40} διαφορετικοί συνδυασμοί. Η υπολογιστική ισχύς που απαιτείται σε αυτές τις περιπτώσεις είναι διαθέσιμη . Για κλειδί 56 bits η παραβίαση γίνεται με ειδικό λογισμικό του οποίου το κόστος είναι αρκετά μεγάλο, για περισσότερα Βλ.Κ. Πατσάκης, Ε. Φούντας, Κρυπτογραφία και εφαρμογές, Τόμος Πρώτος, Εκδόσεις Βαρβαρήγου, 2008, σελ.200

των κρυπτογραφικών κλειδιών επιλέγεται με τρόπο τέτοιο, ώστε να απαιτείται υπερβολικά μεγάλος χρόνος υπολογισμών (με βάση τις τρέχουσες υπολογιστικές δυνατότητες) και άρα να μην έχει χρηστική αξία μία τέτοιου είδους επίθεση. Ωστόσο, πολλά υπολογιστικά συστήματα έχουν κατά καιρούς γίνει στόχος brute force attack, με περισσότερο γνωστά τα συστήματα του Πενταγώνου και αστυνομικών αρχών των ΗΠΑ[187].

Στις πιο απλές μορφές επίθεσης ωμής βίας ο επιτιθέμενος χρησιμοποιεί έτοιμες λίστες με συνήθη ονόματα χρηστών και κωδικούς πρόσβασης και δοκιμάζει πιθανούς συνδυασμούς, προκειμένου να αποκτήσει πρόσβαση σε ένα σύστημα.

2.5 **Παράγοντες που βοηθούν τη διάδοση απειλών**

Είδαμε σε προηγούμενες ενότητες τις διάφορες απειλές που υπάρχουν και τους κινδύνους που εγκυμονούν για τα πληροφοριακά συστήματα και την παραβίαση της ιδιωτικότητας. Σε αυτή την ενότητα θα δούμε τους παράγοντες που ευνοούν αυτές τις απειλές. Οι λεγόμενες απειλές, δεν είναι τίποτα άλλο παρά κακόβουλο λογισμικό, το οποίο αποτελείται από διάφορα είδη ανάλογα με τον τρόπο που λειτουργεί και το οποίο εκμεταλλεύεται κάποιο τρωτό(αδύναμο) σημείο ενός υπολογιστικού συστήματος, για να εισβάλει χωρίς άδεια σε αυτό. Τα τρωτά σημεία οφείλονται σε λανθασμένες ενέργειες των χρηστών ή σε σχεδιαστικά κατασκευαστικά λάθη.

2.5.1 **Αφαιρούμενα μέσα**

Με τον όρο αυτό εννοούμε τα αφαιρούμενα μέσα μεταφοράς όπως είναι για παράδειγμα τα CD (οπτικοί δίσκοι), οι σκληροί δίσκοι, οι USB συσκευές μεταφοράς δεδομένων ή άλλα παρόμοια μέσα. Όλα τα παραπάνω λοιπόν μπορούν να θεωρηθούν σαν μία ακόμη πιθανή πηγή μόλυνσης και υποκλοπής σημαντικών δεδομένων. Όπως είναι γνωστό τα διάφορα είδη κακόβουλου λογισμικού χρησιμοποιούν τέτοια μέσα προκειμένου να διαδίδονται, οπότε και γίνεται προφανής ο κίνδυνος που απορρέει από την εγκατάσταση ενός τέτοιου μέσου σε ένα σταθμό εργασίας. Συχνά παρατηρείται το φαινόμενο κάποιος χρήστης να εγκαθιστά ένα τέτοιο μέσο το οποίο έχει κάποια αρχεία μολυσμένα, με αποτέλεσμα να μολύνεται το σύστημα και να περνά αυτό και στο υπόλοιπο δίκτυο

2.5.2 **Περιήγηση στο διαδίκτυο** (Web surfing)-**κατέβασμα αρχείων** (Downloading)

Το διαδίκτυο και γενικότερα η περιήγηση σε αυτό, το γνωστό σε όλους Web browsing ή Web surfing, αποτελεί μία μόνιμη πηγή κινδύνου για την ασφάλεια των σταθμών εργασίας αλλά και γενικότερα του δικτύου σε ένα οργανισμό ή σε μία εταιρεία. Οι χρήστες επισκέπτονται διαδικτυακές τοποθεσίες που περιέχουν επισφαλές περιεχόμενο και συχνά κατεβάζουν από αυτές αρχεία τα οποία το πιθανότερο είναι να είναι μολυσμένα με κακόβουλο λογισμικό. Αυτό το εκμεταλλεύονται μετά κάποιοι κακόβουλοι χρήστες προκειμένου να αποκτήσουν πρόσβαση στο σύστημα και να το κάνουν δικό τους. Επίσης συχνό είναι και το φαινόμενο όπου χρήστες επισκέπτονται σελίδες με πορνογραφικό περιεχόμενο με αποτέλεσμα στις περισσότερες των

[187] http://www.onlycy.com/119262- συνελήφθη-χάκερ-επιθέσεις-πεντάγωνο

περιπτώσεων να εγκαθίσταται εν αγνοία του χρήστη ένας dialer που κάνει κλήσεις σε απομακρυσμένες περιοχές. Ο λογαριασμός τηλεφώνου που θα πρέπει να πληρώσει μετά είναι αρκετά αυξημένος. Το κατέβασμα αρχείων από άγνωστες και επισφαλείς τοποθεσίες με ταυτόχρονη χρησιμοποίηση των συστημάτων και του δικτύου μιας εταιρείας ή ενός οργανισμού, μπορεί να οδηγήσει σε επιβλαβή αποτελέσματα: μπορεί να οδηγηθούν σε καταστάσεις στις οποίες αρχεία και δεδομένα χάνονται, καταστρέφονται ή ακόμα και σε μερικές περιπτώσεις παραποιούνται. Αυτό αποτελεί σήμερα ένα συχνό φαινόμενο, καθώς πολλές φορές οι χρήστες κατεβάζουν από το διαδίκτυο αρχεία χωρίς να δίδουν τη δέουσα προσοχή.

2.5.3 **Ηλεκτρονικό ταχυδρομείο** (email)

Το ηλεκτρονικό ταχυδρομείο αποτελεί μία από τις πιο διαδεδομένες και χρησιμοποιούμενες υπηρεσίες του διαδικτύου. Είναι το κύριο μέσο επικοινωνίας μεταξύ των χρηστών και αποτελεί ένα από τα βασικά εργαλεία μιας εταιρείας ή ενός οργανισμού. Αποτελεί όμως και τον κύριο εκπρόσωπο μέσω του οποίου διαδίδεται κακόβουλο λογισμικό με τη μορφή επισυναπτόμενων αρχείων. Ο χρήστης ανοίγει τα αρχεία που δέχεται χωρίς να τα ελέγχει με αποτέλεσμα να μολύνεται το σύστημα. Η μη σωστή χρήση του αποτελεί ένα τρωτό σημείο το οποίο μπορεί να οδηγήσει στη παραβίαση της ασφάλειας του δικτύου. Ενδεικτικά μπορούμε να αναφέρουμε σαν μη σωστή χρήση, όπως είπαμε και πιο πάνω, το άνοιγμα κάποιων αρχείων από άτομα που δεν ξέρουμε, τη μη χρήση πρωτοκόλλων ασφάλειας για κρυπτογράφηση και επιβεβαίωση της πηγής που έστειλε το μήνυμα. Συχνά οι χρήστες δίνουν το email που διατηρούν σε μια εταιρεία σε ιστοσελίδες με αμφίβολο περιεχόμενο προκειμένου να καλύψουν κάποιες προσωπικές ανάγκες. Και αυτό αποτελεί ένα τρωτό σημείο διότι μπορεί να χρησιμοποιηθεί για την παραλαβή spam μηνυμάτων προς τον χρήστη.

2.5.4 **Ελαττώματα λογισμικού πρωτοκόλλων**

Τα πρωτόκολλα είναι αυτά που ορίζουν τους κανόνες και τις μεθόδους για να μπορούν οι υπολογιστές να επικοινωνούν μεταξύ τους στο δίκτυο. Αν το πρωτόκολλο έχει σχεδιαστικό λάθος είναι επισφαλές σε εκμετάλλευση, ανεξάρτητα από το πόσο καλά υλοποιήθηκε. Όταν σχεδιάζεται το λογισμικό χωρίς η ασφάλεια να συμπεριλαμβάνεται στις αρχικές προδιαγραφές, υπάρχει το ενδεχόμενο, το επιπλέον τμήμα που προστίθεται για την ενίσχυση της ασφάλειας, να μην αλληλεπιδρά όπως είχε αρχικά σχεδιαστεί και να προκύπτουν απρόσμενα τρωτά σημεία, τα οποία μπορούν να εκμεταλλευτούν κακόβουλοι χρήστες προκειμένου μέσω αυτών να διαδώσουν το κακόβουλο λογισμικό.

2.5.5 **Εφαρμογές** instant messaging

Πολλοί χρήστες χρησιμοποιούν αυτές τις εφαρμογές προκειμένου να επικοινωνήσουν με φίλους, να στείλουν ή να δεχθούν αρχεία, μηνύματα, καθώς αυτές οι εφαρμογές προσπαθούν να ξεγελάσουν τα προγράμματα που φιλτράρουν τις πληροφορίες που εισέρχονται και εξέρχονται από ένα δίκτυο, ώστε να περάσουν και δεδομένα που μπορεί να περιέχουν κακόβουλο λογισμικό. Ωστόσο οι χρήστες δεν συνειδητοποιούν τους κινδύνους που κρύβουν αυτές οι εφαρμογές και την πιθανή καταστροφή που μπορεί να επιφέρουν. Ποτέ δεν μπορούμε να είμαστε σίγουροι για το ποιος είναι στο άλλο άκρο της γραμμής. Μπορεί πράγματι να είναι κάποιος φίλος μας ή ένας κακόβουλος χρήστης. Οι περισσότερες από αυτές τις εφαρμογές

περιέχουν τρωτά σημεία, η εκμετάλλευση των οποίων από γνώστες του είδους θα μπορούσε να δημιουργήσει σοβαρά προβλήματα. Ένα αρχείο που θα πάρουμε μπορεί να είναι μολυσμένο και να οδηγήσει με η σειρά του στη μόλυνση του συστήματος και του δικτύου γενικότερα.

2.5.6 **Κωδικοί πρόσβασης**

Οι κωδικοί πρόσβασης είναι τα κλειδιά που χρησιμοποιούμε για να προσπελάσουμε προσωπικά στοιχεία που έχουμε αποθηκεύσει στον υπολογιστή σας και στους διαδικτυακούς μας λογαριασμούς. Εάν κάποιοι εγκληματίες ή άλλοι κακόβουλοι χρήστες κλέψουν τα στοιχεία αυτά, μπορούν να χρησιμοποιήσουν το όνομά μας για να καρπωθούν οικονομικά ή άλλα οφέλη. Σε πολλές περιπτώσεις η διαπίστωση ότι είμαστε θύμα επίθεσης έρχεται αργά, όταν έχει ήδη ξεκινήσει η ζημιά που έχουμε υποστεί. Το γεγονός ότι πολλές φορές οι χρήστες χρησιμοποιούν απλούς γενικά κωδικούς πρόσβασης[188] για τα συστήματα, εκμεταλλεύονται κακόβουλοι χρήστες, ώστε να αποκτήσουν πρόσβαση και δικαιώματα στο σύστημα του χρήστη. Κάνοντας χρήση αυτοματοποιημένων προγραμμάτων(κακόβουλο λογισμικό) καταφέρνουν και αποκτούν τον κωδικό πρόσβασης, πλήττοντας την ασφάλεια των συστημάτων και των δικτύων.

Για να αποφύγουμε τα παραπάνω είναι αναγκαίο να δημιουργούμε ένα ισχυρό κωδικό πρόσβασης. Για να το επιτύχουμε αυτό, ο κωδικός πρόσβασης θα πρέπει να πληροί τα παρακάτω κριτήρια: Να αποτελείται από πολλούς χαρακτήρες. Κάθε χαρακτήρας που προσθέτετε στον κωδικό πρόσβασης αυξάνει την ασφάλεια που σας παρέχει στο πολλαπλάσιο. Οι κωδικοί πρόσβασής σας θα πρέπει να έχουν μήκος 8 χαρακτήρες ή περισσότερους. Το ιδανικό είναι 14 χαρακτήρες ή περισσότεροι. Συνδυάζουμε γράμματα, αριθμούς και σύμβολα. Όσο μεγαλύτερη ποικιλία χαρακτήρων έχει ο κωδικός πρόσβασής σας, τόσο δυσκολότερο είναι να αποκαλυφθεί. Ένας ιδανικός κωδικός πρόσβασης συνδυάζει μήκος και διαφόρους τύπους συμβόλων. Ο κωδικός πρόσβασής θα είναι πολύ πιο ισχυρός αν επιλέξουμε από όλα τα σύμβολα του πληκτρολογίου, συμπεριλαμβανομένων των σημείων στίξης. Αποφεύγουμε να γράφουμε τους κωδικούς πρόσβασης σε λογισμικό διαχείρισης κωδικών, τοποθεσία Web ή άλλο εργαλείο αποθήκευσης λογισμικού[189].Υπάρχουν προγράμματα στο web που μπορεί να ελεγχθεί πόσο ισχυρός είναι ο κωδικός πρόσβασης που δημιουργούμε, καθώς πληκτρολογείτε , όπως το Password Checker[190] .

---

[188] Οι πιο συνηθισμένοι κωδικό πρόσβασης που χρησιμοποιούνται από χρήστες καταγράφονται στην ιστοσελίδα: http://www.imperva.com/news/press/2010/01_21_Imperva_Releases_Detailed_Analysis_of_32_Million_Passwords.html

[189] Βλ: http://www.microsoft.com/hellas/athome/security/privacy/password.mspx

[190] Βλ:https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx επίσης http://www.passwordmeter.com

2.5.7 **Έλλειψη προγραμμάτων προστασίας**

Νομίζοντας οι χρήστες ότι είναι προστατευμένοι στο εσωτερικό δίκτυο μιας εταιρείας, δεν εγκαθιστούν προγράμματα προστασίας από κακόβουλο λογισμικό ή κάποιο τείχος προστασίας, με αποτέλεσμα να μολύνονται από κάποιο ιό ή να παραβιάζεται η ασφάλεια του συστήματός τους από κάποιο επίδοξο hacker. Αυτό μπορεί να οδηγήσει στη συνέχεια στη παραβίαση της ασφάλειας ολόκληρου του δικτύου που χρησιμοποιεί ο χρήστης. Όπως μπορούμε να δούμε από όλα τα παραπάνω, το κρίσιμο στοιχείο σε καθένα από αυτά είναι ο χρήστης. Μπορούμε να πούμε ότι αυτός είναι, χωρίς υπερβολή, το τρωτό σημείο του διαδικτύου. Αυτός με τις ενέργειες που εκτελεί στο σύστημα και κατ'επέκταση στο διαδίκτυο. Και επειδή σε καμία περίπτωση δεν μπορούμε να εξαλείψουμε το χρήστη, αυτό που μπορούμε και πρέπει να κάνουμε είναι να του παρέχουμε τα κατάλληλα εφόδια ώστε να συνειδητοποιήσει τους κινδύνους που απορρέουν από κάθε ενέργειά του στο διαδίκτυο. Να συνειδητοποιήσει δηλαδή ότι κάθε πράξη του πιθανώς να έχει και κάποιο αρνητικό αποτέλεσμα.

3 **ΚΕΦΑΛΑΙΟ**: **Μέτρα προστασίας**

Μαύρη οθόνη, κόλλημα υπολογιστή, άνοιγμα παραθύρων χωρίς ενέργεια χρήστη, αδυναμία ανοίγματος κάποιου αρχείου ή τρεξίματος μιας εφαρμογής, απώλεια αρχείων,αδυναμία εκκίνησης του υπολογιστή είναι εικόνες και καταστάσεις που μπορεί να αντιμετωπίσει ένας χρήστης υπολογιστών. Συχνά συμβαίνουν όταν ο υπολογιστής και το δίκτυο που χρησιμοποιούμε μένει χωρίς προστασία. Βέβαια σε πολλές περιπτώσεις το κακόβουλο λογισμικό λειτουργεί εν αγνοία του χρήστη. Αυτές οι δραστηριότητες συχνά αφορούν την διασπορά ιών ή επιθέσεων με στόχο τον υπολογιστή μας ή και άλλους υπολογιστές αφού βέβαια χρησιμοποιηθεί ο δικός μας σαν μεσάζοντας-ενδιάμεσος.

Σίγουρα δεν πρέπει να βιώσουμε τέτοιες καταστάσεις για να πάρουμε μέτρα προστασίας. Μάλιστα σε πολλές περιπτώσεις δεν υπάρχουν «ορατά συμπτώματα» και όλα παρουσιάζονται φυσιολογικά. Χρειάζεται να πάρουμε μέτρα που θα προστατεύουν τις πληροφορίες του συστήματός μας από κάθε επίδοξο εισβολέα.

3.1 **Γενικές συμβουλές**

☞ **Φυσική ασφάλεια**. Το πρώτο που πρέπει να αναφέρουμε στα μέτρα προστασίας είναι η φυσική ασφάλεια που πρέπει να έχει ο υπολογιστής και το δίκτυό μας. Συνίσταται στην προστασία του εξοπλισμού μας από φυσικές καταστροφές όπως φωτιά , πλημμύρα, βανδαλισμό, κλοπή κ.α.

☞ **Αφαιρούμενα μέσα**. Ιδιαίτερη προσοχή όταν αντιγράφουμε αρχεία στον υπολογιστή σας από DVD, CD-ROM, USB ή άλλα αποσπώμενα μέσα. Ακόμα και αν εμπιστευόμαστε τον προμηθευτή του αφαιρούμενου μέσου, μπορεί να έχει μολυνθεί το μέσο χωρίς να έχει γνώση ίδιος. Για το λόγο αυτό πριν αντιγράψουμε τα αρχεία από το αφαιρούμενο μέσο, κάνουμε έλεγχο του αφαιρούμενου μέσου με το αντιϊκό πρόγραμμα (antivirus).

☞ **Αντιϊκό πρόγραμμα (antivirus**). Φροντίδα για εγκατάσταση και ενεργοποίηση ενός καλού (antivirus). Καλό θα είναι το antivirus να παρέχει προστασία και για εντοπισμό spyware/adware.

Τακτική (καθημερινή) ενημέρωση Update αυτών των προγραμμάτων. Έλεγχος του υπολογιστή τακτικά μέσω του antivirus για τυχόν μόλυνση.

☞ **Τείχος Προστασίας**. Πρέπει να έχουμε εγκαταστημένο και ενεργοποιημένο το τείχος προστασίας (Firewall).

☞ **Ενημέρωση (Update) λειτουργικού** συστήματος. Το λειτουργικό που χρησιμοποιούμε χρειάζεται να ενημερώνεται προκειμένου να επιλύονται και θέματα που αφορούν τρωτά σημεία τους ή κενά ασφαλείας.

☞ **Ηλεκτρονικό ταχυδρομείο (e-mail)**. Δεν ανοίγουμε μηνύματα από αγνώστους ή όσα μας φαίνονται ύποπτα , αλλά τα διαγράφουμε. Δεν ανοίγουμε ποτέ συνημμένα με εκτελέσιμα αρχεία .exe, .com , .vbs γιατί μπορεί να περιέχουν επιβλαβή κώδικα και να μολύνει τον υπολογιστή μας. Πολλά e-mails που κυκλοφορούν στο Internet «ενημερώνουν» τους χρήστες για την ύπαρξη ενός νέου ιού και παροτρύνουν τους χρήστες να το στείλετε και σ' άλλους .Σε αρκετές περιπτώσεις αυτά είναι ψεύτικα και μπορεί να περιέχουν ιό.

☞ **Ρυθμίσεις φυλλομετρητή (browser).** Χρειάζεται ενεργοποίηση ρυθμίσεων ασφαλείας στο browser. Ένα παράδειγμα αποτελεί ι το μπλοκάρισμα των αναδυόμενων παραθύρων (pop-up). Στον Internet Explorer το σχετικό εργαλείο βρίσκεται στην διαδρομή Tools > Internet Options > Privacy > Block Pop Ups ή στο Tools > Popup Blocker > Turn on Pop up blocker.

☞ **Εφαρμογές Instant Messaging.** Όταν κάνουμε χρήση προγραμμάτων Instant Messaging (πχ. MSN Messenger, ICQ κλπ.), χρειάζεται να έχουμε απενεργοποιήσει τη δυνατότητα για απευθείας αποστολή αρχείων καθώς μπορεί να περιέχουν ιούς.

☞ **Περιήγηση- κατέβασμα αρχείων (surfing download)**.Χρειάζεται μεγάλη προσοχή ποιες σελίδες επισκεπτόμαστε ειδικά αν θέλουμε να κάνουμε ασφαλείς συναλλαγές[191]. Επίσης το κατέβασμα χρήσιμων αρχείων πρέπει να γίνεται από αξιόπιστες πηγές.

3.2 **Τρόποι προστασίας**

Η ασφάλεια στα δίκτυα υπολογιστών και στο internet έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων. Ποιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με: Συστήματα πρόληψης

3.2.1 **Συστήματα πρόληψης**

Πρόληψη (prevention) : Το σύνολο των μέτρων –ενεργειών που πρέπει να ληφθούν από τον administrator προκειμένου να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών ή σε άλλα προβλήματα. Στοχεύει στην αποτροπή μιας επίθεσης πριν αυτή να εκδηλωθεί. Για

[191] Προσέχουμε η διεύθυνση να ξεκινά με https αντί του γνωστού http.

παράδειγμα η χρήση ενός τείχους προστασίας (firewall) σε ένα σύστημα αποσκοπεί στο να αποτρέψει τη μη εξουσιοδοτημένη είσοδο σε αυτό το σύστημα.

3.2.2 **Συστήματα ανίχνευσης**

Ανίχνευση (detection) : Το σύνολο των μέτρων –ενεργειών για να βρεθεί πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες. Με τη διαρκή εξέλιξη της πληροφορικής, όσα μέτρα πρόληψης και να ληφθούν κανένα σύστημα δεν μπορούμε να πούμε πως εξασφαλίζει απόλυτη ασφάλεια. Για το λόγο αυτό στο σχεδιασμό της ασφάλειας θα πρέπει να λαμβάνονται μέτρα για την ανίχνευση μιας εισβολής στο σύστημα, όταν αυτή θα συμβεί. Παράδειγμα αποτελεί το Σύστημα Ανίχνευσης Εισβολής(ΣΑΕ) (αγγλ. Intrusion Detection System, IDS)

3.2.3 **Συστήματα αντίδρασης - επιδιόρθωσης**

Αντίδραση (reaction) : Το σύνολο των μέτρων –ενεργειών που πρέπει να ληφθούν για να γίνει η αποκατάσταση του συστήματος. Αφορούν τα μέτρα εκείνα που στόχο έχουν να μειώσουν το χρόνο ανάκαμψης του συστήματος μετά από την εκδήλωση επίθεσης. Παράδειγμα αποτελεί η χρήση εργαλείων αφαίρεσης κακόβουλου λογισμικού, αυτόματη λήψη ή και επαναφορά αντιγράφων ασφαλείας (backup).

3.3 **Ανιχνευτής Ιών**, **αντιϊκό πρόγραμμα** (Antivirus)

Οι ιοί όπως αναφέραμε εκτενέστερα σε προηγούμενη ενότητα αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού, ένα σημαντικό πρόβλημα για τους χρήστες και τους διαχειριστές πληροφοριακών συστημάτων . Στις σημερινές συνθήκες , η ανάκαλυψή τους από τον απλό χρήστη είναι δύσκολη , καθώς πολλοί από αυτούς δεν μπορούν να εντοπισθούν ούτε και από τους πεπειραμένους χωρίς τη χρήση κατάλληλου λογισμικού.

Για το λόγο αυτό και για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, που είναι γνωστή σαν **αντιϊκό πρόγραμμα (antivirus).** Τα προγράμματα αυτά έχουν σαν βασική αποστολή τους να εντοπίζουν τους ιούς και να τους εξαλείφουν. Αυτό το πετυχαίνουν πραγματοποιώντας έλεγχο (Scanning) των μονάδων και των αρχείων του υπολογιστή. Για την ασφαλέστερη λειτουργία του υπολογιστή τα antivirus ξεκινούν τη λειτουργία τους αυτόματα χωρίς εντολή από το χρήστη, μαζί με το λειτουργικό σύστημα κατά την εκκίνηση του υπολογιστή. Παραμένουν δε σε συνεχή επαγρύπνηση, σαν διαδικασίες στη μνήμη του υπολογιστή μας, έτοιμα να ανιχνεύσουν και να «συλλάβουν» κάθε απρόσκλητο επισκέπτη.

3.3.1 **Λειτουργία** (Antivirus)

Τα Antivirus είναι προγράμματα τα οποία ψάχνουν για ασυνήθιστες αλλαγές στα αρχεία ενός υπολογιστή καθώς επίσης και για κομμάτια αρχείων που ταιριάζουν με κώδικα γνωστών ιών. Οι δημιουργοί ιών κατασκευάζουν αδιάκοπα νέους και ενημερωμένους ιούς, έτσι είναι σημαντικό να υπάρχουν πάντα οι πιο **πρόσφατες ενημερώσεις (Updates)** του **Antivirus** στον υπολογιστή που είναι εγκατεστημένο ένα τέτοιο πρόγραμμα. Συχνά τέτοιες βάσεις δεδομένων ενημερώνονται άμεσα μόλις εντοπιστεί κάποιος ιός από τον οργανισμό ή εταιρεία που ενημερώνει τη βάση δεδομένων και συνεπώς θα βοηθήσουν τον ανιχνευτή ιών να βρει ακόμη και τους πιο πρόσφατους ιούς[192]. Τα Antivirus πρέπει να αναβαθμίζονται σε τακτική βάση, για να μπορούν με επιτυχία να αντιμετωπίζουν νέους ιούς.

Το Antivirus αφού εγκατασταθεί δίνει αρκετές επιλογές στον χρήστη , όπως έλεγχο των μέσων αποθήκευσης για κακόβουλο λογισμικό καθώς επίσης και έλεγχο στο δίκτυο με το οποίο είναι συνδεδεμένος ο υπολογιστής. Επίσης ο χρήστης μπορεί να ορίσει προγραμματισμένους ελέγχους στο σύστημα για κακόβουλο λογισμικό, σε συγκεκριμένες ημερομηνίες και ώρες αυτοματοποιώντας τον έλεγχο που πλέον γίνεται χωρίς την δική του παρέμβαση παρά μόνο όταν ειδοποιηθεί από το Antivirus για την ανίχνευση κάποιου ύποπτου λογισμικού στο σύστημα. Κάθε Antivirus πρόγραμμα έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Τα περισσότερα μπορούν να εργάζονται σε πραγματικό χρόνο (real time), εντοπίζοντας τους ιούς τη στιγμή ακριβώς που προσπαθούν να εισέλθουν στο σύστημα.

3.3.2 **Μέθοδοι Αντιϊκών** (Antivirus)

Βάση Δεδομένων. Ένα πρόγραμμα antivirus τηρεί μια Βάση Δεδομένων με τις υπογραφές[193] όλων των γνωστών ιών, και ελέγχει τον κώδικα όλων των εκτελέσιμων αρχείων ενός Η/Υ για τον εντοπισμό μιας υπογραφής που έχει ήδη αποθηκευτεί στη Βάση δεδομένων. Στην περίπτωση που βρει κάποιο ταίριασμα (matching), το antivirus μπλοκάρει την εκτέλεση του κακόβουλου προγράμματος και ταυτόχρονα ενημερώνει το χρήστη με κατάλληλο μήνυμα, για να αποφασίσει αν επιθυμεί: α) διαγραφή (delete), β) απομόνωση (quarantine) γ) επιδιόρθωση (repair) του αρχείου που είναι μολυσμένο. Βέβαια η μέθοδος αυτή μπορεί να λειτουργήσει με την προϋπόθεση ότι ο ιός είναι καταχωρημένος στη βάση δεδομένων. Έτσι το antivirus που χρησιμοποιεί μια τέτοια μέθοδο μπορεί να εντοπίσει και να απομακρύνει αποτελεσματικά ιούς που είναι ήδη γνωστοί. Αδυνατεί όμως να παρέχει προστασία απέναντι σε ιούς που δεν είναι ακόμα γνωστοί και δεν είναι καταχωρημένοι στη βάση δεδομένων με κάποια ενημέρωση(Updates).Το πρόβλημα αυτό προσπαθούν να επιλύσουν διάφορες προηγμένες μέθοδοι, όπως ευρετικές μέθοδοι (heuristic scanning, έλεγχος συμπεριφοράς (behavior blocking) και έλεγχος ακεραιότητας (integrity checking)

Ευρετικές μέθοδοι (heuristic analysis) . Χρησιμοποιούνται ευρετικοί αλγόριθμοι (heuristic algorithm) οι οποίοι αναζητούν στο λογισμικό (εκτελέσιμο κώδικα ενός αρχείου), ύποπτα

---

[192] Καραυγουστής Ανέστης, Χρήση Νέων Τεχνολογιών στις επιχειρήσεις, ΥΠΕΠΘ-Γ.Γ.Ε.Ε.-Ι.Δ.Ε.Κ.Ε

[193] Υπογραφή είναι το τμήμα του κώδικα του ιού που τον χαρακτηρίζει βλ http://di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20B.pdf

κομμάτια κώδικα που θα μπορούσαν να ανήκουν σε κάποιον ιό ο οποίος δεν είναι καταχωρημένος στην βάση δεδομένων με τις γνωστές υπογραφές. Τέτοιο παράδειγμα μπορεί να αποτελεί η ύπαρξη μακροεντολών σε ένα έγγραφο Office.

Έλεγχος συμπεριφοράς (behavior blocking) . Σε αντίθεση με την προηγούμενη μέθοδο (heuristic), δεν ελέγχεται ο κώδικας του εκτελέσιμου αρχείου, αλλά η συμπεριφορά του προγράμματος καθώς εκτελείται. Έχοντας δηλαδή κατά βάση ένα σύνολο από συμπεριφορές που θεωρούνται ύποπτες (π.χ. κλήση του Μητρώου του συστήματος, προσπάθεια διαγραφής ή μετονομασίας αρχείων, κ.λ.π) το antivirus προσπαθεί να ανιχνεύσει και να αποτρέψει σε πραγματικό χρόνο τις παρενέργειες ενός (άγνωστου) ιού, εφαρμόζοντας την πολιτική ασφαλείας που διαμορφώνει ο χρήστης μέσα από τις επιλογές-ρυθμίσεις του προγράμματος.

Έλεγχος ακεραιότητας (integrity checking) . Η μέθοδος αυτή υπολογίζει το μέγεθος του αρχείου όταν αποθηκεύεται καθώς και ένα άθροισμα ελέγχου (checksum[194]). Κάθε φορά που εκτελείται ένα αρχείο, το antivirus υπολογίζει το άθροισμα ελέγχου και κάνει σύγκριση με αυτό που έχει αποθηκεύσει. Αν οι δύο αυτοί αριθμοί δεν είναι ίδιοι και δεν έχει γίνει παρέμβαση από το νόμιμο χρήστη , τότε πιθανόν την τροποποίηση του κώδικα του αρχείου έκανε κάποιος ιός.

3.3.3 **Απαιτήσεις** (Antivirus)

Για να μπορεί το Antivirus να αποδόσει και να παρέχει ικανοποιητική ασφάλεια θα πρέπει να έχει σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να καλύπτει ένα σύνολο απαιτήσεων που απαιτούνται κατά την εκτέλεση διάφορων προγραμμάτων και χρήση υπηρεσιών. Κάποιες από αυτές είναι:

☞ Αυτόματη ενημέρωση (Updates). Στις σημερινές συνθήκες με την γιγάντωση του internet επιβάλλεται η ενημέρωση της βάσης δεδομένων του Antivirus να γίνεται αυτόματα με τις πιο πρόσφατες υπογραφές των ιών (virus definitions).

☞ Προστασία σε πραγματικό χρόνο(real-time protection). Αυτό γίνεται καθώς το Antivirus ξεκινά και ανεβαίνει στη μνήμη RAM με την εκκίνηση του υπολογιστή και τη φόρτωση του λειτουργικού συστήματος και διάφορων άλλων εφαρμογών.

☞ Προστασία Ηλεκτρονικής Αλληλογραφίας (e-mail). Η προστασία μιας δημοφιλής υπηρεσίας όπως το e-mail πρέπει να βρίσκεται μέσα στις βασικές απαιτήσεις που πρέπει να έχει ένα Antivirus, προκειμένου να κάνει έλεγχο των μηνυμάτων καθώς και των επισυναπτόμενων αρχείων που υπάρχουν σε αυτό.

☞ Τακτικός Προγραμματισμένος Έλεγχος. Χρειάζεται το antivirus να πραγματοποιεί προγραμματισμένους ελέγχους σε τακτά χρονικά διαστήματα σε όλες τις αποθηκευτικές μονάδες του συστήματος(σκληρούς δίσκους, αφαιρούμενους δίσκουςκ.λ.π).

[194] Το άθροισμα ελέγχου είναι ένας αριθμός μοναδικός για το αρχείο αυτό. Η αλλαγή έστω και ενός bit στο αρχείο θα έχει ως αποτέλεσμα την αλλαγή του αθροίσματος ελέγχου, βλ http://el.wikipedia.org/wiki/Cksum

☞ Δισκέτα Εκκίνησης: Για να μπορεί να γίνεται εκκίνηση του υπολογιστή σε περίπτωση που κάποιος ιός τύπου boot sector[195] εισχωρήσει στο σύστημα με αποτέλεσμα να μην μπορεί να φορτωθεί το λειτουργικό και να εκκινήσει ο υπολογιστής.

☞ Λειτουργικό με χαμηλή δέσμευση πόρων. Ένα κριτήριο για την επιλογή ενός antivirus πέρα από την ασφάλεια που πρέπει να προσφέρει είναι και η λειτουργικότητά του καθώς επίσης και η χαμηλή δέσμευση πόρων του συστήματος. Σε αντίθετη περίπτωση μιλάμε για «βαρύ» antivirus που δημιουργεί προβλήματα στη λειτουργία διαφόρων εφαρμογών και προγραμμάτων.

☞ Καταγραφή Συμβάντων (event logging). Η υπηρεσία αυτή καταγράφει συμβάντα εφαρμογών, ασφαλείας και συστήματος στην Προβολή Συμβάντων. Τα αρχεία καταγραφής συμβάντων βοηθούν στην αναγνώριση και τη διάγνωση της προέλευσης προβλημάτων συστήματος.

Συμπερασματικά τα προγράμματα antivirus δεν είναι πανάκεια. Η χρήση τους συνήθως πρέπει να συνδυάζεται και με άλλα εργαλεία όπως firewalls, εργαλεία Ανίχνευσης Εισβολών(IDS), προγράμματα ανίχνευσης Spyware-Adware, εργαλεία ανίχνευσης ευπαθειών, μηχανισμοί backup και μεθόδους όπως κρυπτογραφία, ψηφιακές υπογραφές κ.ά.

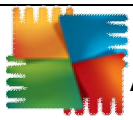
3.3.4 **Προγράμματα Αντιϊκά** (Antivirus)

Η αναγκαιότητα της προστασίας του υπολογιστή με αντιϊκά (antivirus) προγράμματα μας κάνει να παραθέσουμε παρακάτω πίνακα με γνωστά τέτοια προγράμματα, τα οποία ο αναγνώστης έχει τη δυνατότητα να πληροφορηθεί τόσο για τις δυνατότητες αυτών όσο και να κάνει χρήση κάποιου από αυτά.

α/α	Ονομασία	Ιστοσελίδα λήψης	Πληροφορίες[196]
1	**Avira AntiVir Personal**	Λήψη	Δωρεάν πρόγραμμα ικανό να εντοπίζει με επιτυχία κακόβουλες απειλές. Καταναλώνει ελάχιστους
2	**Avast! Free Antivirus**	Λήψη	Δωρεάν πρόγραμμα ικανό να εντοπίζει τους περισσότερους ιούς, worms και trojans που υπάρχουν στο internet.

[195] boot sector (Τομέας εκκίνησης) , είναι η περιοχή εκείνη του σκληρού δίσκου που περιέχει εντολές για την εκκίνηση του λειτουργικού συστήματος.

[196] Οι πληροφορίες και τα προγράμματα προέρχονται από την ιστοσελίδα: http://sxoleio.eu/Antivirus.php

3	 **AVG Antivirus Free**	Λήψη	Δωρεάν πρόγραμμα, εντοπίζει και διαγράφει όλων των ειδών τις ηλεκτρονικές απειλές, τους ιούς και τα spyware
4	 **Pc Tools AntiVirus Free**	Λήψη	Δωρεάν βασική προστασία για τον υπολογιστή σας από κακόβουλο λογισμικό
5	 **BitDefender Antivirus Free**	Λήψη	Δωρεάν πρόγραμμα με όλες τις κλασικές δυνατότητες όπως άμεσο scan αρχείων, προγραμματισμένο scan, quarantine κ.ά
6	 **Panda Cloud Antivirus**	Λήψη	Δωρεάν λογισμικό προστασίας από κακόβουλο λογισμικό. Εύκολο στη χρήση ,διαθέτει γραφικό περιβάλλον.
7	 **Comodo Antivirus**	Λήψη	Ευέλικτο δωρεάν λογισμικό με πάρα πολλές δυνατότητες.
8	 **ClamAV**	Λήψη	Ελαφρύ ανοικτού λογισμικού πρόγραμμα αντιμετώπισης ιών
9	 **McAfee Labs Stinger**	Λήψη	Αναγνωρίζει χιλιάδες ιούς, trojans και άλλα συναφή κακόβουλα προγράμματα.
10	 **ClamWin Free Antivirus**	Λήψη	Πρόγραμμα ανοιχτού λογισμικού κατάλληλο για την αντιμετώπιση διάφορων άλλων απειλών. Μικρές απαιτήσεις σε πόρους συστήματος

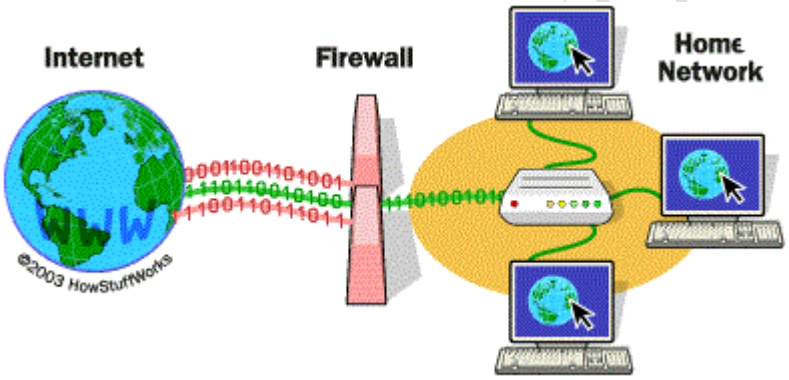
11	**Comodo Cleaning Essentials**	**Λήψη**	Βοηθά στον εντοπισμό και την κατάργηση κακόβουλου λογισμικού του υπολογιστή

Πίνακας 9. Προγράμματα Αντιϊκά (Antivirus)

πηγή : http://sxoleio.eu/Antivirus.php

3.4 **Τείχος προστασίας** (Firewall)

Ο τοίχος προστασίας[197] ή (αλλιώς (firewall[198]) είναι ένα σύστημα το οποίο παρεμβάλλεται μεταξύ του ιδιωτικού δικτύου και του δημοσίου δικτύου (αλλά και μεταξύ τμημάτων του ιδιωτικού δικτύου) για να ελέγχει την κίνηση των δεδομένων μεταξύ των δύο δικτύων. Ένα firewall χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με βασικό σκοπό την ασφάλεια του δικτύου. Μέσα από αυτό διέρχονται τα πακέτα που αποτελούν τις πληροφορίες που λαμβάνουμε αλλά και στέλνουμε προς το internet. Ο τοίχος προστασίας μπορεί να είναι υπό μορφή **software** (συνήθως σε υπολογιστές για προσωπική χρήση) είτε με μορφή **hardware** (μηχανικές συσκευές σε εταιρικά περιβάλλοντα με αυξημένες απαιτήσεις ασφαλείας).



Σχήμα 23. Τείχος προστασίας

Πηγή: http://computer.howstuffworks.com/firewall.htm

[197] Υπάρχουν και άλλες ονομασίες που θα βρούμε στη βιβλιογραφία όπως φράγματα ασφαλείας ,αντιπυρική ζώνη, τοίχοι πυρασφάλειας , πυρότοιχοι προστασίας, αναχώματα ασφαλείας, το τείχος προστασίας.

[198] Ο όρος firewall είναι αρκετά παλιός. Πρωτοεμφανίστηκε στις αρχές του 20ού αιώνα, όταν οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα για τους εσωτερικούς τοίχους ούτως ώστε να τα κάνουν πιο ανθεκτικά στην διάδοση της φωτιάς. Σήμερα ο όρος αυτός έφτασε να σημαίνει το λογισμικό ή υλικό που παρεμβάλλεται μεταξύ δικτύων υπολογιστών ούτως ώστε να αποτρέψει την διάδοση ιών, δούρειων ίππων και τις επιθέσεις από κακόβουλους χρήστες βλ: http://el.wikipedia.org/wiki/Firewall

3.4.1 **Τρόπος Λειτουργίας**

Ένα (firewall) έχει σχεδιαστεί προκειμένου να εμποδίζει την πρόσβαση από ή προς ένα δίκτυο χωρίς κατάλληλη εξουσιοδότηση και ρυθμίζεται με γνώμονα την πολιτική ασφαλείας που υιοθετεί ο διαχειριστής του συστήματος. Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο από τη μια μεριά και ένα εσωτερικό τοπικό δίκτυο από την άλλη. Τα δύο αυτά μέρη έχουν διαφορετικό επίπεδο εμπιστοσύνης ως προς την ασφάλεια. Έτσι το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης ενώ το τοπικό δίκτυο το μέγιστο βαθμό εμπιστοσύνης. Ο τοίχος προστασίας (firewall) μπαίνει ανάμεσα στα δίκτυα με διαφορετικά επίπεδα εμπιστοσύνης λειτουργώντας σαν φράγμα μέσα από το οποίο θα ελεγχθεί η δικτυακή κυκλοφορία και προς τις δύο κατευθύνσεις των δικτύων που βρίσκονται σε επικοινωνία. Έτσι μέσα από τον έλεγχο και το φιλτράρισμα των πακέτων κάποια θα περάσουν , ενώ τα ύποπτα θα μπλοκαρισθούν.

Βέβαια η προμήθεια και εγκατάσταση ενός firewall συνήθως δεν είναι αρκετή. Χρειάζεται η σωστή ρύθμισή του με βάση τους κανόνες σύμφωνα με τους οποίους θα γίνεται η κυκλοφορία των πακέτων ανάμεσα στα δίκτυα, κανόνες που υπαγορεύονται από το γενικότερο σχέδιο και πολιτική ασφαλείας που έχει υιοθετηθεί. Το εκάστοτε firewall υλοποιεί αυτή την πολιτική ασφάλειας η οποία καθορίζει τις ισορροπίες μεταξύ διατήρησης της ασφάλειας και ευκολίας χρήσης. Η σωστή ρύθμιση του τείχους προστασίας απαιτεί μεγάλη ικανότητα και προσοχή από το διαχειριστή. Χρειάζεται κατανόηση των πρωτοκόλλων δικτύου και της ασφαλείας των υπολογιστών. Ακόμα και μικρά λάθη μπορούν να καταστήσουν το τείχος σαν άχρηστο εργαλείο ασφαλείας.

Οι σύγχρονες εκδόσεις των λειτουργικών συστημάτων έχουν ενσωματωμένο τείχος προστασίας με προεπιλεγμένες ρυθμίσεις. Έτσι η ρύθμιση παραμέτρων του τείχους προστασίας των windows 7 περιλαμβάνει τα εξής βήματα:

1. Κλικ στο μενού Έναρξη (Start), πίνακας ελέγχου (control panel), τείχος προστασίας (firewall).
2. Το παράθυρο Τείχος προστασίας των Windows (Windows Firewall) περιλαμβάνει τις ακόλουθες καρτέλες:

● Να επιτρέπεται ένα πρόγραμμα ή μια δυνατότητα μέσω του τείχους προστασίας των των Windows. Μέσα από αυτή την επιλογή μπορούμε να δούμε τα προγράμματα και τις θύρες που επιτρέπει το firewall να λειτουργήσουν.

● Αλλαγή ρυθμίσεων ειδοποίησης. Η επιλογή αυτή δίνει τη δυνατότητα να γίνεται προσαρμογή των ρυθμίσεων για κάθε τύπο δικτύου (Ιδιωτικού ή δημόσιου).

● Ενεργοποίηση ή απενεργοποίηση του τείχους προστασίας των Windows.

● Επαναφορά προεπιλογών

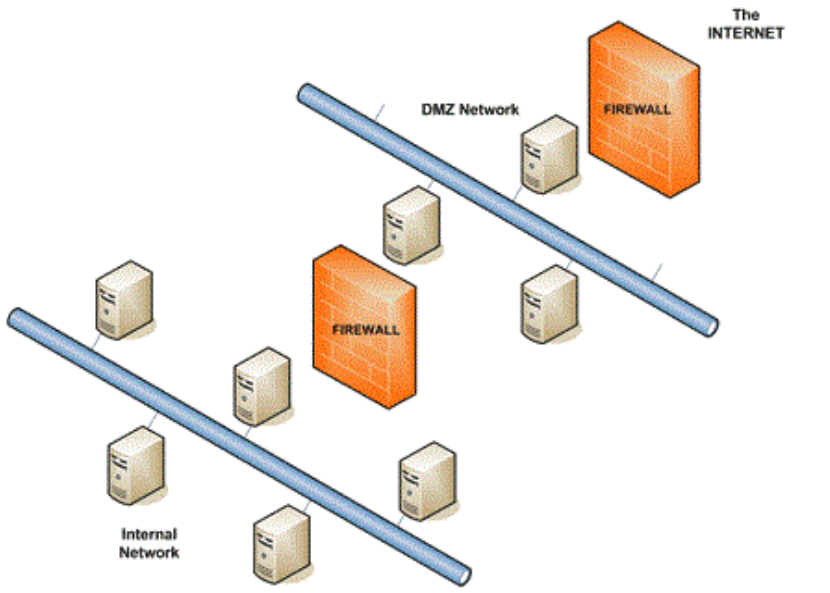
● Ρυθμίσεις για προχωρημένους

● Αντιμετώπιση προβλημάτων του δικτύου μου

Ζώνη αποστρατικοποίησης και Proxy Servers .Πολλές φορές χρησιμοποιείται μια ζώνη με ένα ενδιάμεσο επίπεδο εμπιστοσύνης, που βρίσκεται ανάμεσα στο Internet και σε ένα έμπιστο εσωτερικό δίκτυο και ονομάζεται **ζώνη αποστρατικοποίησης** (**De**militarized **Z**one -**DMZ**). Η

ζώνη αυτή βρίσκεται ανάμεσα στο ιδιωτικό δίκτυο που προφυλάσσει το firewall και το διαδίκτυο. Ο σκοπός της ζώνης αυτής είναι στρατηγικής σημασίας για την ασφάλεια του δικτύου μας και επιτρέπει στην ουσία την προσπέλαση σε υπηρεσίες και κόμβους του εσωτερικού δικτύου. Έτσι οι εξωτερικοί χρήστες του διαδικτύου μπορούν να προσπελάσουν μόνο τους κόμβους της ζώνης αυτής, ενώ αυτοί μπορούν να προσπελάσουν και κόμβους του εσωτερικού δικτύου. Σε περίπτωση επίθεσης ο hacker έχει να αντιμετωπίσει ένα δεύτερο τείχος άμυνας[199].

Συχνά ένα firewall συνδυάζεται με τον διακομιστή μεσολάβησης (proxy server). Ο proxy server χρησιμοποιείται για να υπάρχει πρόσβαση στις ιστοσελίδες από τους άλλους υπολογιστές. Όταν κάποιος άλλος υπολογιστής ζητάει μια ιστοσελίδα, αυτή ανακτάται από τον proxy server και μετά στέλνεται στον υπολογιστή που την ζήτησε. Το αποτέλεσμα αυτής της ενέργειας είναι ότι ο απομακρυσμένος υπολογιστής που περιέχει την ιστοσελίδα δεν έρχεται ποτέ σε άμεση επαφή με τους υπολογιστές του δικτύου μας, παρά μόνο με τον proxy server.Οι proxy servers μπορούν επίσης να κάνουν την πρόσβασή μας στο Internet να εργάζεται πιο αποδοτικά. Αν κατεβάσουμε μια ιστοσελίδα από ένα Web site, αυτή αποθηκεύεται στον proxy server. Αυτό σημαίνει ότι την επόμενη φορά που θα επανέλθουμε σ' αυτήν την ιστοσελίδα, δεν θα χρειασθεί να φορτωθεί εκ νέου από το Web site, αλλά θα φορτωθεί αμέσως από τον proxy server.



Σχήμα 24. Ζώνη αποστρατικοποίησης με Firewall

Πηγή: http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/5756029

[199] Βλ.ό.π., Θ.Κομνηνός , Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002, σελ. 113

Η εγκατάσταση μιας DMZ είναι πολύ εύκολη. Αν έχουμε πολλούς υπολογιστές, μπορούμε να επιλέξουμε να τοποθετήσουμε έναν υπολογιστή ανάμεσα στη σύνδεση με το Internet και το firewall. Τα περισσότερα από τα software firewalls μάς δίνουν τη δυνατότητα να καθορίσουμε έναν κατάλογο (directory) στον υπολογιστή αυτόν ως DMZ [200].

3.4.2 **Τύποι τείχους προστασίας**(Firewalls)

1. **Φίλτρα πακέτων (Packet filtering**). Η τεχνική αυτή εφαρμόζεται στο επίπεδο δικτύου και ελέγχει ποιά δεδομένα μπορούν να περάσουν από και προς το δίκτυο. Για να το πετύχει αυτό χρησιμοποιεί λίστες ελέγχου πρόσβασης (Access Control Lists) οι οποίες είναι λίστες από ένα σύνολο κανόνων που θα πρέπει η συσκευή να εφαρμόσει στα πακέτα που παραλαμβάνει. Οι κανόνες υποδεικνύουν ποιά πακέτα επιτρέπεται να περάσουν και ποιά όχι. Τα κριτήρια με τα οποία γίνεται το φιλτράρισμα είναι[201]:

- ☞ Διεύθυνση IP προέλευσης. Πρόκειται για τη διεύθυνση IP του συστήματος που έφτιαξε το πακέτο.
- ☞ Διεύθυνση IP προορισμού. Η διεύθυνση IP που προορίζεται να φτάσει το πακέτο.
- ☞ Θύρα (Port) εφαρμογής αποστολέα
- ☞ Θύρα Port εφαρμογής παραλήπτη
- ☞ Είδος πρωτοκόλλου (TCP, ή UDP) που δημιουργεί τα πακέτα.

2. **Πληρεξούσια φράγματα (proxy firewalls):** Λειτουργούν σαν ενδιάμεσοι μεταξύ των δικτύων. Δέχονται μηνύματα (εισερχόμενα- εξερχόμενα) από το δίκτυο, και αφού τα ελέγξουν ότι δεν περιέχουν κακόβουλα δεδομένα, τα δρομολογούν στον προορισμό τους. Διακρίνονται σε δύο κατηγορίες[202]:

☞ Πύλη επιπέδου εφαρμογής(application- level gateway): Ελέγχουν όλο το περιεχόμενο του πακέτου και αποφασίζει με βάση αυτό για την προώθηση ή όχι. Μια πύλη επιπέδου εφαρμογών εργάζεται για μια υπηρεσία ή ένα πρωτόκολλο. Επομένως, πρέπει να υπάρχει μια πύλη επιπέδου εφαρμογών για κάθε υπηρεσία που μπορεί να παρέχει ένας υπολογιστής (HTTP, FTP, SMTP, Telnet).

---

[200] Βλ http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html επίσης

http://support.microsoft.com/kb/191146/el

[201] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 473.

[202] http://infoman.teikav.edu.gr/e_education/70/InfoSystemSechandouts.ppt

☞ Πύλη επιπέδου κυκλώματος (circuit – level gateway): Η πύλη επιπέδου κυκλώματος δημιουργεί δύο συνδέσεις TCP, μία ανάμεσα σε αυτή και ένα χρήστη σε ένα εσωτερικό υπολογιστή και μία ανάμεσα σε αυτή και ένα χρήστη σε ένα εξωτερικό υπολογιστή. Μετά την εγκαθίδρυση των συνδέσεων αυτών η πύλη αναμεταδίδει πακέτα χωρίς να εξετάζει το περιεχόμενο τους. Γνωρίζει την πηγή και τον προορισμό και παίρνει αποφάσεις σύμφωνα με αυτές τις πληροφορίες. Η λειτουργία αποτελείται από την εύρεση των συνδέσεων που επιτρέπονται. Συνήθως χρησιμοποιείται όταν εμπιστευόμαστε τους εσωτερικούς χρήστες και επιτρέπουμε συνδέσεις προς το εξωτερικό δίκτυο[203].

3. **Διπλά συνδεδεμένα φράγματα ασφαλείας (Dual - Homed Gateway):** Το Dual - Homed Gateway είναι ένα firewall που αποτελείται από ένα σύστημα με δύο τουλάχιστον κάρτες δικτύου και λειτουργεί σαν δρομολογητής για την κίνηση ανάμεσα στα πακέτα που διακινούνται στα δύο υποδίκτυα που βρίσκονται συνδεδεμένα στις δύο κάρτες. Απενεργοποιώντας την αυτόματη δρομολόγηση επιτρέπουμε τη διέλευση στο άλλο υποδίκτυο σε συγκεκριμένα πακέτα που τηρούν τους κανόνες ασφαλείας. Δηλαδή τα συστήματα του εσωτερικού δικτύου όπως και του Internet έχουν τη δυνατότητα να επικοινωνούν με το σύστημα αυτό αλλά όχι και μεταξύ τους. Χρησιμοποιείται για να διαιρέσει ένα εσωτερικό έμπιστο δίκτυο από ένα εξωτερικό μη έμπιστο[204].

4. **Σταθμός-οχυρό (bastion host):** Το σύστημα αυτό είναι ένα σύστημα που προσδιορίζεται από το διαχειριστή του firewall σαν κρίσιμο ισχυρό σημείο για την ασφάλεια του δικτύου και το οποίο αποτελεί τη βάση πάνω στο οποίο θα λειτουργήσει το λογισμικό του firewall. Είναι προσβάσιμος από όσους θέλουν να εισέλθουν ή να εξέλθουν στο προστατευμένο δίκτυο. Πρόκειται για ένα σταθμό ο οποίος βρίσκεται στην πρώτη γραμμή άμυνας, ορατός από όλους και εκτεθειμένος σε επιθέσεις. Για το λόγο αυτό πρέπει να προστατεύεται επαρκώς και να μην υπάρχουν τρωτά σημεία τα οποία μπορεί να εκμεταλλευτεί ο εν δυνάμει επιτιθέμενος. Χρειάζεται επίσης οι πόρτες που δε χρειάζονται πρέπει να είναι κλειστές, οι υπηρεσίες που δεν είναι απαραίτητες καθώς και αχρησιμοποίητοι λογαριασμοί χρηστών πρέπει να έχουν απενεργοποιηθεί[205].

Μια ολοκληρωμένη υπηρεσία firewall πολλές φορές παρέχεται με συνδυασμό των τεχνικών που αναπτύσσονται στους παραπάνω τύπους firewalls.

[203] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 479

[204] Βλ.ό.π., Θ.Κομνηνός,Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002, σελ. 120

[205] http://infoman.teikav.edu.gr/e_education/70/InfoSystemSechandouts.ppt

3.4.3 **Πλεονεκτήματα** - **μειονεκτήματα**(Firewalls)

Πλεονεκτήματα[206] **:**

- Προστατεύουν το εσωτερικό δίκτυο από διάφορες επιθέσεις
- Παρέχουν ελεγχόμενη προσπέλαση στους πόρους του εσωτερικού δικτύου
- Κρύβουν πληροφορίες για το εσωτερικό δίκτυο προς τον έξω κόσμο
- Καταγράφουν τα διερχόμενα πακέτα και ειδοποιούν σε περίπτωση κινδύνου
- Λειτουργούν αποτελεσματικά στην προώθηση της πολιτικής ασφάλειας του συστήματος.
- Προστατεύουν από τρωτά σημεία υπηρεσιών δικτύων
- Συγκεντρώνουν υπηρεσίες ασφάλειας σε μια καλά ορισμένη και οχυρωμένη ζώνη
- Μπορεί να λειτουργήσουν και σαν πύλη κρυπτογράφησης

Μειονεκτήματα:

- Χρειάζονται γνώση για να γίνει σωστή εγκατάσταση και ρύθμιση
- Η χρήση τους μειώνει την κυκλοφορία των δεδομένων
- Η χρήση τους περιορίζει υπηρεσίες που θα ήθελαν να έχουν οι χρήστες
- Δεν προστατεύουν από κακόβουλο λογισμικό που μπορεί να ταξιδεύει με το ηλεκτρονικό ταχυδρομείο.
- Δεν δίνουν προστασία από τους εσωτερικούς εχθρούς που βρίσκονται εντός έμπιστου δικτύου και εξαπολύουν επίθεση.
- Αποτελούν στόχο των hacker .
- Δεν μπορούν να ελέγξουν το περιεχόμενο μηνυμάτων

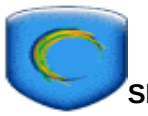
[206] http://www.inf.teilam.gr/OLD/course_material/examino_st/asfalia_firewalls.pdf

3.4.4 **Προγράμματα** (Firewalls)

Στο χώρο των personal computers τα λειτουργικά συστήματα παρέχουν ενσωματωμένα firewall. Επιπλέον οι προχωρημένοι χρήστες μπορούν να εγκαταστήσουν κάποιο άλλο τείχος ασφαλείας αφού τέτοιου είδους προγράμματα μπορεί να τα βρει κανείς εύκολα στο διαδίκτυο. Παραθέτουμε πίνακα με τέτοια προγράμματα, τα οποία ο αναγνώστης μπορεί να πάρει πληροφορίες αλλά και να κάνει λήψη του αντίστοιχου προγράμματος.

α/α	**Ονομασία**	**Ιστοσελίδα λήψης**	**Πληροφορίες**[207]
1	**Online Armor Free**	**Λήψη**	Θεωρείται ένα από τα καλύτερα firewall σήμερα, το οποίο αν και free είναι πανίσχυρο.
2	**Outpost Firewall Free**	**Λήψη**	Παρακολουθεί και εξερχόμενες συνδέσεις
3	**Comodo Firewall**	**Λήψη**	Το Comodo Firewall θεωρείται το καλύτερο από τα free και ανώτερο από τα περισσότερα εμπορικά firewalls.
4	**PC Tools Firewall Plus**	**Λήψη**	Ελέγχει την εισερχόμενη και εξερχόμενη κίνηση του δικτύου παρακολουθώντας παράλληλα κάθε πρόγραμμα που τρέχει στον υπολογιστή
5	**ZoneAlarm Free**	**Λήψη**	Ευκολία στην εγκατάσταση.

[207] Οι πληροφορίες και τα προγράμματα προέρχονται από την ιστοσελίδα: http://sxoleio.eu/Firewalls.php

6	 **Ashampoo Firewall Free**	**Λήψη**	Επιλογή για αρχάριους χρήστες που θέλουν προστασία, αλλά δεν είναι σε θέση να κάνουν δύσκολες ρυθμίσεις
7	 **Privatefirewall**	**Λήψη**	μπλοκάρει και βάζει σε καραντίνα δραστηριότητες γνωστών κακόβουλων λογισμικών, hacking, phishing και άλλες μορφές απειλών
8	 **Filseclab Personal Firewall Professional**	**Λήψη**	Μπορεί να εμποδίσει τις περισσότερες επιθέσεις από ιούς τύπου worm και ιούς τύπου trojan, μπορεί επίσης να μπλοκάρει κάποια κύρια adware και spyware.
9	 **SoftPerfect Personal Firewall**	**Λήψη**	Είναι εύκολο στη χρήση και διατίθεται δωρεάν
10	 **Hotspot Shield**	**Λήψη**	Κρύβει την ip διεύθυνση σας

Πίνακας 10. Προγράμματα Firewalls

Πηγή: http://sxoleio.eu/Firewalls.php

3.5 **Συστήματα ανίχνευσης εισβολέων** (Intrusion Detection System, IDS)

Ο αυξανόμενος αριθμός υπολογιστικών συστημάτων που βρίσκονται δικτυωμένοι έχει σαν αποτέλεσμα πέραν των άλλων και στην αύξηση των παράνομων δραστηριοτήτων τόσο από εξωτερικούς εισβολείς, όσο και από εσωτερικούς εχθρούς (εντός δικτύου) που προσπαθούν να αποκτήσουν μη νόμιμη πρόσβαση σε πόρους του συστήματος και επιτίθενται. Για την ανίχνευση των εισβολέων και κάθε παράνομης δραστηριότητας, χρησιμοποιούνται εργαλεία που ονομάζονται Συστήματα ανίχνευσης εισβολέων (**I**ntrusion **D**etection **S**ystem **IDS)**[208]**.**

[208] Βλ.ό.π., Θ.Κομνηνός,Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002, σελ. 186

Τα Συστήματα Ανίχνευσης Εισβολής (**I**ntrusion **D**etection **S**ystem **IDS**) είναι συστήματα λογισμικού τα οποία παρακολουθούν και αναλύουν τα συμβάντα, τα οποία λαμβάνουν χώρα στους υπολογιστές και στα δίκτυα υπολογιστών. Η βασική τους αποστολή είναι η εύρεση ενδείξεων για πιθανές εισβολές, όπου μέσα από αυτές συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πόρων ενός πληροφοριακού συστήματος. Οι επιθέσεις εισβολής μπορεί να προέρχονται από εξωτερικούς χρήστες προς το εσωτερικό δίκτυο, οι οποίοι επιθυμούν μη νόμιμη πρόσβαση στους πόρους του συστήματος παρακάμπτοντας τους μηχανισμούς ασφαλείας. Επίσης, οι εισβολείς μπορεί να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα πρόσβασης[209].

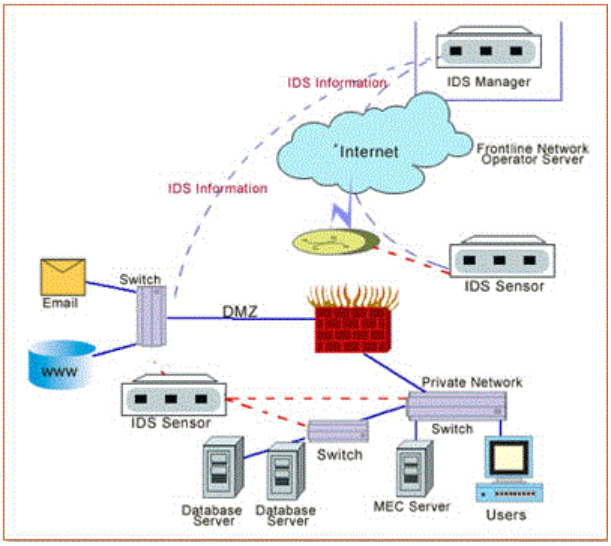
Διάκριση Συστημάτων Ανίχνευσης Εισβολής (IDS). Η βασική διάκριση στα IDS είναι παθητικά και ενεργητικά συστήματα. Ένα **παθητικό** (passive) IDS, ανιχνεύει μια επίθεση χωρίς να μπορεί όμως να την αντιμετωπίσει. Απλά ειδοποιεί τον διαχειριστή για την ύπαρξή της επίθεσης. Λειτουργούν όπως ακριβώς ένας συναγερμός σε ένα σπίτι που στην περίπτωση που ανιχνεύσει ύποπτη κίνηση ειδοποιεί με ηχητικό σήμα. Σε ένα **ενεργητικό** (reactive) σύστημα IDS υπάρχουν περισσότερες δυνατότητες από αυτές που υπάρχουν στα παθητικά συστήματα, που έχουν να κάνουν πέραν της ανίχνευσης μιας εισβολής και με την αντιμετώπιση αυτής. Μια άλλη διάκριση είναι με κριτήριο που χρησιμοποιούνται. Έτσι έχουμε:

☞ Συστήματα ανίχνευσης επιθέσεων εγκαταστημένα σε υπολογιστές (host-based IDS – **HIDS**).Τέτοια συστήματα είναι εγκατεστημένα σε κάποιο τοπικό σύστημα υπολογιστή (host) και ανιχνεύουν ύποπτη και μη συνηθισμένη δραστηριότητα σε αυτό τον υπολογιστή, όπως μετατροπές σε δικαιώματα αρχείων, παράξενη πρόσβαση σε αρχεία κ.α.

☞ Συστήματα ανίχνευσης επιθέσεων **Δικτυακά** (Network-based IDS – **NIDS**). Ένα δικτυακό IDS αποτελείται από δύο μέρη: Τους αισθητήρες που βρίσκονται σε κάποια μέρη του δικτύου και παρακολουθούν την κίνηση του δικτύου και τον σταθμό διαχείρισης που λαμβάνει τα δεδομένα των αισθητήρων και σε περίπτωση ύποπτης κίνησης ειδοποιεί τον διαχειριστή του συστήματος[210].

[209] http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[210] Βλ.ό.π., Θ.Κομνηνός,Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002, σελ. 189-191



Σχήμα 25. Σύστημα ανίχνευσης εισβολών (IDS)

Πηγή:http://indiacyberlab.in/security-awareness/security-technologies.htm

Μέθοδοι ανίχνευσης εισβολών. Για την ανίχνευση εισβολών χρησιμοποιούνται από τα Συστήματα ανίχνευσης εισβολέων (Intrusion Detection System, IDS) οι μέθοδοι:

☞ Στατιστική ανίχνευση ανωμαλιών. Περιλαμβάνει τη συλλογή δεδομένων που έχουν να κάνουν με τη νόμιμη συμπεριφορά των εξουσιοδοτημένων χρηστών για ένα χρονικό διάστημα. Τα δεδομένα αυτά αποθηκεύονται και δημιουργείται ένα πρότυπο συμπεριφοράς. Στη συνέχεια εφαρμόζονται στατιστικοί έλεγχοι στην συμπεριφορά που παρατηρείται και ελέγχεται αν είναι νόμιμη συμπεριφορά χρήστη.

☞ Ανίχνευση ανωμαλιών βασισμένη στους κανόνες. Περιλαμβάνει την προσπάθεια να καθοριστούν ένα σύνολο κανόνων που μπορούν να χρησιμοποιηθούν για να αποφασιστεί αν μια δεδομένη συμπεριφορά ανήκει σε κάποιον εισβολέα.

Η στατιστική ανίχνευση ανωμαλιών είναι αποτελεσματική απέναντι στους εισβολείς, που δεν μπορούν να μιμηθούν τα πρότυπα συμπεριφοράς των λογαριασμών που χρησιμοποιούν παράνομα. Αντίθετα μέθοδοι που βασίζονται σε κανόνες είναι κατάλληλες να αναγνωρίσουν παράνομους χρήστες που βρίσκονται στο εσωτερικό δίκτυο και επιχειρούν πρόσβαση χωρίς δικαιώματα και εξουσιοδότηση. Στην πράξη, τα Συστήματα ανίχνευσης εισβολέων (IDS) χρησιμοποιούν συνήθως ένα συνδυασμό και των δύο μεθόδων για να είναι αποτελεσματικά απέναντι σε πάρα πολλές επιθέσεις[211].

Οι λόγοι εγκατάστασης ενός συστήματος ανίχνευσης εισβολής ποικίλουν. Οι πιο σημαντικοί από αυτούς τους λόγους είναι η πρόληψη προβλημάτων, η ανίχνευση παραβιάσεων, η τεκμηρίωση

[211] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 403.

υπαρκτών απειλών, ο έλεγχος ποιότητας για το σχεδιασμό ασφαλείας, καθώς και η θωράκιση παλαιών συστημάτων σε περίπτωση που κρίνεται αναγκαία η διατήρησή τους.

3.6 **Αντίγραφα Ασφαλείας** (Back Up)

Ένα πρόβλημα που μπορεί αντιμετωπίσουν οι χρήστες υπολογιστικών συστημάτων είναι η απώλεια δεδομένων, αρχείων ή και ρυθμίσεων σε κάποια προγράμματα. Οι αιτίες για τέτοιες απώλειες δεδομένων είναι πολλές, από μια απλή διακοπή ρεύματος , μια διαγραφή ενός αρχείου που έγινε κατά λάθος, μια επίθεση στο πληροφοριακό σύστημα, μόλυνση από ένα ιό κ.λ.π. Για το λόγο αυτό χρειάζεται η λήψη αντιγράφων ασφαλείας των σημαντικών αρχείων και δεδομένων σε τακτική βάση , ώστε σε περίπτωση που παρουσιασθεί κάποιο πρόβλημα να μην υπάρχει απώλεια των δεδομένων αλλά να μπορούμε να επαναφέρουμε τα απολεσθέντα αρχεία.

Η διαδικασία της δημιουργίας και αποθήκευσης αντιγράφων ασφαλείας πληροφοριακών πόρων του συστήματος (π.χ. δεδομένα, προγράμματα, βάσεις δεδομένων), ονομάζεται αντίγραφο ασφάλειας (backup data). Στην περίπτωση που υπάρχει απώλεια πόρων του συστήματος (δεδομένων, αρχείων , ρυθμίσεων), τότε επαναφέρεται το αντίγραφο ασφαλείας που έχει ληφθεί. Τα αντίγραφα ασφάλειας μπορεί να αποθηκευθούν σε εγγράψιμα CD, DVD, σκληρούς δίσκους, μαγνητικές ταινίες, εξωτερικούς σκληρούς δίσκους, μνήμες αποθήκευσης flash ή σε άλλο υπολογιστή που βρίσκεται στο δίκτυο.

Τα αντίγραφα ασφάλειας συνίστανται :

☞ Στην λήψη και επαναφορά συγκεκριμένων αρχείων και δεδομένων στην περίπτωση προβλήματος σε κάποια από αυτά.

☞ Στην λήψη και επαναφορά ολόκληρου του συστήματος (Λειτουργικό Σύστημα, δεδομένα, προγράμματα και εφαρμογές, ρυθμίσεις) στην περίπτωση που έχουμε πρόβλημα σε ολόκληρο το σύστημα που μπορεί να οφείλεται σε διάφορους λόγους («χτύπημα» σκληρού δίσκου, μόλυνση από κακόβουλο λογισμικό , επίθεση hacker κ.λ.π).

3.6.1 **Προγράμματα** (**BA**CK UP)

α/α	Ονομασία	Ιστοσελίδα λήψης	Πληροφορίες[212]
1	**Paragon Backup and Recovery Free**	**Λήψη**	Γρήγορο επαγγελματικό εργαλείο backup. Μπορεί να χρησιμοποιηθεί για backup ολόκληρου σκληρού δίσκου ή μεμονωμένων τμημάτων του.
2	**SyncBackFreeware**	**Λήψη**	Δωρεάν και εύχρηστο εργαλείο. Είναι βολικό γιατί έχει την δυνατότητα να κάνει προγραμματισμένη εργασία backup. Προσθέτει μόνο τα αρχεία που έχουν αλλάξει μέγεθος και ας έχουν το ίδιο όνομα, ενώ τα ίδια δεν τα πειράζει καθόλου.
3	**Easeus Todo Backup**	**Λήψη**	Απλό στην χρήση και αποτελεσματικό εργαλείο, σχεδιασμένο να κρατάτε backup τον δίσκο σας ή ένα partition και μετά να επαναφέρετε τα δεδομένα σε ένα άλλο δίσκο ή υπολογιστή.
4	**Comodo BackUp**	**Λήψη**	Δωρεάν πρόγραμμα, τόσο λειτουργικό, που μπορεί άξια να ανταγωνιστεί πολλά εμπορικά αντίστοιχα προϊόντα.
5	**O&O DiskImage Express**	**Λήψη**	Διαθέτει μόνο βασικές λειτουργίες, δηλαδή την επιλογή δημιουργίας backup image του δίσκου ή των partition και την επιλογή restore του image που έχετε δημιουργήσει.

[212] Οι πληροφορίες και τα προγράμματα προέρχονται από την ιστοσελίδα: http://sxoleio.eu/Backup-tools.php

6	 **Macrium Reflect Free**	Λήψη	Δημιουργεί ένα ακριβές αντίγραφο όλου του σκληρού δίσκου που έχουμε εγκατεστημένο το λειτουργικό μας, σε έναν εξωτερικό ή δεύτερο δίσκο μας στην μορφή ενός και μόνο αρχείου.
7	 **O&O AutoBackup**	Λήψη	Δημιουργεί ένα backup και επαναφέρει τα βασικά αρχεία και τις ρυθμίσεις συστήματος, γρήγορα και εύκολα.
8	 **GFI Backup Home**	Λήψη	Ένα επαγγελματικό, φιλικό προς τον χρήστη και γεμάτο δυνατότητες εργαλείο αντιγραφών ασφαλείας που δεν κοστίζει τίποτα.
9	 **Fbackup**	Λήψη	Δωρεάν λογισμικό δημιουργίας αντιγράφων ασφαλείας, σε οποιαδήποτε συσκευή usb, firewire, τοπικό δίσκο ή τοποθεσία δικτύου.
10	 **Easeus Disk Copy Free**	Λήψη	Προσφέρει ακόμα και τη δημιουργία image backup, το οποίο μπορεί να χρησιμοποιηθεί για να ανακτήσει κανείς το σύστημα του μαζί με τα προγράμματα.
11	 **Cobian Backup**	Λήψη	Ένα απλό αλλά με πολλά χαρακτηριστικά πρόγραμμα που κάνει εύκολη την διαδικασία να ορίσετε αρχεία και φακέλους που θα θέλατε να προστατέψετε.
12	 **MozBackup**	Λήψη	Εύχρηστο εργαλείο που μπορεί να δημιουργήσει αντίγραφα ασφαλείας για Firefox και Thunderbird τα οποία μπορείτε να τα χρησιμοποιήσετε για να επαναφέρετε όλες τις ρυθμίσεις σας.

13	 **Genie Timeline Free**	**Λήψη**	Δωρεάν εργαλείο δημιουργίας αντιγράφων ασφαλείας, που δουλεύει απλά, κάνοντας ευχάριστη αυτήν την βαρετή διαδικασία.

Πίνακας 11. Προγράμματα BACK UP

Πηγή :http://sxoleio.eu/Backup-tools.php

3.7 Τεχνολογίες για τη διασφάλιση της ιδιωτικότητας των χρηστών

Anonymizer. Ο anonymizer ή anonymous proxy είναι ένα εργαλείο που δίνει τη δυνατότητα σε αυτόν που το χρησιμοποιεί να περιηγηθεί στο διαδίκτυο χωρίς να φανερώσει την ταυτότητά του. Ο anonymizer αποκτά πρόσβαση στο παγκόσμιο ιστό για λογαριασμό του χρήστη αποκρύπτοντας πληροφορίες που μπορεί να φανερώσουν την ταυτότητά του. Η χρήση του anonymizer βοηθά επίσης στην αποφυγή κλοπής προσωπικών στοιχείων, καθώς και στην προστασία από τη δημοσιοποίηση ιστορικών αναζήτησης χρηστών από τρίτους. Μπορεί όμως να χρησιμοποιηθεί και για κακόβουλη δραστηριότητα, όπως είναι η παιδική πορνογραφία.

SSL. Το πρωτόκολλο SSL (Secure Sockets Layer) δημιουργήθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο όπως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ ηλεκτρονικών υπολογιστών επιτυγχάνοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Περισσότερα για το πρωτόκολλο SSL βλέπε παρακάτω στην ενότητα 3.12.

P3P. Το P3P είναι μια ειδική πλατφόρμα προστασίας δεδομένων, η οποία δίνει την δυνατότητα σε ιστοσελίδες να υλοποιήσουν τις πρακτικές προστασίας προσωπικών δεδομένων σε τυποποιημένη μορφή έτσι ώστε να μπορούν να ανακτηθούν αυτόματα και να ερμηνεύονται εύκολα από τους χρήστες. Στο P3P οι διαχειριστές επιτρέπουν στους χρήστες να ενημερώνονται για νέες πρακτικές και να παίρνουν αυτόματα αποφάσεις. Ως εκ τούτου οι χρήστες δεν χρειάζεται να διαβάζουν τις πολιτικές απορρήτου σε κάθε ιστοσελίδα που επισκέπτονται[213].

Pretty Good Privacy. Το Pretty Good Privacy (PGP) είναι ένα χρήσιμο πρόγραμμα για κρυπτογράφηση αλλά και για αποκρυπτογράφηση δεδομένων, που χρησιμοποιούνται στη χρήση του ηλεκτρονικού ταχυδρομείου. Παρέχει ιδιωτικότητα και πιστοποίηση αυθεντικότητας για δεδομένα που ανταλλάσσονται μεταξύ χρηστών. Επίσης χρησιμοποιείται για ψηφιακή υπογραφή, κρυπτογράφηση και αποκρυπτογράφηση αρχείων κειμένου, αρχείων ηλεκτρονικού

[213] Βλ.http://welcome.hp.com/country/gr/el/privacy/p3p_popup.html

ταχυδρομείου, καταλόγων και ολόκληρων τμημάτων σκληρών δίσκων, έτσι ώστε να αυξήσει την προστασία της επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου. Εκτενέστερα το θέμα αυτό αναλύεται στην επόμενη ενότητα 3.8.1.

Virtual Private Network-VPN. Η υπηρεσία εικονικού ιδιωτικού δικτύου Virtual Private Network - VPN δίνει τη δυνατότητα στους χρήστες της να αναγνωρίζονται (βάσει της δικτυακής διεύθυνσης IP του υπολογιστή τους) με αποτέλεσμα να έχουν πρόσβαση σε όσες υπηρεσίες εξαρτώνται από αυτή την αναγνώριση. Η λειτουργία της υπηρεσίας βασίζεται στην εγκατάσταση ενός SSL (Secure Sockets Layer) τούνελ εικονικού ιδιωτικού δικτύου (VPN tunnel) μεταξύ του υπολογιστή του μετακινούμενου χρήστη και του εξυπηρετητή (VPN server). Όλη η δικτυακή κίνηση μεταξύ των δύο αυτών υπολογιστών κρυπτογραφείται. Ο VPN server που παραλαμβάνει την δικτυακή κίνηση από τον χρήστη, την αποκρυπτογραφεί και τη δρομολογεί στο υπόλοιπο δίκτυο. Από τη στιγμή που εγκατασταθεί το VPN tunnel, όλη η δικτυακή κίνηση του υπολογιστή του χρήστη δρομολογείται πίσω στο δίκτυο[214].

Anonymous remailer. Anonymous remailer ονομάζεται ένας εξυπηρετητής ο οποίος λαμβάνει μηνύματα με ενσωματωμένες οδηγίες για το που θα αποσταλούν στη συνέχεια. Αυτά τα μηνύματα στη συνέχεια προωθούνται χωρίς να αποκαλύπτεται η αρχική πηγή προέλευσης τους. Κάθε πακέτο που στέλνεται περιέχει τις IP διευθύνσεις του αποστολέα και των κόμβων παραλαβής. Οι remailers αναλαμβάνουν να αλλάξουν αυτές τις διευθύνσεις και να τις αντικαταστήσουν με πλαστές διευθύνσεις προέλευσης. Έτσι η IP προέλευσης μπορεί να αντικατασταθεί με αυτήν του κεντρικού εξυπηρετητή . Οι remailers μπορεί να μεταβιβάσουν το μήνυμα σε άλλους remailers και μετά από πολλούς κύκλους τελικά να καταλήξει στο προοριζόμενη διεύθυνση[215].

Freenet. Το Freenet, είναι λογισμικό το οποίο επιτρέπει σε κάποιον να περιηγηθεί στο διαδίκτυο, να διανέμει αρχεία, καθώς επίσης να μιλά σε forum αλλά και να επισκέπτεται ιστοτόπους μέσω του προγράμματος αυτού ανώνυμα. Έχει σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να αποκεντρώνει το δίκτυο των υπολογιστών παρέχοντας στον χρήστη ανωνυμία και κάνοντας αυτόν λιγότερο ευάλωτο σε επιθέσεις. Η επικοινωνία μεταξύ των υπολογιστών είναι κρυπτογραφημένη και το δίκτυο δεν περιλαμβάνει εξυπηρετητές και καθοδηγείται μέσα από άλλους κόμβους, πράγμα που κάνει πολύ δύσκολο να βρεθεί ποιος ζητά πληροφορία, ποιος την έλαβε αλλά και ποιο είναι το περιεχόμενο της[216].

CGIProxy. Το CGIProxy (Common Gateway Interface Proxy), είναι ένα πακέτο λογισμικού για διαμεσολαβητές (proxys) διαδικτύου, το οποίο έχει τη μορφή ιστοσελίδας και επιτρέπει στο χρήστη να έχει ανώνυμη πρόσβαση σε οποιαδήποτε άλλη ιστοσελίδα. Αυτό επιτυγχάνεται αντικαθιστώντας το ψηφιακό ίχνος του χρήστη με το ίχνος του server που εκτελεί το λογισμικό[217].

---

[214] Για περισσότερα βλ: http://noc.auth.gr/services/connectivity/vpn/

[215] Για περισσότερα βλ: http://el.wikibooks.org/wiki Τεχνική Νομοθεσία Για Μηχανικούς Πληροφορικής

[216] Για περισσότερα βλ: http://en.wikipedia.org/wiki/Freenet επίσης https://freenetproject.org/papers/freenet-0.7.5-paper.pdf.

[217] Για περισσότερα βλ: http://rosinstrument.com/cgi-proxy.htm

The Amnesic Incognito Live System (Tails). Το Tails είναι ένα σύστημα το οποίο στοχεύει στην διατήρηση της ιδιωτικότητας και της ανωνυμίας. Βοηθάει τον χρήστη να χρησιμοποιήσει το διαδίκτυο ανώνυμα από όπου και να βρίσκεται και οποιονδήποτε ηλεκτρονικό υπολογιστή και αν χρησιμοποιεί χωρίς να αφήσει ίχνη πίσω του. Πρόκειται για ένα πλήρες λειτουργικό σύστημα το οποίο έχει σχεδιαστεί να φορτώνεται στον υπολογιστή από ένα DVD ή από ένα USB ,ανεξάρτητο από το κύριο λειτουργικό σύστημα του.

3.8 **Ασφάλεια ηλεκτρονικού ταχυδρομείου**

Όπως αναφέραμε σε προηγούμενη ενότητα η υπηρεσία ηλεκτρονικής αλληλογραφίας (email) είναι μια από τις πλέον διαδεδομένες και δημοφιλείς υπηρεσίες του Διαδικτύου. Η υπηρεσία αυτή βοηθά στην ανταλλαγή μηνυμάτων μεταξύ απλών χρηστών , εταιρειών , οργανισμών και οποιονδήποτε επιθυμεί να επικοινωνήσει με αμεσότητα, ευκολία και χωρίς ιδιαίτερη επιβάρυνση. Τα μηνύματα σε πολλές περιπτώσεις περιέχουν εμπιστευτικές πληροφορίες τις οποίες πολλοί θα ήθελαν νε έχουν πρόσβαση. Για το λόγο αυτό η υπηρεσία ηλεκτρονικής αλληλογραφίας(e-mail) θα πρέπει να περιβάλλεται με ασφάλεια και να παρέχει τις παρακάτω υπηρεσίες ασφάλειας :

☞ **Αυθεντικότητα** : Η βεβαιότητα πως αυτός που έστειλε το μήνυμα(αποστολέας) είναι αυτός που γράφει η επικεφαλίδα.

☞ **Ακεραιότητα** : Η σιγουριά ότι το μήνυμα δεν τροποποιήθηκε κατά τη διάρκεια της μεταφοράς του.

☞ **Εμπιστευτικότητα**: Το περιεχόμενο του μηνύματος να μπορεί να διαβαστεί μόνο από τον αποδέκτη - παραλήπτη και από κανένα άλλο.

Ένα καλό εργαλείο που παρέχει αυτές τις υπηρεσίες είναι το PGP (Pretty Good Privacy).

3.8.1 **Πρόγραμμα** (Pretty Good Privacy, PGP)

Το πρόγραμμα PGP (Pretty Good Privacy),είναι ένα δωρεάν λογισμικό ανοιχτού κώδικα και χρησιμοποιείται για την ασφάλεια του ηλεκτρονικού ταχυδρομείου. Δημιουργός του ο Philip Zimmermann καθηγητής στο πανεπιστήμιο του MIT. Αποτελεί ένα ανοικτό πρότυπο (Open PGP) και υποστηρίζει μια σειρά από αλγόριθμους κρυπτογράφησης (ιδιωτικού και δημόσιου κλειδιού), συναρτήσεις κατακερματισμού (Hash Function), και ψηφιακών υπογραφών (Digital signature). Σύμφωνα με τον William Stallings (2010), το PGP (Pretty Good Privacy) προσφέρει:

☞ Πιστοποίηση αυθεντικότητας με χρήση ψηφιακών υπογραφών.

☞ Εξασφάλιση του απορρήτου με χρήση κρυπτογραφίας .

☞ Συμπίεση μέσω του αλγόριθμου ZIP .

☞ Συμβατότητα ηλεκτρονικού ταχυδρομείου με χρήση κωδικοποίησης.

☞ Κατάτμηση και επανασυναρμολόγηση για μηνύματα μεγάλου μεγέθους[218].

Ο πηγαίος κώδικάς του (source code) είναι διαθέσιμος (ανοικτός) στους χρήστες, ενώ το πρόγραμμα χρησιμοποιείται εδώ και πολύ καιρό και θεωρείται σε μεγάλο βαθμό αξιόπιστο. Χρησιμοποιεί τόσο αλγορίθμους δημοσίου κλειδιού για τη διαχείριση των κλειδιών και για ψηφιακές υπογραφές αλλά και συμμετρικούς αλγορίθμους για τη κρυπτογράφηση δεδομένων[219]. Το PGP, πιο συγκεκριμένα το PGPi, στη διεθνή έκδοσή του, μπορούμε να κατεβάσουμε και να χρησιμοποιήσουμε δωρεάν από την επίσημη ιστοσελίδα http://www.pgpi.org[220].

3.8.2 **Κανόνες ασφαλούς λειτουργίας** (e-mail)

Η χρήση του ηλεκτρονικού ταχυδρομείου επιβάλλει από την μεριά των χρηστών ένα σύνολο κανόνων που πρέπει να εφαρμόζονται και να τηρούνται με ευλάβεια[221].

☞ Δεν ανοίγουμε ύποπτα συνημμένα αρχεία που έρχονται στο e-mail μας, προερχόμενα από άγνωστους αποστολείς.

☞ Δεν δημοσιοποιούμε τη διεύθυνση του ηλεκτρονικού μας ταχυδρομείου με ευκολία. Με τη συχνή χρήση του ηλεκτρονικού μας ταχυδρομείου σε σελίδες που απαιτούν εγγραφή είναι πολύ πιθανό να γίνουμε στόχος υπερβολικής ή ανεπιθύμητης αλληλογραφίας. Μια καλή πρακτική είναι να έχουμε ένα δεύτερο λογαριασμό ηλεκτρονικού ταχυδρομείου, τον οποίο θα χρησιμοποιούμε σε τέτοιες περιπτώσεις. Η δημοσιοποίηση της διεύθυνσης του e-mail μας γίνεται περιγραφικά ή με αρχείο εικόνας (βλ. προηγούμενη ενότητα 2.3.10- Μη ζητηθείσα ηλεκτρονική επικοινωνία αντιμετώπιση Spam e-mails).

☞ Δεν αποκαλύπτουμε προσωπικά δεδομένα (π.χ. αριθμό πιστωτικής κάρτας) μέσω ηλεκτρονικού ταχυδρομείου ούτε απαντάμε σε μηνύματα που υποτίθεται μας στέλνει η τράπεζα και μας ζητούν να δώσουμε κωδικούς για e-banking. Τα mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν αυτά τα στοιχεία.

☞ Χρειάζεται τακτικά να γίνεται αλλαγή του κωδικού πρόσβασης του λογαριασμού email . Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail.Σε αυτούς τους λογαριασμούς

---

[218] Βλ. ό.π., William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010, σελ. 184.

[219] Μάγκος Ε., Ασφάλεια Υπολογιστών και Προστασία Δεδομένων, Κέρκυρα, 2007,σελ. 11-13 στο: http://di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20A.pdf.

[220] Για περισσότερα σχετικά με την εγκατάσταση του PGP βλ. περιοδικό “It Security”, για την ασφάλεια στην πληροφορική, στο:
http://www.securitymanager.gr/it_security/protection_article.php?id=3&set=13&title=Privacy29&PHPSESSID=8c9
επίσης http://www.pgp.com, επίσης http://www.ekoletsou.gr/pdfFiles/PGP.pdf

[221] Βλ : http://www.pi.ac.cy/InternetSafety/parent_xrisimes_simboules.html
επίσης http://www.pgp.com, επίσης http://www.ekoletsou.gr/pdfFiles/PGP.pdf

υπάρχει η δυνατότητα[222] για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, η οποία δεν πρέπει να ενεργοποιείται.

☞ Χρήση κρυπτογραφίας στα μηνύματα που αποστέλλουμε με κατάλληλα εργαλεία καθώς και χρήση ψηφιακής υπογραφής.

3.9 **Κρυπτολογία-Κρυπτογραφία**

Ένα σημαντικό μέρος της προσπάθειας για μεγαλύτερη ασφάλεια αποτελεί η επιστήμη της κρυπτολογίας (cryptology). Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και την λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση[223](cryptanalysis) με παρεμφερή κλάδο την Στεγανογραφία[224] και αντίστοιχα την Στεγανοανάλυση. Η κρυπτογράφηση είναι μια μέθοδος προστασίας των δεδομένων που μπορεί να λειτουργεί αποτελεσματικά παρέχοντας ασφάλεια, ακόμη και αν παραβιαστεί κάποιο πληροφοριακό σύστημα. Με την βοήθεια της κρυπτογραφίας μπορούμε να αντιμετωπίσουμε τα σημαντικότερα προβλήματα ασφάλειας: Μυστικότητα (secrecy), Ακεραιότητα (integrity), Πιστοποίηση (authentication), Ταυτοποίηση (non-repudiation).

Η κρυπτογραφία αποτελεί κλάδο των μαθηματικών η οποία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Με την **Κρυπτογράφηση** (encryption*)* έχουμε μετατροπή ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου έτσι ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση** *(*decryption*)*. Κρυπτογραφικός αλγόριθμος (cipher) είναι η διαδικασία μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους σε μη εξουσιοδοτημένα μέρη. Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός **αλγόριθμου κρυπτογράφησης** (cipher) και ενός **κλειδιού κρυπτογράφησης** (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στην μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι

---

[222] Η δυνατότητα αυτή εξυπηρετεί τον χρήστη να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή (απομνημόνευση ID σε αυτό τον υπολογιστή).

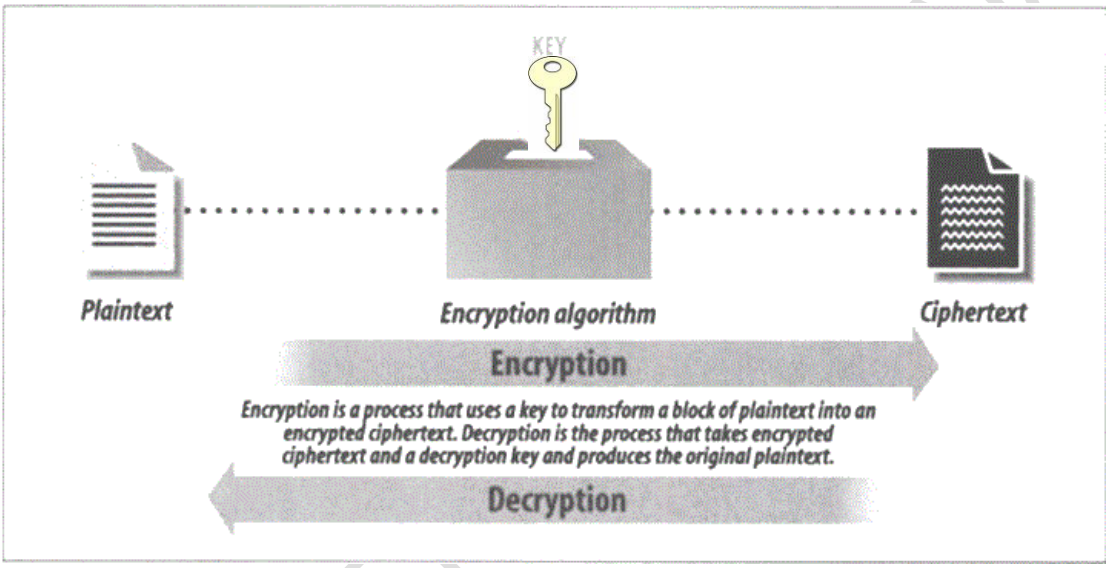
[223] Η επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής έτσι ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί

[224] Όπως καταλαβαίνουμε και από το όνομά της, η στεγανογραφία είναι η τέχνη, που στις μέρες μας έχει εξελιχθεί και σε τεχνική, της επικοινωνίας κατά τρόπο τέτοιο που να κρύβεται η ίδια η ύπαρξη της επικοινωνίας. Σε αντίθεση με τη κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει τη πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της, βλ. Βασίλειος Ζορκάδης, Κρυπτογραφία, Πάτρα 2002, ΕΑΠ, σελ 16

βλ http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/steganografia.htm

το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς.

Κατά τη διαδικασία της κρυπτογράφησης έχουμε το αρχικό κείμενο (plaintext) το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης. Χρησιμοποιώντας ένα Κλειδί (key) σαν είσοδος στην συνάρτηση κρυπτογράφησης(αλγόριθμος),παράγεται το κρυπτογραφημένο κείμενο (ciphertext) που είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο. Με την αντίστροφη διαδικασία έχουμε την αποκρυπτογράφηση του μηνύματος , όπου το κωδικοποιημένο κείμενο (ciphertext) μετατρέπεται πίσω στο αρχικό κείμενο (plaintext) χρησιμοποιώντας μια μαθηματική συνάρτηση (αλγόριθμο) και ένα κλειδί (βλέπε σχήμα 26).



Σχήμα 26. Κρυπτογράφηση και αποκρυπτογράφηση

Πηγή: Simson Garfinkel, Gene Spafford, Alan Scbwartz, Practical Unix & Internet Security σελ 162 στο: http://books.google.com/books?id=t0IExLP-MPMC&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Η κρυπτογράφηση είναι απαραίτητη κατά την επικοινωνία μέσω Διαδικτύου γιατί διασφαλίζει τα παρακάτω:

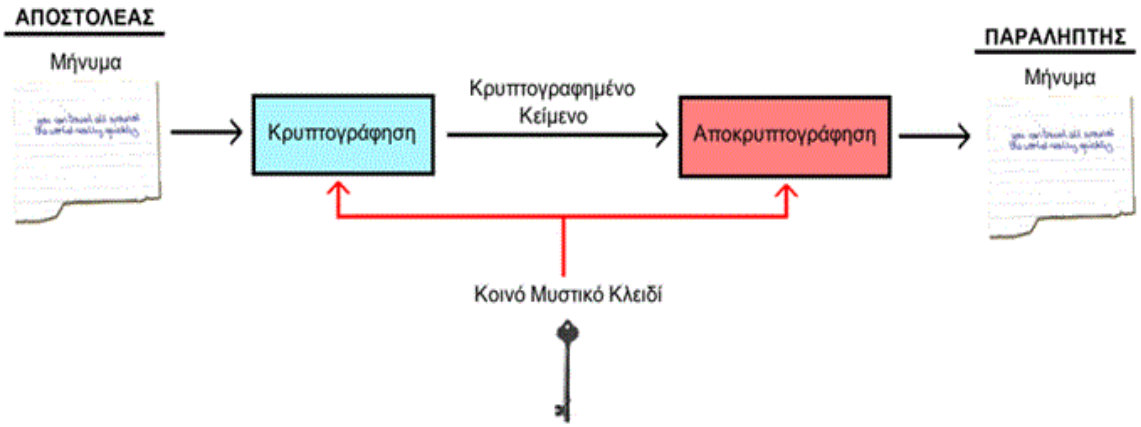
- Ιδιωτικότητα
- Πιστοποίηση
- Ακεραιότητα
- Υπευθυνότητα

Λέγοντας ιδιωτικότητα εννοούμε ότι η μετάδοση δεδομένων παραμένει ιδιωτική ακόμα και αν έχουμε παραβίαση πληροφοριακών συστημάτων και υποκλοπή των δεδομένων μετάδοσης. Η πιστοποίηση αποδεικνύει την ταυτότητα κάνοντας σωστή χρήση της κρυπτογραφίας. Το user name και το password που δίνονται για τη δημιουργία μιας σύνδεσης

αποτελούν δύο μοναδικά κλειδιά. Η ακεραιότητα ορίζεται σαν μια κατάσταση ολότητας του μηνύματος χωρίς τροποποιήσεις και αλλαγές, αυτό δε εξασφαλίζεται με χρήση ψηφιακής υπογραφής (βλέπε παρακάτω κεφάλαιο για τις ψηφιακές υπογραφές) [225]. Η υπευθυνότητα σημαίνει ότι ο συγγραφέας υπογράφοντας ψηφιακά , δεν μπορεί να αρνηθεί τη δημιουργία αυτού μεταγενέστερα, όπως επίσης και κανείς άλλος δεν μπορεί να διεκδικήσει την πατρότητα του μηνύματος. Υπάρχουν δύο βασικές μέθοδοι κρυπτογράφησης σε χρήση σήμερα: Κρυπτογραφία ιδιωτικού κλειδιού ή συμμετρική κρυπτογραφία (Symmetric Cryptography) και η Κρυπτογραφία δημόσιου κλειδιού (Public Key Cryptography) ή ασύμμετρη κρυπτογραφία (Asymmetric Cryptography).

3.9.1 **Συμμετρική κρυπτογραφία ή Κρυπτογραφία ιδιωτικού κλειδιού**

Είναι η παλαιότερη μέθοδος κρυπτογραφίας η οποία βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Αυτός ο τύπος είναι γνωστός και ως κρυπτογραφία ιδιωτικού κλειδιού ή μυστικού κλειδιού. Η διαδικασία (βλέπε σχήμα 27) της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ σε σχέση με την κρυπτογράφηση δημόσιου κλειδιού.



Σχήμα 27. Κρυπτογράφηση συμμετρικού Κλειδιού

Πηγή: http://el.wikipedia.org/wiki/Κρυπτογράφηση_Συμμετρικού_Κλειδιού E%AC%%8D

[225] Βλ. Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 200, σελ.191

Βασικό μειονέκτημα της συμμετρικής κρυπτογραφίας είναι ότι τα συμβαλλόμενα μέρη πρέπει να συμφωνούν κάθε φορά για το κλειδί και αυτή η διαδικασία πρέπει να γίνεται με μυστικό και ασφαλή τρόπο, ενώ αν κάποιος χρήστης επικοινωνεί με πολλούς άλλους χρήστες θα πρέπει κάθε φορά να θυμάται το σωστό κλειδί. Επίσης επειδή πάντα υπάρχει η πιθανότητα το ίδιο κλειδί να χρησιμοποιείται από διαφορετικούς χρήστες, δεν είναι πάντα ξεκάθαρο, το ποιός είναι ο αποστολέας του μηνύματος. Συγκεκριμένα σε κάποιο σύστημα που χρησιμοποιείται μόνο η κρυπτογράφηση ιδιωτικού κλειδιού, κάποιος που κατέχει το μυστικό κλειδί μπορεί να υποδυθεί την ταυτότητα οποιουδήποτε άλλου που κατέχει το ίδιο μυστικό κλειδί και μετά να ισχυριστεί ότι «το έκανε ο άλλος» και δεν υπάρχει τρόπος να αποδειχθεί το αντίθετο. Το πρόβλημα αυτό λύνεται μέσω των ψηφιακών υπογραφών που χρησιμοποιούν κρυπτογράφηση δημόσιου κλειδιού και ενσωματώνονται σε κάθε μήνυμα, επιβεβαιώνοντας την ταυτότητα του αποστολέα. Συνεπώς οι απαιτήσεις κατά τη χρήση ενός συμμετρικού αλγορίθμου κρυπτογράφησης απαιτούν τη χρήση ενός μυστικού κλειδιού το οποίο γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης, ύπαρξη ενός ασφαλούς καναλιού για τη διανομή του κλειδιού καθώς και χρήση του ίδιου αλγορίθμου από τα συναλλασσόμενα μέρη.

Γνωστοί αλγόριθμοι συμμετρικής κρυπτογραφία είναι ο Data Encryption Standard (*DES* 1988], ο Triple DES (*3DES*), ο Advanced Encryption Standard (*AES* 2001) , ο *RC2*,ο *RC4* , ο *IDEA*, ο *Camellia* και ο *Blowfish*[226].

3.9.2 **Ασύμμετρη κρυπτογραφία ή Κρυπτογραφία δημοσίου κλειδιού**

Η κρυπτογράφηση δημοσίου κλειδιού[227] (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και χρησιμοποιεί έναν διαφορετικό τρόπο διαχείρισης των κλειδιών κρυπτογράφησης, σε σχέση με την συμμετρική κρυπτογραφία που είδαμε προηγουμένως. Εδώ αποστολέας και ο παραλήπτης διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί 1024 bits αντίστοιχα το καθένα, τα οποία αναπαρίστανται ως μία ακολουθία αλφαριθμητικών χαρακτήρων. Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: Το ιδιωτικό κλειδί (private key) θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντίθετα το δημόσιο κλειδί (public key) θα πρέπει να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων

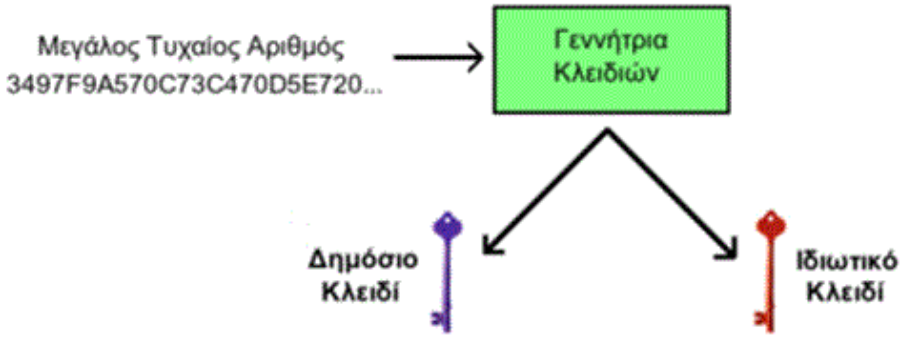
---

[226] Βλ. Δέσποινα Πολέμη, Σημειώσεις του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων, Πειραιάς, Μάρτιος 2007, σελ 8

[227] Οι αλγόριθμοι αυτοί ονομάζονται «δημόσιου κλειδιού» επειδή το κλειδί κρυπτογράφησης μπορεί να γίνει δημόσια γνωστό. Ο οποιοσδήποτε μπορεί να χρησιμοποιήσει αυτό το κλειδί κρυπτογραφώντας ένα κείμενο, αλλά μόνο το συγκεκριμένο άτομο που γνωρίζει το αντίστοιχο κλειδί αποκρυπτογράφησης μπορεί να διαβάσει το κείμενο.

βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης[228].

Κάθε χρήστης παράγει το δικό του ζεύγος κλειδιών (δημόσιο και ιδιωτικό κλειδί). Στη συνέχεια ανακοινώνει το δημόσιο κλειδί σε όλους τους χρήστες, οι οποίοι μπορούν να το χρησιμοποιήσουν για να του στείλουν κρυπτογραφημένα μηνύματα. Έτσι ο κάτοχος του δημόσιου κλειδιού μπορεί να στείλει μηνύματα μυστικά, αλλά μόνο ο δημιουργός του ζεύγους κλειδιών μπορεί να τα αποκρυπτογραφήσει (διαβάσει) αφού είναι ο μοναδικός κάτοχος του ιδιωτικού κλειδιού αποκρυπτογράφησης[229]. Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται σαν είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Όσο πιο τυχαίος είναι ο αριθμός που δίνεται σαν είσοδο στην γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται (βλέπε σχήμα 28) .



Σχήμα 28. Τρόπος λειτουργίας της γεννήτριας κλειδιών.

Πηγή: http://el.wikipedia.org/wiki/%CE%F%CF%8D

Χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού εξασφαλίζουμε ότι το κρυπτογραφημένο μήνυμα που θα στείλουμε σε έναν παραλήπτη θα είναι κατανοητό και αναγνώσιμο μόνο σε αυτόν και κανένα άλλο, δηλαδή έχουμε ***διασφάλιση της εμπιστευτικότητας*** (confidentiality) του μηνύματος. Για να επιτευχθεί αυτό, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στην συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Επειδή το ιδιωτικό κλειδί του παραλήπτη

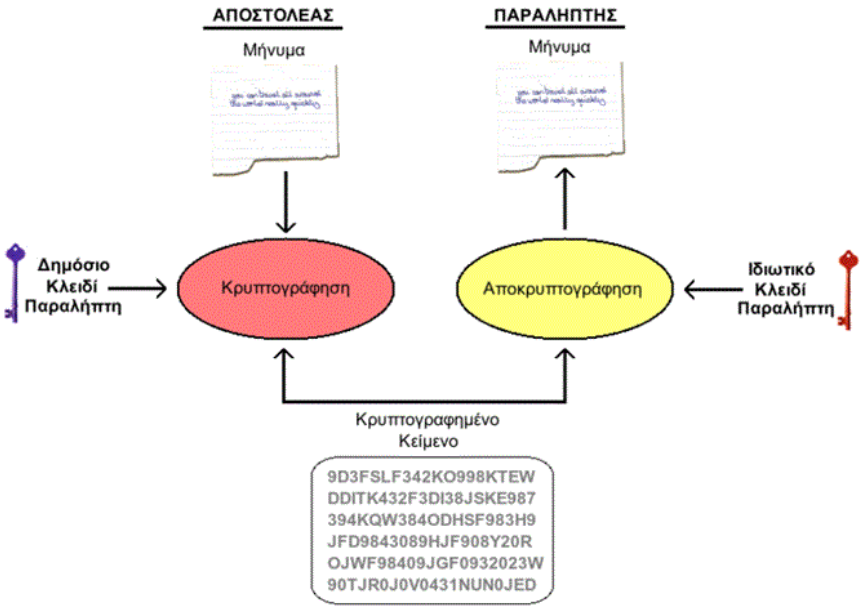
[228] Βλ. http://www.nonpaper.net/security/ssl_asymmetric.html

[229] Βλ. ό.π., Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 200, σελ.210

είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει και κανένας άλλος.

Η παραπάνω διαδικασία μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα. Το πρόβλημα υπάρχει τη στιγμή που ο αποστολέας δηλώσει ψευδή ταυτότητα με στόχο την παραπλάνηση του παραλήπτη, πιστεύοντας πως το συγκεκριμένο μήνυμα προήλθε από κάποιο άλλο πρόσωπο. Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί *πιστοποίηση* (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στην συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα[230].

Παρόλο που η παραπάνω μέθοδος εξασφαλίζει την πιστοποίηση της ταυτότητας του αποστολέα, δεν μπορεί από μόνη της , να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Και αυτό γιατί το μήνυμα μπορεί να το αποκρυπτογραφήσει ο κάτοχος του δημόσιου κλειδιού του αποστολέα. Με βάση όμως όσα έχουμε αναφέρει στις προηγούμενες παραγράφους, το δημόσιο κλειδί είναι γνωστό σε όλη την διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος**.**



Σχήμα 29. Κρυπτογράφηση με δημόσιο κλειδί

Πηγή: http://el.wikipedia.org/wiki/Κρυπτογράφηση_Δημόσιου_κλειδιού

[230] Βλ. ό.π., Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 200, σελ.211-212.

Προκειμένου να έχουμε διασφάλιση της εμπιστευτικότητας του μηνύματος και πιστοποίηση της ταυτότητας του αποστολέα, συνδυάζουμε τις δύο τεχνικές που παρουσιάστηκαν παραπάνω. Ο αποστολέας κρυπτογραφεί το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στην συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στην συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση). Έτσι, αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Στην πράξη βέβαια ο αποστολέας πρώτα υπογράφει ψηφιακά το μήνυμά του, κάνοντας χρήση της ψηφιακής υπογραφής του(την οποία θα δούμε αναλυτικά παρακάτω) και στην συνέχεια το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη[231].

Η κρυπτογράφηση δημόσιου κλειδιού είναι μια σύγχρονη ανακάλυψη και απαιτεί την χρήση μαθηματικών, χρησιμοποιείται δε συχνότερα για την δημιουργία ψηφιακών υπογραφών (digital signatures) σε δεδομένα, όπως το ηλεκτρονικό ταχυδρομείο (e-mail), για την πιστοποίηση της πηγής των δεδομένων και την ακεραιότητα αυτών. Ένας δημοφιλής αλγόριθμος κρυπτογραφίας δημοσίου κλειδιού είναι ο RSA[232], τον οποίον ανακάλυψαν ο R. Rivest, ο A. Shamir και ο L. Adleman. Άλλοι γνωστοί αλγόριθμοι είναι ο ElGamal, ο DSS και το κρυπτοσύστημα Paillier.

Το αρνητικό χαρακτηριστικό της κρυπτογραφίας δημοσίου κλειδιού είναι το αυξημένο υπολογιστικό κόστος της. Ακόμη και με σύγχρονους υπολογιστές, θεωρείται αργή λόγω των πολύπλοκων υπολογισμών που περιλαμβάνει. Γι' αυτό το λόγο, στην πράξη, αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού χρησιμοποιούνται μόνο για την κρυπτογράφηση περιορισμένου μεγέθους πληροφορίας, όπως για παράδειγμα ένα κλειδί συμμετρικού αλγορίθμου όπως ο DES ή ο 3DES. Το δεύτερο αυτό κλειδί χρησιμοποιείται με έναν αλγόριθμο συμμετρικής κρυπτογραφίας ο οποίος αναλαμβάνει να κρυπτογραφήσει μεγαλύτερους όγκους δεδομένων με πιο αποδοτικό τρόπο[233]. Έτσι οι δύο βασικές μέθοδοι κρυπτογραφίας που παρουσιάστηκαν χρησιμοποιούνται συμπληρωματικά, με την καθεμία να εκτελεί διαφορετικές λειτουργίες. Το πλεονέκτημα ταχύτητας της κρυπτογράφησης ιδιωτικού κλειδιού σημαίνει ότι χρησιμοποιείται για την κρυπτογράφηση του κύριου όγκου δεδομένων ενώ η κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιείται σε εφαρμογές που είναι λιγότερο απαιτητικές για του πόρους του υπολογιστικού συστήματος.

3.10 **Ψηφιακά πιστοποιητικά**

Στον αχανή κόσμο του Internet καθημερινά διακινείται μεταξύ των χρηστών τεράστιος όγκος πληροφοριών και δεδομένων, πολλές από τις οποίες χρειάζεται να προστατευθούν αλλά και να εξακριβωθεί η **πιστοποίηση της ταυτότητας του αποστολέα**. Πρόκειται για έναν παγκόσμιο

---

[231] βλέπε http://www.nonpaper.net/security/ssl_asymmetric.html

[232] Ο αλγόριθμος RSA θεωρείται από τους ασφαλέστερους αλγόριθμους παρά το γεγονός ότι έχει μελετηθεί όσο κανένας άλλος. Η ασφάλεια αυτή πηγάζει από το πρόβλημα της ανάλυσης ενός αριθμού σε γινόμενο πρώτων αριθμών για περαιτέρω μελέτη βλέπε Κ.Πατσάκη ,Ε.Φούντα, Κρυπτογραφία και εφαρμογές ,τόμος πρώτος, εκδόσεις Βαρβαρήγου, Πειραιάς 2009 ,σελ 314

[233] Βλ. Δ. Πολέμη ,Σημειώσεις του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων, Πειραιάς, Μάρτιος,2007,σελ.9

εικονικό κόσμο στον οποίο δεν βλέπουμε αυτούς με τους οποίους επικοινωνούμε παίρνοντας και δίνοντας πληροφορίες. Δεν βλέπουμε για παράδειγμα τον χρήστη στον οποίο στέλνουμε ένα e-mail, αλλά εμπιστευόμαστε ότι είναι αυτός που ισχυρίζεται ότι είναι. Στην περίπτωση όμως οικονομικών συναλλαγών η εμπιστοσύνη δεν είναι αρκετή. Στο δίκτυο μπορεί να υπάρχουν hackers, που μπορεί να κλέψουν τον αριθμό μιας πιστωτικής κάρτας ή που θα ήθελαν να μάθουν τα προσωπικά, επαγγελματικά ή οικονομικά μυστικά κάποιου. Κατά τον ίδιο τρόπο οι επιχειρήσεις (βλ. ηλεκτρονικό εμπόριο), πρέπει να γνωρίζουν ότι το πρόσωπο που στέλνει έναν αριθμό πιστωτικής κάρτας είναι πράγματι αυτός που δηλώνει ότι είναι και όχι ένας απατεώνας που κατόρθωσε να κλέψει τον αριθμό της πιστωτικής κάρτας κάποιου άλλου. Ο σημαντικότερος τρόπος αποφυγής του προαναφερθέντος προβλήματος είναι η **χρήση των ψηφιακών πιστοποιητικών** (digital certificates).

Τα ψηφιακά πιστοποιητικά είναι ηλεκτρονικά έγγραφα, ένα είδος ηλεκτρονικής ταυτότητας, που χρησιμοποιούνται για την αναγνώριση μιας οντότητας και την συσχέτισή της με ένα δημόσιο κλειδί[234].Χρησιμοποιούνται για να πιστοποιήσουν ότι το άτομο που στέλνει πληροφορίες (π.χ έναν αριθμό πιστωτικής κάρτας ή ένα μήνυμα στο Internet) είναι πραγματικά αυτό που δηλώνει ότι είναι, καθώς η Αρχή Πιστοποίησης (ΑΠ) που τα εκδίδει εγγυάται την **εγκυρότητα των στοιχείων του κατόχου τους**. Τα πιστοποιητικά τοποθετούν τις πληροφορίες στον σκληρό δίσκο του χρήστη και χρησιμοποιούν τεχνολογία απόκρυψης για να δημιουργήσουν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη. Όταν κάποιος που διαθέτει ένα ψηφιακό πιστοποιητικό επισκεφθεί κάποιο site ή στείλει e-mail το πιστοποιητικό αυτό παρουσιάζεται στο site ή επισυνάπτεται στο e-mail και πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Τα ψηφιακά πιστοποιητικά είναι αρκετά ασφαλή επειδή χρησιμοποιούν πανίσχυρη τεχνολογία απόκρυψης. Στην πραγματικότητα είναι πιο ασφαλή ακόμη και από τις υπογραφές. Τα ψηφιακά πιστοποιητικά εκδίδονται έναντι χρεώσεως από ιδιωτικές εταιρίες που ονομάζονται Digital Authorities. Μία τέτοια εταιρία είναι η πολύ γνωστή VeriSign[235].

Υπάρχουν διάφοροι τύποι ψηφιακών πιστοποιητικών. Αναφέρουμε κάποια που χρησιμοποιούνται στο Internet[236]:

- **Προσωπικά πιστοποιητικά**: Αυτά τα πιστοποιητικά προσδιορίζουν άτομα. Μπορεί να χρησιμοποιηθούν για έλεγχο ταυτότητας χρηστών με ένα διακομιστή ή για την ενεργοποίηση της ασφάλειας σε μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας S Mime.

- **Πιστοποιητικά διακομιστή**: Τα πιστοποιητικά διακομιστή προσδιορίζουν τους διακομιστές που συμμετέχουν σε ασφαλείς επικοινωνίες με άλλους υπολογιστές, χρησιμοποιώντας πρωτόκολλα επικοινωνίας, όπως το SSL. Τα πιστοποιητικά αυτά επιτρέπουν σε ένα διακομιστή να επιβεβαιώσει την ταυτότητά του σε υπολογιστές-πελάτες.

---

[234] Βλ. ό.π., Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 200, σελ.219.

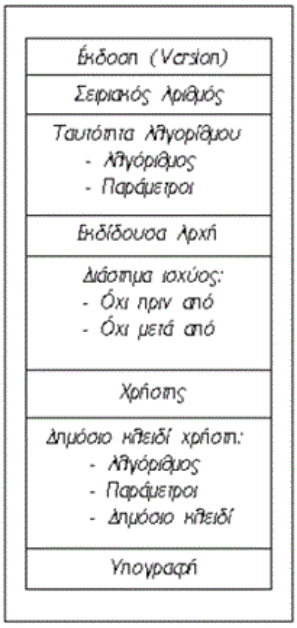
[235] Βλ. http://www.e-papadakis.gr/ola18.htm

[236] Βλ. http://support.microsoft.com/kb/195724/el

☞ **Πιστοποιητικά εκδότη λογισμικού**: Αυτά τα πιστοποιητικά χρησιμοποιούνται για την πιστοποίηση της υπογραφής του εκδότη του λογισμικού που διανέμεται μέσω του Internet[237].

☞ **Πιστοποιητικό έκδοσης πιστοποιητικών**: Το πιστοποιητικό έκδοσης πιστοποιητικών αναφέρεται στην αρχή που το εκδίδει η οποία μπορεί να είναι αρχή έκδοσης πιστοποιητικών ρίζας (VeriSign) , ή ενδιάμεση αρχή έκδοσης πιστοποιητικών. Αρχές έκδοσης πιστοποιητικών ρίζας έχουν τη δυνατότητα να αντιστοιχίσουν πιστοποιητικά για ενδιάμεσες αρχές έκδοσης πιστοποιητικών. Μια ενδιάμεση αρχή πιστοποίησης έχει τη δυνατότητα να εκδώσει πιστοποιητικά διακομιστή, προσωπικά πιστοποιητικά, publisher πιστοποιητικά ή πιστοποιητικά για άλλες ενδιάμεσες αρχές έκδοσης πιστοποιητικών.

Τα ψηφιακά πιστοποιητικά περιλαμβάνουν διάφορες πληροφορίες όπως το όνομα του χρήστη, το όνομα της εταιρίας που το εκδίδει, έναν σειριακό αριθμό και άλλες παρόμοιες πληροφορίες. Οι πληροφορίες έχουν κωδικοποιηθεί μ' έναν τρόπο που τις κάνει μοναδικές για τον κάθε χρήστη. Όπως στα περισσότερα πράγματα στο Internet έτσι και στην περίπτωση των ψηφιακών πιστοποιητικών υπάρχει ένα πρότυπο που επικρατεί και είναι γνωστό με την ονομασία X.509, (βλέπε σχήμα 30) **.**



Σχήμα 30.Ένα πιστοποιητικό X.509.

Πηγή: Ε. Μπόζιος , Σημειώσεις ασφάλειας πληροφοριακών συστημάτων, Θεσσαλονίκη 2004, σελ 255.

[237] Για να προβάλετε μια λίστα με αξιόπιστους εκδότες λογισμικού στον Internet Explorer, κάντε κλικ στην εντολή " Επιλογές Internet " από το μενού Εργαλεία , κάντε κλικ στην καρτέλα " περιεχόμενο " και στη συνέχεια κάντε κλικ στο κουμπί εκδότες. Μπορείτε επίσης να καταργήσετε αξιόπιστους εκδότες, κάνοντας κλικ στο κουμπί Κατάργηση σε αυτήν την οθόνη, βλ. http://support.microsoft.com/kb/195724/el

Το πεδίο έκδοσης καθορίζει την μορφή του πιστοποιητικού. Ο σειριακός αριθμός είναι μοναδικός για την ΑΠ (κάτι σαν αύξων αριθμός). Το επόμενο πεδίο καθορίζει τον αλγόριθμο που χρησιμοποιήθηκε για την υπογραφή του πιστοποιητικού, μαζί με οποιεσδήποτε αναγκαίες παραμέτρους. Ο εκδότης είναι το όνομα της ΑΠ. Η διάρκεια ισχύος είναι ένα ζευγάρι αριθμών· το πιστοποιητικό είναι έγκυρο για το χρονικό διάστημα ανάμεσα στις δύο τιμές. Το πεδίο χρήστης είναι το όνομα του χρήστη. Αμέσως μετά περιλαμβάνονται πληροφορίες για το δημόσιο κλειδί του χρήστη, που περιλαμβάνουν το όνομα του αλγόριθμου, αναγκαίες παραμέτρους και το ίδιο το δημόσιο κλειδί. Το τελευταίο πεδίο είναι η υπογραφή της Αρχής[238].

3.11 **Ψηφιακές υπογραφές**

Οι ψηφιακές υπογραφές ή ηλεκτρονικές υπογραφές (όπως είδαμε σε προηγούμενη ενότητα) χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης έχει στη διάθεσή του δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν μεταξύ τους μαθηματική σχέση. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Έτσι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Με την ψηφιακή υπογραφή έχουμε εξασφάλιση της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου και πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον δημιουργό του (αποστολέα) που το υπέγραψε ηλεκτρονικά[239].

Κατά τη δημιουργία και επαλήθευση της ψηφιακής υπογραφής χρησιμοποιείται η συνάρτηση κατακερματισμού (one way hash), η οποία δημιουργεί σε ένα μήνυμα ανεξάρτητα από το μέγεθός του, **μια σύνοψη** η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη αυτή είναι μία ψηφιακή αναπαράσταση του μηνύματος και αντιπροσωπεύει αυτό με μοναδικό τρόπο. Η συνάρτηση κατακερματισμού είναι μονόδρομη γιατί από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι πολύ μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του, ενώ είναι πρακτικά αδύνατο δύο διαφορετικά μηνύματα να δώσουν την ίδια σύνοψη. Η μεγάλη αυτή ευαισθησία στα δεδομένα εισόδου αποτελεί μια από τις πολυτιμότερες ιδιότητες (δυνατότητες) των συναρτήσεων hash Οποιαδήποτε αλλαγή (έστω και μικρή) σε ένα μήνυμα έχει σαν αποτέλεσμα να δημιουργείται διαφορετική σύνοψη[240].

Ο αποστολέας χρήστης στη συνέχεια κρυπτογραφεί μετά με το ιδιωτικό του κλειδί τη σύνοψη που έχει δημιουργηθεί. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο αρχικό κείμενο και μεταδίδεται μαζί του, χωρίς να είναι απαραίτητη και η κρυπτογράφηση του αρχικού κειμένου. Στη λήψη, ο παραλήπτης αποσπά από το μήνυμα την

---

[238] Βλ. Ε. Μπόζιος , Σημειώσεις ασφάλειας πληροφοριακών συστημάτων, Θεσσαλονίκη 2004, σελ 255

[239] Βλ. http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#3

[240] Βλ.ό.π., http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cryptography-DigitalSignature.html

κρυπτογραφημένη σύνοψη και εφαρμόζει στο κανονικό κείμενο τον ίδιο αλγόριθμο κατακερματισμού, ώστε να δημιουργήσει μια δική του σύνοψη. Μετά αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα την κρυπτογραφημένη σύνοψη του μηνύματος και συγκρίνει τις δύο συνόψεις. Αν οι δύο αυτές συνόψεις βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο, ενώ αν βρεθούν διαφορετικές, θα σημαίνει ότι το μήνυμα αλλοιώθηκε κατά τη μετάδοσή του. Η ψηφιακή υπογραφή, στην ουσία είναι η κρυπτογραφημένη σύνοψη με το ιδιωτικό κλειδί του αποστολέα. Έτσι η ψηφιακή υπογραφή είναι διαφορετική για κάθε μήνυμα σε αντίθεση με την ιδιόχειρη υπογραφή [241].

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος. Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί)[242].

Η σπουδαιότητα της ηλεκτρονικής υπογραφής έγκειται πέραν της ειδικής της λειτουργίας, στην ενθάρρυνση του ηλεκτρονικού εμπορίου, αλλά και στο γεγονός ότι διασφαλίζει το ηλεκτρονικό έγγραφο στο οποίο έχει τεθεί και πιστοποιεί για την γνησιότητά του[243]. Τα είδη των ηλεκτρονικών υπογραφών, σύμφωνα με το νομοθετικό πλαίσιο (ΠΔ.150/2001 σε προσαρμογή της Οδηγίας 99/93/ΕΚ) είναι η ηλεκτρονική υπογραφή και η προηγμένη ηλεκτρονική υπογραφή. Έτσι ως «ηλεκτρονική υπογραφή» θεωρούνται δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα και χρησιμεύουν για την απόδειξη της γνησιότητας αυτών. Ενώ «προηγμένη ηλεκτρονική υπογραφή» είναι η ψηφιακή υπογραφή που πρέπει να πληροί τους όρους: α) Συνδέεται μονοσήμαντα με τον υπογράφοντα και μπορεί να καθορίσει την ταυτότητα του. β) δημιουργείται με μέσα τα οποία ο υπογράφων διατηρεί στον αποκλειστικό του έλεγχο γ) συνδέεται με τα δεδομένα με τέτοιο τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων[244].

Δημιουργία και επαλήθευση ψηφιακής υπογραφής

Η χρήση της ψηφιακής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της ψηφιακής υπογραφής και μετά την επαλήθευσή της. Στη συνέχεια περιγράφονται οι ενέργειες των οντοτήτων που βρίσκονται σε επικοινωνία (Αποστολέας-Παραλήπτης), προκειμένου να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

---

[241] Βλ.ό.π., http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cryptography-DigitalSignature.html

[242] Βλ Σ. Γκρίτζαλη , Σ.Κάτσικα, Δ. Γκρίτζαλη, Ασφάλεια Δικτύων Υπολογιστών, Αθήνα,2003,Παπασωτηρίου, σελ 136-138. βλέπε επίσης
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#5

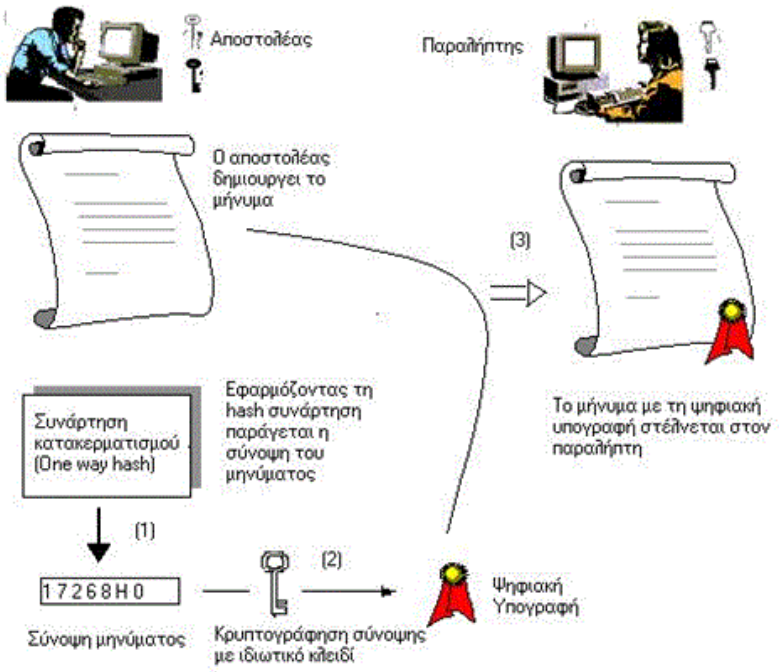
[243] Βλ Ιγγλεζάκης Ι. Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη 2003, σελ.624.

Αποστολέας

☞ Ο αποστολέας χρήστης χρησιμοποιώντας κάποια συνάρτηση κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Η σύνοψη αυτή δημιουργείται ανεξάρτητα από το μέγεθος του μηνύματος και αποτελείται από μία συγκεκριμένου μήκους σειρά ψηφίων(bits).

☞ Στη συνέχεια ο αποστολέας κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί. Αυτό που παράγεται είναι η ψηφιακή υπογραφή.

☞ Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου στον παραλήπτη, βλ.σχήμα 31.



Σχήμα 31 . Δημιουργία ψηφιακής υπογραφής

πηγή:http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#5

[244] Βλ άρθ. 2 ΠΔ.150/2001 στο: http://nomothesia.ependyseis.gr/eu-law/getFile/%CE%A0%CE%94+150+2001.pdf?bodyId=481283

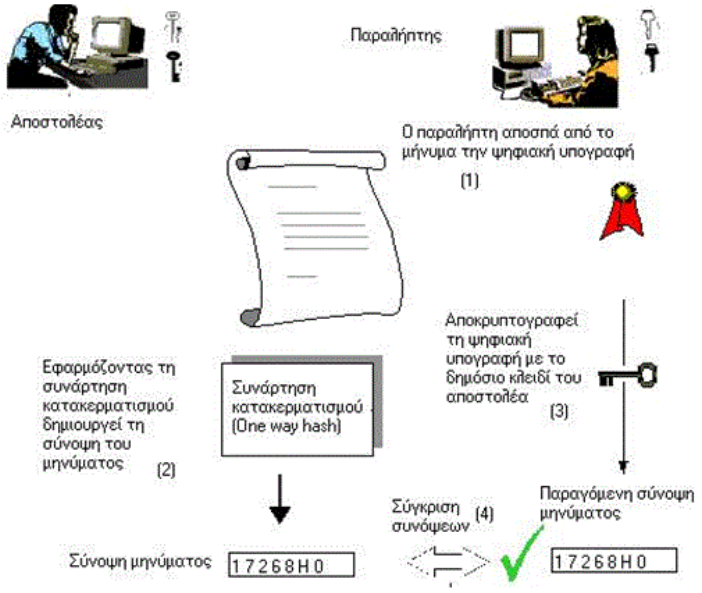
Παραλήπτης

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

☞ Μετά εφαρμόζει στο μήνυμα που έλαβε την ίδια συνάρτηση κατακερματισμού (one way hash) και δημιουργεί τη σύνοψη του μηνύματος (message digest).

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

☞ Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Στην περίπτωση που το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί, βλέπε σχήμα 32.



Σχήμα 32. Επαλήθευση ψηφιακής υπογραφής
πηγή:http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#5

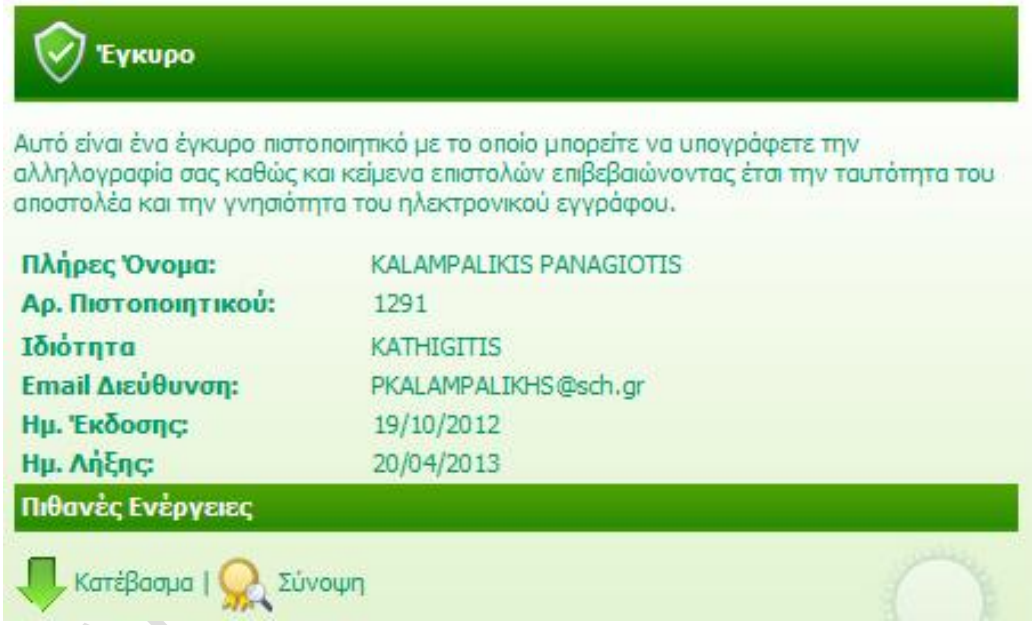
3.11.1 **Ψηφιακή υπογραφή εγγράφων** pdf **–μελέτη περίπτωσης**

Η επικύρωση ψηφιακών εγγράφων αποτελεί μία νέα διαδικασία που πλέον είναι εφικτή και ολοκληρώνεται με την χρήση του ελεύθερου λογισμικού **Sinadura**. Για την υπογραφή ψηφιακών κειμένων PDF είναι αναγκαία η εγκατάσταση του προγράμματος Sinadura, το οποίο διατίθεται ελεύθερα και μπορούμε να το κατεβάσουμε από τη διεύθυνση:

https://ca.sch.gr/download/sch_sign.exe

Εγκατάσταση Sinadura. Αφού κάνουμε λήψη του προγράμματος εγκαθιστούμε αυτό στο σκληρό δίσκο σε κοινό φάκελο και όχι στο program files[245]. Τελειώνοντας την εγκατάσταση πηγαίνουμε να κάνουμε ρυθμίσεις στο πρόγραμμα. Οι ρυθμίσεις όμως απαιτούν δημιουργία πιστοποιητικού ασφαλείας.

Δημιουργία πιστοποιητικού ψηφιακής υπογραφής .Είναι απαραίτητο στις ρυθμίσεις του Sinadura να έχει δημιουργηθεί ένα ψηφιακό πιστοποιητικό για την επικύρωση των αρχείων μας. Για να μπορέσουμε να το δημιουργήσουμε πηγαίνουμε στη διεύθυνση https://ca.sch.gr/index.php του πανελλήνιου σχολικού δικτύου και κάνουμε σύνδεση με τα στοιχεία του λογαριασμού μας στην υπηρεσία[246].Στη συνέχεια πατάμε Δημιουργία πιστοποιητικού , μετά επόμενο επιλέγουμε χρήση προσωπικού υπολογιστή, μετά επιβεβαιώνουμε τα στοιχεία μας και πατάμε επόμενο, στη συνέχεια βλέπουμε την διάρκεια ισχύος του πιστοποιητικού (6 μήνες) και βάζουμε το μέγεθος του κλειδιού (2048 Υψηλού επιπέδου).Ολοκληρώνοντας έχουμε την δημιουργία του ψηφιακού πιστοποιητικού το οποίο κατεβάζουμε στον υπολογιστή μας, βλ εικόνα 6.



Εικόνα 6. Δημιουργία πιστοποιητικού ψηφιακής υπογραφής

Ρυθμίσεις λογισμικού Sinadura. Η διαδικασία της ψηφιακής υπογραφής εγγράφου pdf απαιτεί την ρύθμιση του Sinadura. Αρχικά όταν εισερχόμαστε στο περιβάλλον του προγράμματος

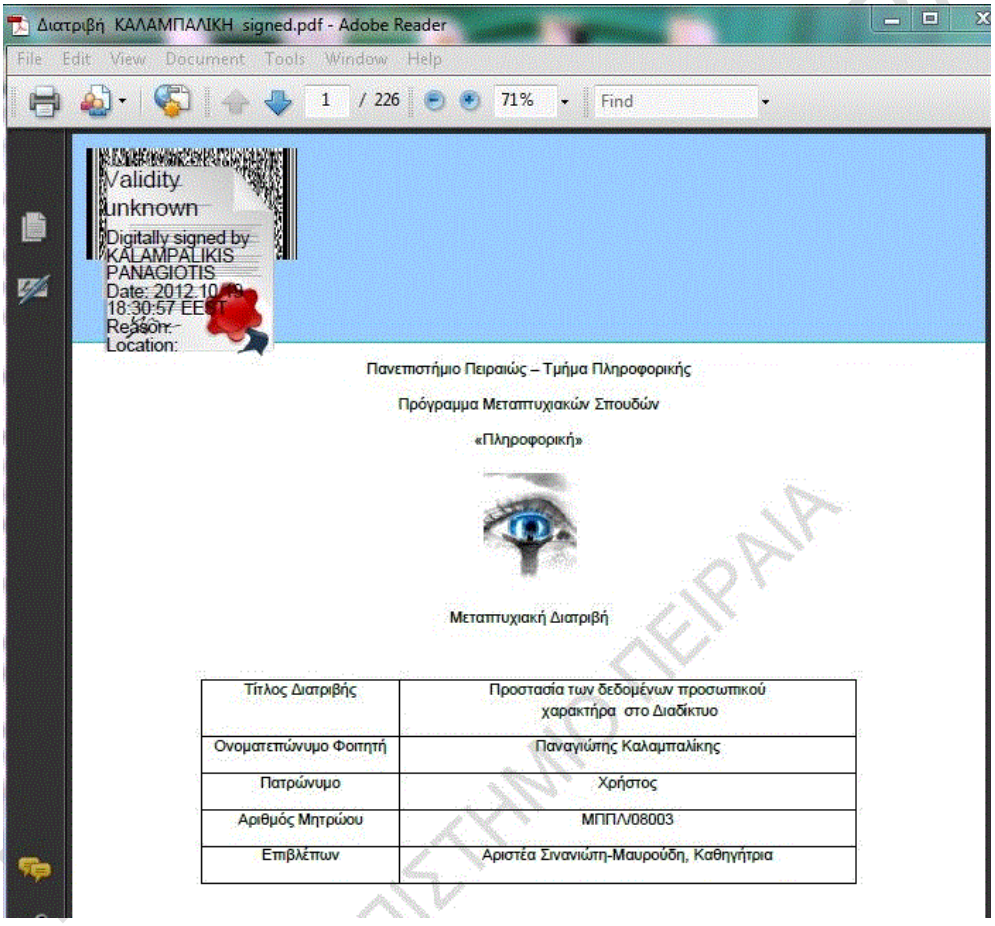
[245] Διαπιστώθηκε ότι το συγκεκριμένο λογισμικό δεν εκτελείται όταν ο χρήστης των Windows έχει ιδιότητα διαχειριστή (administrator) και ταυτόχρονα δεν έχει πρόσβαση σε περιορισμένους φακέλους όταν το τρέχει από λογαριασμό κοινού χρήστη . Για το λόγο αυτό έγινε απεγκατάσταση και επανεγκατάσταση του προγράμματος σε κοινό φάκελο (C:Sinadura) επειδή προηγουμένως ήταν εγκατεστημένο στο Program Files.

[246] Η είσοδος γίνεται πατώντας στην υπερσύνδεση «Συνδεθείτε στην υπηρεσία» και απαιτούνται όνομα χρήστη και κωδικό, που δίνονται στα μέλη του Πανελλήνιου Σχολικού Δικτύου.

πρέπει να εισάγουμε έναν κωδικό. Στην συνέχεια επιλέγουμε την διαμόρφωση του Sinadura ώστε να εισάγουμε το ψηφιακό πιστοποιητικό και να επικυρώσουμε τα αρχεία μας.

Έτσι επιλέγουμε Tools \ Personal Configuration\sign και κάνουμε κλικ στις επιλογές : Add PDF417, Add sign stamp, Send email, visible sign και πατάμε Apply OK.Στη συνέχεια πηγαίνουμε Certificates management, πατάμε Add και βάζουμε όνομα cert 1, επιλογή αποθηκευμένου πιστοποιητικού (με κατάληξη αρχείου .p12 που δημιουργήσαμε πριν και κατεβάσαμε στον υπολογιστή μας) ,εισαγωγή του κωδικού που δηλώθηκε όταν αποθηκεύσαμε το πιστοποιητικό , μετά Type PKCS12 και τέλος OK.

Εφόσον ολοκληρωθούν με επιτυχία οι παραπάνω ενέργειες, μπορούμε να υπογράψουμε οποιοδήποτε έγγραφο pdf αρκεί να το προσθέσουμε στο πρόγραμμα Sinadura και να επιλέξουμε Sign Files όπως , Add files , μετά επιλογή pdf αρχείου από υπολογιστή ,μετά Sign files, βλ εικόνα 7

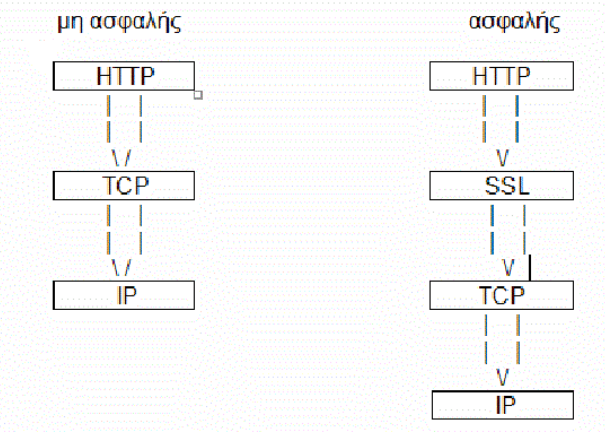


Εικόνα 7. Επικύρωση ψηφιακού εγγράφου

Έτσι έχουμε την δυνατότητα να επικυρώσουμε όσα ψηφιακά έγγραφα επιθυμούμε αλλά και να έχουμε εύκολα πρόσβαση σε αυτά καθώς αποθηκεύονται αυτόματα στον κατάλογο του λογισμικού Sinadura που δημιουργήθηκε κατά την εγκατάσταση και συγκεκριμένα στον φάκελο My Signed Documents.

3.12 **Πρωτόκολλο** Secure Socket Layer (SSL)

Το πρωτόκολλο SSL[247] αναπτύχθηκε από την Netscape Communications Corporation σε συνεργασία με την RSA Data Security Inc, για την ασφαλή μετάδοση και επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών, για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου. Το πρωτόκολλο SSL βασίζεται σε κρυπτογραφικές τεχνικές Δημόσιου Κλειδιού και ιδιωτικού κλειδιού(βλέπε προηγούμενα κεφάλαια).Σκοπός του είναι η προστασία (ενθυλάκωση) πρωτοκόλλων υψηλότερου επιπέδου και η δημιουργία ενός ιδιωτικού καναλιού μεταξύ των εφαρμογών επικοινωνίας, το οποίο να εξασφαλίζει τη μυστικότητα των δεδομένων, την αυθεντικοποίηση των εμπλεκόμενων μερών και την ακεραιότητα[248]. Χρησιμοποιείται ευρέως σε Ενδοδίκτυα (intranets) αλλά και στο Internet, κυρίως σε συναλλαγές ηλεκτρονικού εμπορίου. Η τελευταία έκδοση αποτέλεσε τη βάση για την ανάπτυξη ενός άλλου πρωτοκόλλου του TLS (Transport Layer Security) που διαδέχθηκε το Secure Sockets Layer (SSL) και χρησιμοποιείται σε τραπεζικές συναλλαγές μέσω internet. Το TLS (Transport Layer Security) είναι ένα πρωτόκολλο που εγγυάται ότι κατά την επικοινωνία εξυπηρέτη - πελάτη (server -client) μέσω του Διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος τρίτος που θα "υποκλέψει" το περιεχόμενο της επικοινωνίας. Κάνοντας χρήση του πρωτοκόλλου SSL επιτυγχάνουμε μια ασφαλή σύνδεση μεταξύ του πελάτη και του εξυπηρετητή. Οι διευθύνσεις ιστού που διασφαλίζονται με SSL ξεκινούν με https: (https://ebank.emporiki.gr/EMPB_EBANKWeb/transactions/login/Index.jsp) αντί για http: που υπάρχει στις μη ασφαλείς ιστοσελίδες (βλέπε σχήμα 33).



Σχήμα 33. Το πρωτόκολλο ασφαλείας SSL

Πηγή: Σημειώσεις του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων, Πειραιάς, Μάρτιος 2007, σελ 37

---

[247] Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0) και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή RFC (Request For Comments). Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Η παρούσα έκδοση του SSL, version 3.0, παρουσιάσθηκε στο κοινό στα τέλη του 1995, ενώ από τα μέσα του 1995 είχε αρχίσει να εφαρμόζεται σε προϊόντα της εταιρίας, όπως τον Netscape Navigator,βλ:

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ssl.htm

[248] Βλ. Πολέμη Δ., Σημειώσεις του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων, Πειραιάς, Μάρτιος 2007, σελ 36-42

Χρησιμοποιώντας το SSL, έχουμε πιστοποίηση του server από τον client και αντίστοιχη πιστοποίηση του client από τον server, καθώς επίσης εγκατάσταση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών. Οι αλγόριθμοι που χρησιμοποιούνται είναι οι εξής: *DES* (Data Encryption Standard), *DSA*(Digital Signature Algorithm, KEA(Key Exchange Algorithm, ένας αλγόριθμος που χρησιμοποιείται για την ανταλλαγή κλειδιών), MD5(Message Digest Algorithm, αλγόριθμος που αναπτύχθηκε από τον Rivest), *RC2 και RC4* ciphers κρυπτογράφησης του Rivest που αναπτύσσονται για την RSA Data Security, *RSA* (*τα αρχικά των ονομάτων που τον δημιούργησαν* Rivest, Shamir, και Adleman, *ένας* αλγόριθμος δημοσίου-κλειδιού που χρησιμοποιείται για κρυπτογράφηση και για αυθεντικοποίηση, *RSA Key-Exchange, ένας* αλγόριθμος ανταλλαγής-κλειδιών για τη SSL βασισμένος στον αλγόριθμο RSA, *SHA-1* (Secure Hash Algorithm ,συνάρτηση κατακερματισμού, SKIPJACK (ένας απόρρητος αλγόριθμος δημοσίου-κλειδιού που εφαρμόζεται στο FORTEZZA), Triple DES (DES που εφαρμόζεται τρεις φορές)[249].

3.12.1 **Αρχιτεκτονική του** SSL

Το πρωτόκολλο SSL έχει σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να εξασφαλίζει ασφάλεια στην επικοινωνία μεταξύ δύο οντοτήτων, από τα οποία η μία λειτουργεί σαν client και η άλλη σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, πιστοποίηση της ταυτότητας του server και της ταυτότητας του client[250], μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός[251].

Στην ιεραρχία των πρωτοκόλλων, το πρωτόκολλο SSL βρίσκεται ακριβώς επάνω από το *επίπεδο Μεταφοράς* TCP[252] και Δικτύου IP[253] και κάτω από το επίπεδο Εφαρμογής[254] βλέπε σχήμα 34.

---

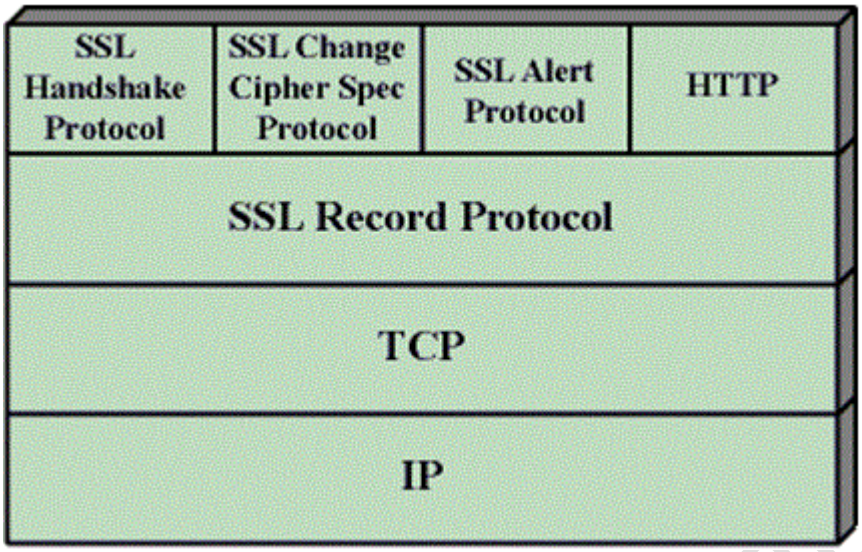
[249] Βλ. ό.π Δέσποινα Πολέμη, Σημειώσεις του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων, Πειραιάς, Μάρτιος 2007, σελ 36-42 βλ. επίσης http://el.wikipedia.org/wiki/SSL

[250] Η έκδοση ssl 2.0 υποστηρίζει μόνο αυθεντικοποίηση server , ενώ η έκδοση ssl 3.0 παρέχει επιπλέον και αυθεντικοποίηση client, βλ. Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 2002, σελ 241.

[251] Βλ. ό,π. http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ssl.htm

[252] Το TCP (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς) είναι ένα από τα κυριότερα πρωτόκολλα Διαδικτύου και με αυτό εξασφαλίζεται η αξιόπιστη αποστολή και λήψη δεδομένων χωρίς λάθη και με τη σωστή σειρά μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) για περισσότερα βλέπε Andrew S. Tanenbaum, Δίκτυα υπολογιστών,τέταρτη αμερικάνικη έκδοση, εκδόσεις Κλειδάριθμος Αθήνα 2006, σελ 68.

[253] Το Πρωτόκολλο Διαδικτύου IP (Internet Protocol), αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το Διαδίκτυο με τη μετάδοση αυτοδύναμων πακέτων δεδομένων (datagrams).Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, για



Σχήμα 34. Η αρχιτεκτονική θέση του πρωτοκόλλου SSL

Πηγή : http://technet.microsoft.com/en-us/library/cc767139.aspx

Το πρωτόκολλο SSL όπως φαίνεται και στο σχήμα 34, περιέχει δύο υποεπίπεδα πρωτοκόλλων τα οποία περιλαμβάνουν:

Το Πρώτο επίπεδο το SSL Record Protocol, και το δεύτερο επίπεδο αποτελείται από το πρωτόκολλο χειραψίας (Handshake protocol), το πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας (change Cipher Spec Protocol) και το πρωτόκολλο προειδοποίησης (Alert Protocol)[255].

Πρωτόκολλο Εγγραφής SSL (SSL Record Protocol). Το Πρωτόκολλο Εγγραφής SSL σύμφωνα με το οποίο επιτρέπεται η ενθυλάκωση (προστασία) των πρωτοκόλλων υψηλότερου επιπέδου όπως του πρωτόκολλου χειραψίας, του SSL Alert πρωτοκόλλου και του HTTP. Το SSL Record Protocol αποτελεί τη βάση για ολόκληρη τη μεταφορά δεδομένων, οικοδομώντας τη διαδρομή δεδομένων μεταξύ αποστολέα και παραλήπτη. Επίσης πριν αποσταλούν τα δεδομένα κρυπτογραφεί τη διαδρομή τους , που ξεκινά όμως χωρίς κρυπτογράφηση.

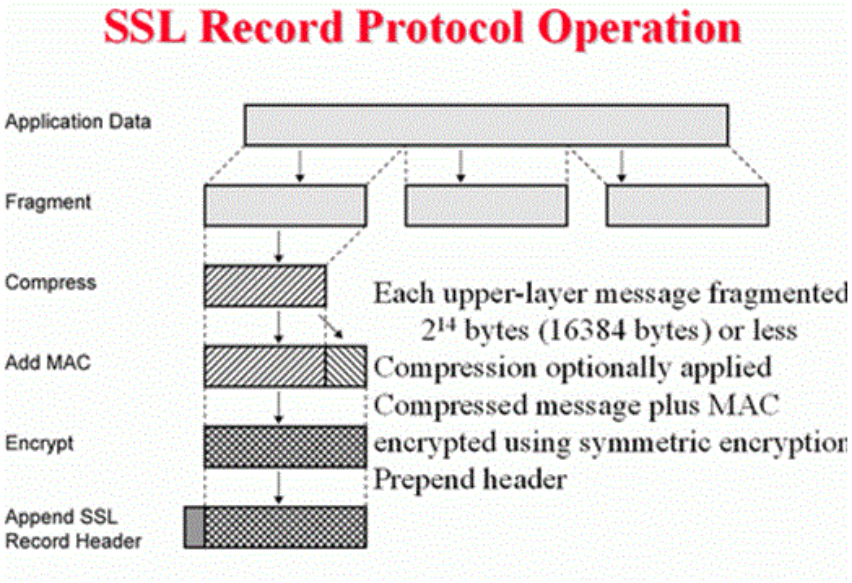
περισσότερα βλέπε Andrew S. Tanenbaum, Δίκτυα υπολογιστών, τέταρτη αμερικάνικη έκδοση, εκδόσεις Κλειδάριθμος Αθήνα 2006, σελ 504.

[254] Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν:Το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, http, η κύρια μέθοδος που χρησιμοποιούν τα πρωτόκολλα του Παγκοσμίου Ιστού για να μεταφέρουν δεδομένα ανάμεσα σε έναν διακομιστή (server) και ένα πελάτη (client), Το πρωτόκολλο Simple Mail Transfer Protocol (SMTP) για την μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου, Το File Transfer Protocol (FTP-Πρωτόκολλο Μεταφοράς Αρχείων), το Telnet (TELecommunication NETwork, είναι ένα πρωτόκολλο επικοινωνίας διασυνδεδεμένων σε δίκτυο υπολογιστών) κ.λ.π.

[255] Βλ Σ. Γκρίτζαλη,Σ.Κάτσικα, Δ. Γκρίτζαλη, Ασφάλεια Δικτύων Υπολογιστών, Αθήνα,2003,Παπασωτηρίου, σελ 465-466

Το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και ασχολείται με τον κατακερματισμό τη συμπίεση , την αυθεντικοποίηση και την κρυπτογράφηση των δεδομένων. Η λειτουργία του (αφορά την αποστολή δεδομένων) φαίνεται αναλυτικά στο σχήμα 35, όπου:

Στο πρώτο στάδιο γίνεται τμηματοποίηση των δεδομένων (fragmentation) και στο δεύτερο συμπίεση (compress). Στη συνέχεια στο τρίτο στάδιο εφαρμόζεται η τεχνική του Message Authentication Codes[256] (MAC), με τη χρήση ενός κλειδιού που διαμοιράζεται πάνω από τα συμπιεσμένα δεδομένα, ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Στο τέταρτο στάδιο έχουμε κρυπτογράφηση των παραπάνω με χρήση ιδιωτικού κλειδιού(συμμετρική κρυπτογράφηση) και τέλος προστίθεται μια επικεφαλίδα που περιέχει: την κύρια έκδοση, την δευτερεύουσα έκδοση, τον τύπο του περιεχομένου και το συμπιεσμένο μήκος. Με την ολοκλήρωση των παραπάνω έχουμε αποστολή του πακέτου. Η λειτουργία του SSL Record Protocol για τη λήψη δεδομένων, ακολουθεί αντίστροφη διαδικασία, δηλ πρώτα γίνεται η αποκρυπτογράφηση, μετά η επαλήθευση και η αποσυμπίεση και τέλος η συναρμολόγηση και η διανομή στους χρήστες ανωτέρων επιπέδων.



Σχήμα 35. Η λειτουργία του SSL Record Protocol

Πηγή: http://www.cse.wustl.edu/~jain/cse473-05/ftp/i_isec/sld010.htm

Πρωτόκολλο χειραψίας (Handshake protocol).Το Πρωτόκολλο χειραψίας το οποίο χρησιμοποιεί το Record πρωτόκολλο για την ανταλλαγή των μηνυμάτων μεταξύ του server και

[256] Ο Message Authentication Code (MAC), είναι ένας κώδικας (λέγεται και checksum) που πιστοποιεί την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος. Για την παραγωγή τους εφαρμόζεται στο μήνυμα ένας από τους τρόπους κρυπτογράφησης σε συνδυασμό με ένα μυστικό κλειδί, βλ: http://www.rsa.com/rsalabs/node.asp?id=2177

του client, στους οποίους έχει ενεργοποιηθεί το SSL και συνδέονται για πρώτη φορά. Με την εγκαθίδρυση της σύνδεσης, η ανταλλαγή αυτή των μηνυμάτων έχει σκοπό να ενεργοποιήσει τα ακόλουθα:

- Να επικυρώσει το διακομιστή(server) στον πελάτη(client)
- Να επιτρέψει στον client και στον server την κατάλληλη επιλογή κρυπτογραφικών αλγορίθμων που υποστηρίζουν.
- Να ταυτοποιήσει τον πελάτη με τον διακομιστή (προαιρετικά)
- Να δημιουργήσει κοινά μυστικά κλειδιά με χρήση κρυπτογράφησης δημόσιου κλειδιού
- Να δημιουργήσει μια κρυπτογραφημένη σύνδεση SSL[257].

Πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας (change Cipher Spec Protocol).Το πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας χρησιμοποιείται για την αλλαγή μιας προδιαγραφής κρυπτογραφίας σε μια άλλη. Κανονικά μια προδιαγραφή κρυπτογραφίας αλλάζει στο τέλος μιας SSL χειραψίας. Μπορεί όμως να τροποποιηθεί και σε οποιαδήποτε άλλη στιγμή. Είναι το απλούστερο από τα πιο πάνω πρωτόκολλα.

Πρωτόκολλο προειδοποίησης (Alert Protocol).Το Πρωτόκολλο προειδοποίησης (SSL Alert Protocol) χρησιμοποιείται για να μεταφέρει προειδοποιήσεις (alerts) στο χρήστη, μέσω του SSL Record Protocol. Οι προειδοποιήσεις αυτές είναι συνήθως μηνύματα προβλημάτων ή λαθών που αφορούν τη σύνδεση και τη μετάδοση μηνυμάτων μεταξύ δύο οντοτήτων. Έτσι ενημερώνεται ο χρήστης ώστε να κάνει τις απαραίτητες ενέργειες που απαιτούνται[258].

Με το πρωτόκολλο SSL έχουμε συνδυασμό της κρυπτογράφησης δημοσίου (ασύμμετρου) και ιδιωτικού (συμμετρικού) κλειδιού. Κάνοντας χρήση κρυπτογράφησης συμμετρικού κλειδιού πετυχαίνουμε ταχύτητα και απόδοση σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, με την οποία όμως εξασφαλίζουμε καλύτερη πιστοποίηση.

Ένα διαφορετικό κλειδί συνόδου (session key) χρησιμοποιείται σε κάθε σύνδεση πελάτη εξυπηρετητή. Αυτό το κλειδί κάθε συνόδου λήγει όταν περάσουν 24 ώρες. Το SSL χρησιμοποιεί την κρυπτογραφία δημοσίου κλειδιού για την ανταλλαγή αυτού του κλειδιού, καθώς και για την ταυτοποίηση των οντοτήτων που βρίσκονται σε συναλλαγή. Για την κρυπτογράφηση της συνόδου το SSL κάνει χρήση της συμμετρικής κρυπτογραφίας καθώς έχει μεγαλύτερη ταχύτητα[259]. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που

---

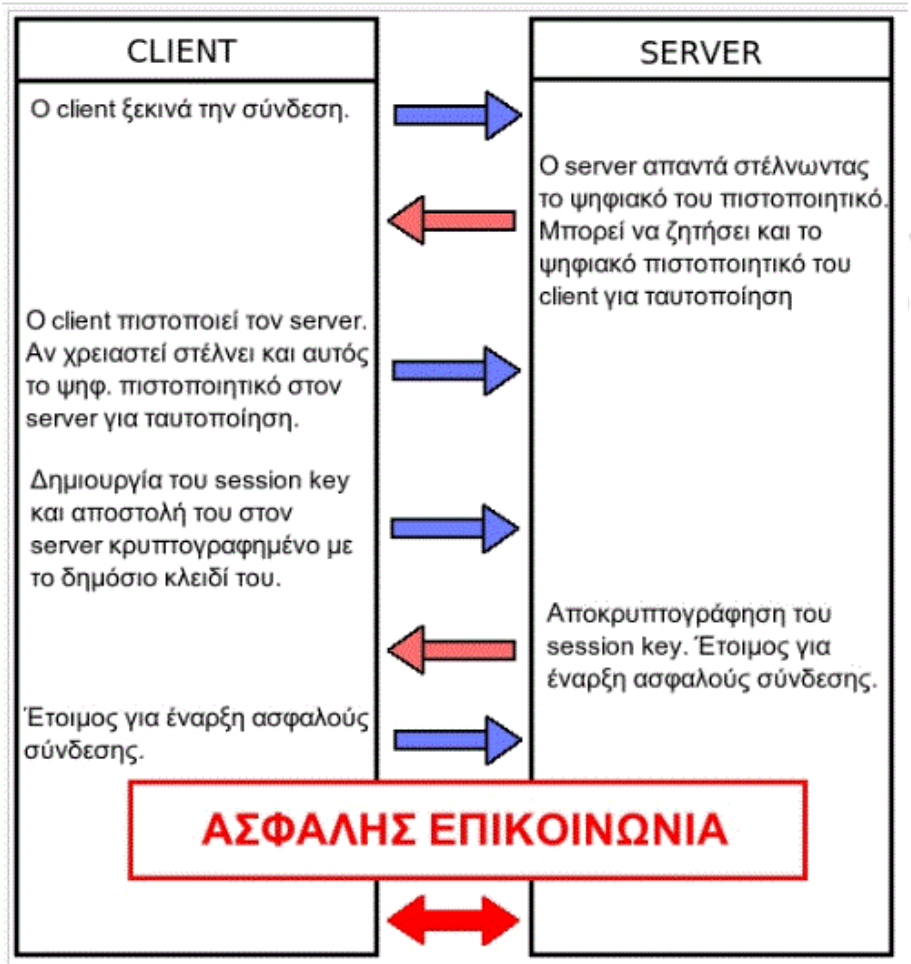
257 Βλ. άρθ.του John Michael Pierobon στο: http://www.pierobon.org/ssl/ch2/record.htm

258 Βλ. ό.π., άρθ.του John Michael Pierobon στο: http://www.pierobon.org/ssl/ch2/alert.htm

259 Βλ. ό.π., Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 200, σελ.241.

θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους [260].

Η διαδικασία της χειραψίας περιγράφεται στο παρακάτω σχήμα 36.



Σχήμα 36. Η διαδικασία της χειραψίας μεταξύ client και server σύμφωνα με το πρωτόκολλο SSL

Πηγή: http://el.wikipedia.org/wiki/SSL

Το πρωτόκολλο SSL βασίζεται στην ιδέα του ασφαλούς καναλιού επικοινωνίας. Είναι σχεδιασμένο για να παρέχει διαφανείς υπηρεσίες στο χρήστη. Ένας SSL Web server δέχεται μία αίτηση για «ασφαλή» σύνδεση (HTTPS) στη θύρα (port) 443, η οποία είναι διαφορετική από αυτήν των απλών αιτήσεων HTTP που χρησιμοποιούν την θύρα (port) 80. Το URL για συνδέσεις στην port 443 είναι της μορφής: https://www.google.gr. Όταν ο client συνδέεται σε αυτήν την θύρα, αρχικοποιεί τη σύνοδο SSL (βλέπε «χειραψία» - SSL handshake).Το SSL

[260] http://www.nonpaper.net/security/ssl_how.html

δημιουργεί μια σύνοδο κατά τη διάρκεια της οποίας το handshake χρειάζεται να πραγματοποιηθεί μόνο μια φορά. Όταν ολοκληρωθεί η χειραψία, η επικοινωνία κρυπτογραφείται και οι έλεγχοι ακεραιότητας εκτελούνται έως ότου εκπνεύσει η σύνοδος SSL.

Το πρωτόκολλο SSL παρέχει ασφάλεια TCP/IP έτσι ώστε:

- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού.
- Εξασφάλιση εμπιστευτικότητας των μεταδιδομένων μηνυμάτων, αφού η σύνδεση κρυπτογραφείται μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
- Προστασία της ακεραιότητας των μεταδιδομένων μηνυμάτων, καθώς τα μηνύματα αυθεντικοποιούνται και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs[261].

3.12.2 **Αντοχή του πρωτοκόλλου** ssl **σε επιθέσεις**

Στα χαρακτηριστικά του ssl αναφέρεται ιδιαίτερα η αντοχή του σε επιθέσεις κακόβουλων χρηστών. Ας δούμε την συμπεριφορά του ssl σε κάποιες από αυτές[262].

Επίθεση λεξικού (Dictionary Attack). Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος του μη κρυπτογραφημένου κειμένου βρεθεί σε κακόβουλο χρήστη. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα εξετάζεται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί. Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit.

Βίαιη επίθεση (Brute Force Attack). Η επίθεση αυτή πραγματοποιείται κάνοντας χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits δεν έχει αποτέλεσμα[263]. Μόνο ο DES 56 bit είναι ευαίσθητος σε αυτήν την επίθεση.

Επίθεση επανάληψης (Replay Attack). Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server (πελάτη και εξυπηρετητή) και προσπαθεί να χρησιμοποιήσει πάλι τα μηνύματα του πελάτη για να αποκτήσει πρόσβαση στον εξυπηρετητή, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του αναγνωριστικού σύνδεσης (connection-id), το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των

---

[261] Βλ Σ. Γκρίτζαλη,Σ.Κάτσικα, Δ. Γκρίτζαλη, Ασφάλεια Δικτύων Υπολογιστών, Αθήνα,2003,Παπασωτηρίου, σελ 459-461.

[262] Βλ: http://caclab.csd.auth.gr/SSL-SET1.pdf

[263] Τα 2^{128} κλειδιά που καλείται να υπολογίσει κάποιος επιτιθέμενος είναι απίστευτα μεγάλος αριθμός.

είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για επιπλέον ασφάλεια.

Επίθεση ενδιάμεσου (Man-In-The-Middle-Attack). Η επίθεση ενδιάμεσου συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τα τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Με τον ίδιο τρόπο λειτουργεί και για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.Το SSL όμως υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση δεν μπορεί να επιτευχθεί. Έτσι ο επιτιθέμενος δεν μπορεί να πείσει τον client ότι είναι ο server.

4 ΚΕΦΑΛΑΙΟ: Το νομοθετικό πλαίσιο

Η αλματώδης εξέλιξη της τεχνολογίας και του Διαδικτύου, σαν επακόλουθο της ραγδαίας ανάπτυξης της Πληροφορικής και των πληροφοριακών συστημάτων, με την ταυτόχρονη εξάπλωση σε παγκόσμιο επίπεδο του ηλεκτρονικού εμπορίου, την τεχνολογική πρόοδο των τηλεπικοινωνιών και των νέων τεχνολογιών, μέσα σε ένα διεθνές περιβάλλον παγκοσμιοποίησης, καθιστούν επιτακτική την δημιουργία κατάλληλου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων, αλλά και της ιδιωτικότητας του ατόμου-χρήστη των σύγχρονων αυτών τεχνολογιών[264].

4.1 Διεθνές δίκαιο

Η προστασία της προσωπικότητας και του ιδιωτικού βίου κατοχυρώνεται διεθνώς με μια πληθώρα διατάξεων, μεταξύ των οποίων διεθνείς Συμβάσεις, όπως:

- Η Οικουμενική Διακήρυξη των Δικαιωμάτων του ανθρώπου του ΟΗΕ (10.12.1948)[265].

- Η Σύμβαση της Ρώμης για την προάσπιση των δικαιωμάτων και των θεμελιωδών ελευθεριών του ατόμου - ΕΣΔΑ[266] (4.11.1950), με την οποία προβλέπεται η ανάγκη προστασίας της ιδιωτικότητας[267].

---

[264] Βλ. Σινανιώτη-Μαρούδη Αριστέα, Ιωάννης Δ. Φαρσαρώτας, Ηλεκτρονική τραπεζική , εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα 2005, σελ 367.

[265] Η Οικουμενική Διακήρυξη των Δικαιωμάτων του ανθρώπου, άρθρο 12 ρητά αναφέρει: «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους», στο: http://www.unric.org/el/index.php/human-rights-greek/18 .

[266] Η ΕΣΔΑ(Ευρωπαϊκή Σύμβαση Δικαιωμάτων του ανθρώπου), όπως διαφορετικά αναφέρεται η Σύμβαση της Ρώμης, ψηφίστηκε στις 4/11/1950 στην Ρώμη, κυρώθηκε στην Ελλάδα με το Ν.Δ. 53 της 19/20.9.1974, βλ Ν.Δ 53 στο: http://www.nis.gr/npimages/docs/ESDA.pdf (προσπελάστηκε στις 12/05/2010)

[267] Η Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ), στο άρθρο 8 αναφέρει: « Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν

● Το Διεθνές Σύμφωνο περί Ατομικών και Πολιτικών Δικαιωμάτων (ΔΣΑΠΔ) που υπογράφηκε στις 16.12.1966 στη Νέα Υόρκη[268] από τη Γενική Συνέλευση του ΟΗΕ με το οποίο προβλέπεται το απαραβίαστο της ιδιωτικής ζωής η ελευθερία της σκέψης, της συνείδησης και της θρησκείας και η ελευθερία της γνώμης και της έκφρασης[269]. Η Ελλάδα κύρωσε το παραπάνω ΔΣΑΠΔ με το Ν.2462/1997.

● Η Απόφαση 2450/19.12.1968 του ΟΗΕ για τα ανθρώπινα δικαιώματα και την ανάπτυξη της επιστήμης και της τεχνολογίας Η Απόφαση αυτή αναφέρεται στα προβλήματα που λαμβάνουν χώρα, από την ανάπτυξη της επιστήμης και της τεχνολογίας και μάλιστα από τη χρήση ηλεκτρονικών μέσων σε σχέση με τα ανθρώπινα δικαιώματα[270].

4.2 Η ευρωπαϊκή ένωση (Ε.Ε) και η προστασία των προσωπικών δεδομένων

Σε εναρμόνιση με το διεθνές δίκαιο έχουμε συμφωνίες –συμβάσεις[271] που έχουν λάβει χώρα στην ευρωπαϊκή ένωση όπως:

4.2.1 Η Σύμβαση 108 του Συμβουλίου της Ευρώπης

Η Ευρωπαϊκή Σύμβαση για την προστασία των ατόμων από την αυτόματη επεξεργασία των προσωπικών πληροφοριών, γνωστή και ως σύμβαση 108 του Συμβουλίου της Ευρώπης, υπογράφηκε στο Στρασβούργο στις 28/01/1981 και αναφέρεται σαν « Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα»[272], καθορίζει τις αρχές και τις διατάξεις για την προστασία του ατόμου από την επεξεργασία των προσωπικών του δεδομένων με αυτοματοποιημένο τρόπο, χρησιμοποιώντας ηλεκτρονικά μέσα.

δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημέριαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων», στο:

http://www.nis.gr/npimages/docs/ESDA.pdf (προσπελάστηκε στις 12/05/2010), βλ επίσης Α. Γέροντα, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Αθήνα-Κομοτηνή,2002,Σάκουλα,σελ102

[268] Η Ελλάδα κύρωσε το παραπάνω ΔΣΑΠΔ με το Ν. 2462/1997 (ΦΕΚ Α' 25/26.2.1997),βλ Ν.2462?1997 στο: http://www.nis.gr/npimages/docs/2462-97.pdf (προσπελάστηκε στις 12/05/2010)

[269] Το ΔΣΑΠΔ αναφέρει στο άρθρο 17: « Κανείς δεν υπόκειται σε αυθαίρετες ή παράνομες παρενοχλήσεις της ιδιωτικής του ζωής, της οικογένειας, της κατοικίας ή της αλληλογραφίας του, ούτε σε παράνομες προσβολές της τιμής και της υπόληψής του. Κάθε πρόσωπο έχει δικαίωμα προστασίας από το νόμο έναντι τέτοιων παρενοχλήσεων ή προσβολών», στο: http://www.nis.gr/npimages/docs/2462-97.pdf (προσπελάστηκε στις 12/05/2010).

[270] Βλ.Ελισάβετ Σαατζίδου-Παντελιάδου, Το παράδειγμα της νομικής ρύθμισης της Ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων , με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς στο: http://dspace.lib.uom.gr/bitstream/2159/371/5/saatzidou.pdf (προσπελάστηκε στις 12/05/2010).

[271] Στην Ευρώπη η πρώτη νομοθεσία για την προστασία των προσωπικών δεδομένων ήταν ο νόμος του γερμανικού κρατιδίου της Έσσης (Hessen) το 1970.Ακολούθησε η Σουηδία το 1973, η Ομοσπονδιακή Δημοκρατία της Γερμανίας το 1977, Η Αυστρία, η Γαλλία, η Δανία και η Νορβηγία το 1978, τα νομοθετήματα των οποίων αποκαλούνται «πρώτης γενεάς». Στη συνέχεια θεσπίστηκαν τη δεκαετία του 1980 τα νομοθετήματα «δεύτερης γενεάς»σε χώρες όπως η Μ. Βρετανία, Ιρλανδία, Ολλανδία, Βέλγιο, Ισπανία και Πορτογαλία, βλ Ι.Εγγλεζάκη , Το Δίκαιο της πληροφορικής σελ 221

[272] Βλ Σύμβαση στο: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Η Σύμβαση αυτή ήταν το πρώτο δεσμευτικό κείμενο που θέτει τις γενικές κατευθύνσεις για την προστασία κάθε φυσικού προσώπου από την αυθαίρετη επεξεργασία των προσωπικών του στοιχείων, η οποία γίνεται με τη βοήθεια αυτοματοποιημένων μέσων(μηχανικών και κυρίως ηλεκτρονικών),ιδρύοντας παράλληλα ένα ικανό πλέγμα εγγυήσεων και δικαιωμάτων υπέρ του παραπάνω προσώπου και προβλέποντας την δημιουργία Εθνικών Αρχών με αρμοδιότητες τον έλεγχο της εφαρμογής της Σύμβασης. Η αυτόματη επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται σύμφωνα με ορισμένες αρχές[273] και τα κράτη μέλη οφείλουν να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας για την προστασία των πληροφοριών προσωπικού χαρακτήρα[274]καθώς και κατοχύρωση των δικαιωμάτων του υποκειμένου. Ταυτόχρονα θέσπισε κανόνες για την προστασία των προσωπικών δεδομένων στην περίπτωση της διασυνοριακής ροής πληροφοριών.

Σύμφωνα με τη σύμβαση αυτή τα μέλη του Συμβουλίου της Ευρώπης πρέπει με την εσωτερική τους νομοθεσία να λάβουν όλα τα αναγκαία μέτρα για την υλοποίηση των κατευθυντήριων γραμμών που ορίζει η Σύμβαση, όπως το δικαίωμα πρόσβασης στο αρχείο πληροφοριών, δικαίωμα διόρθωσης πληροφοριών, ρύθμιση σκοπών αρχειοθέτησης κ.λπ. Τα κράτη μέλη επιχειρούν να συμβιβάσουν την ανάγκη σεβασμού της ιδιωτικής ζωής από την μια μεριά και την ελεύθερη κυκλοφορία των πληροφοριών από την άλλη.

Η Σύμβαση δεν ήταν άμεσης εφαρμογής . Η Ισχύς της στο εσωτερικό δίκαιο των συμβαλλομένων χωρών θα εξαρτιόταν από την κύρωσή της και τη θέσπιση εσωτερικών ρυθμίσεων και προσαρμογών[275].Η χώρα μας κύρωσε την παραπάνω Σύμβαση 108 με το Ν. 2068/1992 (ΦΕΚ Α' 118/9.7.1992) «Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα»[276] .

4.2.2 **Η Συμφωνία Σένγκεν**

Η Συμφωνία Σένγκεν υπογράφηκε στις 14/06/1985 στην πόλη Σένγκεν του Λουξεμβούργου ανάμεσα σε πέντε κράτη μέλη (Γερμανία, Βέλγιο, Γαλλία , Λουξεμβούργο και Κάτω Χώρες) και επικυρώθηκε στην πορεία από τις άλλες χώρες[277]. Είχε

---

[273] Οι προσωπικές πληροφορίες που υφίστανται αυτοματοποιημένη επεξεργασία πρέπει α. να έχουν αποκτηθεί με νόμιμο τρόπο β. να αποθηκεύονται μόνο για ορισμένους σκοπούς και να μην χρησιμοποιούνται κατά τρόπο που δεν συμβαδίζει με τους σκοπούς αυτούς γ. να είναι πρόσφορες και όχι υπέρμετρες σε σχέση με τους σκοπούς για τους οποίους έχουν καταχωρηθεί δ. να είναι ακριβείς και ενημερωμένες ε. να διατηρούνται σε τέτοια μορφή που να επιτρέπει την εξακρίβωση της ταυτότητας των προσώπων τα οποία αφορούν οι πληροφορίες, Βλ Α. Γέροντα, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Αθήνα-Κομοτηνή,2002,Σάκουλα,σελ 107-108.

[274] Βλ επίσης Α. Γέροντα, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Αθήνα-Κομοτηνή,2002,Σάκουλα,σελ106-110.

[275] Βλ Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Ζητήματα από το Δίκαιο της Πληροφορικής,2002, Σάκουλα σελ49.

[276] Βλ κύρωση της σύμβασης Ν. 2068/1992 στο: http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=Nh-i7eUlbMc%3d&tabid=132 (προσπελάστηκε 12/03 2011)

[277] Ο χώρος Σένγκεν επεκτάθηκε σιγά σε όλα σχεδόν τα κράτη μέλη. Η Ιταλία υπέγραψε τις συμφωνίες στις 27 Νοεμβρίου 1990, η Ισπανία και η Πορτογαλία στις 25 Ιουνίου 1991, η Ελλάδα στις 6 Νοεμβρίου 1992, η Αυστρία στις 28 Απριλίου 1995 και η Δανία, η Φινλανδία και η Σουηδία στις 19 Δεκεμβρίου 1996. Η Τσεχική Δημοκρατία, η Εσθονία, η Λεττονία, η Λιθουανία, η Ουγγαρία, η Μάλτα, Πολωνία, η Σλοβενία και η Σλοβακία εντάχθηκαν στις 21 Δεκεμβρίου 2007

ως στόχο την κατάργηση των ελέγχων στα σύνορα και την ελεύθερη κυκλοφορία για όλα τα πρόσωπα υπηκόους των κρατών που υπέγραψαν τη Συμφωνία καθώς και αστυνομική και δικαστική συνεργασία[278]. Αυτή η κατάργηση των ελέγχων είχε στόχο τη δημιουργία ενός συλλογικού συστήματος ελέγχων στα εξωτερικά σύνορα των χωρών που υπέγραψαν την συμφωνία, όπου μεταφερόταν το βάρος των σχετικών ελέγχων σε θέματα ασφάλειας, δημόσιας τάξης, λαθρεμπορίου ναρκωτικών όπλων, τελωνειακά, ελέγχου εισόδου και παραμονής αλλοδαπών. Προκειμένου να αντισταθμιστεί το έλλειμμα ασφάλειας που θα προέκυπτε από την ελεύθερη κυκλοφορία προσώπων και αγαθών στο εσωτερικό των χωρών, η Σύμβαση Εφαρμογής της Συμφωνίας Σένγκεν καθιερώνει τη δημιουργία του Συστήματος Πληροφοριών Σένγκεν (SIS), για τη διατήρηση της ασφάλειας στα κράτη μέλη. Το σύστημα στηρίζεται στη σύγχρονη τεχνολογία και πληροφορική, όπου λειτουργεί μια κοινή βάση δεδομένων , η οποία εμπλουτίζεται από τα εθνικά δεδομένα των κρατών μελών και την οποία χρησιμοποιούν όλα τα συμβαλλόμενα μέρη. Στο Σύστημα αυτό περιλαμβάνονται πλέον των άλλων , στοιχεία που αφορούν καταζητούμενα ή εξαφανισθέντα πρόσωπα, ανεπιθύμητους αλλοδαπούς, πρόσωπα που χρειάζονται προστασία (π.χ μάρτυρες σε δικαστικές υποθέσεις), κλεμμένα ή απολεσθέντα οχήματα, όπλα, τραπεζογραμμάτια, έγγραφα ταυτότητας, διαβατήρια[279].

Τα μέτρα που υιοθετήθηκαν από τα κράτη στο πλαίσιο της συνεργασίας Σένγκεν περιλαμβάνουν[280]:

- άρση των ελέγχων στα εσωτερικά σύνορα
- κοινή σειρά κανόνων που εφαρμόζονται σε άτομα που διασχίζουν τα εξωτερικά σύνορα των κρατών μελών της ΕΕ
- εναρμόνιση των κανόνων σχετικά με τους όρους εισόδου και θεώρησης διαβατηρίου για σύντομες διαμονές.
- ενισχυμένη αστυνομική συνεργασία (συμπεριλαμβανομένων των δικαιωμάτων διασυνοριακής παρακολούθησης και συνεχούς καταδίωξης)
- ενισχυμένη δικαστική συνεργασία μέσω ενός ταχύτερου συστήματος έκδοσης και καλύτερης μεταβίβασης της εκτέλεσης των κατασταλτικών δικαστικών αποφάσεων
- θέσπιση και ανάπτυξη του συστήματος πληροφόρησης Σένγκεν (SIS). Αυτό το Σύστημα στηρίζεται στη σύγχρονη τεχνολογία, εμπλουτίζεται από τα εθνικά δεδομένα των Συμβαλλομένων.

και η Ελβετία, συνδεδεμένη χώρα, στις 12 Δεκεμβρίου 2008. Η Βουλγαρία, η Κύπρος και η Ρουμανία δεν είναι ακόμη πλήρη μέλη του χώρου Σένγκεν. Οι έλεγχοι στα σύνορα μεταξύ των χωρών αυτών και του χώρου Σένγκεν διατηρούνται έως ότου το Συμβούλιο της ΕΕ αποφασίσει ότι πληρούνται οι όροι για την άρση των ελέγχων στα εσωτερικά σύνορα, βλ στο:
http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_el.htm

http://www.consilium.europa.eu/showPage.aspx?id=1157&lang=el

278 http://el.wikipedia.org/wiki/Συμφωνία Σένγκεν

279 Βλ Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Ζητήματα από το Δίκαιο της Πληροφορικής,2002, Σάκουλα σελ 51.

280 http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_el.htm

Η Σύμβαση Εφαρμογής προβλέπει επεξεργασία δεδομένων προσωπικού χαρακτήρα. Με την υπογραφή της, τα Συμβαλλόμενα Μέρη ανέλαβαν την υποχρέωση να θεσπίσουν την «αναγκαία εθνική νομοθεσία»[281] ώστε να εξασφαλιστεί ένα επίπεδο προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η Ελλάδα κύρωσε τη συμφωνία Σένγκεν με το ν. 2514/1997.

4.2.3 **Η οδηγία** 95/46/**ΕΚ**

Η Οδηγία 95/46/Ε.Κ.[282] του Ευρωπαϊκού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Στόχος της Οδηγίας είναι η ισοδύναμη προστασία (των δεδομένων) που θα προκύψει από την προσέγγιση των εθνικών νομοθεσιών και για το λόγο αυτό, τα κράτη μέλη δεν θα μπορούν πλέον να εμποδίζουν την μεταξύ τους ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα για λόγους προστασίας των δικαιωμάτων και ελευθεριών των φυσικών προσώπων και κυρίως της ιδιωτικής ζωής. Η υλοποίηση της ίσης προστασίας σε όλα τα κράτη-μέλη είναι ζωτικής σημασίας για την Εσωτερική Αγορά, γιατί έτσι εξασφαλίζεται η ελεύθερη κυκλοφορία εμπορευμάτων, προσώπων, υπηρεσιών και κεφαλαίων και γι αυτό απαιτείται όχι μόνο η δυνατότητα κυκλοφορίας των προσωπικών δεδομένων μεταξύ των κρατών-μελών αλλά και η προστασία των θεμελιωδών δικαιωμάτων του ατόμου. Οι ρυθμίσεις της οδηγίας επιδιώκουν ένα υψηλό επίπεδο προστασίας, παρέχοντας στον εθνικό νομοθέτη περιθώρια πρωτοβουλίας και προσαρμογής στις εθνικές ιδιομορφίες κάθε χώρας[283].

Άρα, στο πλαίσιο της Ε.Ε., η ρύθμιση της Οδηγίας αποτελεί το μέσο[284] για την ελεύθερη κυκλοφορία των προσωπικών δεδομένων μεταξύ των κρατών μελών, την προστασία του ανταγωνισμού και, περαιτέρω, την υλοποίηση της Εσωτερικής Αγοράς.

Με την παραπάνω κοινοτική οδηγία εναρμονίστηκε η χώρα μας θεσπίζοντας τον ν. 2472/1997, προσπαθώντας ο έλληνας νομοθέτης να συγκεράσει την ελεύθερη διακίνηση προσωπικών δεδομένων και την υπεράσπιση των δικαιωμάτων και της ιδιωτικής ζωής του έλληνα πολίτη.

---

[281] Βλ. άρθρο 126 παρ. 1 ν. 2514/1997, Βλ. επίσης Γέροντα Α., Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδόσεις Σάκουλα, Αθήνα 2002, σελ. 111.

[282] Για περισσότερη μελέτη βλ.το πλήρες κείμενο της οδηγίας 95/46/ΕΚ στην διεύθυνση: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/%CE%9F%CE%94%CE%97%CE%93%CE%8A%CE%91%2095-46.RTF

[283] Βλ Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Ζητήματα από το Δίκαιο της Πληροφορικής,2002, Σάκουλα σελ 52.

[284] Βλ. Ιγγλεζάκη Ι., ό.π., σελ. 173

4.2.4 **Η οδηγία** 97/66/**ΕΚ**

Η Οδηγία 97/66/Ε.Κ. της 15.12.1997 εξειδίκευσε και συμπλήρωσε την προγενέστερη της Οδηγία 95/46/ΕΚ, συμπεριλαμβάνοντας στο προστατευτικό πεδίο της και διατάξεις για την προστασία όχι μόνο των φυσικών προσώπων αλλά και διατάξεις για την προστασία των έννομων συμφερόντων των συνδρομητών - νομικών προσώπων. Η Ελλάδα εναρμονίστηκε με την εν λόγω Οδηγία με τον ν. 2774/1999 με τίτλο «προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

4.2.5 **Η οδηγία** 2002/58/**ΕΚ**

Με την Οδηγία 2002/58/ΕΚ [285] αυτή προστατεύονται τα δεδομένα προσωπικού χαρακτήρα από την επεξεργασία στον τομέα των ηλεκτρονικών επικοινωνιών και διασφαλίζεται η ελεύθερη επικοινωνία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Κοινότητα (άρθρο 1 παρ. 1).

Η οδηγία αυτή συμπληρώνει και εξειδικεύει την Οδηγία 95/46/ΕΚ και τα κράτη-μέλη όφειλαν να την ενσωματώσουν στο εσωτερικό τους δίκαιο πριν την 31 Οκτωβρίου 2003[286] και εφεξής. Επίσης η οδηγία 2002/58/Ε.Κ. καταργεί [287] και αντικαθιστά την Οδηγία 97/66/Ε.Κ. επειδή κρίθηκε αναγκαία η προσαρμογή των υπηρεσιών ηλεκτρονικών επικοινωνιών στις νέες εξελίξεις των αγορών και των τεχνολογιών. Η Οδηγία αποσκοπεί στην παροχή ισοδύναμου επιπέδου προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό, ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες, και παρέχει , επιπλέον, προστασία στα έννομα συμφέροντα των συνδρομητών που είναι νομικά πρόσωπα.

5 **ΚΕΦΑΛΑΙΟ** : **Το ελληνικό νομοθετικό πλαίσιο για τα προσωπικά δεδομένα**

5.1 **Το Σύνταγμα**

Στο ελληνικό δίκαιο η προστασία της προσωπικότητας και της ιδιωτικότητας, κατοχυρώνεται μέσα από τα άρθρα του Συντάγματος, που επιβάλλει το σεβασμό και την προστασία της αξίας του ανθρώπου ως πρωταρχική υποχρέωση της πολιτείας[288], καθιερώνει το δικαίωμα του

---

[285] Το πλήρες κείμενο της οδηγίας 2002/58/ΕΚ στην διεύθυνση:

http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/ODHGIA%202002_58_EK%20_3.PDF

[286] Βλ. Οδηγία 2002/58/ΕΚ της 12.7.2002 (317.2002 Ε 201/37). (άρθρο 17 παρ. 1)

[287] Βλ. Οδηγία 2002/58/ΕΚ της 12.7.2002 (317.2002 Ε 201/37). (άρθρο 19)

[288] *Βλ. Σύνταγμα άρθρο 2 παρ.1*

προσώπου να αναπτύσσει ελεύθερα την προσωπικότητα του[289],το δικαίωμα στην πληροφόρηση καθώς και το δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας[290], που προστατεύει την ιδιωτική και οικογενειακή ζωή του προσώπου[291], τα προσωπικά δεδομένα[292], την ελευθερία της θρησκευτικής συνείδησης[293], το απόρρητο των επικοινωνιών[294], καθορίζει τα όρια της προστασίας των ατομικών και κοινωνικών δικαιωμάτων και απαγορεύει την καταχρηστική τους άσκηση[295], κατοχυρώνει τις ανεξάρτητες Αρχές και ρυθμίζει τα θέματα συγκρότησης και λειτουργίας τους[296]. Η ελευθερία πρόσβασης και επικοινωνίας γενικά και ειδικότερα στο Διαδίκτυο, αλλά και το απόρρητο της επικοινωνίας στο Διαδίκτυο εξασφαλίζεται με τις διατάξεις του ΑΚ και ΠΚ, τους πιο πάνω αναφερόμενους νόμους, συμπεριλαμβανομένου και του ν. 2225/1994 σχετικά με την προστασία της ελευθερίας της ανταπόκρισης, με βάση τον οποίο ιδρύθηκε η Εθνική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών[297].

Όμως, οι γενικές διατάξεις προστασίας της προσωπικότητας δεν αρκούν για την προστασία του ατόμου από την πληροφορική. Η εξέλιξη της τεχνολογίας και οι κίνδυνοι που προκύπτουν από την απεριόριστη συλλογή και επεξεργασία πληροφοριών είναι πιο άμεσοι και διαφορετικής τάξης για το άτομο από τις συνηθισμένες προσβολές της προσωπικότητας[298]. Έτσι, θεωρήθηκε επιτακτική ανάγκη η θέσπιση ειδικής νομοθετικής προστασίας για τα προσωπικά δεδομένα, προκειμένου να γίνει κατάλληλη εξειδίκευση και να διασφαλιστεί «ο φιλελεύθερος χαρακτήρας της τεχνολογικής ανάπτυξης.

Η παραπάνω επιτακτική ανάγκη οδήγησε στη θέσπιση του ν. 2472/1997 (ΦΕΚ Α' 50/10.4.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, αλλά και του ν. 2774/1999 (ΦΕΚ Α' 287/22.12.1999) για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, όπως ισχύουν σήμερα.

5.2 **Ο νόμος** 2472/1997

---

289 *Βλ. Σύνταγμα ό.π άρθρο 5 παρ.1*

290 *Βλ. Σύνταγμα ό.π άρθρο 5Α*

291 *Βλ. Σύνταγμα ό.π άρθρο 9 παρ.1 εδ. β'*

292 Το άρθρο 9Α ορίζει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή που συγκροτείται και λειτουργεί, όπως νόμος ορίζει»

293 *Βλ. Σύνταγμα ό.π άρθρο 13 παρ.1 εδ α΄.*

294 *Βλ. Σύνταγμα ό.π., άρθρο 19.*

295 *Βλ. Σύνταγμα ό.π άρθρο 25.*

296 *Βλ. ό.π, Σύνταγμα άρθρο 101Α*

297 Βλ. Καράκωστα, Δίκαιο και internet σελ 144-146

298 Βλ. Εισηγητική Έκθεση του ν. 2472/1997, σελ. 501

Ο ν. 2472/1997[299], αποτελεί σύνολο ειδικών νομοθετικών ρυθμίσεων με τις οποίες θεσπίζονται οι προϋποθέσεις της νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα με σκοπό την προστασία των δικαιωμάτων και των ελευθεριών του ατόμου. Με την παραπάνω νομοθετική ρύθμιση η Ελλάδα συμμορφώθηκε προς τις διεθνείς και τις ευρωπαϊκές υποχρεώσεις της[300] .

Η ειδική νομοθετική ρύθμιση στηρίζεται στο σύστημα των ουσιαστικών και τυπικών προϋποθέσεων της νομιμότητας της επεξεργασίας, στο σύστημα των δικαιωμάτων του υποκειμένου των δεδομένων και των εγγυήσεων για την προστασία του και στο σύστημα του θεσμικού ελέγχου με την ίδρυση της Αρχής Προστασίας Προσωπικών Δεδομένων.

5.2.1 **Προσωπικά δεδομένα έννοια**

Προσωπικά δεδομένα[301] είναι κάθε πληροφορία που αναφέρεται σε ένα άτομο και περιγράφει αυτό , όπως : *στοιχεία αναγνώρισης* (ονοματεπώνυμο, ηλικία, κατοικία , επάγγελμα ,οικογενειακή κατάσταση κλπ.), *φυσικά χαρακτηριστικά*, *εκπαίδευση* , *εργασία* (προϋπηρεσία , εργασιακή συμπεριφορά κλπ), *οικονομική κατάσταση* (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), *ενδιαφέροντα*, *δραστηριότητες* , συνήθειες. Βασικό στοιχείο του προσωπικού δεδομένου είναι η σύνδεσή του με συγκεκριμένο πρόσωπο, έτσι ώστε να προκύπτει η ταυτότητα του τελευταίου είτε άμεσα (με αναφορά στο όνομά του) είτε έμμεσα (με τη φωτογράφησή του). Από αυτό προκύπτει ότι μέχρι μια πληροφορία να συνδεθεί με συγκεκριμένο πρόσωπο δεν αποτελεί προσωπικό δεδομένο. Επίσης όταν ένα προσωπικό δεδομένο αποσυνδεθεί από το πρόσωπο παύει να θεωρείται προσωπικό δεδομένο[302]. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

Τα προσωπικά δεδομένα αποτελούν ένα ιδιαίτερο ευαίσθητο τομέα στο χώρο των ανθρωπίνων δικαιωμάτων και της προστασίας της προσωπικότητας , το οποίο είναι εξαιρετικά επίκαιρο με βαρύνουσα σημασία λόγω των απεριορίστων τεχνικών επεξεργασίας που προσφέρει η σύγχρονη τεχνολογία της Πληροφορικής.

Ο όρος που έχει επικρατήσει διεθνώς σε σχέση με την προστασία των δεδομένων του υποκειμένου είναι αδόκιμος. Στα ελληνικά αποδίδεται με τον όρο «προσωπικά δεδομένα»,κατ' αντιστοιχία των ξενικών όρων data protection,Datenschutz, έννοια που ανταποκρίνεται

---

299 Ο Ν. 2472/1997 αφορά κάθε πρόσωπο που βρίσκεται στη ζωή. Τα νομικά πρόσωπα δεν έχουν προσωπικά δεδομένα.

300 Για το ζήτημα της προστασίας του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων βλ. Γέροντα Α., ό.π., Η προστασία του πολίτη από την επεξεργασία προσωπικών δεδομένων, εκδόσεις Σάκουλα, Αθήνα 2002, σελ. 178.

301 Βλ. http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL

302 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.33-35, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

περισσότερο σε τεχνητά στοιχεία, αριθμούς και όχι σε ανθρώπινα δικαιώματα και ελευθερίες του φορέα των δεδομένων [303].

5.2.2 **Η διάκριση των προσωπικών δεδομένων σε απλά και ευαίσθητα**

Απλά προσωπικά δεδομένα θεωρούνται οι πληροφορίες με αναφορά στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα , χωρίς να εισέρχονται πολύ στην ιδιωτικότητα του ατόμου. Για παράδειγμα το όνομα , το επώνυμο, το επάγγελμα, το μορφωτικό επίπεδο, οι καταναλωτικές συνήθειες , η οικογενειακή και περιουσιακή κατάσταση, τραπεζικοί λογαριασμοί.

Ευαίσθητα προσωπικά δεδομένα είναι οι πληροφορίες που αποτελούν τον πυρήνα της ιδιωτικής ζωής κάθε ατόμου *και αναφέρονται σ*τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία (όπως φυσική ή ψυχική κατάσταση, χρήση εξαρτησιογόνων ουσιών, λήψη φαρμάκων), την κοινωνική πρόνοια(π.χ ευαίσθητα στοιχεία για υιοθεσίες, ή στοιχεία για δικαιούχους συντάξεων πολεμικών- αναπηρικών), την ερωτική ζωή (με αναφορά στις προτιμήσεις του ατόμου για το ίδιο ή έτερο φύλο) καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες» [304] [305].

Σχετικά με την παραπάνω διάκριση διατυπώθηκε σχεδόν παράλληλα και η αντίθετη άποψη[306], δηλαδή, ότι όλες οι πληροφορίες (δεδομένα) είναι σημαντικές και ευαίσθητες σε σχέση με τη δυνατότητα αξιοποίησης τους αλλά και σε σχέση με το σκοπό για τον οποίο θα χρησιμοποιηθούν. Μάλιστα, σύμφωνα με την παραπάνω άποψη, η δυνατότητα αξιοποίησης των δεδομένων του προσώπου παρουσιάζεται αυξημένη εξαιτίας της ηλεκτρονικής συλλογής και επεξεργασίας η οποία μπορεί, μέσω συσχετισμού και με άλλα δεδομένα, να παράγει «νέα πληροφορία» και έτσι να καταστήσει δυνατή την προσβολή της προσωπικότητας και των συνταγματικών ελευθεριών του προσώπου.

Σημειώνεται ότι στον κατάλογο των ευαίσθητων δεδομένων του άρθρου 2 περ. β' του νόμου προστέθηκαν οι δηλώσεις και τα στοιχεία της αίτησης του αιτούντος άσυλο καθώς και τα δεδομένα των ληπτών και Δωρητών ανθρωπίνων ιστών και οργάνων. Ακόμη τα γενετικά δεδομένα θεωρούνται ευαίσθητα και η συλλογή και επεξεργασία τους υπόκειται στις ιδιαίτερες προϋποθέσεις και εγγυήσεις του νόμου, επειδή η χρήση τους ενέχει σοβαρότατους κινδύνους για τους πολίτες και τα δικαιώματα τους και, επιπλέον, «η

---

303 Βλ. Σινανιώτη-Μαρούδη Αριστέα , Ιωάννης Δ. Φαρσαρώτας, Ηλεκτρονική τραπεζική» , εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα 2005, σελ.369.

304 Βλ. Νόμος 2472/1997, άρθρο 2 περ. β' .

305 Το παραπάνω άρθρο προσθέτει και χαρακτηρίζει σαν ευαίσθητα, κατ' απόκλιση του άρθρου 8 παρ.1 της Οδηγίας, και τα δεδομένα που αφορούν την «κοινωνική πρόνοια» καθώς και «τα σχετικά με ποινικές διώξεις ή καταδίκες». Βλ. Μήτρου Α., Η Αρχή Προστασίας Προσωπικών Δεδομένων, σελ. 25.

306 σχετικά με την απόφαση Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας του 1983 που απορρίπτει τη διάκριση των πληροφοριών σε κατηγορίες και δέχεται ότι η προστασία τους πρέπει να διαφοροποιείται ανάλογα με το που θα χρησιμοποιηθούν, Βλ. Γέροντα Α., Πληροφορική και Δίκαιο ,Αθήνα –Κομοτηνή 1990 , σελ. 69-70.

γνωστοποίηση των δεδομένων που προκύπτουν από τις γενετικές εξετάσεις μπορεί να οδηγήσει σε κατηγοριοποίηση των ανθρώπων και σε τελευταία ανάλυση στον στιγματισμό και τον κοινωνικό αποκλεισμό τους[307]. Ανάλογη προς τα γενετικά δεδομένα πρέπει να είναι και η αντιμετώπιση των δεδομένων που προκύπτουν από τη χρήση βιομετρικών μεθόδων. Μάλιστα, η χρήση ορισμένων τέτοιων μεθόδων «θίγει κατάφορα την ανθρώπινη αξιοπρέπεια και την προσωπικότητα». Κατά συνέπεια τα βιομετρικά δεδομένα[308] που προκύπτουν από τέτοιες μεθόδους παρέχουν τη δυνατότητα αναγνώρισης των φυσικών προσώπων. Ειδικότερα, όσον αφορά την επεξεργασία βιομετρικών δεδομένων με τη μέθοδο συλλογής των δακτυλικών αποτυπωμάτων για τον έλεγχο εισόδου και εξόδου των εργαζομένων στο χώρο εργασίας, η Αρχή, αφού καταρχήν δέχεται ότι η αναγνώριση του υποκειμένου με τη μέθοδο της δακτυλοσκόπησης εξυπηρετεί από πολλά χρόνια την αντεγκληματική πολιτική, έκρινε ότι «η συγκεκριμένη συλλογή και επεξεργασία υπερβαίνει τα επιβαλλόμενα όρια. Μια εξαίρεση θα μπορούσε να γίνει δεκτή μόνο σε ειδικές περιπτώσεις π.χ. για το σκοπό ελέγχου πρόσβασης σε χώρους απορρήτων αρχείων ή εγκαταστάσεων»[309].

Η διάκριση των δεδομένων προσωπικού χαρακτήρα σε απλά και ευαίσθητα έχει σημασία πρακτική. Και αυτό γιατί τα ευαίσθητα δεδομένα απολαμβάνουν ενισχυμένη νομική προστασία σε σχέση με τα απλά, αφού έχουν θεσπιστεί αυστηρότερες προϋποθέσεις για την επεξεργασία των ευαίσθητων δεδομένων προσωπικού χαρακτήρα σε σχέση με τα απλά. Έτσι για τη νόμιμη επεξεργασία απλών δεδομένων αρκεί η προφορική συγκατάθεση του υποκειμένου και η γνωστοποίηση στην Αρχή. Αντίθετα για την νόμιμη επεξεργασία των ευαίσθητων δεδομένων απαιτείται η γραπτή συγκατάθεση του υποκειμένου και η λήψη σχετικής άδειας από την Αρχή Προστασίας Προσωπικών Δεδομένων, για να διενεργηθεί ο αναγκαίος προληπτικός έλεγχος[310].

5.2.3 **Επεξεργασία δεδομένων προσωπικού χαρακτήρα**

Στην αναφορά επεξεργασία δεδομένων προσωπικού χαρακτήρα εννοείται κάθε εργασία που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, όπως: συλλογή, καταχώριση, οργάνωση, διατήρηση ή αποθήκευση, τροποποίηση, εξαγωγή, χρήση, διαβίβαση, διάδοση, συσχέτιση ή συνδυασμός, διασύνδεση, δέσμευση, διαγραφή, καταστροφή. Κάθε φυσικό ή νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα που τηρεί και επεξεργάζεται προσωπικά δεδομένα ονομάζεται *υπεύθυνος επεξεργασίας.* Κάθε φυσικό ή νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα που επεξεργάζεται δεδομένα για λογαριασμό κάποιου υπεύθυνου επεξεργασίας ονομάζεται *εκτελών την επεξεργασία*[311].

---

307 Βλ. Γνωμοδότηση αρ. 15/2001 (401-15-2-2001 Οδηγία για το DNA) της Αρχής στο: http://www.dpa.gr/portal/page?_pageid=33,6948&_dad=portal&_schema=PORTAL

Βλ. επίσης Ιγγλεζάκη Ι., ό.π., σελ. 100

308 Βλ Γέροντα Α., Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, ό.π., σελ. 203, Ιγγλεζάκη Ι., ό.π., σελ. 210

309 Βλ. υπ' αριθ. 245/9/20.3.2000 απόφαση της Αρχής

310 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.37, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007

311 Βλ. Νόμος 2472/1997 στο: http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL.

Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει απαραίτητα να τηρεί κάποιες βασικές αρχές[312]., οι οποίες προβλέπονται από το νόμο ,όπως:

α) Η αρχή της νομιμότητας του σκοπού και του τρόπου επεργασίας[313].

β) Η αρχή της αναλογικότητας[314].

γ) Η αρχή της ακρίβειας[315].

δ) Η αρχή της χρονικής διάρκειας[316].

Η τήρηση των διατάξεων της προηγούμενης παραγράφου βαρύνει τον υπεύθυνο επεξεργασίας. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας.

Προϋποθέσεις επεξεργασίας Για να διαπιστωθεί η νομιμότητα της επεξεργασίας πρέπει να υπάρχουν 3 βασικές προϋποθέσεις[317]:

1) Στην αρχή εξετάζεται αν η επεξεργασία ακολουθεί τις 4 βασικές αρχές επεξεργασίας όπως αυτές περιγράφονται παραπάνω. Στην περίπτωση που βρεθεί πως δεν τηρούνται (έστω και μία από αυτές), η επεξεργασία κρίνεται παράνομη και δεν εξετάζονται άλλες προϋποθέσεις.

2) Στην περίπτωση που τηρούνται οι 4 βασικές αρχές επεξεργασίας εξετάζεται αν υπάρχει η συγκατάθεση του υποκειμένου[318] [319].

---

312 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.45, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

313 Βλ.άρθρο 4 παρ.1α, Νόμος 2472/1997σύμφωνα με το οποίο «Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει : α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών».

314 Βλ.άρθρο 4 παρ.1β, Νόμος 2472/1997σύμφωνα με το οποίο «Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει : β) Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας».

315 Βλ.άρθρο 4 παρ.1γ, Νόμος 2472/1997σύμφωνα με το οποίο «Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει : γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση ».

316 Βλ.άρθρο 4 παρ.1δ, Νόμος 2472/1997σύμφωνα με το οποίο «Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει : δ) Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων».

317 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.40, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007

318 Βλ.άρθρο 5 παρ.1, Νόμος 2472/1997.

3) Εάν δεν υπάρχει η συγκατάθεση του υποκειμένου, εξετάζεται αν η συγκεκριμένη επεξεργασία περιλαμβάνεται στις εξαιρέσεις που ο νόμος ορίζει[320].

Επεξεργασία ευαίσθητων δεδομένων: Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων.

Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής, στις ακόλουθες περιπτώσεις :

α) Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο μη νόμιμο[321].

β) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου (κυοφορούμενου), εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του[322].

γ) Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου[323].

δ) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται με την παροχή υπηρεσιών υγείας (επαγγελματικά) και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας[324].

---

319 Ξεχωριστή περίπτωση αφορά η συγκατάθεση , η οποία παρέχεται μέσω Διαδικτύου, δηλ σε απευθείας σύνδεση (on-line) μέσω του Web ή μέσω του ηλεκτρονικού ταχυδρομείου (e-mail) με χρήση της ηλεκτρονικής ψηφιακής υπογραφής, για περισσότερα βλέπε Ιωάννη Ιγγλεζάκη, Ευαίσθητα προσωπικά δεδομένα –η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειες, σελ 216 εκδόσεις , Σάκκουλα Αθήνα - Θεσσαλονίκη 2003.

320 Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση του υποκειμένου όταν: « α) Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο. β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.γ) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του. δ) Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα. ε) Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών» άρθρο 5 παρ.2, Νόμος 2472/1997.

321 Βλ.άρθρο7 παρ.2α, Νόμος 2472/1997.

322 Βλ. .άρθρο7 παρ.2β, Νόμος 2472/1997 , βλ επίσης Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.66, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007

323 Βλ.άρθρο7 παρ.2γ, Νόμος 2472/1997

324 Η εξαίρεση αφορά όχι μόνο τα ιατρικά δεδομένα αλλά γενικότερα τα προσωπικά δεδομένα που υφίστανται επεξεργασία και η οποία αφορά θέματα υγείας, για περισσότερα βλέπε Ιωάννη Ιγγλεζάκη, Ευαίσθητα προσωπικά

ε) Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία για λόγους εθνικής ασφάλειας ,για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας, για λόγους προστασίας της δημόσιας υγείας, για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών[325].

στ) Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς[326].

ζ) Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος[327].

Η Αρχή χορηγεί άδεια[328] συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο του και τον εκτελούντα την επεξεργασία. Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Κάθε μεταβολή των στοιχείων γνωστοποιείται χωρίς καθυστέρηση στην Αρχή.

<u>Γνωστοποίηση αρχείων</u>

Ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή, τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας[329]. Στην περίπτωση που το αρχείο

δεδομένα –η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειες, σελ 212-254, εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη 2003, Βλ. επίσης άρθρο7 παρ.2δ, Νόμος 2472/1997.

325 Βλ.άρθρο7 παρ.2ε, Νόμος 2472/1997

326 και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται Βλ.άρθρο7 παρ.2στ, Νόμος 2472/1997

327 Η άδεια της αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται καθ' οιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής Βλ.άρθρο7 παρ.2ζ, Νόμος 2472/1997

328 Η άδεια περιέχει απαραιτήτως: Τα στοιχεία του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του, Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο, το είδος των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να περιληφθούν στο αρχείο, το χρονικό διάστημα για το οποίο χορηγείται η άδεια, τους τυχόν όρους και προϋποθέσεις που έχει επιβάλει η Αρχή για την ίδρυση και λειτουργία του αρχείου και την υποχρέωση γνωστοποίησής του αρχείου. Βλ.άρθρο7 παρ.5 , Νόμος 2472/1997.

329 Με τη ρύθμιση αυτή ο νόμος γίνεται εφαρμόσιμος και αποτελεσματικός καθώς δεν χρειάζεται άδεια για κάθε αρχείο από την Αρχή Προστασίας Προσωπικών δεδομένων και η Αρχή μπορεί να λειτουργήσει χωρίς γραφειοκρατική επιβάρυνση , βλ Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.69, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007, Βλ. επίσης άρθρο 6 παρ. 1, Νόμος 2472/1997.

περιέχει ευαίσθητα δεδομένα χρειάζεται σχετική άδεια της Αρχής μετά από αίτηση του υπεύθυνου επεξεργασίας[330].

Με τη γνωστοποίηση της προηγούμενης παραγράφου ο υπεύθυνος επεξεργασίας πρέπει απαραιτήτως να δηλώνει:

α) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του, και τη διεύθυνσή του.

β) Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία.

γ) Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

δ) Το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.

ε) Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει το αρχείο.

στ) Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνει ή ενδέχεται να ανακοινώνει τα δεδομένα προσωπικού χαρακτήρα.

ζ) Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.

η) Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας[331].

Τα στοιχεία της προηγούμενης παραγράφου καταχωρίζονται στο Μητρώο Αρχείων και Επεξεργασιών που τηρεί η Αρχή. Κάθε μεταβολή των στοιχείων πρέπει να γνωστοποιείται εγγράφως και χωρίς καθυστέρηση από τον υπεύθυνο στην Αρχή.

<u>Απαλλαγή υποχρέωσης γνωστοποίησης και λήψης άδειας</u>

Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης αρχείων και από την υποχρέωση λήψης άδειας επεξεργασίας ευαίσθητων προσωπικών δεδομένων του άρθρου 7 του παρόντος νόμου στις ακόλουθες περιπτώσεις:

α) Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για

---

330 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.70, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

331 Βλ. άρθρο 6 παρ. 2, Νόμος 2472/1997.

την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί[332].

β) Όταν η επεξεργασία αφορά πελάτες ή προμηθευτές, εφόσον τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους[333].

γ) Όταν η επεξεργασία γίνεται από σωματεία, εταιρείες, ενώσεις προσώπων και πολιτικά κόμματα και αφορά δεδομένα των μελών ή εταιρειών τους, εφόσον αυτοί έχουν δώσει την συγκατάθεσή τους και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους[334].

δ) Όταν η επεξεργασία αφορά δεδομένα υγείας και γίνεται από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας[335].

ε) Όταν η επεξεργασία γίνεται από δικηγόρους, συμβολαιογράφους, άμισθους υποθηκοφύλακες και δικαστικούς επιμελητές ή εταιρείες των προσώπων αυτών και αφορά στην παροχή νομικών υπηρεσιών προς πελάτες τους[336].

στ) Όταν η επεξεργασία γίνεται από δικαστικές αρχές στο πλαίσιο απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους[337].

<u>Διασύνδεση αρχείων</u>

Διασύνδεση αρχείων είναι μια μορφή επεξεργασίας που συνίσταται στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα άλλου αρχείου (ή και αρχείων). Οι διασυνδέσεις αρχείων συναντάται συχνά στη σύγχρονη οικονομική και κοινωνική ζωή, όπως διασύνδεση αρχείων που τηρούν οι τράπεζες με δυσμενή οικονομικά στοιχεία πελατών τους με

---

332 Βλ. άρθρο 7Α παρ. 1α, Νόμος 2472/1997.

333 Δεν απαλλάσσονται από την υποχρέωση γνωστοποίησης οι ασφαλιστικές εταιρείες για όλους τους κλάδους ασφάλισης, οι φαρμακευτικές εταιρείες, οι εταιρείες εμπορίας πληροφοριών και τα χρηματοπιστωτικά νομικά πρόσωπα, όπως οι τράπεζες και οι εταιρείες έκδοσης πιστωτικών καρτών, βλ. άρθρο 7Α παρ. 1β, Νόμος 2472/1997.

334 Δεν λογίζονται τρίτοι τα μέλη ή εταίροι, εφόσον η διαβίβαση γίνεται προς αυτούς για τους σκοπούς των ως άνω νομικών προσώπων ή ενώσεων, ούτε τα δικαστήρια και οι δημόσιες αρχές, εφόσον τη διαβίβαση επιβάλλει νόμος ή δικαστική απόφαση, βλ. άρθρο 7Α παρ. 1γ, Νόμος 2472/1997.

335 Με την προϋπόθεση « ο υπεύθυνος επεξεργασίας να δεσμεύεται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει νόμος ή κώδικας δεοντολογίας και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους ».Βλ. άρθρο 7Α παρ. 1δ, Νόμος 2472/1997

336 Εφόσον ο υπεύθυνος επεξεργασίας και τα μέλη των εταιρειών δεσμεύονται από υποχρέωση απορρήτου που προβλέπει νόμος και τα δεδομένα δεν διαβιβάζονται ούτε κοινοποιούνται σε τρίτους, εκτός από τις περιπτώσεις που αυτό είναι αναγκαίο και συνδέεται άμεσα με την εκπλήρωση εντολής του πελάτη, βλ. άρθρο 7Α παρ. 1ε, Νόμος 2472/1997

337 Βλ. άρθρο 7Α παρ. 1στ, Νόμος 2472/1997

το αρχείο Τειρεσίας [338] [339]. Κάθε διασύνδεση γνωστοποιείται στην Αρχή με δήλωση την οποία υποβάλλουν από κοινού οι υπεύθυνοι επεξεργασίας ή ο υπεύθυνος επεξεργασίας που διασυνδέει δύο ή περισσότερα αρχεία που εξυπηρετούν διαφορετικούς σκοπούς.

Εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων, ή εάν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνον με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης[340]).

Διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες της Ευρωπαϊκής Ένωσης είναι ελεύθερη. Η διαβίβαση προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση δεδομένων προσωπικού χαρακτήρα, τα οποία έχουν υποστεί ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται ύστερα, από άδεια της Αρχής. Η Αρχή παρέχει την άδεια μόνον εάν κρίνει ότι η χώρα αυτή εξασφαλίζει ικανοποιητικό επίπεδο προστασίας [341].
Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της Αρχής, εφ' όσον συντρέχει μία ή περισσότερες από τις κατωτέρω προϋποθέσεις[342]:

α) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη.

β) Η διαβίβαση είναι απαραίτητη i) για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφόσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή ii) για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπεύθυνου επεξεργασίας ή μεταξύ του υπεύθυνου επεξεργασίας και τρίτου προς το συμφέρον του

---

[338] Η ΤΕΙΡΕΣΙΑΣ Α.Ε είναι διατραπεζική εταιρεία που εξειδικεύεται στη συγκέντρωση και διάθεση πληροφοριών οικονομικής συμπεριφοράς για επιχειρήσεις και ιδιώτες, δεδομένων συγκέντρωσης χορηγήσεων για ιδιώτες και μικρές επιχειρήσεις, υποθηκών και προσημειώσεων καθώς και στοιχείων που συνδράμουν στην αποτροπή απάτης στις τραπεζικές συναλλαγές, τα οποία παρέχει μέσω αξιόπιστων πληροφορικών συστημάτων, για περισσότερα βλ.: http://www.tiresias.gr/index.html.

[339] Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, σελ.77, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

[340] Η άδεια διασύνδεσης χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων και περιέχει απαραιτήτως: α) Τον σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία. β) Το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση. γ) Το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση. δ) Τους τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων**.** Βλ. άρθρο 8 παρ. 4, Νόμος 2472/1997.

[341] Βλ. σχετικά άρθρο 9 παρ. 1, Νόμος 2472/1997, βλέπε επίσης Γέροντας Απόστολος Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων σ 217, επίσης Ιγγλεζάκης Ιωάννης Δ. Ευαίσθητα Προσωπικά Δεδομένα – Η επεξεργασία ειδικών κατηγοριών δεδομένων και οι συνέπειές της, σ 75 επ

[342] Βλ. σχετικά άρθρο 9 παρ. 2, Νόμος 2472/1997, βλέπε επίσης Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων σ 217-218.

υποκειμένου των δεδομένων, ή iii) για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί κατ΄αίτηση του υποκειμένου των δεδομένων.

γ) Η διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημόσιου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες αρχές της άλλης χώρας, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου.

ε) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, το οποίο σύμφωνα με το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιτό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προϋποθέσεις για την πρόσβαση στο μητρώο.

στ) Ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των υποκειμένων και την άσκηση των σχετικών δικαιωμάτων τους, όταν οι εγγυήσεις προκύπτουν από συμβατικές ρήτρες, σύμφωνες με τις ρυθμίσεις του παρόντος νόμου. Δεν απαιτείται άδεια εάν η Ευρωπαϊκή Επιτροπή έκρινε, κατά το άρθρο 26 παρ. 4 της Οδηγίας 95/46/ΕΚ, ότι ορισμένες συμβατικές ρήτρες παρέχουν επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων[343].

Απόρρητο και ασφάλεια της επεξεργασίας

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Πραγματοποιείται αποκλειστικά και μόνο από πρόσωπα[344] που βρίσκονται κάτω από τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας[345].

Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει

---

343 Βλέπε Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων σ 217-218, Μιχ. Κ Αυγουστιανάκης. «Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων – Προβλήματα και αντιμετώπιση από το δίκαιο»στο: ΔτΑ 11/2001 σ 673-675 .

344 Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου, Βλ. σχετικά άρθρο 10 παρ. 2 Νόμος 2472/1997.

345 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου ό.π., Προσωπικά Δεδομένα, σελ.83-84, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν[346].

5.2.4 **Δικαιώματα του Υποκειμένου των δεδομένων**

Ο έλληνας νομοθέτης ακολουθώντας το ευρωπαϊκό δίκαιο[347], δημιούργησε ένα πλέγμα έννομης προστασίας του υποκειμένου των δεδομένων, με την θεσμοθέτηση και κατοχύρωση δικαιωμάτων, τη θέσπιση σημαντικών εγγυήσεων προκειμένου να εξασφαλίζεται, η προάσπιση των δικαιωμάτων του υποκειμένου, των δεδομένων προσωπικού χαρακτήρα[348]. Τα δικαιώματα αυτά είναι το δικαίωμα της ενημέρωσης, το δικαίωμα πρόσβασης, το δικαίωμα αντίρρησης και το δικαίωμα προσωρινής δικαστικής προστασίας.

Η παροχή δικαιωμάτων από το νόμο έχει ως κύρια αποστολή την προστασία του δικαιώματος της προσωπικότητας από ενδεχόμενες προσβολές στα πλαίσια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα[349]. Τα δικαιώματα αυτά εντάσσονται στα «μέσα άμυνας» των ατόμων και επιτρέπουν σε αυτά να μπορούν να γνωρίζουν ποιες πληροφορίες επιτρέπεται να αποτελέσουν αντικείμενο επεξεργασίας[350].

<u>Δικαίωμα ενημέρωσης</u>

Θα πρέπει να τονιστεί ότι το υποκείμενο δικαιωμάτων δεδομένων προσωπικού χαρακτήρα διατηρεί πάντοτε το δικαίωμα ενημέρωσης για τα προσωπικά δεδομένα του, τα οποία υφίστανται επεξεργασία και πληροφορείται σχετικά με τις συνθήκες αλλαγής αυτών[351]. Βάσει αυτού εξασφαλίζεται η διαφανής και σύννομη επεξεργασία των δεδομένων προσωπικού χαρακτήρα και διευκολύνεται η άσκηση των προβλεπόμενων ρητά στο νόμο δικαιωμάτων πρόσβασης και αντίρρησης που αναλύονται παρακάτω[352].

Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

α. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του

---

346 Βλ. σχετικά άρθρο 10 παρ. 4 Νόμος 2472/1997.

347 Βλ. σχετική οδηγία 95/46/ΕΚ.: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

348 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου ό.π., Προσωπικά Δεδομένα, σελ.85, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

349 Βλ. Αριστέα Σινανιώτη-Μαυρουδή & Ιωάννη Δ. Φαρσαρώτα, Ηλεκτρονική Τραπεζική, σελ.384, εκδόσεις Σάκκουλα , Αθήνα 2005.

350 Βλ. Λίλιαν Μήτρου, Η αρχή προστασίας προσωπικών δεδομένων, εκδόσεις Σάκκουλα , Αθήνα 1999, σελ.29.

351 Βλ. σχετικά, άρθρο 11 Νόμος 2472/1997.

352 Βλ. Αριστέα Σινανιώτη-Μαυρουδή & Ιωάννη Δ. Φαρσαρώτα, Ηλεκτρονική Τραπεζική, ό,π., σελ.385.

β. τον σκοπό της επεξεργασίας.

γ. τους αποδέκτες των δεδομένων.

δ. την ύπαρξη του δικαιώματος πρόσβασης.

ε. για τα δικαιώματά του[353].

Εάν τα δεδομένα ανακοινώνονται σε τρίτους, το υποκείμενο ενημερώνεται για την ανακοίνωση πριν από αυτούς[354].

Με απόφαση της Αρχής, μπορεί να αρθεί η υποχρέωση ενημέρωσης , εφόσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Σε επείγουσες περιπτώσεις η άρση της υποχρέωσης ενημέρωσης μπορεί να γίνει με προσωρινή, άμεσα εκτελεστή, απόφαση του Προέδρου, ο οποίος πρέπει να συγκαλέσει το συντομότερο την Αρχή για την έκδοση οριστικής απόφασης επί του θέματος. Η υποχρέωση ενημέρωσης επίσης δεν υφίσταται όταν η συλλογή γίνεται αποκλειστικά για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα, με κάποιες επιφυλάξεις[355].

Δικαίωμα πρόσβασης Καθένας έχει δικαίωμα να γνωρίζει εάν δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Για το σκοπό αυτό, ο υπεύθυνος επεξεργασίας, έχει υποχρέωση να του απαντήσει εγγράφως[356].

Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο σαφή, τις ακόλουθες πληροφορίες:

α) Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους.

β) Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.

γ) Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του.

δ) Τη λογική της αυτοματοποιημένης επεξεργασίας.

---

353 *Εάν για τη συλλογή των δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας ζητεί την συνδρομή του υποκείμενου, οφείλει επιπλέον να το ενημερώσει ειδικώς και εγγράφως για τα παραπάνω στοιχεία καθώς και για τα δικαιώματά του,ενημέρωσης και αντίρρησης.. Με την ίδια ενημέρωση ο υπεύθυνος επεξεργασίας γνωστοποιεί στο υποκείμενο εάν υποχρεούται ή όχι να παράσχει τη συνδρομή του, με βάση ποιες διατάξεις, καθώς και για τις τυχόν συνέπειες της αρνήσεώς του βλ.* άρθρο 11 παρ. 2, Νόμου 2472/1997.

354 *Βλ.* άρθρο 11 παρ. 3, Νόμου 2472/1997.

355 Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου ό.π., Προσωπικά Δεδομένα, σελ.89, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.

356 *Βλ.* άρθρο 12 παρ. 1, Νόμου 2472/1997.

ε) Κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλείδωμα) των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων.

στ) την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης (κλειδώματος) που διενεργείται σύμφωνα με την περίπτωση ε', εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες [357].

Το δικαίωμα πρόσβασης μπορεί να ασκείται από το υποκείμενο των δεδομένων, κατόπιν σχετικής επιστολής[358] στον υπεύθυνο της επεξεργασίας και ταυτόχρονη καταβολή χρηματικού ποσού, το ύψος του οποίου, ο τρόπος καταβολής του και κάθε άλλο συναφές ζήτημα ρυθμίζονται με απόφαση της Αρχής. Το ποσό αυτό επιστρέφεται στον αιτούντα εάν το αίτημα διόρθωσης ή διαγραφής των δεδομένων κριθεί βάσιμο είτε από τον υπεύθυνο της επεξεργασίας είτε από την Αρχή, σε περίπτωση προσφυγής του σ' αυτήν. Ο υπεύθυνος έχει υποχρέωση στην περίπτωση αυτή να χορηγήσει στον αιτούντα, χωρίς καθυστέρηση δωρεάν και σε γλώσσα κατανοητή, αντίγραφο του διορθωμένου μέρους της επεξεργασίας που τον αφορά. Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εντός δεκαπέντε (15) ημερών ή εάν η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή. Στην περίπτωση κατά την οποία ο υπεύθυνος επεξεργασίας αρνηθεί να ικανοποιήσει το αίτημα του ενδιαφερόμενου, κοινοποιεί την απάντησή του στην Αρχή και ενημερώνει τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν. Σε περίπτωση αδυναμίας ικανοποίησης του δικαιώματος πρόσβασης δημιουργείται η υποχρέωση διαγραφής των δεδομένων του υποκειμένου από το αρχείο και επιβολή των αντίστοιχων ποινών[359].

Με απόφαση της Αρχής, ύστερα από αίτηση του υπεύθυνου επεξεργασίας, η υποχρέωση πληροφόρησης, μπορεί να αρθεί, εφ' όσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στην περίπτωση αυτή ο Πρόεδρος της Αρχής ή ο αναπληρωτής του προβαίνει σε όλες τις αναγκαίες

---

[357] Βλ. άρθρο 12 παρ. 2, Νόμου 2472/1997, βλ. επίσης , Αριστέα Σινανιώτη-Μαυρουδή & Ιωάννη Δ. Φαρσαρώτα, Ηλεκτρονική Τραπεζική, ό,π., σελ.389-390.

[358] Η επιστολή είναι απλή: Κύριε/κυρία … Παρακαλώ, σύμφωνα με το νόμο 2472/1997 άρθρο 12, ενημερώστε με γραπτώς και με σαφήνεια ποια προσωπικά μου δεδομένα τηρείτε στα αρχεία σας …
βλ σχετικά: http://www.dpa.gr/portal/page?_pageid=33,19005&_dad=portal&_schema=PORTAL

[359] Βλ. σχετική απόφαση 28/2003 της Αρχής , για μη ικανοποίηση δικαιώματος πρόσβασης ,σύμφωνα με την οποία επιβλήθηκε σε Τράπεζα πρόστιμο 30.000 € , η οποία αδυνατούσε να ικανοποιήσει το δικαίωμα πρόσβασης του υποκειμένου, στο:
http://www.dpa.gr/portal/page?_pageid=33%2C15453&_dad=portal&_schema=PORTAL&_piref33_15473_33_15453_15453.etos=2003&_piref33_15473_33_15453_15453.arithmosApofasis=28&_piref33_15473_33_15453_15453.thematikiEnotita=-1&_piref33_15473_33_15453_15453.ananeosi=%CE%91%CE%BD%CE%B1%CE%BD%CE%AD%CF%89%CF%83%CE%B7

ενέργειες και έχει ελεύθερη πρόσβαση στο αρχείο [360]. Δεδομένα που αφορούν την υγεία γνωστοποιούνται στο υποκείμενο μέσω ιατρού[361].

Δικαίωμα αντίρρησης

Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή[362]. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα. Η απάντηση σε περίπτωση απόρριψης των αντιρρήσεων πρέπει να κοινοποιείται και στην Αρχή[363].

Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή και να ζητήσει την εξέταση των αντιρρήσεών του. Εάν η Αρχή πιθανολογήσει ότι οι αντιρρήσεις είναι εύλογες και ότι συντρέχει κίνδυνος σοβαρής βλάβης του υποκειμένου από την συνέχιση της επεξεργασίας, μπορεί να επιβάλλει την άμεση αναστολή της επεξεργασίας έως ότου εκδώσει οριστική απόφαση επί των αντιρρήσεων[364].

Καθένας έχει δικαίωμα να δηλώσει στην Αρχή ότι δεδομένα που τον αφορούν δεν επιθυμεί να αποτελέσουν αντικείμενο επεξεργασίας από οποιονδήποτε, για λόγους προώθησης πωλήσεως αγαθών ή παροχής υπηρεσιών εξ αποστάσεως. Η Αρχή τηρεί μητρώο με τα στοιχεία ταυτότητας των ανωτέρω. Οι υπεύθυνοι επεξεργασίας των σχετικών αρχείων έχουν την υποχρέωση να συμβουλεύονται πριν από κάθε επεξεργασία το εν λόγω μητρώο και να διαγράφουν από το αρχείο τους τα πρόσωπα της παραγράφου αυτής[365].

Δικαίωμα προσωρινής δικαστικής προστασίας

---

360 Βλ. άρθρο 12 παρ. 5, Νόμου 2472/1997, βλ. επίσης , Αριστέα Σινανιώτη-Μαυρουδή & Ιωάννη Δ. Φαρσαρώτα, Ηλεκτρονική Τραπεζική, ό,π., σελ.389-390.

361 Βλ. άρθρο 12 παρ. 6, Νόμου 2472/1997.

362 Η επιστολή είναι απλή: Κύριε/κυρία … Παρακαλώ, σύμφωνα με το νόμο 2472/1997 άρθρο 13, διορθώστε ως εξής (…) ή διαγράψτε τα προσωπικά μου δεδομένα που τηρείτε στα αρχεία σας**…** βλ.σχετικά στο:
http://www.dpa.gr/portal/page?_pageid=33,19005&_dad=portal&_schema=PORTAL

363 Βλ. άρθρο 13 παρ. 1, Νόμου 2472/1997, βλ. επίσης , Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία Ζητήματα από το Δίκαιο της Πληροφορικής ., Εκδόσεις Σάκκουλα, Αθήνα 2002, σελ 39 , επίσης Τουντόπουλος Βασίλειος «Το δικαίωμα αντίρρησης του υποκειμένου των δεδομένων» στο περιοδικό:ΤοΣ 1/1999 σ 21 επ.

364 *Βλ.* άρθρο 13 παρ. 2, Νόμου 2472/1997, βλ. επίσης , Ιωάννης Δ. Ιγγλεζάκης, Ευαίσθητα Προσωπικά Δεδομένα – Η επεξεργασία ειδικών κατηγοριών δεδομένων και οι συνέπειές της ,ό.π. σ 80 .

365 *Βλ.* άρθρο 13 παρ. 3, Νόμου 2472/1997, βλ. επίσης , Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων ό.π., σ 232 .

Το δικαίωμα αυτό αποτελεί μια θεσμική κατοχύρωση για τον πολίτη ο οποίος μπορεί να προστρέξει στην δικαιοσύνη ζητώντας την άμεση προστασία του όσον αφορά στην επεξεργασία προσωπικών του στοιχείων. Σύμφωνα με το Νόμο κάθε άτομο έχει δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, την οποία έχει λάβει διοικητική αρχή, νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του[366].

5.3 **Ο νόμος** 2774/1999

Ο Ν. 2774/1999 αποτελεί την συνέχεια του Ν. 2472/1997 με αναφορά στο ειδικότερο θέμα της προστασίας δεδομένων προσωπικού χαρακτήρα των χρηστών και των συνδρομητών στον τηλεπικοινωνιακό τομέα, σε ευθυγράμμιση με την Οδηγία 97/66/Ε.Κ. Ο παρών νόμος έχει εφαρμογή και στις περιπτώσεις που συνδρομητές , πέραν των φυσικών προσώπων (κατά τους ορισμούς του νόμου αυτού) είναι και νομικά πρόσωπα[367]. Ως γενική αρχή καθιερώνει, ότι οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών[368] .

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν τον τηλεπικοινωνιακό τομέα επιτρέπεται μόνον όταν:

α) Ο συνδρομητής ή ο χρήστης έχει δώσει τη συγκατάθεσή του μετά από ενημέρωση για το είδος των δεδομένων, τον σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.

β) Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης στην οποία ο συνδρομητής ή ο χρήστης είναι συμβαλλόμενο μέρος ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο μετά από αίτηση του συνδρομητή.

γ) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο απολύτως αναγκαίο για την εξυπηρέτηση των σκοπών της.

δ) Ο παροχέας δικτύου-τηλεπικοινωνιακής υπηρεσίας δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς και ιδίως για σκοπούς διαφήμισης ή εμπορικής έρευνας αγοράς προϊόντων και υπηρεσιών εκτός εάν ο συνδρομητής ή ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεσή του. Η συγκατάθεση

---

366 *Βλ.* άρθρο 14 παρ. 1, Νόμου 2472/1997, βλ. επίσης , Ιγγλεζάκης Ιωάννης Δ. Ευαίσθητα Προσωπικά Δεδομένα – Η επεξεργασία ειδικών κατηγοριών δεδομένων και οι συνέπειές της ό.π., σ 81.

367 *Σε αντίθεση με το Ν.2472/1997 που έχει αναφορά μόνο στα φυσικά πρόσωπα* .

368 *Η άρση του απορρήτου σε δημόσιες αρχές είναι επιτρεπτή μόνο για τους λόγους και υπό τους όρους και διαδικασίες που ορίζει ο Ν. 2225/94 (ΦΕΚ 121 Α' /20.07.1994), όπως ισχύει, βλ. άρθρο 4 παρ.1 Ν. 2774/1999*.

απαιτείται να είναι έγγραφη εφόσον τα δεδομένα διαβιβάζονται σε τρίτους[369].

Τα δεδομένα κίνησης[370] των συνδρομητών-χρηστών πρέπει να απαλείφονται ή να καθίστανται ανώνυμα κατά τη λήξη της κλήσης . Για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων επιτρέπεται η επεξεργασία προσωπικών δεδομένων ,στο βαθμό που είναι αναγκαία [371]. Η λήψη αναλυτικού λογαριασμού[372], η ένδειξη και η απόκρυψη της ταυτότητας του καλούντος , η απόρριψη της εισερχόμενης κλήσης ,η ενημέρωση για τις δυνατότητες αυτές και η κατ' εξαίρεση εξουδετέρωση της δυνατότητας του καλούντος να αποκρύψει την ταυτότητά του[373], η παρεμπόδιση αυτόματης προώθησης κλήσεως από τρίτους στην τερματική συσκευή του[374],αποτελούν δικαιώματα του συνδρομητή.

Τα δεδομένα προσωπικού χαρακτήρα που περιέχονται στους καταλόγους συνδρομητών (έντυπους ή ηλεκτρονικούς) ή λαμβάνονται μέσω των υπηρεσιών πληροφοριών καταλόγου πρέπει να περιορίζονται μόνο στα απαραίτητα (ονοματεπώνυμο, πατρώνυμο, διεύθυνση) ,εκτός αν ο συνδρομητής έχει δώσει τη συγκατάθεσή του για τη δημοσίευση συμπληρωματικών δεδομένων . Επίσης ο συνδρομητής δικαιούται να ζητήσει να μη συμπεριληφθεί σε κατάλογο[375].

Μία από τις σημαντικότερες ρυθμίσεις που θεσμοθετείται συνίσταται στην καθιέρωση του συστήματος « opt - in » [376], σύμφωνα με το οποίο η αποστολή ηλεκτρονικών μηνυμάτων για διαφημιστικούς σκοπούς είναι επιτρεπτή μόνο στην περίπτωση συνδρομητών που έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους. Έτσι , η αποστολή μη ζητηθέντος ηλεκτρονικού μηνύματος συνιστά παράνομη επεξεργασία, εφόσον τα υποκείμενα δεν είχαν δώσει προηγουμένως τη ρητή συγκατάθεσή τους. Για τα νομικά πρόσωπα συνδρομητές επιτρέπεται ,εκτός αν δηλωθεί από τον νόμιμο εκπρόσωπό τους ότι δεν επιθυμεί τη λήψη τέτοιων κλήσεων[377]. Οι πάροχοι τηλεπικοινωνιακών υπηρεσιών οφείλουν να λαμβάνουν όλα τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών αυτών και, σε περίπτωση ιδιαίτερου κινδύνου, να ενημερώνουν σχετικά τους

---

[369] *Βλ. άρθρο 4 παρ.2,3,4 Ν. 2774/1999.*

[370] *Που υποβάλλονται σε επεξεργασία για την πραγματοποίηση κλήσεων και αποθηκευόμενα από τον παροχέα δικτύου-τηλεπικοινωνιακής υπηρεσίας, βλ. άρθρο 5 παρ.1 Ν. 2774/1999.*

[371] *Βλ. άρθρο 5 παρ.2 Ν. 2774/1999.*

[372] *Βλ. άρθρο 5 παρ.5 Ν. 2774/1999.*

[373] *Βλ. άρθρο 6 Ν. 2774/1999.*

[374] *Βλ. άρθρο 7 Ν. 2774/1999.*

[375] *Βλ. άρθρο 8 Ν. 2774/1999.*

[376] *Κάθε ηλεκτρονικό μήνυμα που αποστέλλεται χωρίς την πρότερη ρητή συγκατάθεση του υποκειμένου, δηλαδή κάθε μήνυμα spam, είναι παράνομο. Το σύστημα αυτό είναι γνωστό στη διεθνή ορολογία ως σύστημα «opt-in»,*

βλ. ό.π., http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL.

[377] *Βλ. άρθρο 9 Ν. 2774/1999.*

συνδρομητές [378]. Η παραβίαση των διατάξεων του ν. 2774/1999, όσον αφορά τα δικαιώματα των συνδρομητών-χρηστών, δημιουργεί αστική ευθύνη στον παραβάτη[379] με καταβολή αποζημίωσης για περιουσιακή ζημία και ηθική βλάβη. Παράλληλα θεσπίζονται και ποινικές κυρώσεις για τους παραβάτες [380].

Η ραγδαία εξέλιξη των τεχνολογιών στα δημόσια δίκτυα επικοινωνίας έχουν σαν αποτέλεσμα τη διαρκή αναπροσαρμογή των νομοθετικών ρυθμίσεων προκειμένου να διασφαλίζονται τα προσωπικά δεδομένα των πολιτών. Έτσι στην Ευρωπαϊκή Ένωση η Οδηγία 97/66/Ε.Κ. (περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στις τηλεπικοινωνίες) αντικαταστάθηκε με την Οδηγία 2002/58/Ε.Κ.Η παραπάνω Οδηγία μεταφέρθηκε στην ελληνική έννομη τάξη με το Ν.3471/2006 , ο οποίος τροποποίησε το Ν 2472/1997(ΦΕΚ Α' 133/28/6/2006) και κατήργησε τον Ν 2774/1999[381].

5.4 **Ο νόμος** 3471/2006

Η θέσπιση του Ν. 3471/2006[382] για την «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών ήταν αναγκαία, προκειμένου να γίνει ενσωμάτωση της Οδηγίας 2002/58/ΕΚ[383] στην ελληνική νομοθεσία. Οι διατάξεις του Ν. 3471/2006 αποτελούν συμπλήρωση και εξειδίκευση του Ν.2472/1997 (ο οποίος αναλύθηκε παραπάνω), στο χώρο των ηλεκτρονικών επικοινωνιών. Ο Νόμος έχει εφαρμογή σε κάθε φυσικό ή νομικό πρόσωπο[384], «κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών», ενώ για τις υπόλοιπες περιπτώσεις εφαρμόζεται ο Ν 2472/1997[385]. Από τις πρώτες διατάξεις και στο παρόντα νόμο, είναι η ρύθμιση για την προστασία του απορρήτου σαν γενική αρχή για οποιαδήποτε χρήση τηλεπικοινωνιακών υπηρεσιών. Πιο εδικά ορίζεται ότι «απαγορεύεται η

---

[378] *Βλ. άρθρο 10 Ν. 2774/1999.*

[379] *Βλ. άρθρο 12 Ν. 2774/1999.*

[380] *Βλ. άρθρο 13 Ν. 2774/1999.*

[381] Βλ. , Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, Προσωπικά Δεδομένα, Εκδόσεις Αντ.Ν. Σάκκουλα, Θεσσαλονίκη 2007,ό.π., σελ 112.

[382] Η ψήφιση του Ν.3471/2006 έφερε την κατάργηση του Ν.2774/1999 βλ. άρθρο 17 Ν. 3471/2006.

[383] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002 βλ. Ν. 3471/2006, κεφ πρώτο.

[384] Όπως και ο Ν. 2774/1999, βλ. άρθρο 2 παρ. 1,2 Ν. 3471/2006.

[385] Βλ. άρθρο 3 παρ. 1,2 Ν. 3471/2006.

ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο»[386]. Γίνεται σαφές ότι απαγορεύεται η χρήση λογισμικού υποκλοπής των δεδομένων που διαβιβάζονται μέσω Διαδικτύου(packet sniffing), η αποθήκευση των δεδομένων κίνησης με σκοπό τη δημιουργία πορτρέτων προσωπικότητας των χρηστών χωρίς την συγκατάθεσή τους[387], καθώς και αρχείων Cookies.

Με τον Ν. 3471/2006 καθορίζονται προϋποθέσεις που θεμελιώνουν τη δυνατότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών: α) Συγκατάθεση του συνδρομητή ή του χρήστη[388] β) η επεξεργασία να είναι αναγκαία για την εκτέλεση της σύμβασης[389] γ) Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της[390].

Στις ρυθμίσεις του νόμου περιλαμβάνονται ζητήματα σχετικά με την αναλυτική χρέωση των παρεχόμενων υπηρεσιών[391], την ένδειξη της ταυτότητας και τον περιορισμό της αναγνώρισης καλούσας και συνδεδεμένης γραμμής[392], την αυτόματη προώθηση κλήσεων[393]. Επίσης παρέχεται το δικαίωμα στους συνδρομητές ηλεκτρονικών επικοινωνιών να επιλέγουν εάν θα συμπεριλαμβάνονται σε έντυπο ή ηλεκτρονικό κατάλογο συνδρομητών. Σε κάθε περίπτωση όμως, σύμφωνα με το ίδιο άρθρο, οι κατάλογοι αυτοί πρέπει να περιέχουν μόνο τα στοιχεία εκείνα που κρίνονται απαραίτητα για την αναγνώριση της ταυτότητας συγκεκριμένου συνδρομητή, εκτός εάν ο συνδρομητής έχει δώσει τη ρητή συγκατάθεσή του για τη δημοσίευση συμπληρωματικών δεδομένων προσωπικού χαρακτήρα[394].

Περαιτέρω, ο Νόμος ρυθμίζει θέματα σχετικά με επικοινωνίες που δεν έχουν ζητηθεί , με

---

386 Βλ. άρθρο 4 παρ.2 Ν. 3471/2006.

387 Εξαίρεση αποτελεί όταν η καταγραφή συνδιαλέξεων και δεδομένων κίνησης γίνεται στα πλαίσια νόμιμης επαγγελματικής δραστηριότητας για περισσότερα βλ άρθρο 4 παρ 3 Ν. 3471/2006, βλ.επίσης, Ιωάννη Δ.Ιγγλεζάκη ό.π., Δίκαιο της Πληροφορικής, σελ258, εκδόσεις Σάκκουλα Αθήνα- Θεσσαλονίκη 2008 .

388 Όπου ο παρών νόμος απαιτεί τη συγκατάθεση του συνδρομητή ή χρήστη, η σχετική δήλωση δίδεται εγγράφως ή με ηλεκτρονικά μέσα, β*λ. άρθρο 5 παρ. 2,3 Ν. 3471/2006.*

389 Βλ. άρθρο 5 παρ. 2, Ν. 3471/2006.

390 Βλ. άρθρο 5 παρ. 1, Ν. 3471/2006.

391 Βλ. άρθρο 7 , Ν. 3471/2006.

392 Βλ. άρθρο 8, Ν. 3471/2006.

393 Βλ. άρθρο 9, Ν. 3471/2006.

394 Βλ. άρθρο 10, Ν. 3471/2006.

σκοπό την προώθηση προϊόντων ή υπηρεσιών ή τη διαφήμιση[395] , για την ασφάλεια των δεδομένων που βρίσκονται προς επεξεργασία[396], καθώς και για τις αρμοδιότητες της Αρχής Προστασίας Προσωπικών Δεδομένων και Αρχής Διασφάλισης του Απορρήτου των επικοινωνιών[397], σχετικά με την εποπτεία εφαρμογής του νόμου[398].Για τυχόν παραβάσεις του νόμου προβλέπονται διοικητικές[399], αστικές[400] και ποινικές κυρώσεις[401].

5.5 **Ο νόμος** 3917/2011

Ο Νόμος 3917/2011 (ΦΕΚ 22/Α/21.2.2011) αναφέρεται στη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

Με τον Ν. 3917/2011 έχουμε ενσωμάτωση της οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού κοινοβουλίου που παράγονται ή υποβάλλονται σε επεξεργασία, σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και τροποποίηση της οδηγίας 2002/58/ΕΚ[402]. Οι πάροχοι υποχρεούνται να διατηρούν τα δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του εγγεγραμμένου χρήστη που υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων[403].

<u>Οι κατηγορίες των διατηρούμενων δεδομένων είναι</u>[404]:

---

[395] Βλ. άρθρο 11, Ν. 3471/2006.

[396] Βλ. άρθρο 12, Ν. 3471/2006.

[397] Βλ. άρθρο 13, Ν. 3471/2006.

[398] Βλ. , Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, Προσωπικά Δεδομένα, Εκδόσεις Αντ.Ν. Σάκκουλα, Θεσσαλονίκη 2007,ό.π., σελ 113.

[399] Βλ. άρθρο 13, παρ 4, Ν. 3471/2006.

[400] Βλ. *άρθ. 14, Ν. 3471/2006.*

[401] Βλ. *άρθ. 15, Ν. 3471/2006.*

[402] Βλ. κεφ.α , Ν. 3917/2011, στο:
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/ODIGIES/ITEMS/3917_2011.PDF

[403] Βλ.ό.π, άρθ 1 παρ.1,2 , Ν. 3917/2011

[404] Βλ.ό.π, άρθ 5 , Ν. 3917/2011

1) Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας: ο τηλεφωνικός αριθμός του καλούντος, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή του εγγεγραμμένου χρήστη, ο αποδοθείς κωδικός ταυτότητας χρήστη, ο κωδικός ταυτότητας χρήστη και ο τηλεφωνικός αριθμός που δίνονται σε κάθε επικοινωνία που εισέρχεται στο δημόσιο τηλεφωνικό δίκτυο, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί κατά το χρόνο επικοινωνίας διεύθυνση IP (πρωτοκόλλου διαδικτύου), κωδικός ταυτότητας χρήστη ή αριθμός τηλεφώνου

2) Δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας: ο αριθμός ή οι αριθμοί τηλεφώνου που κλήθηκαν, στις δε περιπτώσεις όπου έχουμε προώθηση/εκτροπή κλήσης, ο αριθμός ή οι αριθμοί τηλεφώνου προς τους οποίους προωθήθηκε η κλήση, τα ονοματεπώνυμα και οι διευθύνσεις των συνδρομητών ή εγγεγραμμένων χρηστών, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη και ο κωδικός ταυτότητας χρήστη του παραλήπτη της επικοινωνίας, ο κωδικός ταυτότητας χρήστη ή ο αριθμός τηλεφώνου του παραλήπτη διαδικτυακής τηλεφωνικής κλήσης

3) Δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας της επικοινωνίας: Η ημερομηνία και η ώρα έναρξης και λήξης της επικοινωνίας, η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το διαδίκτυο με βάση συγκεκριμένη ωριαία ζώνη, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), είτε δυναμική είτε στατική, που απέδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη, η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου, με βάση συγκεκριμένη ωριαία ζώνη

4) Δεδομένα αναγκαία για τον προσδιορισμό του είδους της επικοινωνίας: Η χρησιμοποιηθείσα τηλεφωνική υπηρεσία, η χρησιμοποιηθείσα διαδικτυακή υπηρεσία

5) Δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών ή του φερομένου ως εξοπλισμού επικοινωνίας τους

6) Δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας.

Τα δεδομένα παράγονται και αποθηκεύονται σε φυσικά μέσα, τα οποία βρίσκονται μέσα στα όρια της Ελληνικής Επικράτειας, εντός της οποίας και διατηρούνται για 12 μήνες από την ημερομηνία της επικοινωνίας. Τα δεδομένα καταστρέφονται στο τέλος του χρονικού διαστήματος διατήρησης με αυτοματοποιημένη διαδικασία από τον πάροχο, εκτός από εκείνα στα οποία έχει αποκτηθεί νομίμως πρόσβαση[405].

Τα διατηρούμενα δεδομένα είναι ίδιας ποιότητας και έχουν την ίδια προστασία και ασφάλεια με τα δεδομένα που περιέχει το δίκτυο. Λαμβάνονται τα κατάλληλα μέτρα προστασίας των δεδομένων κατά τυχαίας ή παράνομης καταστροφής τους ή τυχαίας απώλειας, αλλοίωσης, μη εξουσιοδοτημένης ή παράνομης αποθήκευσης, επεξεργασίας, πρόσβασης ή αποκάλυψης και για να διασφαλισθεί ότι στα δεδομένα έχει πρόσβαση μόνον ειδικά εξουσιοδοτημένο προσωπικό. Οι πάροχοι επίσης υποχρεούνται να εφαρμόζουν ειδικό σχέδιο πολιτικής ασφάλειας και αναθέτουν την εφαρμογή του σχεδίου αυτού σε εξουσιοδοτημένο στέλεχος, το

[405] Βλ.ό.π, άρθ 6, Ν. 3917/2011

οποίο ορίζεται ως υπεύθυνος ασφάλειας δεδομένων[406]. Οι Εποπτεύουσες Αρχές για την τήρηση του νομοθετικού πλαισίου είναι η Α.Δ.Α.Ε.και η Α.Π.Δ.Π.Χ. [407].

Η μη τήρηση των διατάξεων του παρόντος νόμου επιφέρει ποινές, όπως διοικητικές κυρώσεις και ποινές αστικής ευθύνης [408]. Στο Β μέρος του Ν. 3917/2011 γίνεται αναφορά στην εγκατάσταση και λειτουργία συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους, εφόσον συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σε ποιες περιπτώσεις επιτρέπεται:

α) τη διαφύλαξη της εθνικής άμυνας,

β) την προστασία του πολιτεύματος και την αποτροπή εγκλημάτων προδοσίας της χώρας,

γ) την αποτροπή και καταστολή εγκλημάτων που συνιστούν επιβουλή της δημόσιας τάξης,

δ) την αποτροπή και καταστολή εγκλημάτων βίας, εμπορίας ναρκωτικών, κοινώς επικίνδυνων εγκλημάτων, εγκλημάτων κατά της ασφάλειας των συγκοινωνιών και εγκλημάτων κατά της ιδιοκτησίας, όταν με βάση πραγματικά στοιχεία συντρέχουν επαρκείς ενδείξεις ότι τελέσθηκαν ή πρόκειται να τελεσθούν τέτοιες πράξεις

ε) τη διαχείριση της κυκλοφορίας

Η εγκατάσταση και λειτουργία των συστημάτων επιτήρησης σε δημόσιους χώρους γίνεται μόνο από κρατικές αρχές με τήρηση της αρχής της αναλογικότητας[409].

6 **ΚΕΦΑΛΑΙΟ**: **Ανεξάρτητες Αρχές προστασίας προσωπικών δεδομένων**

Οι Ανεξάρτητες Αρχές δεν ανήκουν σε καμία από τις παραδοσιακές λειτουργίες άσκησης εξουσίας (νομοθετική, δικαστική και εκτελεστική λειτουργία).Τουναντίον έχουν προικισθεί με εγγυήσεις πλήρους ανεξαρτησίας απέναντι στην εκάστοτε Κυβέρνηση και διακρίνονται από την εξειδίκευση, την εμπειρία και την τεχνοκρατική γνώση των μελών που τις απαρτίζουν σε σχέση με τον τομέα που έχουν υπό την εποπτεία τους. Επίσης συμβάλλουν στην ανανέωση των θεσμών και αποτελούν, στη σύντομη ιστορία τους, κεκτημένο του ευρωπαϊκού θεσμικού πολιτισμού. Δεν υπάρχει πια ευρωπαϊκή χώρα, χωρίς Ανεξάρτητες Αρχές. Απόδειξη αυτού είναι ότι οι ανεξάρτητες αρχές αναφέρονται ρητά και στο Χάρτη για τα Θεμελιώδη Δικαιώματα, την πιο πρόσφατη έκφραση της θεσμικής εξέλιξης της Ευρωπαϊκής Ένωσης. Με δύο λόγια, οι

[406] Βλ.ό.π, άρθ 7, Ν. 3917/2011

[407] Βλ.ό.π, άρθ 9, Ν. 3917/2011

[408] Βλ.ό.π, άρθ 12 και 13, Ν. 3917/2011

[409] Βλ.ό.π, άρθ 14, Ν. 3917/2011

ανεξάρτητες αρχές αποτελούν βασική παράμετρο του ευρωπαϊκού θεσμικού πολιτισμού και του υπό διαμόρφωση ευρωπαϊκού Συντάγματος[410].

Στον τομέα της προστασίας των πληροφοριών κατά την διακίνησή τους στις επικοινωνίες και ειδικότερα της προστασίας των δεδομένων προσωπικού χαρακτήρα με βάση το νομοθετικό πλαίσιο έχουμε τις ακόλουθες Ανεξάρτητες Αρχές τις οποίες θα ασχοληθούμε στη συνέχεια:

- **Α**ρχή **Π**ροστασίας **Δ**εδομένων **Π**ροσωπικού **Χ**αρακτήρα (**ΑΠΔΠΧ**)
- **Ε**θνική **Ε**πιτροπή **Τ**ηλ/νιών και **Τ**αχυδρομείων (**Ε.Ε.Τ.Τ**)
- **Α**ρχή **Δ**ιασφάλισης του **Α**πορρήτου των **Ε**πικοινωνιών (**Α.Δ.Α.Ε**)

6.1 **Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα** (**ΑΠΔΠΧ**)

Η νομοθεσία προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν θα είχε καμιά αξία, αν παράλληλα δεν είχε προβλεφθεί ένα όργανο που βασική του αποστολή θα ήταν η εποπτεία , ο έλεγχος και η εφαρμογή της σχετικής νομοθεσίας. Έτσι δημιουργήθηκε η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (**ΑΠΔΠΧ**) , η οποία είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή και δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο. Η ΑΠΔΠΧ είναι θεμέλιο του ελληνικού συστήματος προστασίας δεδομένων προσωπικού χαρακτήρα[411], ιδρύθηκε με το νόμο 2472/1997[412], ο οποίος ενσωματώνει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ[413]. Επίσης, όσον αφορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η ΑΠΔΠΧ εφαρμόζει τον νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 58/2002. Πέραν της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), οργάνου σε επίπεδο χώρας , υπάρχει και Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων σε επίπεδο Ευρωπαϊκής Ένωσης[414].

---

[410] Παπαδημητρίου Γ., Οι Ανεξάρτητες Αρχές Πορίσματα Συνεδρίου, Δημοσιεύθηκε στον τόμο: Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Η πορεία προς το Ευρωπαϊκό Σύνταγμα και η πρόσφατη αναθεώρηση του Ελληνικού Συντάγματος, Πρόλογος Β. Σκουρή, Επιμέλεια Κ. Γώγου, Αθήνα-Κομοτηνή (Εκδόσεις Αντ. Ν. Σάκκουλα) 2002, σ. 248-253

[411] Βλ. Ιωάννη Δ. Ιγγλεζάκη, Δίκαιο της Πληροφορικής, ό.π., σ 253 .

[412] Η λειτουργία της Αρχής ξεκίνησε στις 10 Νοεμβρίου 1997, *Βλ.* άρθρο 25, Νόμου 2472/1997.

[413] Η Οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης,για περισσότερα βλ http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML Σημειώνεται ότι σε κάθε χώρα της Ευρωπαϊκής Ένωσης υπάρχει μία εθνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Βλ.Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου ό.π., Προσωπικά Δεδομένα, σελ.105, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007, Βλ.επίσης Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων,ό.π., σ 235.

[414] Η θέση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) δημιουργήθηκε το 2001. Έργο του ΕΕΠΔ είναι να εξασφαλίζει ότι τα όργανα και οι οργανισμοί της Ένωσης σέβονται το δικαίωμα ιδιωτικής ζωής των πολιτών όταν

6.1.1 **Αποστολή της Αρχής**

Αποστολή της Αρχής είναι η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν. 2472/1997 και 3471/2006.Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.ο.κ). Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών[415].

6.1.2 **Οργάνωση της Αρχής**

Η Αρχή συγκροτείται από τον Πρόεδρο και έξι μέλη, και εξυπηρετείται από Γραμματεία που λειτουργεί σε επίπεδο Διεύθυνσης. Ο Πρόεδρος[416] είναι απαραίτητα δικαστικός λειτουργός βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω. Τόσο ο Πρόεδρος όσο και τα μέλη, καθώς και οι ισάριθμοι αναπληρωτές τους, διορίζονται με τετραετή θητεία που μπορεί να ανανεωθεί μία μόνο φορά. Η Γραμματεία της Αρχής αποτελείται από τρία Τμήματα: Ελεγκτών, Επικοινωνίας, Διοικητικών και Οικονομικών Υποθέσεων. Η Αρχή συνεδριάζει σε Ολομέλεια και σε Τμήμα[417].

6.1.3 **Αρμοδιότητες της Αρχής**

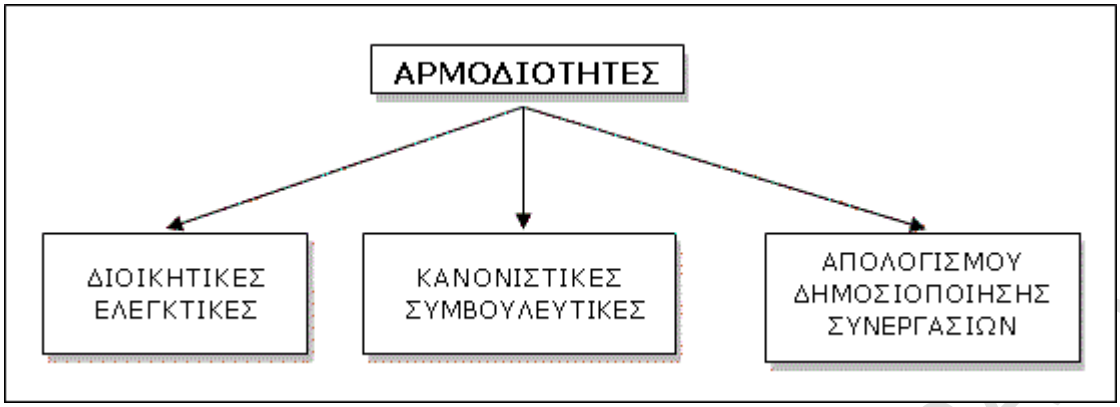
Οι αρμοδιότητες της Αρχής μπορούν να ομαδοποιηθούν σε τρεις τομείς όπως φαίνεται στην παρακάτω εικόνα: Διοικητικές ελεγκτικές, κανονιστικές συμβουλευτικές, απολογισμού δημοσιοποίησης συνεργασιών.

επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για περισσότερα βλ: http://europa.eu/about-eu/institutions-bodies/edps/index_el.htm.

[415] Βλ σχετ: http://www.dpa.gr/portal/page?_pageid=33,14970&_dad=portal&_schema=PORTAL.

[416] Πρώτος Πρόεδρος της Αρχής διετέλεσε ο επίτιμος αντιπρόεδρος του Αρείου Πάγου Κωνσταντίνος Δαφέρμος, γι' αυτό και τα πρώτα χρόνια η Αρχή ήταν γνωστή και με την ονομασία «Επιτροπή Δαφέρμου», ενώ σήμερα Πρόεδρος της Αρχής είναι ο Πέτρος Χριστόφορος, Επίτιμος Σύμβουλος της Επικρατείας..

[417] Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου ό.π., Προσωπικά Δεδομένα, σελ.106, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007.



Σχήμα 37. Αρμοδιότητες ΑΠΔΠΧ

Πηγή: http://www.dpa.gr/portal/page?_pageid=33,14983&_dad=portal&_schema=PORTAL

α. <u>Διοικητικές ελεγκτικές και εποπτικές αρμοδιότητες</u>

Η Ανεξάρτητη Αρχή ασκεί τις παρακάτω ελεγκτικές και εποπτικές αρμοδιότητες:

- Αρχείο γνωστοποιήσεων – Έκδοση αδειών.

Οι υπεύθυνοι επεξεργασίας υποχρεούνται να υποβάλλουν γνωστοποίηση προς την Αρχή για σύσταση και λειτουργία αρχείου. Βάσει των ανωτέρω γνωστοποιήσεων , η Αρχή εκδίδει άδειες[418], για τη Συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, για τη διαβίβαση δεδομένων σε χώρες εκτός Ε.Ε. ή και για τη διασύνδεση δεδομένων.

- Επίβλεψη της ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και έκδοση σχετικών οδηγιών[419].

- Άσκηση ελέγχου στο εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν[420], καθώς επίσης σε φορείς που προβλέπονται από διεθνείς συμβάσεις , όπως π.χ της **Europol(N.**

[418] Οι άδειες χορηγούνται με συγκεκριμένους όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος της ιδιωτικής ζωής των υποκειμένων ή τρίτων, ενώ η Αρχή απευθύνει υποδείξεις και συστάσεις σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας , βλ:
http://www.dpa.gr/portal/page?_pageid=33,23031&_dad=portal&_schema=PORTAL .

[419] Όπως οδηγίες για την επεξεργασία δεδομένων των εργαζομένων (1830/20.9.2001 / 115/2001), Οδηγία για την ασφαλή καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας για περισσότερα . Για περισσότερα βλ.
http://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL
Βλ. επίσης Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου ό.π., Προσωπικά Δεδομένα, σελ.107, εκδόσεις Αντ.Ν.Σάκκουλα Θεσσαλονίκη 2007 .

[420] « Κάθε συμβαλλόμενο μέρος ορίζει μια αρχή ελέγχου η οποία, τηρουμένης της εθνικής νομοθεσίας, είναι επιφορτισμένη να ασκεί ανεξάρτητο έλεγχο του αρχείου του εθνικού τμήματος του συστήματος πληροφοριών Σένγκεν και να ελέγχει αν η επεξεργασία και η χρήση των καταχωρημένων στο σύστημα πληροφοριών Σένγκεν δεδομένων δεν

2605/1998 ΦΕΚ 88 Α')[421] , αρμοδιοτήτων της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 17 της Σύμβασης για τη χρήση της πληροφορικής στον τελωνειακό τομέα (Ν. 2706/1999 ΦΕΚ 77 Α'), καθώς και αρμοδιοτήτων εποπτείας που προκύπτουν από οποιαδήποτε άλλη διεθνή συμφωνία.

- Διενέργεια διοικητικών ελέγχων, αυτεπαγγέλτως ή κατόπιν καταγγελίας , σε αρχεία, τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Οι έλεγχοι διενεργούνται από εντεταλμένους υπαλλήλους του Τμήματος των Ελεγκτών, οι οποίοι συνοδεύονται σε περιπτώσεις που κρίνονται σημαντικές από μέλη της Αρχής. Οι διενεργούντες τον έλεγχο, ως ειδικοί ανακριτικοί υπάλληλοι, έχουν δικαίωμα πρόσβασης σε κάθε αρχείο χωρίς να μπορεί να τους αντιταχθεί κανενός είδους απόρρητο. Κατά τον έλεγχο εξετάζεται καταρχήν η εναρμόνισή του ελεγχόμενου με τις απαιτήσεις των Ν.2472/97, 3471/2006 (γνωστοποίηση, ενημέρωση, λοιπές υποχρεώσεις κατά περίπτωση, αποδεικτικά στοιχεία). Στη συνέχεια πραγματοποιείται έλεγχος του πληροφοριακού του συστήματος, όπου σύμφωνα με τα άρθρα 6 και 10 του ν. 2472/1997, εξετάζονται τα βασικά χαρακτηριστικά του συστήματος, η φύση των δεδομένων, καθώς και το επίπεδο ασφαλείας που εξασφαλίζουν τα οργανωτικά και τεχνικά μέτρα που έχει λάβει ο υπεύθυνος επεξεργασίας για την προστασία των δεδομένων.

παραβιάζουν τα δικαιώματα του οικείου προσώπου. Προς τον σκοπό αυτόν, η αρχή ελέγχου έχει πρόσβαση στο αρχείο του εθνικού τμήματος του συστήματος πληροφοριών Σένγκεν», όπως χαρακτηριστικά αναφέρει η σύμβαση Σένγκεν, άρθρο 114 παρ.1(2514/1997 ΦΕΚ 140 Α'), βλ στο:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922%2802%29:el:HTML

επίσης στο: http://schengen.consilium.europa.eu/about.aspx?lang=el

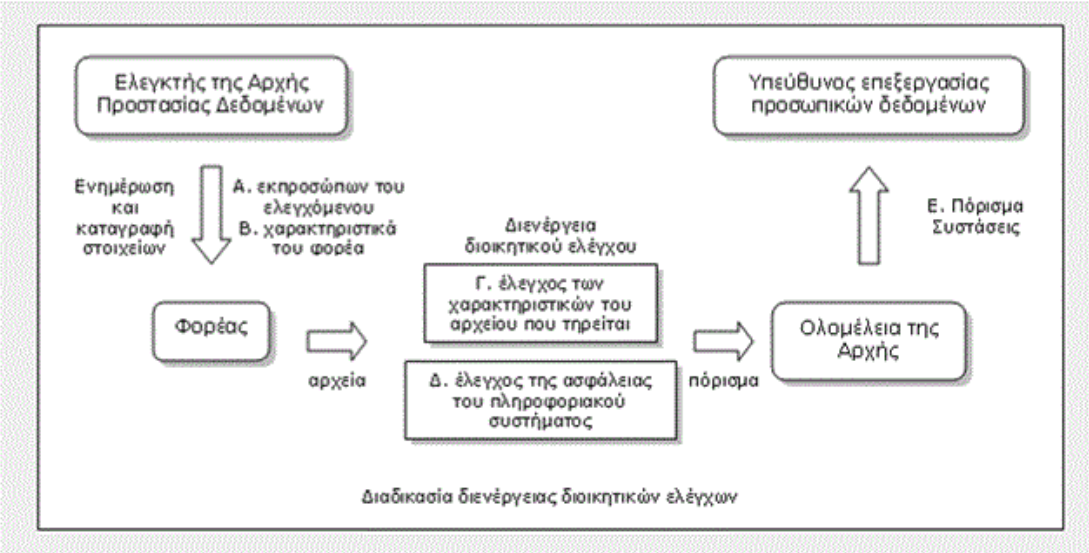
421 Η Ευρωπόλ (EUROPOL, από τις αγγλικές λέξεις European Police Office), όπως αποδίδεται στην ελληνική, είναι ο οργανισμός που ιδρύθηκε και τέθηκε σε πλήρη λειτουργία την 1 Ιανουαρίου 1999,για να συνδράμει τα κράτη μέλη της ΕΕ στην πρόληψη και καταπολέμηση σοβαρών μορφών διεθνούς εγκληματικότητας, μόνο στην περίπτωση που η συγκεκριμένη εγκληματική πράξη συνδέεται με δομή οργανωμένου εγκλήματος και θίγει δύο τουλάχιστον κράτη μέλη. Σε πρακτικό επίπεδο, κύριο καθήκον της Ευρωπόλ είναι η διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και η παροχή αναλυτικών υπηρεσιών εμπειρογνωμοσύνης. Δεδομένου ότι η Ευρωπόλ χειρίζεται μεγάλο όγκο ευαίσθητων πληροφοριών προσωπικού χαρακτήρα, η σύμβαση Ευρωπόλ περιέχει διάφορες διατάξεις που απαιτούν από αυτήν να λαμβάνει υπόψη τα δικαιώματα του ατόμου όταν κάνει χρήση των πληροφοριών αυτών. Η σύμβαση προβλέπει επίσης την ίδρυση της Κοινής Εποπτικής Αρχής − μιας ανεξάρτητης αρχής επιφορτισμένης με τη διασφάλιση της συμμόρφωσης της Ευρωπόλ προς τις βασικές αρχές της προστασίας δεδομένων. Η Αρχή Προστασίας Δεδομένων εκπροσωπείται στην Κοινή Εποπτική Αρχή (ΚΕΑ) για την Ευρωπόλ, όπως επίσης στην Κοινή Εποπτική Αρχή για τα Τελωνεία που συνεδριάζουν στην έδρα του Συμβουλίου στις Βρυξέλλες, με δύο τακτικά και δύο αναπληρωματικά μέλη. Εκπροσωπείται επίσης στην Επιτροπή Προσφυγών που λειτουργεί στο πλαίσιο της ΚΕΑ Ευρωπόλ με ένα τακτικό και ένα αναπληρωματικό μέλος. για περισσότερα βλέπε:

http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/l14005b_el.htm

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999F0330:EL:HTML

http://europoljsb.consilium.europa.eu/about.aspx?lang=el

.



Σχήμα 38. Διαδικασία διενέργειας διοικητικών ελέγχων.

Πηγή: http://www.dpa.gr/portal/page?_pageid=33,23031&_dad=portal&_schema=PORTAL

Η ολοκλήρωση του ελέγχου οδηγεί στην σύνταξη πορίσματος το οποίο υποβάλλεται στην ολομέλεια της Αρχής. Η γενική διαδικασία ενός ελέγχου περιγράφεται στο παραπάνω σχήμα 38.

- Εξέταση προσφυγών- καταγγελιών-ερωτημάτων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων και εκδίδει σχετικές Αποφάσεις. Επίσης, επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον νόμο 2472/97 και από κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τέλος, η Αρχή μπορεί να καταγγέλλει τις παραβάσεις των διατάξεων του νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

β. Κανονιστικές συμβουλευτικές . Η Αρχή εκδίδει Οδηγίες με σκοπό ενιαία εφαρμογή των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επίσης, απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές, και υποστηρίζει τα επαγγελματικά σωματεία και λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία στην κατάρτιση κωδίκων δεοντολογίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα. Τέλος, η Αρχή γνωμοδοτεί για κάθε ρύθμιση που αφορά στην επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

γ. Δημοσιοποίησης απολογισμού συνεργασιών. Στόχος της ΑΠΔΠΧ είναι η ενημέρωση και ευαισθητοποίηση των υποκειμένων των δεδομένων καθώς και των υπεύθυνων επεξεργασίας ως προς τα δικαιώματα και τις υποχρεώσεις τους. Έτσι η Αρχή:

• Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος[422].

• Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

• Συνεργάζεται με αντίστοιχες αρχές άλλων κρατών μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της[423].

6.1.4 **Γνωμοδοτήσεις – αποφάσεις της Αρχής**

Υπάρχει μια πληθώρα γνωμοδοτήσεων και αποφάσεων της ΑΠΔΠΧ, μέσα από το οποίο φαίνεται το σπουδαίο έργο αυτής της Ανεξάρτητης Αρχής και την αναγκαιότητα της ύπαρξής της. Αναφέρουμε σημαντικές αποφάσεις γνωμοδοτήσεις της Αρχής παρακάτω. Η ταξινόμηση αφορά τις ενότητες Τεχνολογίες INTERNET, Ηλεκτρονικές επικοινωνίες και μέσα μαζικής επικοινωνίας. Για περισσότερα ο αναγνώστης μπορεί να ανατρέξει στον δικτυακό τόπο τη Αρχής[424].

Ενότητα Τεχνολογίες INTERNET

ΑΠΟΦΑΣΗ ΑΡ.59/2012 - Παραβίαση προσωπικών δεδομένων σε εταιρεία παραγωγής φωνογραφημάτων, φορέων ήχου και εικόνας.

ΑΠΟΦΑΣΗ ΑΡ.54/2011 - Για τη δημοσιοποίηση στο διαδίκτυο στοιχείων φορολογικών παραβατών απαιτείται ρητή νομοθετική πρόβλεψη.

ΑΠΟΦΑΣΗ ΑΡ.13/2011 - Αναδημοσίευση προσωπικών δεδομένων στο διαδίκτυο.

ΑΠΟΦΑΣΗ ΑΡ. 43/2009 - Δημοσίευση δικαστικής απόφασης σε δικτυακό τόπο δικηγορικού γραφείου και σε έντυπες και ηλεκτρονικές εκδόσεις αλλοδαπών νομικών επιθεωρήσεων.

ΑΠΟΦΑΣΗ ΑΡ. 37/2007 Έλεγχος υπολογιστή εργαζομένου.

ΑΠΟΦΑΣΗ ΑΡ. 20/2008- Ζωντανή μετάδοση στο διαδίκτυο από κλειστό κύκλωμα τηλεόρασης εγκατεστημένο σε χώρους διασκέδασης και εστίασης (καφέ, μπαρ, κλπ).

[422] Βλ .τον αναλυτικό πίνακα Ετήσιων Εκθέσεων της ΑΠΔΠΧ για τα έτη 1999-2010 στο:http://www.dpa.gr/portal/page?_pageid=33,15078&_dad=portal&_schema=PORTAL

[423] Βλ .σχ. ό.π. http://www.dpa.gr/portal/page?_pageid=33,23266&_dad=portal&_schema=PORTAL

Ενότητα: Ηλεκτρονικές Επικοινωνίες

ΑΡ.132/2012 - Επιβολή χρηματικού προστίμου ύψους τριάντα χιλιάδων (30.000,00) Ευρώ σε πάροχο τηλεπικοινωνιακών υπηρεσιών για παράβαση του άρθρου 13 παρ. 1 του Ν. 2472/1997 και του άρθρου 8 παρ. 2 του Ν. 2774/1999.

ΑΠΟΦΑΣΗ ΑΡ.112/2012 - Όροι και προϋποθέσεις για τη σύμφωνη με την προστασία δεδομένων προσωπικού χαρακτήρα παροχή υπηρεσιών γεωεντοπισμού ευπαθών ομάδων και ανηλίκων.

ΑΠΟΦΑΣΗ ΑΡ.29/2012 - Δημοσίευση προσωπικών δεδομένων σε ιστοσελίδα του διαδικτύου.

ΟΔΗΓΙΑ ΑΡ.2/2011 - Ηλεκτρονική συγκατάθεση στο πλαίσιο του άρθρου 11 του ν. 3471/2006.

ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ.4/2010 - Ηλεκτρονική κάρτα αποδείξεων.

ΑΠΟΦΑΣΗ ΑΡ. 31/2010 - Πιλοτικό βιομετρικό σύστημα ελέγχου πρόσβασης σε κρίσιμες εγκαταστάσεις του Διεθνούς Αερολιμένα «Μακεδονία».

ΑΠΟΦΑΣΗ ΑΡ. 91/2009 - Υπηρεσία εικονικής περιήγησης στους δρόμους ελληνικών περιοχών.

ΑΠΟΦΑΣΗ ΑΡ. 83/2009 - Παράνομη η συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου και άλλων προσωπικών δεδομένων από ιστοσελίδες και επαγγελματικές ενώσεις χωρίς συγκατάθεση των συνδρομητών.

ΑΠΟΦΑΣΗ ΑΡ. 17/2007 - Απώλεια προσωπικών δεδομένων από αντικατάσταση σκληρού δίσκου κατά την επισκευή από εταιρεία.

ΑΠΟΦΑΣΗ ΑΡ. 55/2006 - Πρόστιμο σε εταιρεία παροχής τηλεπικοινωνιακών υπηρεσιών για παραβίαση του Άρθρου 5 παρ.1 (συγκατάθεση του υποκειμένου) και του Άρθρου 13 παρ. 1 (δικαίωμα αντίρρησης) του Ν. 2472/97.

ΑΠΟΦΑΣΗ ΑΡ. 37/2004 Χορήγηση στοιχείων συνδρομητή / δράστη κακόβουλων κλήσεων από εταιρεία παροχής τηλεπικοινωνιακών υπηρεσιών.

ΑΠΟΦΑΣΗ ΑΡ. 33/2004 Ανακοίνωση γεωγραφικής θέσης κινητού με σκοπό την υπεράσπιση δικαιώματος ενώπιον δικαστηρίου.

ΑΠΟΦΑΣΗ ΑΡ. 27/2003 - Παράνομη επεξεργασία προσωπικών δεδομένων συνδρομητή τηλεπικοινωνιακών υπηρεσιών.

ΑΠΟΦΑΣΗ ΑΡ. 79/2002 Γνωμοδότηση σχετικά με ανακοίνωση προσωπικών δεδομένων συνδρομητών εταιρείας κινητής τηλεφωνίας σε αιτούντες τρίτους, εισαγγελείς, ανακριτικούς ή προανακριτικούς υπαλλήλους ή πολίτες.

ΑΠΟΦΑΣΗ ΑΡ. 1697/2000 - Άρση απορρήτου των τηλεπικοινωνιακών υπηρεσιών και άρση ενημέρωσης υποκειμένου.

---

[424] Βλ .σχ. http://www.dpa.gr/portal/page?_pageid=33,23266&_dad=portal&_schema=PORTAL

Ενότητα:Μέσα Μαζικής Ενημέρωσης

ΑΠΟΦΑΣΗ ΑΡ.63/2010 - Παράνομη δημοσίευση προσωπικών δεδομένων, ιδίως φωτογραφιών, σε εφημερίδα, χωρίς να θεμελιώνεται ως υπερέχον το δικαίωμα του κοινού στην πληροφόρηση.

ΑΠΟΦΑΣΗ ΑΡ. 8/2010 - Παράνομη δημοσιοποίηση ευαίσθητων δεδομένων από εφημερίδα. Απαγόρευση αναδημοσίευσης του επίμαχου δημοσιεύματος στην έντυπη έκδοση της εφημερίδας. Υποχρέωση ανωνυμοποίησης των στοιχείων του προσφεύγοντος στο δημοσίευμα που είναι αναρτημένο στο διαδικτυακό τόπο της εφημερίδας. (Η ΑΠΟΦΑΣΗ ΑΝΑΚΛΗΘΗΚΕ ΜΕ ΤΗΝ ΥΠ` ΑΡΙΘΜ. 73/2011 ΑΠΟΦΑΣΗ ΤΗΣ ΑΡΧΗΣ).

ΠΡΟΣΩΡΙΝΗ ΔΙΑΤΑΓΗ ΑΡ. 3/2009 - Άμεση αναστολή μετάδοσης στο Διαδίκτυο εικόνας σε πραγματικό χρόνο και με συνεχή ροή από τις εισόδους των κεντρικών γραφείων πολιτικών κομμάτων.

ΑΠΟΦΑΣΗ ΑΡ. 11/2008-Περίπτωση νόμιμης δημοσιοποίησης από την εργοδότρια εταιρεία δεδομένων προσωπικού χαρακτήρα μελών της διοίκησης του σωματείου εργαζομένων στην επιχείρηση - Περίπτωση νόμιμης δημοσιοποίησης από το σωματείο εργαζομένων στην επιχείρηση ποινικής καταδίκης του νόμιμου εκπροσώπου της εταιρείας.

ΑΠΟΦΑΣΗ ΑΡ.6/2008 - Επιβολή κυρώσεων στην εταιρεία EXCOM ΑΕ, ιδιοκτήτρια του τηλεοπτικού σταθμού Extra Channel 3, και σε δημοσιογράφο του εν λόγω σταθμού, για αθέμιτη επεξεργασία δεδομένων προσωπικού χαρακτήρα του προσφεύγοντος. (Η ΑΠΟΦΑΣΗ ΑΝΑΚΛΗΘΗΚΕ ΜΕ ΤΗΝ ΥΠ` ΑΡΙΘΜ. 73/2011 ΑΠΟΦΑΣΗ ΤΗΣ ΑΡΧΗΣ).

ΑΠΟΦΑΣΗ ΑΡ. 18/2008 - Επιβολή κυρώσεων στην εκδοτική εταιρεία ΚΟΥΡΗΣ MEDIA GROUP ΜΟΝΟΠΡΟΣΩΠΗ ΕΠΕ, ως υπεύθυνο επεξεργασίας, για τη δημοσίευση στην εφημερίδα ``ΑΥΡΙΑΝΉ`` σειράς φωτογραφιών, που αναφέρονται αποκλειστικά σε στιγμές της ιδιωτικής ζωής των απεικονιζόμενων προσώπων. (Η ΑΠΟΦΑΣΗ ΑΝΑΚΛΗΘΗΚΕ ΜΕ ΤΗΝ ΥΠ` ΑΡΙΘΜ. 73/2011 ΑΠΟΦΑΣΗ ΤΗΣ ΑΡΧΗΣ).

ΑΠΟΦΑΣΗ ΑΡ.4/2008 - Επιβολή κυρώσεων στην εκδοτική εταιρεία ΠΗΓΑΣΟΣ ΕΚΔΟΤΙΚΗ ΑΕ, ως υπεύθυνο επεξεργασίας, για τη δημοσίευση στην εφημερίδα ``ΕΘΝΟΣ`` φωτογραφίας του ανήλικου άρρενος τέκνου των προσφευγόντων κατά τρόπο προσβλητικό για την προσωπικότητά του. (Η ΑΠΟΦΑΣΗ ΑΝΑΚΛΗΘΗΚΕ ΜΕ ΤΗΝ ΥΠ` ΑΡΙΘΜ. 120/2011 ΑΠΟΦΑΣΗ ΤΗΣ ΑΡΧΗΣ).

ΑΠΟΦΑΣΗ ΑΡ. 43/2007 Νόμιμη, κατά τον Ν.2472/97, επεξεργασία προσωπικών δεδομένων για δημοσιογραφικό σκοπό, με δημοσίευμα σε εφημερίδα, σχετικά με τον έλεγχο δημοσίου προσώπου.

ΑΠΟΦΑΣΗ ΑΡ. 38/2005 - Μη νόμιμη επεξεργασία προσωπικών δεδομένων από τηλεοπτικό σταθμό.

ΑΠΟΦΑΣΗ ΑΡ. 6/2005 - Παράνομος σχηματισμός αρχείου με προσωπικά δεδομένα και επεξεργασία (ανακοίνωση) των δεδομένων αυτών σε εκπομπές Τηλ/κού Σταθμού.

6.2 **Εθνική Επιτροπή Τηλ/νιών και Ταχυδρομείων (Ε.Ε.Τ.Τ)**

Η ΕΕΤΤ [425] (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων), είναι η Ανεξάρτητη Αρχή η οποία ελέγχει, ρυθμίζει και εποπτεύει:

☞ την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου

☞ την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Επιπλέον, η ΕΕΤΤ ασκεί τις αρμοδιότητες Επιτροπής Ανταγωνισμού στις εν λόγω αγορές.

6.2.1 **Αρμοδιότητες Ε.Ε.Ε.Τ**

Το νομοθετικό πλαίσιο καθορίζει τις αρμοδιότητες[426] της Εθνική Επιτροπή Τηλ/νιών και Ταχυδρομείων (Ε.Ε.Τ.Τ). Έτσι η Ε.Ε.Τ.Τ:

☞ Ρυθμίζει τα θέματα που αφορούν τον α) καθορισμό σχετικών αγορών, προϊόντων ή υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ελληνική Επικράτεια, β) τον ορισμό και τις υποχρεώσεις Παρόχων με Σημαντική Ισχύ στις ανωτέρω σχετικές αγορές σύμφωνα με την εθνική και κοινοτική νομοθεσία.

☞ Εποπτεύει και ελέγχει τους παρόχους δικτύων, επιβάλλει τις σχετικές κυρώσεις, τηρεί και διαχειρίζεται το Μητρώο Παρόχων Δικτύων και Επικοινωνιών και το εθνικό μητρώο ραδιοσυχνοτήτων.

☞ Εκδίδει Κώδικες Δεοντολογίας για την παροχή δικτύων και υπηρεσιών των ηλεκτρονικών επικοινωνιών.

☞ Μεριμνά για την τήρηση της νομοθεσίας περί ηλεκτρονικών επικοινωνιών, εφαρμόζει τις διατάξεις του Ν. 703/1977, όπως ισχύει, και επιβάλει σχετικές κυρώσεις.

☞ Συνεργάζεται με τις Ρυθμιστικές Αρχές των λοιπών κρατών μελών της Ευρωπαϊκής Ένωσης ή τρίτων κρατών, καθώς και με κοινοτικούς ή διεθνείς φορείς σε θέματα αρμοδιότητάς της.

☞ Ρυθμίζει τα θέματα που αφορούν στις Γενικές Άδειες, τα θέματα φορητότητας αριθμών, της επιλογής ή / και προεπιλογής φορέα και ελέγχει την εφαρμογή των σχετικών διατάξεων.

---

[425] Ιδρύθηκε το 1992 με τον Ν.2075 με την επωνυμία Εθνική Επιτροπή Τηλεπικοινωνιών (ΕΕΤ) και οι αρμοδιότητές της επικεντρώνονταν στην εποπτεία της απελευθερωμένης αγοράς των τηλεπικοινωνιών. Με την ψήφιση του Ν.2668/98 , ανατέθηκε στην ΕΕΤ και η ευθύνη για την εποπτεία και ρύθμιση της αγοράς των ταχυδρομικών υπηρεσιών και μετονομάστηκε σε Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ), για περισσότερα βλ: http://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/

[426] Βλ: http://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/

☞ Διαχειρίζεται το Εθνικό Σχέδιο Αριθμοδότησης (Ε.Σ.Α.).

☞ Χορηγεί τα δικαιώματα χρήσης ραδιοσυχνοτήτων, τις άδειες κατασκευών κεραιών στην ξηρά.

☞ Ρυθμίζει τα θέματα ονομάτων χώρου στο Διαδίκτυο με κατάληξη ".gr" και είναι αρμόδια για θέματα ονομάτων χώρου με κατάληξη ".eu".

☞ Ρυθμίζει τα θέματα της ηλεκτρονικής υπογραφής, πρόσβασης και διασύνδεσης.

☞ Ρυθμίζει και εποπτεύει, θέματα προστασίας του καταναλωτή στον τομέα των ηλεκτρονικών επικοινωνιών και στον τομέα παροχής ταχυδρομικών υπηρεσιών.

☞ Διαχειρίζεται το εμπορικό φάσμα ραδιοσυχνοτήτων με την εξαίρεση της ραδιοφωνίας και της τηλεόρασης.

☞ Καθορίζει τις περιπτώσεις στις οποίες απαιτούνται δικαιώματα χρήσης ραδιοσυχνοτήτων, καθώς και τα τέλη χρήσης ραδιοσυχνοτήτων.

☞ Εποπτεύει και ελέγχει την χρήση του φάσματος επιβάλλοντας σχετικές κυρώσεις.

☞ Είναι ο αρμόδιος φορέας για τα θέματα διάθεσης και χρήσης του τερματικού τηλεπικοινωνιακού εξοπλισμού και του ραδιοεξοπλισμού.

6.3 **Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε)**

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) είναι ανεξάρτητη αρχή, που έχει διοικητική αυτοτέλεια. Έδρα της Α.Δ.Α.Ε. είναι η Αθήνα, μπορεί όμως, με απόφασή της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Η σύστασή της έγινε με την ψήφιση του νόμου 3115/2003 και σύμφωνα με την παράγραφο 2 του άρθρου 19 του Συντάγματος, με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου[427].

6.3.1 **Αρμοδιότητες (Α.Δ.Α.Ε)**

Η Α.Δ.Α.Ε., για την εκπλήρωση της αποστολής της, έχει τις ακόλουθες αρμοδιότητες[428]:

☞ Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, τακτικούς και έκτακτους ελέγχους, σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφο της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με

---

[427] Βλ άρθ.1,παρ.1,2, Ν. 3115/2003 (ΦΕΚ Α΄ 47/27-2-2003) στο: http://www.adae.gr/portal/fileadmin/docs/nomoi/N.3115-2003.pdf

[428] Βλ ό.π , άρθ.6, παρ 1, Ν. 3115/2003 (ΦΕΚ Α΄ 47/27-2-2003)

ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία. Κατά τον έλεγχο αρχείων που τηρούνται για λόγους εθνικής ασφάλειας παρίσταται αυτοπροσώπως ο Πρόεδρος της Α.Δ.Α.Ε.

☞ Λαμβάνει πληροφορίες σχετικές με την αποστολή των παραπάνω υπηρεσιών και καλεί σε ακρόαση, τους νόμιμους εκπροσώπους, τους υπαλλήλους και κάθε άλλο πρόσωπο, το οποίο κρίνει ότι μπορεί να συμβάλλει στην εκπλήρωση της αποστολής της.

☞ Προβαίνει στην κατάσχεση μέσων παραβίασης του απορρήτου, που υποπίπτουν στην αντίληψή της κατά την άσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

☞ Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

☞ Τηρεί αρχείο απόρρητης αλληλογραφίας.

☞ Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών, με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.

☞ Συντάσσει κάθε χρόνο έκθεση πεπραγμένων, στην οποία περιγράφει το έργο της, διατυπώνει παρατηρήσεις, επισημαίνει παραλείψεις και προτείνει τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα διασφάλισης του απορρήτου των επικοινωνιών.

☞ Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

☞ Εκδίδει τον κανονισμό εσωτερικής λειτουργίας της, ο οποίος πρέπει να είναι σύμφωνος με τις διατάξεις του Κώδικα Διοικητικής Διαδικασίας.

☞ Εκδίδει κανονιστικές πράξεις, με τις οποίες ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της, καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών.

7 **ΚΕΦΑΛΑΙΟ**: **Προβληματισμοί-Συμπεράσματα-Προτάσεις**

7.1 **Σκέψεις προβληματισμού**

Η ραγδαία ανάπτυξη του Διαδικτύου τόσο σε επίπεδο πλήθους χρηστών, όσο και σε επίπεδο παρεχόμενων υπηρεσιών και η διείσδυσή του σε περισσότερα στρώματα της Κοινωνίας δημιουργεί τεράστια οφέλη για τα μέλη αυτής της κοινωνίας της επονομαζόμενης Κοινωνία της Πληροφορίας. Ποτέ άλλοτε ο άνθρωπος δεν είχε τόσες ευκαιρίες για ενημέρωση και πρόσβαση σε κάθε είδους πληροφορία. Ο κόσμος φαντάζει μικρός, καθώς ο χρήστης του internet μπορεί να μιλήσει με κάθε άλλο χρήστη σε οποιοδήποτε σημείο του πλανήτη. Τα Πανεπιστήμια με τα προγράμματα που αναπτύσσουν, τα ερευνητικά τους κέντρα, οι βιβλιοθήκες αυτών, επιστημονικά περιοδικά που φιλοξενούν ερευνητικές εργασίες, είναι στη διάθεση κάθε ερευνητή και επιστήμονα που ενδιαφέρεται για την ανάπτυξη της επιστήμης του. Η ψυχαγωγία μέσα από το Διαδίκτυο είναι ελκυστική και άμεση καθώς είναι στη διάθεση κάθε ενδιαφερόμενου ταινίες

κινηματογράφου, τηλεοπτικές σειρές, θεατρικά έργα, μουσική για κάθε επιθυμία, ψυχαγωγικά παιχνίδια που μπορεί να παίξει μόνος του αλλά και με άλλους χρήστες. Μια σειρά λειτουργίες και χρήσεις που παρέχονται, εξυπηρετούν τον χρήστη στην καθημερινότητά του καθώς μπορεί μέσα από την οθόνη του υπολογιστή του να πληρώνει τους λογαριασμούς του να πραγματοποιεί τραπεζικές συναλλαγές, να καταθέτει την φορολογική του δήλωση, να συναλλάσσεται με το Δημόσιο. Η πραγματοποίηση ηλεκτρονικών αγορών από το σπίτι είναι μια πραγματικότητα καθώς υπάρχει η δυνατότητα περιήγησης σε ηλεκτρονικά καταστήματα από όλο τον κόσμο και η επιλογή κατάλληλων προϊόντων για αγορά.

Τα οφέλη που προκύπτουν από τη χρήση του Διαδικτύου είναι τεράστια και πλέον αδιαμφισβήτητα, ιδίως εφόσον πρόκειται για τη συμβολή του στη λειτουργία επιχειρήσεων (ηλεκτρονικό εμπόριο, ψηφιακή οικονομία), οργανισμών αλλά και του ίδιου του κράτους (ηλεκτρονική διακυβέρνηση, ψηφιακή κοινωνία) καθώς και της ίδιας της κοινωνίας με πολυδιάστατη χρήση του Διαδικτύου σε όλες σχεδόν τις εκφράσεις της καθημερινής ζωής.

Η συστηματική χρήση του στην καθημερινότητα , στην εκπαίδευση, στις συναλλαγές, στην ψυχαγωγία έχει δημιουργήσει μια σειρά προβλημάτων, τα οποία χρήζουν βοήθειας τόσο από την Επιστήμη της Πληροφορικής όσο και της Νομικής Επιστήμης. Υπό την επίδραση των τεχνολογικών αλλαγών κάθε βάση δεδομένων με προσωπικές πληροφορίες, κάθε πληροφοριακό σύστημα, κάθε υπολογιστής, καθίσταται δυνητικά πιθανός στόχος κακόβουλης χρήσης και διαχείρισης (ψηφιακής εγκληματικότητας και υποκλοπής). Η εισαγωγή της πληροφοριακής τεχνολογίας σε όλο και περισσότερους τομείς της οικονομικής και κοινωνικής ζωής, η αύξηση της μηχανογράφησης και δικτύωσης της πληροφορίας, οι σύγχρονες μορφές συναλλαγών και οι νέες τεχνολογίες που παρέχουν με ευκολία αυτοματοποιημένη συλλογή και επεξεργασία πληροφοριών καθιστούν το θέμα της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας στο Διαδίκτυο μείζον. Η διαθεσιμότητα και διάδοση της τεχνολογίας καθιστά τον καθένα «εν δυνάμει» πηγή επεξεργασίας πληροφορίας και συνακόλουθα πηγή παραβίασης δικαιωμάτων.

Το παράδειγμα της παράνομης συλλογής προσωπικών δεδομένων από ξεκλείδωτα δίκτυα Wi-Fi που εντόπιζαν τα διερχόμενα αυτοκίνητα της υπηρεσίας Street View της Google στις περιηγήσεις τους ανά τον κόσμο, από το 2008 έως το 2010 δεν φαίνεται να είναι μεμονωμένο περιστατικό[429]. Το παγκόσμιο χωριό Facebook των 900 εκ. μελών, όπου τα μέλη του με δική τους βούληση προβάλλουν προσωπικά στοιχεία και πληροφορίες, δεδομένα θέσης και κίνησης δείχνουν μια επίσης άλλη πλευρά εύκολης συλλογής πληροφοριών. Όπως επισημαίνει η νομικός κυρία Άννα-Μαρία Πισκοπάνη «με τις σελίδες κοινωνικής δικτύωσης τα όρια μεταξύ του ιδιωτικού και του δημόσιου χώρου αναδιατάσσονται και το μέγεθος της έκθεσης των προσωπικών μας δεδομένων θέτει εκ νέου ερωτήματα γύρω από τα όρια της ιδιωτικότητας και της επιτήρησης στον ψηφιακό κόσμο. Το δίκαιο προστασίας της ιδιωτικότητας προς στιγμήν φαίνεται αδύναμο να αντιμετωπίσει αυτές τις νέες προκλήσεις και είναι βέβαιο ότι απαιτείται η αναθεώρησή του. **Οι προσωπικές μας πληροφορίες έχουν τεράστια εμπορική αξία** και το Facebook έχει κάνει μεγάλες προσπάθειες για να τις εκμεταλλευτεί οικονομικά. Χωρίς τη δημιουργία ενός νέου επιχειρηματικού μοντέλου και μιας καινούργιας πολιτικής απορρήτου από

[429] Βλ σχετικό άρθ. στην πύλη ενημέρωσης in.gr στο : http://tech.in.gr/news/article/?aid=1231193654

τις εν λόγω ιστοσελίδες, που θα σέβονται τη συγκατάθεση και την ιδιωτικότητα του χρήστη, οι επισκέπτες ενδέχεται να χάσουν κάθε έλεγχο στα δεδομένα τους»[430].

Στο μεταξύ, καινοτόμες τεχνολογίες καθιερώνουν νέες διαδικτυακές λειτουργίες και υπηρεσίες, με νέους νομικούς προβληματισμούς για τον χρήστη τους. Η καταγραφή των δεδομένων κίνησης και θέσης, η αξιοποίηση των δεδομένων στα δίκτυα κοινωνικής δικτύωσης όπως το Facebook, η αυξημένη χρήση συστημάτων βιομετρίας, η εξόρυξη δεδομένων επιτρέπουν τη διεισδυτική αποτύπωση στα χαρακτηριστικά ενός χρήστη και της σκιαγράφησης της προσωπικότητάς του. Στη χρήση της βιομετρίας συμπεριλαμβάνεται και η χρήση γενετικού υλικού, η συλλογή και ανάλυση του οποίου αποκαλύπτει πληροφορία όχι μόνο για την ταυτότητα αλλά και για τη βιολογική κατάσταση και την υγεία του προσώπου και των συγγενών του[431].

Στην κατεύθυνση αυτή επιβάλλεται η εξεύρεση ολοκληρωμένων λύσεων, ώστε να επιτευχθεί η εξασφάλιση των δικαιωμάτων των ηλεκτρονικά «επικοινωνούντων – συναλλασσομένων», να εδραιωθεί το απαιτούμενο αίσθημα ασφάλειας, αλλά και από την άλλη πλευρά να αξιοποιηθούν οι διαδικτυακές υπηρεσίες που διατίθενται στον μέγιστο βαθμό. Η εξεύρεση λύσεων δεν πρέπει να έχει χαρακτήρα τοπικό αλλά οικουμενικό μέσα από διεθνείς συνεργασίες για μια ομοιογενή επίλυση των θεμάτων που προκαλεί η ραγδαία εξάπλωση του Διαδικτύου και των νέων τεχνολογιών.

7.2 **Συμπεράσματα**

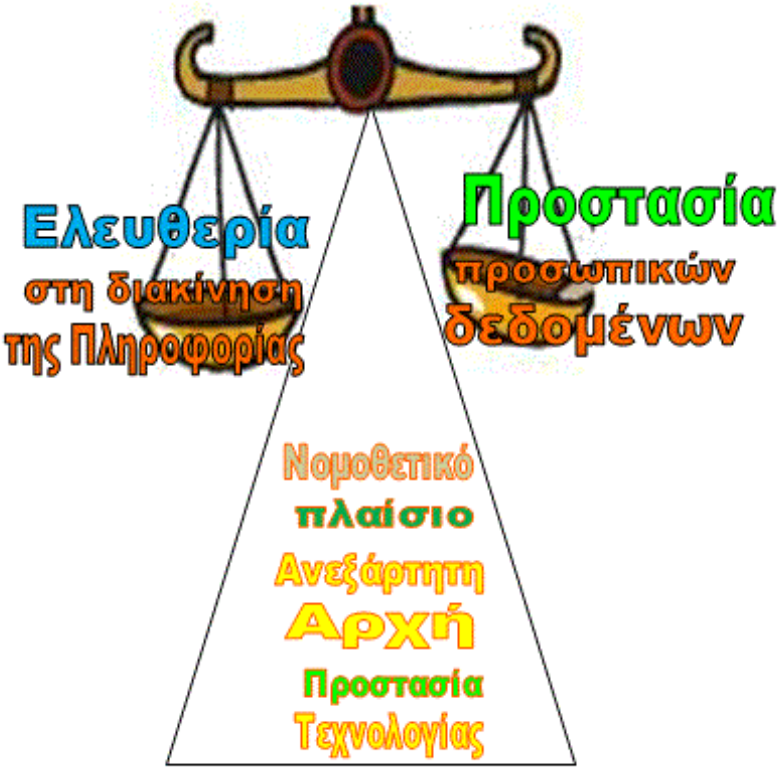
Η διαρκής εξέλιξη του Internet και της τεχνολογίας των δικτύων , δίνει σίγουρα σημαντικά πλεονεκτήματα και δυνατότητες προσφέροντας πολλές υπηρεσίες στο σύγχρονο άνθρωπο, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα που σχετίζονται με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η σύγχρονη Κοινωνία της Πληροφορίας χαρακτηρίζεται, από τη συνεχή τεχνολογική εξέλιξη, τη διεύρυνση και την επέκταση νέων τεχνολογιών στο δημόσιο και ιδιωτικό τομέα, αλλά και στον τομέα των τηλεπικοινωνιών και των μέσων μαζικής ενημέρωσης. Είναι γενικά αποδεκτό η παρουσία και συμβολή που έχει η Τεχνολογία της Πληροφορικής, του Διαδικτύου και των Επικοινωνιών, σε πολλούς τομείς της οικονομικής και κοινωνικής δραστηριότητας του ατόμου, με αυξητικές μάλιστα τάσεις. Επίσης η χρήση των τεχνολογιών αυτών διευκολύνει τη μαζική συλλογή και επεξεργασία κάθε είδους πληροφοριών που αφορούν το άτομο, πολλαπλασιάζοντας, έτσι, τον κίνδυνο προσβολής της προσωπικότητας και της ιδιωτικής ζωής. Δικαιολογημένα πληθαίνουν οι απόψεις που παρατίθενται από διάφορους φορείς, οργανισμούς, επιχειρήσεις, ανεξάρτητες Αρχές, οι οποίοι θέτουν σε προτεραιότητα νομικά ζητήματα που έχουν σχέση με το Διαδίκτυο, το ψηφιακό έγκλημα, την ασφάλεια συστημάτων και δικτύων, την προστασία και θωράκιση των πληροφοριών τόσο κατά την αποθήκευση όσο και κατά την διακίνησή τους.

---

[430] Βλ σχετικό δημοσίευμα της εφημερίδας Βήμα την 18/06/2010 στο : http://www.tovima.gr/society/article/?aid=338325

[431] Βλ, Λίλιαν Μήτρου, Η προστασία της Ιδιωτικότητας την Πληροφορική και τις Επικοινωνίες, διαθέσιμο στο: http://www.icsd.aegean.gr/website_files/proptyxiako/658467167.doc



Σχήμα 39. Η αντίθεση στην Κοινωνία της Πληροφορίας

Η βασική αντίθεση που χαρακτηρίζει την σημερινή Κοινωνία του Διαδικτύου είναι: Από το ένα μέρος κυριαρχεί η άποψη της Ελευθερίας στη διακίνηση της Πληροφορίας που υπάρχει συσσωρευμένη στο Διαδίκτυο και από το άλλο μέρος προβάλλει η προστασία των προσωπικών δεδομένων του υποκειμένου και της Ιδιωτικότητας. Οι οπαδοί της πρώτης άποψης στηρίζουν τα επιχειρήματά τους στην ελευθερία που πρέπει να υπάρχει στο Διαδίκτυο, στην προαγωγή της γνώσης , της επιστήμης και της έρευνας, στην ανάπτυξη της Οικονομίας .Την Δεύτερη άποψη υποστηρίζουν οι υπέρμαχοι της ιδιωτικότητας του ατόμου και της προστασίας των δεδομένων προσωπικού χαρακτήρα που συγκροτούν τις πληροφορίες και είναι στα βασικά συνταγματικά δικαιώματα του ανθρώπου. Ρυθμιστής των δύο αυτών απόψεων είναι η Ανεξάρτητη Αρχή που στηρίζεται στο υπάρχον νομοθετικό πλαίσιο που έχει θεσπίσει η πολιτεία και απορρέει από το διεθνές νομοθετικό πλαίσιο. Πέραν της Ανεξάρτητης Αρχής σημαντικό ρόλο παίζουν τα τεχνολογικά μέτρα που πρέπει να λαμβάνονται καθώς και η πολιτική ασφαλείας που πρέπει να υιοθετείται σε ένα πληροφοριακό- υπολογιστικό σύστημα ευρισκόμενο στο Διαδίκτυο ή και σε ένα απλό Δίκτυο.

Δεν είναι ίσως υπερβολικό να τονίσουμε ότι όσο ο άνθρωπος ανακαλύπτει νέες δυνατότητες στον τομέα της επικοινωνίας και της πληροφορικής, όσο περισσότερο, δηλαδή, εξελίσσεται η Κοινωνία της Πληροφορίας και του Διαδικτύου, τόσο περισσότερο αυξάνεται ο κίνδυνος της προσβολής και στην ουσία της αναίρεσης των ατομικών του δικαιωμάτων.

Για το λόγο αυτό πρέπει το νομοθετικό πλαίσιο προστασίας του πολίτη από τους κινδύνους της τεχνολογίας της πληροφορικής **να εμπλουτίζεται** και να ενδυναμώνεται **με νέες ρυθμίσεις** που θα έχουν ως απώτερο σκοπό την ακώλυτη και αποτελεσματική προστασία του

δικαιώματος της ελεύθερης ανάπτυξης της προσωπικότητας. Η Ανεξάρτητη Αρχή θα πρέπει να πλαισιώνεται τόσο από νομικούς επιστήμονες όσο και από επιστήμονες της Πληροφορικής και ειδικότερα της ασφαλείας των υπολογιστών και Δικτύων, που θα βοηθούν στην κατεύθυνση της καλύτερης προστασίας των δεδομένων των χρηστών. Διότι με τον τρόπο αυτό θωρακίζεται το Κράτος Δικαίου και εν γένει το δημοκρατικό πολίτευμα.

Οι νέες τεχνολογίες δίνουν τη δυνατότητα συγκέντρωσης και επεξεργασίας απεριόριστων ηλεκτρονικών δεδομένων, με ταχύτητα χωρίς γεωγραφικούς περιορισμούς. Το γεγονός αυτό δημιουργεί κινδύνους από την **αλόγιστη χρήση προσωπικών δεδομένων** χωρίς τη συγκατάθεση των υποκειμένων. Η προστασία των προσωπικών δεδομένων αποτελεί πλέον ένα συνταγματικό αναφαίρετο δικαίωμα του πολίτη.Στην κατεύθυνση αυτή και τα νομοθετήματα περί της συλλογής, επεξεργασίας και χρήσης των προσωπικών δεδομένων, υπηρετούν τη βασική αυτή επιταγή του Συντάγματος, καθορίζοντας τις προϋποθέσεις που πρέπει να υπάρχουν για συλλογή και επεξεργασία και χρήση πληροφοριών. Όσο οι τεχνολογικές δυνατότητες διευκολύνουν τη συλλογή προσωπικών δεδομένων χωρίς τη συγκατάθεση του υποκειμένου, τόσο χρειάζεται να διασφαλιστεί το δικαίωμα του κάθε πολίτη να γνωρίζει και να επιλέγει ο ίδιος εάν κάποιος συλλέγει τα προσωπικά του δεδομένα, ποια δεδομένα θα είναι αυτά και για ποιον σκοπό συλλέγονται. Η προστασία της ιδιωτικότητας και η αναγνώριση του δικαιώματος του κάθε ατόμου στην ανωνυμία και τον πληροφοριακό αυτοκαθορισμό[432], αποτελούν θεμελιώδεις αρχές τις οποίες πρέπει να προασπίσουμε και να τις διαφυλάξουμε από όσους τις προσβάλλουν και τις επιβουλεύονται στη σύγχρονη εποχή της Κοινωνίας της Πληροφορίας.

Το Δίκαιο που υπηρετεί μια κοινωνία που κυριαρχεί η πληροφορική, η ψηφιακή τεχνολογία και το διαδίκτυο, πρέπει να βρίσκεται σε διαρκεί εγρήγορση παρακολουθώντας στενά τις ραγδαίες εξελίξεις σε αυτούς τους τομείς. Χρειάζεται να αποβάλλει κάθε στοιχείο στασιμότητας που το καθιστούν απλό θεατή των τεχνολογικών εξελίξεων και να συμβαδίζει παράλληλα με τη δυναμική εξέλιξη των νέων τεχνολογιών. Ο σύγχρονος νομοθέτης επιβάλλεται μέσα από το διάλογο τη συνεργασία των αρμοδίων φορέων, των αναγκών που υπάρχουν, την αρωγή των ειδικών - νομικών επιστημόνων και της πληροφορικής, να επικαιροποιεί και να ανανεώνει το υπάρχον θεσμικό πλαίσιο στην κατεύθυνση των νέων τεχνολογικών εξελίξεων, παρέχοντας ένα ολοκληρωμένο νομοθετικό πλαίσιο ρύθμισης ζητημάτων προστασίας των πληροφοριών και της ιδιωτικότητας. Πρέπει βέβαια να εξετάζονται και τα μέτρα προστασίας που προτείνουν οι επιστήμονες της πληροφορικής και καθορίζονται από τις υπάρχουσες τεχνολογικές εξελίξεις προστασίας της ιδιωτικότητας.

Σε αυτή την κατεύθυνση χρειάζεται βεβαίως και τη χρήση τεχνικών μέτρων ασφαλείας (Antivirus, firewalls, IDS backup κ.ά) που θα πρέπει να υιοθετούνται-τηρούνται σαν μέσο περιορισμού των επιθέσεων που μπορεί να δεχθεί ένα πληροφοριακό σύστημα. Μιλάμε για περιορισμό και όχι για πλήρη εξάλειψη μια και η ψηφιακή εγκληματικότητα όπως και η παραδοσιακή, με τα υπάρχοντα δεδομένα μπορεί να περιορισθεί και όχι να αποτραπεί. Εξάλλου, ο μόνος εντελώς ασφαλής Η/Υ είναι αυτός που δεν είναι καλωδιωμένος και σε κανένα δίκτυο, όπως συχνά αναφέρεται από τους χρήστες και διαχειριστές συστημάτων. Βέβαια για τον επιστήμονα της πληροφορικής η «ανοικτή πρόκληση» είναι η ανάπτυξη συστημάτων και εφαρμογών που θα αποτρέπει παντελώς τις επιθέσεις καθιστώντας τα πληροφοριακά

[432] Πληροφοριακός αυτοκαθορισμός: το δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων, ιδίως με ηλεκτρονικά μέσα

συστήματα, τους υπολογιστές και τα δίκτυα καθολικά ασφαλή. Είναι η απάντηση και η συνεισφορά της επιστήμης της πληροφορικής στην κατεύθυνση αυτή.

Καθώς η εξέλιξη της τεχνολογίας είναι καλπάζουσα με την νομική επιστήμη να ακολουθεί χρειάζεται οι επιστήμονες της πληροφορικής να πάρουν σαν **βασική παράμετρο την ασφάλεια** στον σχεδιασμό συστημάτων, υπηρεσιών και νέων τεχνολογιών για να εδραιώνεται κλίμα εμπιστοσύνης και ασφάλειας ανάμεσα στους χρήστες προκειμένου να γίνεται πλήρη αξιοποίηση αυτών των τεχνολογιών σε όφελος των συναλλασσόμενων μερών.

7.3 **Προτάσεις**

Η προστασία των δεδομένων προσωπικού χαρακτήρα είναι θέμα ασφάλειας δικτύων υπολογιστών αλλά και θέμα προστασίας της ιδιωτικότητας και πληροφοριακού αυτοκαθορισμού. Για το λόγο αυτό χρειάζεται:

- Εκπαίδευση των χρηστών σε θέματα ασφαλείας μέσα από διαρκή επικαιροποίηση αυτών των γνώσεων. Η εκπαίδευση αυτή να είναι καθολική και να διαπερνά το εκπαιδευτικό σύστημα
- Έρευνα, ανάπτυξη και προώθηση τεχνολογιών προστασίας πληροφοριών ενός υπολογιστικού - πληροφοριακού συστήματος και ειδικότερα των δεδομένων προσωπικού χαρακτήρα.
- Σχεδίαση και υλοποίηση λογισμικού και πληροφοριακών συστημάτων με πρώτο κριτήριο την ασφάλεια.
- Ευαισθητοποίηση – ενημέρωση όλων των ενδιαφερομένων για τα ζητήματα προστασίας προσωπικών δεδομένων και διοργάνωση εκπαιδευτικών σεμιναρίων.
- Διαρκής εκπαίδευση και κατάρτιση του ανθρώπινου δυναμικού των ανεξάρτητων αρχών (ΑΠΔΠΧ , Ε.Ε.Ε.Τ , Α.Δ.Α.Ε) σε θέματα νομικής και τεχνικής φύσης. Αναβάθμιση της υπολογιστικής και επικοινωνιακής υποδομής αυτών των Αρχών.
- Προσαρμογή και εξειδίκευση του υφιστάμενου νομοθετικού πλαισίου στις καινοτόμες και νέες τεχνολογίες που αναπτύσσονται στο χώρο της Πληροφορικής του Διαδικτύου και των Επικοινωνιών.
- Συνεργασία σε παγκόσμιο, ευρωπαϊκό και εθνικό επίπεδο με αρμόδιους φορείς-οργανισμούς, πανεπιστήμια, ενώσεις επιστημόνων και επιχειρήσεων.

8 **ΚΕΦΑΛΑΙΟ**: **Υλοποίηση** – **κατασκευή ιστοσελίδας με** joomla

Για την κατασκευή της ιστοσελίδας θα χρησιμοποιήσουμε το Joomla[433] CMS ή Σύστημα Διαχείρισης Περιεχομένου (Content Management System) ονομάζουμε ένα λογισμικό που μας βοηθά να ελέγχουμε και να διαχειριζόμαστε έναν ιστότοπο δημόσιας ή περιορισμένης πρόσβασης. Περιεχόμενο είναι οτιδήποτε αποφασίζουμε να «ανεβάσουμε» στον ιστότοπό μας: κείμενα, φωτογραφίες, μουσική, βίντεο, έγγραφα ή οποιουδήποτε άλλου είδους αρχείο. Ένα ιδανικά σχεδιασμένο CMS μας επιτρέπει να διαχειριζόμαστε τον ιστότοπό μας χωρίς να διαθέτουμε περίπλοκες τεχνικές γνώσεις ή δεξιότητες. Το Joomla είναι ένα ελεύθερο και ανοικτού κώδικα σύστημα διαχείρισης περιεχομένου. Χρησιμοποιείται για τη δημοσίευση

[433] Το όνομα Joomla γεννήθηκε την 01/09/2005 και προήλθε από τη λέξη Jumla που στα Σουαχίλι σημαίνει «όλοι μαζί» βλ.Μαρκατσέλας Μ, Ξαρχάκος Κ., Μαθαίνετε εύκολα Joomla!, εκδόσεις Ξαρχάκος,Αθήνα 2010,σελ11

περιεχομένου στον παγκόσμιο ιστό (World Wide Web) και σε τοπικά δίκτυα - intranets. Είναι γραμμένο σε PHP και αποθηκεύει τα δεδομένα του στη βάση MySQL. Το βασικό χαρακτηριστικό του είναι ότι οι σελίδες που εμφανίζει είναι δυναμικές, δηλαδή δημιουργούνται την στιγμή που ζητούνται. Ένα σύστημα διακομιστή(server) όπως είναι ο Apache λαμβάνει τις αιτήσεις των χρηστών και τις εξυπηρετεί.

Με ερωτήματα προς τη βάση λαμβάνει δεδομένα τα οποία μορφοποιεί και αποστέλλει στον εκάστοτε φυλλομετρητή (web browser) του χρήστη. Το Joomla! έχει και άλλες δυνατότητες εμφάνισης όπως η προσωρινή αποθήκευση σελίδας, RSS feeds, εκτυπώσιμες εκδόσεις των σελίδων, ειδήσεις, blogs, δημοσκοπήσεις, έρευνες, καθώς και πολύγλωσση υποστήριξη των εκδόσεών του.

8.1 **Χαρακτηριστικά** joomla

Στα γενικά χαρακτηριστικά του joomla αναφέρονται:

- Η εφαρμογή joomla είναι ανοιχτού λογισμικού και διατίθεται δωρεάν.
- Μεγάλη κοινότητα χρηστών στο http://www.joomla.gr/ και στο http://www.joomla.org
- Όλο το περιεχόμενο αποθηκεύεται σε βάση Δεδομένων με πλήρη μηχανισμό διαχείρισης της βάσης δεδομένων του site.
- Τρέχει σε πολλά λειτουργικά όπως Windows, Linux, FreeBSD, MacOSX server, Solaris και AIX.
- Πλήρως παραμετροποιήσιμο περιεχόμενο και περιβάλλον(συμπεριλαμβανομένων των θέσεων του αριστερού, κεντρικού και δεξιού μενού) , μεγάλη ευελιξία στη διαχείριση περιεχομένου, αλλαγή της σειράς του περιεχομένου.
- Είναι επεκτάσιμο με πληθώρα λειτουργιών.
- Παρέχει ασφάλεια καθώς οι σελίδες έχουν ενσωματωμένο το ssl, όπως και άλλα πρόσθετα που ενισχύουν την ασφάλεια των ιστοσελίδων του (CAPTCHA,
- Διαχειριστής αρχείων για μεταφόρτωση και διαχείριση των αρχείων
- Διαθέτει πολυγλωσσικότητα
- Εύκολη εγκατάσταση εφαρμογών, προσθέτων
- Δυνατότητα Rss
- Δυνατότητα για δημιουργία δημοσκοπήσεων, ερωτηματολογίων, ψηφοφοριών
- Απομακρυσμένη διαχείρηση Νέων, Άρθρων και Links
- Πολλά επίπεδα χρηστών. Οι θεματικές ενότητες μπορούν να προστεθούν από τους συντάκτες με ανάλογη παροχή δικαιωμάτων από το διαχειριστή.
- Σύστημα αξιολόγησης άρθρων

- Ειδικός μηχανισμός για μηχανή αναζήτησης. Δυνατότητα βελτιστοποίησης της ιστοσελίδας Joomla στις μηχανές αναζήτησης (SEO[434]).
- Διαχείριση διαφημίσεων
- Παροχή στατιστικών στοιχείων
- Ενσωματωμένος text editor (WYSIWYG) παρόμοιος με αυτόν του WORD
- Ανέβασμα φωτογραφιών και δημιουργία photo gallery σε οποιοδήποτε σημείο του site
- Δυνατότητα λήψης αντιγράφου ασφαλείας του site (back up)

8.2 **Εγκατάσταση** joomla

Η εγκατάσταση περιλαμβάνει την τελευταία έκδοση θα πραγματοποιηθεί τοπικά στον υπολογιστή με εγκαταστημένα τα Windows 7 Home Premium. Οι τεχνικές[435] απαιτήσεις του Joomla είναι να έχει εγκατασταθεί ο Apache server, η βάση δεδομένων MySQL καθώς επίσης και η γλώσσα προγραμματισμού PHP. Όλα αυτά μπορούμε να τα βρούμε σε ένα πακέτο λογισμικού το XAMPP το οποίο τα περιλαμβάνει.

Αφού επισκεφθούμε την σελίδα του XAMPP[436], επιλέγουμε XAMPP for Windows, μετά download XAMPP. Υπάρχουν διάφορες εκδόσεις, επιλέγουμε την τελευταία (XAMPP for Windows 1.8.0, 13.7.2012) και πατάμε Installer . Στη συνέχεια επισκεπτόμαστε την σελίδα του Joomla[437] , όπου πηγαίνουμε στα download κατεβάζουμε την τελευταία έκδοση (Joomla! 2.5.x 2.5.7 Full Package) πατώντας ZIP. Στη συνέχεια πηγαίνουμε στη σελίδα με τις μεταφράσεις του Joomla και κατεβάζουμε την ελληνική μετάφραση του Joomla. Αυτή περιέχει ένα συμπιεσμένο αρχείο, το οποίο κατεβάζουμε:

http://joomlacode.org/gf/download/frsrelease/17195/74790/el-GR_joomla_lang_full_2.5.6v1.zip

Στη συνέχεια πηγαίνουμε στο φάκελο με τις λήψεις και αρχίζουμε την εγκατάσταση των προγραμμάτων. Ξεκινάμε με την εγκατάσταση του XAMPP πατώντας xampp-win32-1.8.0-VC9-installer .Προς το τέλος της εγκατάστασης θα πάρουμε μήνυμα πως το Firewall των windows μπλοκάρει τον Apache server θα πατήσουμε να επιτρέπεται (unblock). Αφού έχει εγκατασταθεί το XAMPP, κάνουμε έναρξη στο control panel, πατάμε start στις υπηρεσίες που υπάρχουν στο XAMPP (Apache server, η βάση δεδομένων MySQL καθώς και ο FTP server Filezilla) και έχουμε την εικόνα 8.

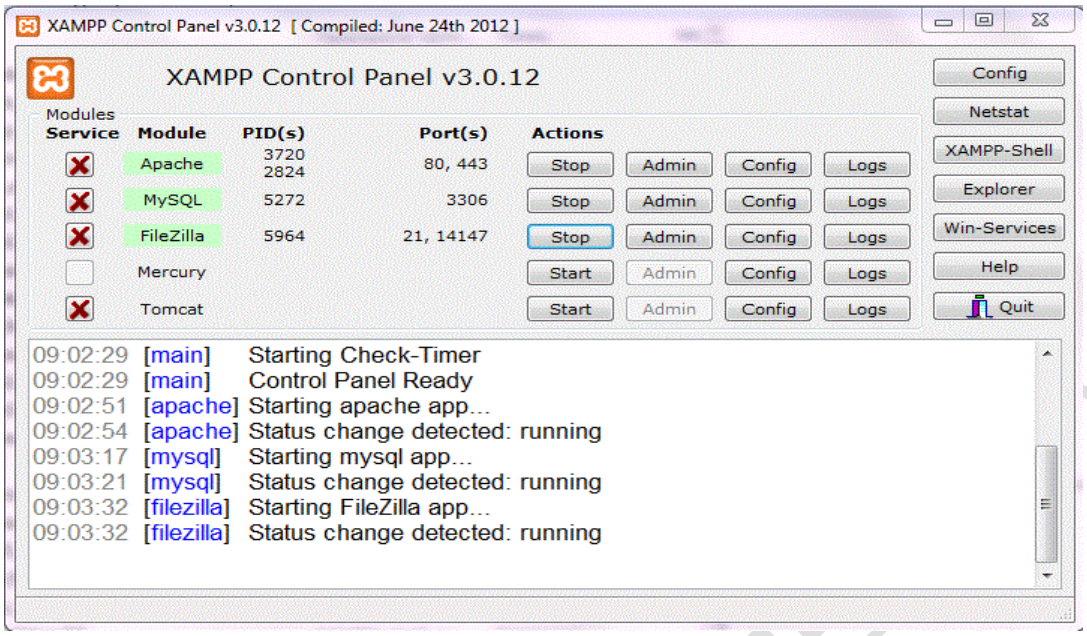
---

[434] Ο όρος Βελτιστοποίηση Ιστοσελίδων για τις Μηχανές Αναζήτησης (**S**earch **E**ngine **O**ptimization- **SEO**) περιγράφει όλες εκείνες τις διαδικασίες-επεμβάσεις που πρέπει να γίνουν στη δομή και το περιεχόμενο μιας ιστοσελίδας ώστε να είναι όσο το δυνατό πιο φιλική στις μηχανές αναζήτησης.

[435] Για τις τεχνικές απαιτήσεις του Joomla βλ: http://www.joomla.org/technical-requirements.html

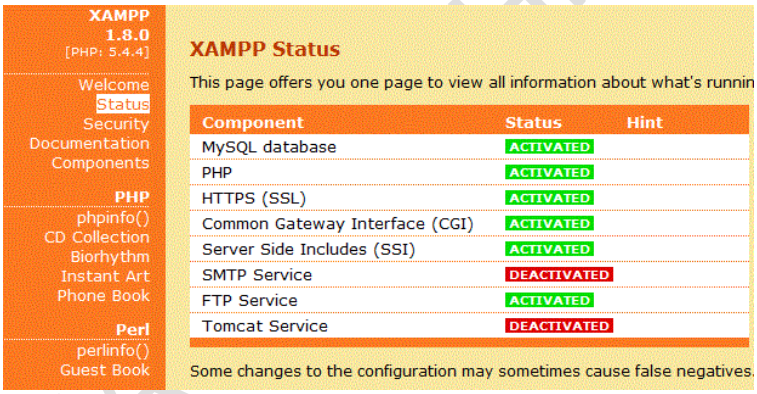
[436] Η σελίδα του XAMPP : http://www.apachefriends.org/en/xampp.html

[437] Η σελίδα του joomla : http://www.joomla.org



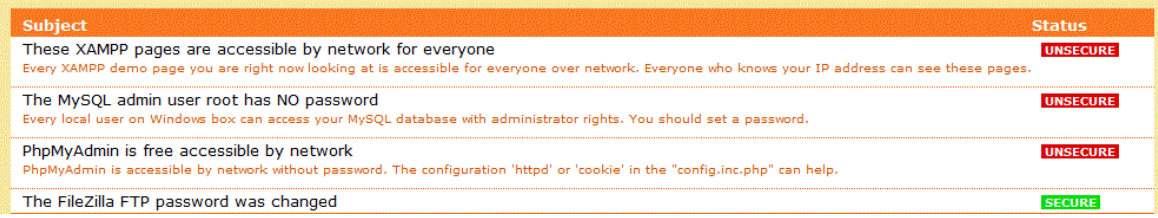
Εικόνα 8. Πίνακας ελέγχου XAMPP

Στη συνέχεια ανοίγουμε το φυλλομετρητή Mozilla Firefox και πληκτρολογούμε τη διεύθυνση http://localhost/xampp/index.php που θα μας φέρει στην αρχική σελίδα του XAMPP. Εκεί πατώντας στο status παίρνουμε πληροφορίες για την κατάσταση που βρίσκεται οι υπηρεσίες του XAMPP (η βάση δεδομένων MySQL και η γλώσσα προγραμματισμού PHP πρέπει να είναι ενεργοποιημένες-ACTIVATED).



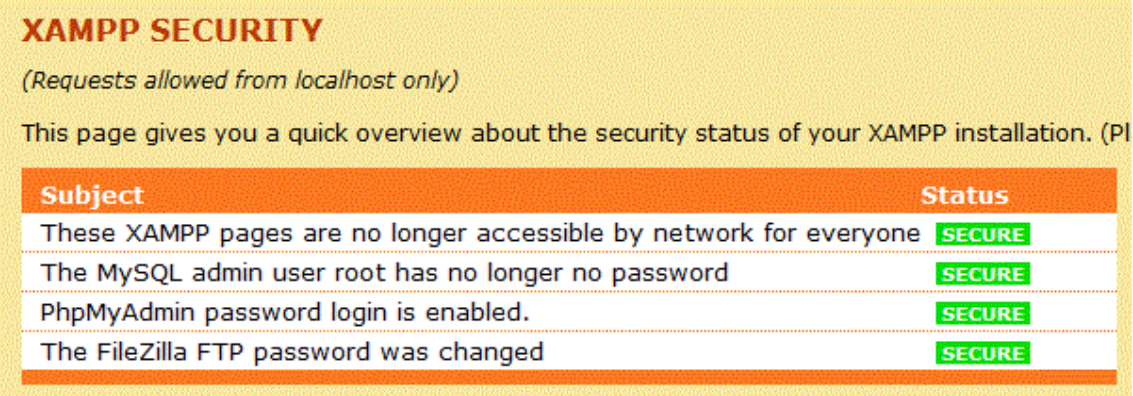
Εικόνα 9 . Κατάσταση XAMPP

Στη συνέχεια πατάμε το security θα ενημερωθούμε για την κατάσταση ασφαλείας του συστήματος. Παρατηρούμε πως οι σελίδες του είναι προσβάσιμες από όλους ο διαχειριστής της βάσης δεδομένων MySQL δεν έχει κωδικό ασφαλείας και το πρόγραμμα διαχείρισης της MySQL είναι ελεύθερα προσβάσιμο από το δίκτυο.



Εικόνα 10. Κατάσταση ασφαλείας XAMPP (μη ενεργοποιημένη)

Για το λόγο αυτό πατάμε στο http://localhost/security/xamppsecurity.php εισάγουμε κωδικό ασφαλείας για τον διαχειριστή root της βάσης δεδομένων MySQL και για να ισχύσει η αλλαγή κωδικού, χρειάζεται επανεκκίνηση η βάση δεδομένων MySQL. Στη συνέχεια για να προστατεύσουμε το φάκελο του XAMPP εισάγουμε όνομα χρήστη και κωδικό χρήστη. Οι αλλαγές που κάναμε φαίνονται αν πάμε με το φυλλομετρητή στη διεύθυνση http://localhost/xampp/index.php θα μας ζητηθεί κωδικός πρόσβασης για το XAMPP και όταν μπούμε στη σελίδα του XAMPP και πάμε στην καρτέλα security θα δούμε ενεργοποιημένες τις υπηρεσίες ασφαλείας για τον διαχειριστή βάσης δεδομένων MySQL και το πρόγραμμα διαχείρισης της MySQL, βλ εικόνα 11.

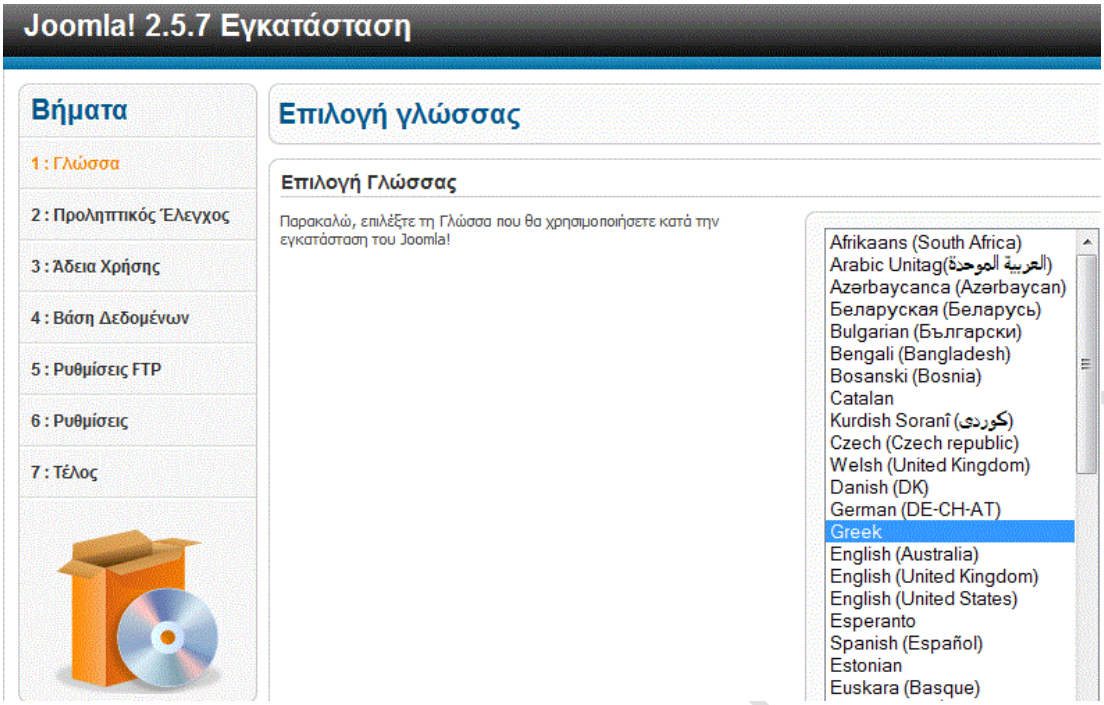


Εικόνα 11. Ασφαλές XAMPP

Στη συνέχεια πηγαίνουμε στην αρχική σελίδα στο μενού με τα εργαλεία του XAMPP και πατάμε στα Tools στο phpMyAdmin το οποίο είναι το εργαλείο της βάσης δεδομένων MySQL. Συμπληρώνουμε όνομα χρήστη root και κωδικό ασφαλείας αυτό που δώσαμε προηγουμένως για τον διαχειριστή root της βάσης δεδομένων MySQL και πηγαίνουμε στην αρχική οθόνη του προγράμματος διαχείρισης της MySQL phpMyAdmin. Εδώ δημιουργούμε μια βάση δεδομένων που θα χρησιμοποιήσουμε στο Joomla, πατώντας create new database με όνομα kal.

Στη συνέχεια μπαίνουμε στο σκληρό δίσκο όπου έχουμε εγκαταστήσει το XAMPP (φάκελλος XAMPP) , στο φάκελλο htdocs και δημιουργούμε ένα φάκελο με όνομα protection όπου εκεί μέσα θα εγκαταστήσουμε το Joomla. Μέσα σε αυτό το φάκελο αποσυμπιέζουμε το αρχείο, Joomla_2.5.7-Stable-Full_Package, που κατεβάσαμε προηγουμένως και στη συνέχεια διαγράφουμε το ζιπαρισμένο αρχείο.

Επόμενο βήμα είναι να πάμε στο φυλλομετρητή και να πληκτρολογήσουμε τη διεύθυνση http://localhost/protection και εμφανίζεται η αρχική εικόνα της εγκατάστασης του Joomla όπου επιλέγουμε την ελληνική γλώσσα σαν γλώσσα εγκατάστασης.

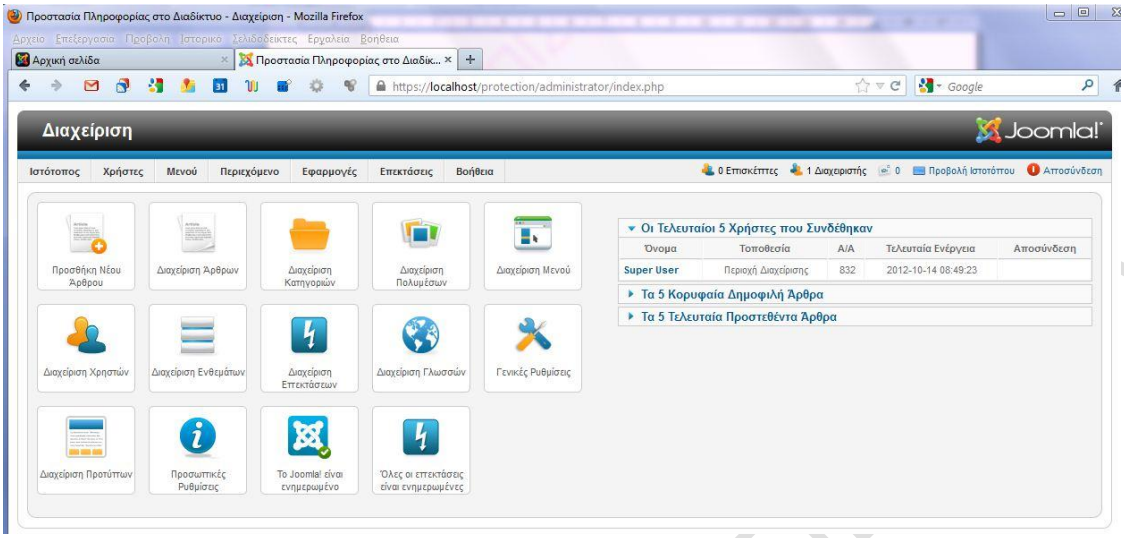


Εικόνα 12. Εγκατάσταση Joomla

Στη συνέχεια το Joomla κάνει ένα προληπτικό έλεγχο , ελέγχει αν το σύστημά μας ικανοποιεί τις ελάχιστες απαιτήσεις και μας ειδοποιεί αν κάτι δεν πάει καλά. Πατώντας επόμενο βλέπουμε την άδεια χρήσης του Joomla και στο επόμενο παράθυρο πρέπει να εισάγουμε τις ρυθμίσεις της βάσης δεδομένων MySQL. Επιλέγουμε είδος βάσης δεδομένων MySQL, όνομα διακομιστή localhost, όνομα χρήστη root, κωδικό ασφαλείας της βάσης δεδομένων που δώσαμε πριν και το όνομα της βάσης δεδομένων που είναι kal και ένα πρόθεμα για τους πίνακες της βάσης δεδομένων από 6 τουλάχιστο χαρακτήρες. Μετά στο επόμενο βήμα στις βασικές ρυθμίσεις FTP δεν χρειάζεται να αλλάξουμε κάτι και στη συνέχεια θα εισάγουμε τις βασικές ρυθμίσεις για τον ιστότοπό μας. Έτσι θα δώσουμε όνομα ιστότοπου protection personal data, θα βάλουμε μια διεύθυνση e-mail, και ένα κωδικό διαχειριστή. Στη συνέχεια επιλέγουμε την φόρτωση ενδεικτικού περιεχομένου και στην τελευταία οθόνη το Joomla μας ειδοποιεί πως η εγκατάσταση πραγματοποιήθηκε επιτυχώς. Απομένει όμως να διαγράψουμε το φάκελο installation από το φάκελο protection που βρίσκεται στη διαδρομή c: xampp\htdocs\protection.

Στη συνέχεια μπορούμε να εισέλθουμε στη σελίδα διαχείρισης του Joomla από όπου μπορούμε να διαχειριζόμαστε τον ιστότοπό μας. Πληκτρολογούμε στο φυλλομετρητή http://localhost/protection/administrator/index.php , βάζουμε όνομα χρήστη (user name): admin και κωδικό (password) διαχειριστή, αυτό που είχαμε δώσει προηγουμένως στις ρυθμίσεις και μπαίνουμε στην αρχική σελίδα διαχείρισης του Joomla. Στη συνέχεια θα εγκαταστήσουμε την ελληνική μετάφραση του Joomla. Στη αρχική σελίδα διαχείρισης του Joomla πηγαίνουμε στο μενού Extensions και πατάμε Extension Manager.Στη θέση Package File αναζητούμε στις λήψεις το συμπιεσμένο αρχείο el-GR_joomla_lang_full_2.5.6v1, που κατεβάσαμε προηγουμένως και κάνουμε Upload & Install.Στη συνέχεια στο μενού Extensions πατάμε Language Manager όπου έχουμε τις επιλογές Installed Site και Installed Administrator.Στην επιλογή Installed Site, κάνουμε κλικ στην ελληνική γλώσσα και πατάμε default.Μετά κλικ στην

επιλογή Installed Administrator, κάνουμε κλικ στην ελληνική γλώσσα και πατάμε default.Έτσι έχουμε την παρακάτω εικόνα 13.



Εικόνα 13. Περιοχή διαχείρισης Joomla

8.3 **Δομή Ιστοσελίδας** joomla

Η ιστοσελίδα μας αποτελείται από δύο τμήματα:

Το **δημόσιο τμήμα (Front End)** που βρίσκεται στην διεύθυνση https://www.localhost/protection. Είναι η ιστοσελίδα μας όπως θα εμφανίζεται στους χρήστες με την δομή που στηρίζεται σε κάποιο πρότυπο[438] (**Templates**) και αποτελείται από το μενού, τις εφαρμογές (**components**), τα ενθέματα (**Modules**), τα πρόσθετα (**Plug-ins**).

Την **περιοχή διαχείρισης (Back End)** που βρίσκεται στην διεύθυνση https://localhost/protection/administrator/index.php**.** Μέσα από αυτή την περιοχή ο διαχειριστής έχει την δυνατότητα να δημιουργεί χρήστες, να προσθέτει ή να αφαιρεί περιεχόμενο, να εμφανίζει ή να αποκρύπτει στοιχεία, εφαρμογές και δυνατότητες του Joomla και γενικά να προβαίνει στις απαιτούμενες και κάθε φορά επιθυμητές ρυθμίσεις. Το πρότυπο που επιλέξαμε για την περιοχή διαχείρισης είναι το Bluestork.

Στην αρχή ξεκινάμε με ρυθμίσεις για τον ιστότοπό μας. Στην περιοχή διαχείρισης και από το μενού ιστότοπος / γενικές ρυθμίσεις, κάνουμε ρυθμίσεις για τον ιστότοπό μας (επιλέγουμε όνομα για τον ιστότοπό μας - **Η Προστασία της Πληροφορίας στο Διαδίκτυο**) ,επιλέγουμε κειμενογράφο(TinyMCE) που θα χρησιμοποιούμε, καθορίζουμε το προεπιλεγμένο επίπεδο πρόσβασης (public). Επίσης προβαίνουμε σε ρυθμίσεις SEO (Search Engine Optimization) για να μπορεί η ιστοσελίδα μας να είναι φιλική για τις Μηχανές Αναζήτησης.

[438] για τον ιστότοπό μας επιλέξαμε το πρότυπο Beez5

Διαχείριση μενού. Τα μενού είναι αντικείμενα τα οποία χρησιμεύουν για την πλοήγηση στην ιστοσελίδα. Η θέση τους στην ιστοσελίδα μπορεί να είναι κατακόρυφη ή οριζόντια και δημιουργούνται δυναμικά. Αυτά συνδέονται με άλλα αντικείμενα του Joomla, όπως ενθέματα, κατηγορίες, άρθρα. Για να δημιουργήσουμε μενού πηγαίνουμε στην περιοχή διαχείρισης, Μενού /Διαχείριση Μενού/Προσθήκη Νέου Μενού, βάζουμε τίτλο και είδος Μενού και συνδέουμε το μενού με κάποιο ένθεμα.

Το πρώτο μενού που δημιουργούμε είναι κατακόρυφο, το ονομάζουμε **Απειλές** και το συνδέουμε με το ένθεμα Απειλές. Στη συνέχεια δημιουργούμε τα αντικείμενα στοιχεία του Μενού Απειλές τα οποία είναι: Επιθέσεις σε Δίκτυα, Κακόβουλο λογισμικό, Παραποίηση ταυτότητας, Μη ζητηθείσα ηλεκτρονική επικοινωνία. Στη συνέχεια δημιουργούμε το μενού **μέτρα προστασίας** με αντικείμενα Νομοθεσία (Ελληνικό Δίκαιο, Ευρωπαϊκό Δίκαιο),Τεχνικά μέτρα προστασίας και Ανεξάρτητες Αρχές. Να σημειώσουμε πως μέσα στο μενού Νομοθεσία δημιουργούμε άλλα μενού, όπως το **Ελληνικό Δίκαιο** με στοιχεία το Σύνταγμα ,ο Ν. 2472/1997, ο Ν. 2774/1999,ο Ν. 3471/2006 και το **Ευρωπαϊκό Δίκαιο** με στοιχεία η Σύμβαση 108 του Συμβουλίου της Ευρώπης, η Συμφωνία Σένγκεν, η οδηγία 2002/58/ΕΚ.

Στη συνέχεια δημιουργούμε το μενού Top που είναι οριζόντια και βρίσκεται στο πάνω μέρος της ιστοσελίδας μας. Δημιουργούμε τα αντικείμενά που θα περιέχει και είναι η αρχική σελίδα, επιθέσεις σε δίκτυα, κακόβουλο λογισμικό, προστασία πληροφορίας, τεχνικά μέτρα προστασίας.

Διαχείριση περιεχομένου. Στην περιοχή διαχείρισης έχουμε τη δυνατότητα να διαχειριζόμαστε το περιεχόμενο προσθέτοντας άρθρα, κατηγορίες καθώς και να ορίσουμε ποια από αυτά θα εμφανίζονται στην πρώτη σελίδα. Αυτό το κάνουμε από το μενού Περιεχόμενο/Διαχείριση Άρθρων/Διαχείριση Κατηγοριών/Κύρια Άρθρα/Διαχείριση Πολυμέσων.

Διαχείριση επεκτάσεων (extensions). Οι επεκτάσεις στο joomla είναι τα ενθέματα, τα πρότυπα, τα πρόσθετα, οι γλώσσες. Οι δυνατότητες επέκτασης του joomla είναι πρακτικά απεριόριστες. Και αυτό γιατί ο κάθε χρήστης μπορεί να γίνει δημιουργός μιας επέκτασης και να την παραχωρήσει στην κοινότητα του joomla. Για να εισάγουμε μια επέκταση π.χ ένα πρότυπο, πηγαίνουμε στο μενού Επεκτάσεις /Διαχείριση επεκτάσεων και κάνουμε μεταφόρτωση και εγκατάσταση του αρχείου που αναφέρεται σε αυτό το πρότυπο και αφού προηγούμενα το έχουμε κατεβάσει στον υπολογιστή μας.

Ενθέματα (Modules). Τα ενθέματα είναι τα κουτιά μέσα στα οποία εμφανίζονται τα μενού, τα περιεχόμενα , οι εφαρμογές και όλα αυτά που θέλουμε να εμφανίζονται στο δημόσιο τμήμα της ιστοσελίδας του joomla (Front End).

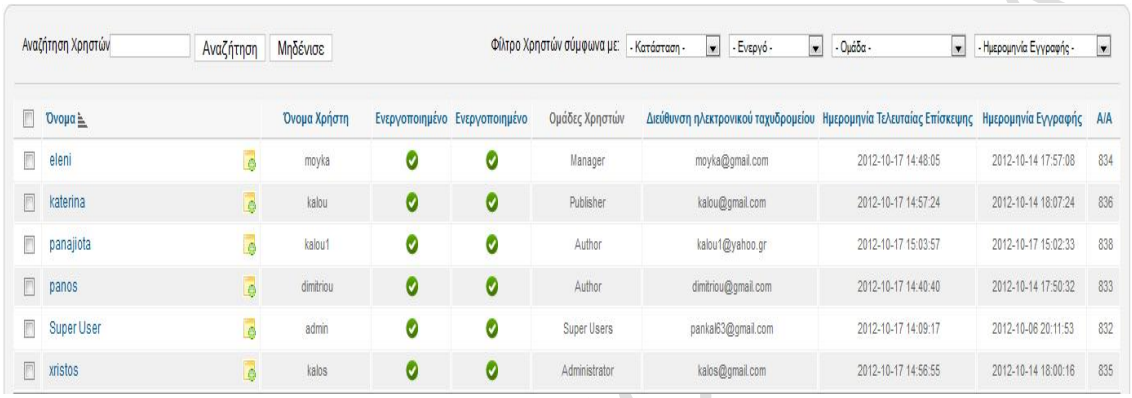
Πρότυπα (Templates). Τα πρότυπα χρησιμεύουν στην εμφάνιση της ιστοσελίδας και είναι ανεξάρτητα από το περιεχόμενο της ιστοσελίδας. Αφορούν τα χρώματα, τη θέση που θα έχουν τα ενθέματα , και όλα τα αντικείμενα του joomla, δηλ. το σχεδιασμό της ιστοσελίδας.

Πρόσθετα (plug- ins). Τα πρόσθετα εκτελούν κάποιες λειτουργίες που διευκολύνουν τόσο τον διαχειριστή της ιστοσελίδας όσο και τον χρήστη. Τέτοιο πρόσθετο είναι η μηχανή αναζήτησης που υπάρχει στο joomla και βοηθά στην αναζήτηση περιεχομένου ή και αρχείου μέσα στην ιστοσελίδα. Επίσης άλλα πρόσθετα είναι ο κειμενογράφος TinyMCE, ο αποκλεισμός αυτοματισμών (Captcha) – ReCaptcha κ.ά.

Εφαρμογές (components). Οι εφαρμογές χρησιμοποιούνται για να μπορεί το Joomla να επεκτείνεται. Άλλες είναι εμπορικές και άλλες ελεύθερης διανομής. Μερικές από αυτές είναι

εφαρμογές για e-shop, για gallery φωτογραφιών, για e-learning κ.ά. Έτσι έχουμε αναζήτηση, ανακατεύθυνση, αποστολή μηνυμάτων στους χρήστες, διαδικτυακούς συνδέσμους, διαφημίσεις, ενημερώση joomla, ροές ειδήσεων.

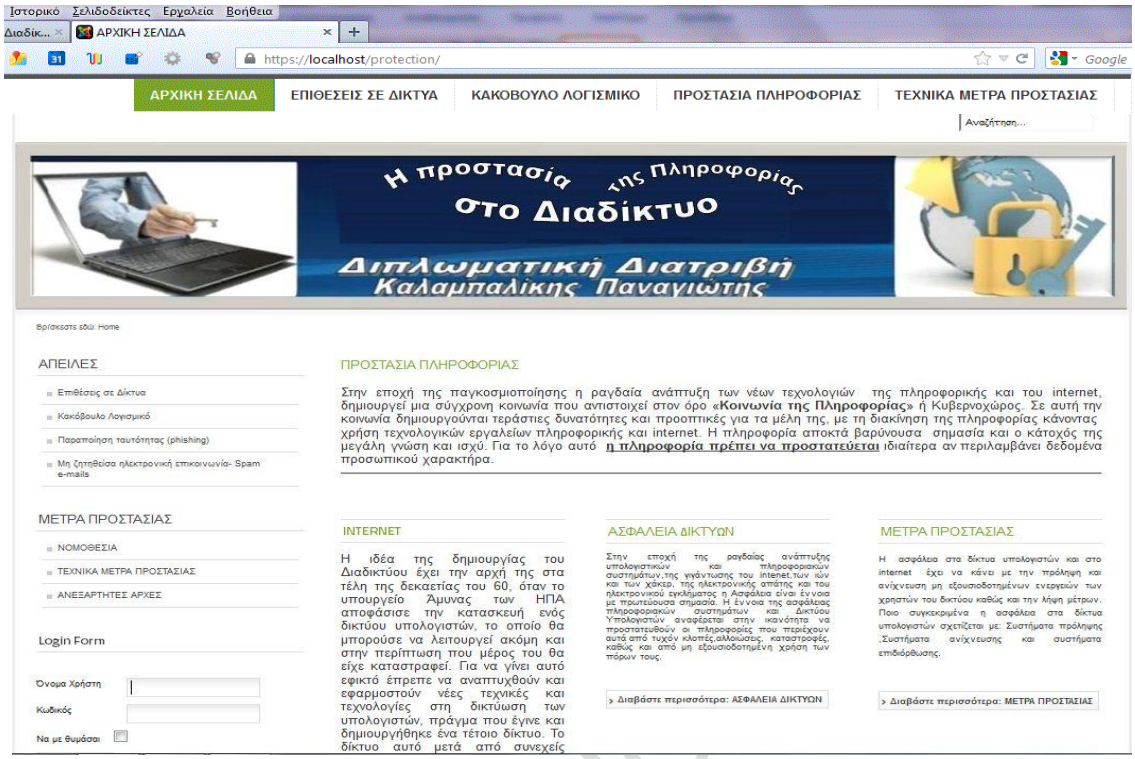
Διαχείριση χρηστών. Μέσα από το μενού χρήστες, μπορούμε να κάνουμε διαχείριση χρηστών, προσθέτοντας ή αφαιρώντας κάποιον χρήστη, να ορίσουμε ομάδες χρηστών καθώς και επίπεδα πρόσβασης που θα έχει ο κάθε χρήστης, και να κάνουμε μαζική αποστολή μηνυμάτων στους χρήστες. Επίσης μέσα από τη διαχείριση χρηστών μπορούμε να πάρουμε πληροφορίες για την ημερομηνία εγγραφής κάθε χρήστη, την ημερομηνία τελευταίας επίσκεψης, την ομάδα που ανήκει ο κάθε χρήστης, βλ εικόνα 14.



Εικόνα 14. Διαχείριση χρηστών Joomla

Αλλαγή του Logo της ιστοσελίδας. Για να μπορέσουμε να αλλάξουμε το προεπιλεγμένο Logo του Joomla, αφού πάρουμε πληροφορίες[439] για την θέση, το είδος του αρχείου εικόνας και τις διαστάσεις του προεπιλεγμένου, δημιουργούμε το δικό μας με ίδιες διαστάσεις και την ίδια μορφή αρχείου (εδώ είναι jpg).Έτσι βλέπουμε πως το προεπιλεγμένο βρίσκεται στη διαδρομή https://localhost/protection/templates/beez5/images/fruits.jpg, με όνομα αρχείου fruits.jpg. Αρκεί να αντιγράψουμε το δικό μας Logo που έχουμε δημιουργήσει μέσα στο φάκελο images,δίνοντας το ίδιο όνομα με το προεπιλεγμένο (fruits). Μετά από τις παραπάνω ρυθμίσεις έχουμε δημιουργήσει την ιστοσελίδα μας με τίτλο «Η προστασία της Πληροφορίας στο διαδίκτυο» ,βλ. εικόνα 15.

[439] κάνοντας δεξί κλικ πάνω σε αυτό και μετά προβολή πληροφοριών εικόνας



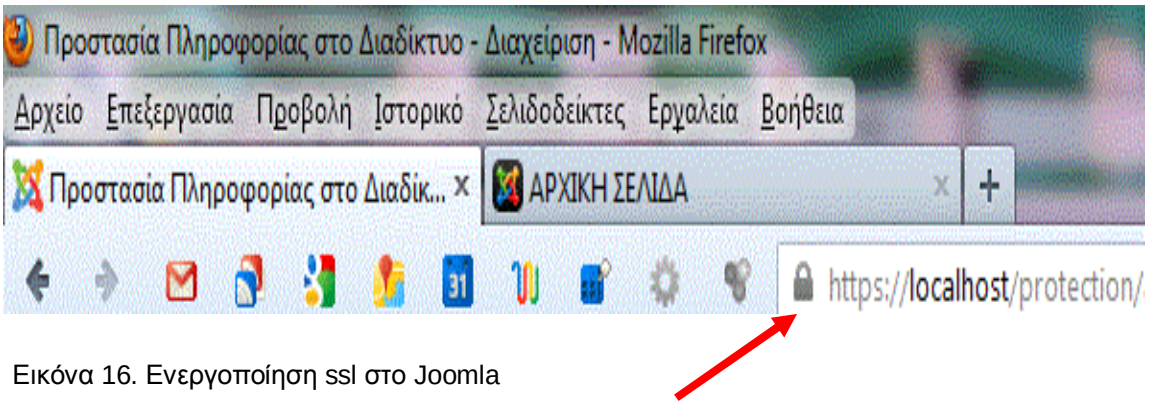
Εικόνα 15. Αρχική σελίδα ιστοσελίδας Protection

8.4 **Ρυθμίσεις ασφαλείας στην ιστοσελίδα** joomla

Αφού δημιουργήσαμε την ιστοσελίδα μας απομένει να πάρουμε βασικά μέτρα για την ασφάλεια αυτής. Έτσι έχουμε:

8.4.1 **Χρήση πρωτοκόλλου** ssl

Είδαμε τη χρησιμότητα του πρωτοκόλλου ssl σε προηγούμενη ενότητα. Για να μπορέσουμε να κάνουμε χρήση αυτού του πρωτοκόλλου πηγαίνουμε στην περιοχή διαχείρισης, στο μενού Ιστότοπος\Γενικές ρυθμίσεις\Διακομιστής και στη θέση «Υποχρεωτική χρήση ssl» επιλέγουμε «ολόκληρος ο ιστότοπος». Έτσι ενεργοποιείται το πρωτόκολλο ssl και τα δεδομένα που ανταλλάσσονται μεταξύ browser και web browser είναι κρυπτογραφημένα. Αυτό φαίνεται και από το γεγονός ότι η διεύθυνση της ιστοσελίδας μας ξεκινάει με **https αντί για http**, βλ εικόνα 16.



Εικόνα 16. Ενεργοποίηση ssl στο Joomla

8.4.2 **Χρήση** CAPTCHA

Το όνομα CAPTCHA αποτελεί ακρωνύμιο για το **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part που πρακτικά περιγράφει ένα είδος αυτόματου τεστ με την δυνατότητα να ξεχωρίζει αν ο χρήστης είναι άνθρωπος ή μηχανή. Η χρήση αυτού του πρόσθετου υπάρχει στο joomla και χρησιμεύει για την αποτροπή αυτοματοποιημένων εγγραφών και μηνυμάτων χρηστών που γίνεται από μηχανές και είναι ψεύτικα. Για να το ενεργοποιήσουμε πηγαίνουμε στην περιοχή διαχείρισης, στο μενού Ιστότοπος\Γενικές ρυθμίσεις\Ιστότοπος και στη θέση Προεπιλεγμένος Αποκλεισμός Αυτοματισμών (Captcha) επιλέγουμε «Αποκλεισμός Αυτοματισμών (Captcha)-ReCaptcha». Αυτό το πρόσθετο αποκλεισμού αυτοματισμών (CAPTCHA) χρησιμοποιεί την υπηρεσία reCaptcha για να αποτρέψει τους αποστολείς ανεπιθύμητων μηνυμάτων ενώ βοηθά να ψηφιοποιηθούν βιβλία, εφημερίδες και παλιές ραδιοφωνικές εκπομπές.

Στη συνέχεια πηγαίνουμε στη διεύθυνση http://www.google.com/recaptcha , προκειμένου να λάβουμε ένα δημόσιο και ένα ιδιωτικό κλειδί για τον ιστοχώρο μας. Μετά πηγαίνουμε στην περιοχή διαχείρισης, στο μενού Επεκτάσεις\Διαχείριση Προσθέτων και πατάμε Αποκλεισμός Αυτοματισμών (Captcha) – ReCaptcha, όπου στις βασικές επιλογές εισάγουμε το δημόσιο και το ιδιωτικό κλειδί που δημιουργήσαμε πριν για τον ιστοχώρο μας και πατάμε αποθήκευση. Για να το χρησιμοποιήσουμε για καταχωρήσεις νέων λογαριασμών, πηγαίνουμε στις Επιλογές της Διαχείρισης Χρηστών και επιλέγουμε, Αποκλεισμός Αυτοματισμών (Captcha) – ReCaptcha ως Αποκλεισμό Αυτοματισμών. Έτσι έχουμε το αποτέλεσμα που δείχνει η εικόνα 17.

Εικόνα 17. Ενεργοποίηση CAPTCHA στο joomla

8.4.3 **Αλλαγή** (username) **Υπερδιαχειριστή στο** joomla.

Στην περιοχή διαχείρισης του joomla το προεπιλεγμένο όνομα χρήστη admin είναι ευάλλωτο σε επίδοξους εισβολείς. Για το λόγο αυτό χρειάζεται να το αλλάξουμε σε κάτι τυχαίο (πχ dbet5rf2f3d), προκειμένου να προστατευθούμε από κακόβουλες επιθέσεις. Η αλλαγή γίνεται από το μενού Χρήστες\Διαχείριση χρηστών, κλικ πάνω στο Super User ,αλλάζουμε το Username σε κάτι άλλο και πατάμε Save. Η αλλαγή αυτή μπορεί να πραγματοποιηθεί και από την περιοχή Διαχείρισης, του μενού ιστότοπος \Προσωπικές Ρυθμίσεις. Παρομοίως και ο κωδικός πρόσβασης (password) θα πρέπει να είναι τυχαίος συνδυασμός αριθμών, χαρακτήρων και συμβόλων, τουλάχιστον 8 ψηφίων, πχ &R!%8354d7@j και σε καμία περίπτωση κάτι εύκολο.

8.4.4 **Αναβάθμιση του** Joomla.

Σημαντικό ρόλο στην ασφάλεια των web εφαρμογών σαν το Joomla, WordPress, Drupal κλπ είναι η άμεση αναβάθμιση στην επόμενη έκδοση όταν κυκλοφορήσει νέα έκδοση της εφαρμογής ή μια μικρότερη (αλλά εξίσου σημαντική) ενημέρωση ασφαλείας (security update). Έτσι, θα διορθωθούν όποια κενά ασφαλείας υπήρχαν και είχαν εντοπιστεί στην προηγούμενη έκδοση. Για το λόγο αυτό κάνουμε εγγραφή στο newsletter του Joomla από τη σελίδα http://www.joomla.org/download.html.

8.4.5 **Προστασία αρχείου** configuration.php

Ένας από τους τρόπους βελτίωσης της ασφάλειας του δικτυακού τόπου είναι η προστασία από την απευθείας πρόσβαση συγκεκριμένων αρχείων php που βρίσκονται στον κατάλογο public_html και περιέχουν εκτελέσιμο κώδικα ή σημαντικά δεδομένα. Υπάρχουν διάφοροι τρόποι για να πετύχουμε αυτό. Απλούστερος και ασφαλέστερος θεωρείται να μην αποθηκεύονται κρίσιμα δεδομένα μέσα στον κατάλογο public_html . Και από τον Apache.org υπάρχει μια συνεχής σύσταση να αποφεύγεται η διατήρηση τέτοιων αρχείων, με κρίσιμα δεδομένα, στον κατάλογο public_html.

Για να προστατεύουμε το αρχείο configuration.php, που είναι το πιο σημαντικό (για τον τομέα της ασφάλειας) ακολουθούμε τα παρακάτω:

Μετακινούμε το αρχείο configuration.php σε ένα ασφαλή κατάλογο, έξω από τον public_html και δίνουμε σε αυτό ένα άλλο όνομα, π.χ joomla.conf.Μετά δημιουργούμε ένα νέο αρχείο configuration.php που περιέχει τον παρακάτω κώδικα:

```
<?php
require( dirname( __FILE__ ) . '/../joomla.conf' );
?>
```

Στη συνέχεια ελέγχουμε το νέο configuration.php να μην είναι εγγράψιμο (444), και να μην αλλάξει το περιεχόμενό του από το com_config. Εάν χρειαστεί να αλλάξουμε κάποια από τις ρυθμίσεις, τις αλλάζουμε με το χέρι στο αρχείο joomla.conf [440].

8.4.6 **Λήψη Αντιγράφων Ασφαλείας** (Backup)

Χρειάζεται σε τακτά χρονικά διαστήματα να κάνουμε backup στο website , ώστε σε περίπτωση που πέσουμε θύμα hacker, να είμαστε σε θέση να αποκαταστήσουμε εύκολα και γρήγορα τη ζημιά. Μια πολύ καλή εφαρμογή γι' αυτό το σκοπό είναι το Akeeba Backup, που είναι μία εφαρμογή για το Joomla, με την οποία μπορούμε να παίρνουμε Backup στην ιστοσελίδας μας. Η ίδια εφαρμογή μας δίνει τη δυνατότητα να επαναφέρουμε το αντίγραφο σε οποιονδήποτε Web Server που υποστηρίζει το Joomla. Τα αντίγραφα που δημιουργεί κρατιούνται σαν αρχείο και είναι διαθέσιμα οποιαδήποτε στιγμή. Το αντίγραφο ασφαλείας περιέχει όλα τα αρχεία της ιστοσελίδας, τα περιεχόμενα της βάσης δεδομένων καθώς και ένα σύστημα εύκολης επαναφοράς. Μπορούμε εάν θέλουμε να κάνουμε αντίγραφο ασφαλείας μόνο τα αρχεία ή μόνο τη βάση δεδομένων. Όλη η λειτουργία του Akeeba Backup είναι βασισμένη στην τεχνολογία Ajax ώστε να αποφεύγονται οι χρόνοι απόκρισης του Web Server ειδικά όταν τα περιεχόμενα της ιστοσελίδας μπορεί να υπερβαίνουν μερικά Gigabytes.Η βασική έκδοση διατίθεται

[440] Χρησιμοποιώντας τη μέθοδο αυτή, ακόμα και αν για κάποιο λόγο ο Web server μεταδώσει τα περιεχόμενα αρχείων php, λόγω κάποιας λανθασμένης ρύθμισης, κανείς δεν θα μπορεί να δει τα περιεχόμενα του πραγματικού αρχείου configuration.php, βλ : http://www.joomla.gr/tutorials/security/349--configurationphp.

δωρεάν[441], ενώ υπάρχουν και 4 εμπορικές εκδόσεις. Το Akeeba Backup έχει δημιουργηθεί από Έλληνες προγραμματιστές με επικεφαλή το Νικόλα Διονυσόπουλο[442].

8.4.7 **Αλλαγή του αρχείου** .htaccess.

Το αρχείο .htaccess βρίσκεται στον πυρήνα του Joomla (μέσα στο φάκελο Protection –που έχουμε δημιουργήσει και εγκαταστήσει το Joomla) και δίνει τη δυνατότητα περισσότερου ελέγχου και τροποποίησης αρκετών ρυθμίσεων για την ενίσχυση της ασφάλειας σε ένα website. Στη συνέχεια αναφέρονται τρόποι για τον περιορισμό της έκθεσης της ιστοσελίδας μας σε διάφορους τύπους επιθέσεων, τους οποίους μπορούμε να τους προσθέσουμε στο αρχείο .htaccess[443].

☞ **Απαγόρευση πρόσβασης στο αρχείο .htaccess**.Με τη ρύθμιση αυτή εμποδίζουμε πρόσβαση στο αρχείο.htaccess.

Prevent access to .htaccess

<Files>

Order allow, deny

Deny from all

</Files>

☞ **Απαγόρευση πρόσβασης σε καταλόγους**.

Disable unauthorized directory browsing

Options All - Indexes

☞ **Απαγόρευση πρόσβασης σε αρχεία**. Αυτός ο κώδικας αποτρέπει πρόσβαση σε συγκεκριμένα αρχεία.

Block access to specific file

<files>

Order allow, deny

Deny from all

---

[441] http://www.akeebabackup.com, επίσης http://www.akeebabackup.com/download/official/akeeba-backup/akeeba-backup-3-1-2.html.

[442] Βλ: http://www.joomplus.gr/reviews/item/783-akeeba-backup.html

[443] Βλ http://blog.dnhost.gr/2012/02/16/htaccess-ρυθμίσεις-ασφαλείας/ επίσης http://www.kagialaris.me/en/tutorials/item/15-htaccess-security-tips

</files>

Αυτός ο κώδικας αποτρέπει πρόσβαση σε πολλαπλούς τύπους αρχείων.

Block access to multiple file types

<FilesMatch>

Order allow, deny

Deny from all

</FilesMatch>

☞ **Απαγόρευση πρόσβασης σε IP's και Domains**. Με αυτόν τον κώδικα έχουμε πρόσβαση σε συγκεκριμένες IP ή domains ή αποκλείει συγκεκριμένες IP διευθύνσεις και domains.

Restrict access to IP's & domains (replace x with numbers)

<Limit>

Order allow, deny

allow from all

deny from xx.xxx.xx.xxx

deny from .*domain\.com.*

</Limit>

☞ **Προστασία Φακέλων και αρχείων με κωδικό.**

Protect a single file

<Files>

AuthType Basic

AuthName "Mypassword"

AuthUserFile /home/path/.htpasswd

Require valid-user

</Files>

Protect multiple files

<FilesMatch>

AuthType Basic

AuthName "Mypassword"

AuthUserFile /home/path/.htpasswd

Require valid-user

</FilesMatch>

☞ **Απενεργοποίηση server signature**

#Disable the server signature

ServerSignature Off

☞ **Προβολή Custom Error Pages**

Display custom error pages

ErrorDocument 400 /errors/400.html

ErrorDocument 404 /errors/404.html

ErrorDocument 500 /errors/500.html

8.4.8 **Απόκρυψη της διαχειριστικής σελίδας**.

Η περιοχή σύνδεσης για το διαχειριστή μπορεί εύκολα να τεθεί σε κίνδυνο από κάθε κακόβουλο χρήστη αφού η πρόσβαση γίνεται συνήθως από το domain/administrator. Για το λόγο αυτό μπορούμε να αλλάξουμε το url στη μορφή domain/administrator?ROCKS1960, όπου ROCKS1960 είναι ο κωδικός που γνωρίζουμε μόνο εμείς. Μια πολύ καλή εφαρμογή που μπορεί να σας βοηθήσει για αυτό το σκοπό είναι το πρόσθετο **AdminExile** που κατεβάζουμε στον υπολογιστή μας[444]. Στη συνέχεια κάνουμε μεταφόρτωση του προσθέτου από το μενού Επεκτάσεις\Διαχείριση Επεκτάσεων στην περιοχή διαχείρισης. Μετά κάνουμε ενεργοποίηση του προσθέτου από το μενού διαχείριση προσθέτων\ System – AdminExile, τοποθετώντας για URL Aceess Key=adminexile, Key Value=ROCKS, Redirect URL=HOME.Έτσι μπορούμε να αποκρύψουμε την περιοχή διαχειριστή σύνδεσης από απρόσκλητους επισκέπτες, καθώς όταν θα πληκτρολογούν:

https://localhost/protection/administrator θα γίνεται ανακατεύθυνση στην αρχική σελίδα (HOME).

Εμείς για να μπορούμε να εισέλθουμε στην περιοχή διαχείρισης αρκεί να πληκτρολογήσουμε: https://localhost/protection/administrator/?adminexile=ROCKS

444 Η διεύθυνση του προσθέτου είναι: http://extensions.joomla.org/extensions/access-a-security/site-security/login-protection/15711

8.5 **Επίλογος**

Η ασφάλεια σε ένα πληροφοριακό σύστημα και ειδικότερα σε ένα σύστημα διαχείρισης περιεχομένου joomla είναι αναπτυγμένη σε αρκετά μεγάλο βαθμό, όμως δεν μπορούμε να πούμε πως έχουμε εξασφαλίσει απόλυτη ασφάλεια. Και αυτό γιατί όπως αναφέρουν, οι Πάγκαλος - Μαυρίδης στο βιβλίο τους «ασφάλεια πληροφοριακών συστημάτων και δικτύων», ο μεγαλύτερος κίνδυνος για μια εφαρμογή σχεδιασμένη για το διαδίκτυο, είναι η ανεπάρκεια των μηχανισμών ασφαλείας του ίδιου του διαδικτύου[445]. Το μεγάλο πλεονέκτημα του joomla είναι ότι καθώς είναι ανοικτού κώδικα η αρχιτεκτονική του είναι γνωστή και μπορούν να διορθωθούν πολλά κενά ασφαλείας, καθώς όλη η κοινότητά του συνεισφέρει με τον ένα ή άλλο τρόπο σε αυτή την κατεύθυνση.

Στην κοινότητα του joomla υπάρχουν πολλές επεκτάσεις και εργαλεία, οι οποίες αφορούν την πρόσβαση και την ασφάλεια σε ένα site joomla. Κάποια αναφέραμε στις προηγούμενες ενότητες. Άλλα μπορεί να βρει κάποιος στις παρακάτω διευθύνσεις:

- ☞ http://extensions.joomla.org/extensions/access-a-security.
- ☞ http://docs.joomla.org/Category:Security_Checklist
- ☞ http://www.rsjoomla.com/joomla-extensions/joomla-security.html
- ☞ http://www.jfirewall.com/overview

Βέβαια είναι γενικά παραδεκτό στην κοινότητα των ειδικών της ασφάλειας πληροφοριακών συστημάτων πως δεν υπάρχει πληροφοριακό σύστημα που να λειτουργεί σε δίκτυο, να είναι εύχρηστο και να εξασφαλίζει απόλυτη ασφάλεια.Και αυτό γιατί τόσο η εξέλιξη της τεχνολογίας όσο και η ανάπτυξη πληροφοριακών συστημάτων και εργαλείων είναι ραγδαία.

Συμπερασματικά το κλειδί για μεγαλύτερη ασφάλεια βρίσκεται στην σχεδίαση, υλοποίηση συστημάτων,εφαρμογών και εργαλείων web, με κύριο γνώμονα την ασφάλεια που θα λειτουργεί σαν οχυρό απέναντι σε κάθε επίδοξο εισβολέα και θα δυσκολεύει το έργο του.Βέβαια ο δρόμος είναι μακρύς, υπάρχουν πολλά που πρέπει να αντιμετωπισθούν μέχρι να φτάσουμε στο σημείο να θεωρούμε το internet, ένα ασφαλές δίκτυο.

[445] Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 2002, σελ. 332

Βιβλιογραφία

Ελληνική

1. Αλεξανδρή Ν., Β. Μπελεσιώτη, Θ. Παναγιωτόπουλου, Εισαγωγή στην επιστήμη των υπολογιστών, Αθήνα 2004,σελ 343-346

2. Αλεξανδρής Ν, Β. Χρυσικόπουλος, Δ. Πεππές, Ασφάλεια Υπολογιστικών Συστημάτων, στο: Ν. Αλεξανδρής,Ε. Κιουντούζης, Β.Τραπεζάνογλου, Ασφάλεια Πληροφοριών-Τεχνικά Νομικά και Κοινωνικά Θέματα, Εκδόσεις Νέων Τεχνολογιών, 1995.

3. Αλεξανδροπούλου –Αιγυπτιάδου Ε., «Προσωπικά δεδομένα» , Αντ. Σάκκουλας, Θεσσαλονίκη 2007.

4. Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία , Ζητήματα από το Δίκαιο της Πληροφορικής ., Εκδόσεις Σάκκουλα, Αθήνα 2002.

5. Αυγουστιανάκης Μιχ. Κ. «Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων – Προβλήματα και αντιμετώπιση από το δίκαιο» στο: ΔτΑ 11/2001 .

6. Γέροντας Απόστολος Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων - μία συμβολή στην ερμηνεία του Ν. 2472/ 1997 «προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» Εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα - Κομοτηνή 2002
7. Γκρίτζαλη Σ., Κάτσικα Σ., Γκρίτζαλη Δ., Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, Αθήνα, 2003.

8. Δουληγέρης Χρήστος Σημειώσεις του μαθήματος «Δίκτυα υπολογιστών» του Προγράμματος Μεταπτυχιακών Σπουδών «Πληροφορική» του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς.

9. Ηλιάδης Γ., Κακόβουλο λογισμικό σε:Σ. Κάτσικα,Δ. Γκρίτζαλη,Σ. Γκρίτζαλη,Ασφάλεια πληροφοριακών συστημάτων , Αθήνα,2004

10. Ζορκάδης Β.,Κρυπτογραφία, Πάτρα 2002, ΕΑΠ.

11. Ζουραράκη Ο., Μασίκου Μ. , Σχεδίαση και εξομοίωση συστήματος ανίχνευσης και αντιμετώπισης κατανεμημένων επιθέσεων (DDoS) , Αθήνα 2004, διαθέσιμο στο: http://artemis-new.cslab.ece.ntua.gr:8080/jspui/handle/123456789/3543

12. Ιγγλεζάκης Ιωάννης Δ. Ευαίσθητα Προσωπικά Δεδομένα – Η επεξεργασία ειδικών κατηγοριών δεδομένων και οι συνέπειές της Εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη 2003.
13. Ιγγλεζάκης Ιωάννης Δ. Δίκαιο της Πληροφορικής, Εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη 2003.
14. Ιγγλεζάκης Ιωάννης Δ. Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη 2003
15. Καράκος Σ., Διαδίκτυο Παγκόσμιος Ιστός & Τεχνικές Προγραμματισμού, εκδόσεις Γκιούρδας, Αθήνα, 2009
16. Καραυγουστής Ανέστης, Χρήση Νέων Τεχνολογιών στις επιχειρήσεις, ΥΠΕΠΘ-Γ.Γ.Ε.Ε.-Ι.Δ.Ε.Κ.Ε.
17. Καράκωστας Ιωάννης Κ. Δίκαιο & Internet Νομικά ζητήματα του Διαδικτύου β΄ έκδοση Εκδόσεις Δίκαιο & Οικονομία Π. Ν. Σάκκουλας Αθήνα 2003.

18. Κάτσικα Σ, Ασφάλεια Υπολογιστών, Πάτρα,2001,ΕΑΠ.
19. Κομνηνός Θ.,Π. Σπυράκης, Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς, Εκδόσεις Ελληνικά Γράμματα, 2002.
20. Λαμπρινουδάκης Κ, Σ. Γκρίτζαλης, Λ. Μήτρου, Σ. Κάτσικας, Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Εκδόσεις Παπασωτηρίου 2010.
21. Λεκάτης Γ, Κλαδάκης Ν., Ασφάλεια δικτύων και συστημάτων, Παπασωτηρίου,Αθήνα, 2001
22. Μάγκος Ε., Ασφάλεια Υπολογιστών και Προστασία Δεδομένων, Κέρκυρα, 2007,σελ. 11-13 στο: http://di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20A.pdf
23. Μαρκατσέλας Μ, Ξαρχάκος Κ., Μαθαίνετε εύκολα Joomla!, εκδόσεις Ξαρχάκος, Αθήνα 2010.
24. Μήτρου Α., Η Αρχή Προστασίας Προσωπικών Δεδομένων
25. Μπαμπινιώτη Γ., λεξικό της Νέας Ελληνικής γλώσσας, β΄έκδοση 2005.
26. Μπόζιος Ε. , Σημειώσεις ασφάλειας πληροφοριακών συστημάτων, Θεσσαλονίκη 2004
27. Πάγκαλος Γ., Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων, εκδόσεις Ανίκουλα, Θεσσαλονίκη, 2002
28. Πατσάκη Κ.,Ε.Φούντα, Κρυπτογραφία και εφαρμογές ,τόμος πρώτος, εκδόσεις Βαρβαρήγου,Πειραιάς 2009.
29. Πολέμη Ν.,Καλιοντζόγλου Α., Πρακτικά Θέματα Ασφαλείας Πληροφοριακών Συστημάτων και Εφαρμογών, Εκδόσεις Νέων Τεχνολογιών, 2008.
30. Πολέμη Δ, Σημειώσεις του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων, Πειραιάς, Μάρτιος 2007.
31. Σαατζίδου –Παντελιάδου Ε., Το παράδειγμα της νομικής ρύθμισης της Ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων , με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς στο:
    http://dspace.lib.uom.gr/bitstream/2159/371/5/saatzidou.pdf
32. Σινανιώτη-Μαρούδη Αριστέα,Ιωάννης Δ. Φαρσαρώτας, Ηλεκτρονική τραπεζική» , εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα 2005.
33. Τουντόπουλος Βασίλειος «Το δικαίωμα αντίρρησης του υποκειμένου των δεδομένων» στο περιοδικό:ΤοΣ 1/1999.

Ξενόγλωσση - Μεταφράσεις

1. Andrew S. Tanenbaum, Δίκτυα υπολογιστών, εκδόσεις Κλειδάριθμος
2. Aycock John, Computer Viruses and Malware, Hardcover , Springer Verlag ,2006.
3. Alfred J. Menezes, Paul C. van Oorschotand Scott A. Vanstone,Handbook of Applied Cryptography, CRC Press, 2001, διαθέσιμο: http://cacr.uwaterloo.ca/hac/
4. Honeycutt Jerry, MRY Ann Pike, μτφ, Ε.Γκαγκάτσιου, Πλήρης Οδηγός του Internet, 3η Αμερικάνικη Έκδοση,Γκιούρδας- Αθήνα
5. Jerry Honeycutt & Mary Ann Pike, Πλήρης Οδηγός του Internet, 3η Αμερικάνικη έκδοση,1996 , μ.τ.φ Ε.Γκαγκάτσιου, Γκιούρδας.
6. M. Laakso , A. Takanen , J. Röning, The Vulnerability Process: A Tiger Team Approach to Resolving Vulnerability Cases (1999), στο:
    http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.39.9438&rep=rep1&type=pdf

7. Mark Gibbs & Richard Smith, Ταξιδεύοντας στο Internet, έκδοση Deluxe,μ.τ.φ Λ. Γατσώρης, Κ. Μπενέκος,εκδ. Anubis.
8. Simson Garfinkel, Gene Spafford, Alan Scbwartz, Practical Unix & Internet Security, O' Reilly & Associates, USA, 2003.
9. Scarfone Karen, Mell Peter,Guide to Intrusion Detection and Prevention Systems, 2007, National Institute of Standards and Technology, (2007)., http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
10. Sterling Bruce , "The Hacker Crackdown: Law and Disorder on the Electronic Frontier" , Bantam Books , Reprint Edition , 1993.
11. William Stallings, Βασικές αρχές ασφάλειας δικτύων: Εφαρμογές και πρότυπα, Τρίτη αμερικάνικη έκδοση, Εκδόσεις Κλειδάριθμος, 2010

Άρθρα

1. Ανδριτσόπουλος Γιάννης, Ο Ομπάμα πάει... Facebook,εφημερίδα Νέα,20-04-2011 στο: http://www.tanea.gr/kosmos/article/?aid=4627714
2. Γαλάνης Δημήτρης, Τα 10 κοινωνικά δίκτυα με τη μεγαλύτερη αξία, εφημερίδα Βήμα, 6-3-2012, στο: http://www.tovima.gr/media/article/?aid=447060
3. BBC NEWS, Teen charged over Sasser virus, 9 September, 2004, http://news.bbc.co.uk/2/hi/technology/3640506.stm
4. Michael Kerner, 'Land' Bug Back to Bedevil Microsoft Servers,2005, στο: http://www.internetnews.com/security/article.php/3488171
5. The New York Times, αναδημοσίευση εφημερίδα Καθημερινή, Το τέλος των κωδικών πρόσβασης, 06-01-2012,στο: http://news.kathimerini.gr/4dcgi/_w_articles_economyagor_1_06/01/2012_468294

Εφημερίδες- Περιοδικά

1. Περιοδικό Επιστημονικό Marketing Management, στο: http://www.epistimonikomarketing.gr/article_show.php?article_id=3113.
2. Περιοδικό για το Enterprise Computing και την Ασφάλεια στην πληροφορική στο: http://www.securitymanager.gr/it_security/protection_article.php?id=5&set=7&titl30a
3. Ελληνικό Ηλεκτρονικό Περιοδικό (Hellenic e-zine), Τεύχος: 04, Μήνας Έκδοσης: Μάιος 2002, Βλ Denial Of Service (D.O.S.) Επιθέσεις,στο: http://www.isee.gr/issues/04/insert/index.html
4. PCnews, Μηνιαία εφημερίδα για τους υπολογιστές και την τεχνολογία http://pc-news.gr/component/content/article/11/266-whatisskype.html
5. Εφημερίδα ,τα Νέα, http://www.tanea.gr/kosmos/article/?aid=4668312
6. Εφημερίδα Ελευθεροτυπία, 19-11-2010,στο: http://www.enet.gr/?i=news.el.article&id=225584
7. Εφημερίδα Καθημερινή στο: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_20/07/2012_453092
8. Μακεδονικό Πρακτορείο Ειδήσεων, 7 Οκτωβρίου 1996,στο:

http://www.hri.org/info/articles/96-10-07.elot.html

Νομοθεσία[446]

1. Σύνταγμα της Ελλάδος
2. Νόμος 2472/1997
3. Νόμος 2774/1999
4. Νόμος 3471/2006
5. Νόμος 3917/2011
6. Νόμος Ν. 2068/1992
   http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=Nh-i7eUlbMc%3d&tabid=132
7. Διεθνές σύμφωνο για τα ατομικά και πολιτικά δικαιώματα(ΟΗΕ),(Ν.2462/1997)
   http://www.nis.gr/npimages/docs/2462-97.pdf
8. Οδηγία 95/46/ΕΚ
9. Η οδηγία 97/66/ΕΚ
10. Οδηγία 2002/58/ΕΚ

Πηγές Internet

1. Αρχή προστασίας προσωπικών δεδομένων www.dpa.gr .
2. Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών. http://www.adae.gr/portal/
3. Η ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων) http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#5
4. Εργαστήριο CONTA του Πανεπιστημίου Μακεδονίας
   http://conta.uom.gr/conta/ekpaideysh/seminaria/M_Telecommunications/html/17/17-3.htm
5. Ένωση Ελλήνων Χρηστών INTERNET http://www.eexi.gr/?q=node/17
6. Ελληνική Ένωση Επαγγελματιών Internet http://www.eeei.gr/odhgos/netsc404/howcooki.htm
7. Ηλεκτρονική Εγκυκλοπαίδεια Βικιπαίδεια : http://el.wikipedia.org
8. Διεθνής οργανισμός Internet. http://www.internic.net
9. Διεθνής οργανισμός Internet. http://www.isoc.org

[446] Η νομοθεσία αντλήθηκε από τον ιστότοπο της Αρχής Προστασίας δεδομένων Προσωπικού χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL

10. Εικονικός Κόσμος (Δεύτερη Ζωή) Second Life

http://xrisoikweb2.pbworks.com/w/page/8263756/Second%20Life

11. Ελληνική Στατιστική Υπηρεσία (ΕΛΣΤΑΤ)
http://www.statistics.gr/portal/page/portal/ESYE/BUCKET/A1901/PressReleases
12. Εταιρεία Τηλεπικοινωνιών Forthnet. http://www.forthnet.gr
13. Ευρωπαϊκή σύμβαση ΕΣΔΑ. http://www.nis.gr/npimages/docs/ESDA.pdf
14. Κέντρο ΠΛΗΝΕΤ Φλώρινας. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Viruses.html
15. Κέντρο Δικτύων (ΚΕΔ) του Ε.Μ.Π
http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104
16. Κέντρο Λειτουργίας Δικτύου ΑΠΘ http://noc.auth.gr/services/voice-video/conferencing
17. Κοινής Εποπτικής Αρχής της Ευρωπόλ (ΚΕΑ).
http://europoljsb.consilium.europa.eu/about.aspx?lang=el
18. Κοινή Εποπτική Αρχή της Σένγκεν
http://schengen.consilium.europa.eu/about.aspx?lang=el
19. Κοινωνικό Δίκτυο LinkedIn. www.linkedin.com
http://social-net.gr/about/ τι-είναι-το-linkedin
20. Κοινωνικό Δίκτυο Flickr .http://www.flickr.com
21. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων
http://europa.eu/about-eu/institutions-bodies/edps/index_el.htm
22. Πανελλήνιο Σχολικό Δίκτυο. http://www.sch.gr.
23. Παρατηρητήριο για την ψηφιακή Ελλάδα. http://www.observatory.gr
24. Πράξη του Συμβουλίου της 12ης Μαρτίου 1999 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999F0330:EL:HTML
25. Σύμβαση εφαρμογής της συμφωνίας του Σένγκεν http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922%2802%29:el:HTML
26. Ο χώρος και η συνεργασία Σένγκεν
http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_el.htm
27. Συμβούλιο της Ευρωπαϊκής Ένωσης
http://www.consilium.europa.eu/showPage.aspx?id=1157&lang=el
28. Σύνοψη της νομοθεσίας της ΕΕ
29. http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/l14005b_el.htm
30. Τραπεζικά συστήματα πληροφοριών Τειρεσίας. http://www.tiresias.gr/index.html

31. Τηλεφωνία μέσω Διαδικτύου (Voice over IP). http://www.skype.com/intl/en/home
32. Η σελίδα της microsoft: https://www.microsoft.com
33. http://www.ahumanright.org
34. http://www.3cx.gr/voip-sip/h323.php
35. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
36. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
37. http://www.ea.gr/ep/agroweb/htmls/lessons/commerce1gr/12.htm
38. http://www.e-papadakis.gr/ola18.htm
39. http://el.computerscience.wikia.com/wiki/%CE%95%CF%%CF%83%CE%B7_Fraggle
40. http://en.kioskea.net/contents/attaques/attaque-land.php3
41. http://el.dbpedia.org/page/B7_Smurf .
42. http://el.computerscience.wikia.com/wiki/Επίθεση_Smurf
43. http://www.email-encoder.net/index.php
44. http://www.ethermanage.com/ethernet/ethernet.html
45. http://www.fcnet.gr/gr/overview/?id=51
46. http://ghostgrid.blog.com/2010/12/16/ping-flooding/
47. http://greek.almeethaq.net/lv/group/view/kl26887/mIRC.htm
48. http://www.iabeurope.eu/research/mediascope-europe.aspx
49. http://www.iliadis.net/presentations/MaliciousSoftware.pdf
50. http://imm.demokritos.gr/publications/books/INTERNET_RELAY_CHAT%20_IRC_.pdf
51. http://www.internetworldstats.com/stats.htm
52. http://infoman.teikav.edu.gr/e_education/70/InfoSystemSechandouts.ppt
53. http://learn-networking.com/network- security/how-to-prevent-denial-of-service-attacks
54. http://learn-networking.com/network-security/securing-cisco-routers-with-no-ip-directed-broadcast
55. http://www.livescience.com/20727-internet-history.html
56. http://library.tee.gr/digital/m2142/m2142_koutepas.pdf
57. http://www.lk.cs.ucla.edu/LK/Bib/REPORT/PhD
58. http://www.maclife.gr/forum/showthread.php/2088-Google-Latitude
59. http://mashable.com/2011/03/22/linkedin-surpasses-100-million-users-infographic/

60. http://networking-basics.wikispaces.com
61. http://www.nonpaper.net/security/ssl_asymmetric.html
62. http://www.no-spam.gr/tools.htm
63. http://www.passwordmeter.com
64. http://www.pierobon.org/ssl/ch2/record.htm
65. http://pirch.en.malavida.com
66. http://www.phonet.gr/tag/latitude/
67. http://www.smartcardbasics.com
68. http://support.google.com/blogger/bin/answer.py?hl=el&answer=175250
69. http://technet.microsoft.com/en-us/library/cc767139.aspx
70. http://www.tutorial5.com/content/view/80/79/
71. http://www.tweaknews.gr/?page=home
72. http://www.us-cert.gov/cas/tips/ST04-015.html.
73. http://www.unric.org/el/index.php/human-rights-greek/18
74. http://www.weknowwhatyouredoing.com
75. http://windows.microsoft.com/el-GR/windows-vista/What-is-a-smart-card-and-how-do-I-use-one
76. http://windows.microsoft.com/el-GR/windows-vista/Telnet-frequently-asked-questions

Μικρό λεξικό

Anti-virus: Λογισμικό αντιμετώπισης ιών το οποίο με την εγκατάστασή του σε ένα υπολογιστή προστατεύει από κακόβουλα προγράμματα.

Back up: Η διαδικασία αντιγραφής σημαντικών αρχείων του υπολογιστή ή και ολόκληρου του σκληρού δίσκου σε αποθηκευτικά μέσα, προκειμένου να αποφευχθούν ανεπιθύμητα αποτελέσματα.

Buffer: Περιοχή της μνήμης που χρησιμοποιεί ο υπολογιστής σαν προσωρινή αποθήκη δεδομένων.

Cookies: Τα cookies είναι μικρά αρχεία κειμένου τα οποία αποθηκεύονται στον υπολογιστή μας κατά την πλοήγησή μας στο διαδίκτυο.

Digital signature (Ψηφιακή υπογραφή). Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα από κρυπτογραφημένα δεδομένα ,που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου.

Firewall (τείχος προστασίας). Ένα σύστημα(συσκευή ή πρόγραμμα) που είναι έτσι ρυθμισμένο έτσι ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

FTP (File Transfer Protocol). Πρωτόκολλο μεταφοράς αρχείων στο Internet.

Hackers. Εισβολείς που εισέρχονται σε υπολογιστές χωρίς νόμιμη πρόσβαση, παρακάμπτοντας το σύστημα ασφαλείας τους.

HTML. Είναι η κύρια γλώσσα σήμανσης για τις ιστοσελίδες, και τα στοιχεία της είναι τα βασικά δομικά στοιχεία των ιστοσελίδων. Χρησιμοποιείται για την δημιουργία ιστοσελίδων στο Internet.

Internet Protocol (IP) address. Είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol standard. Η ηλεκτρονική ταυτότητα ενός υπολογιστή που βρίσκεται σε ένα δίκτυο υπολογιστών ή στο Internet.

IRC (Internet Relay Chat). Υπηρεσία του Internet, σύμφωνα με την οποία οι χρήστες επικοινωνούν με γραπτά μηνύματα σε πραγματικό χρόνο.

ISP (Internet Service Provider). Μια υπηρεσία παροχής Internet (ISP) είναι μια εταιρεία η οποία παρέχει πρόσβαση στο Internet, συνήθως έναντι αντιτίμου.

Usenet –Newsgroups. Είναι κατάλογοι με διευθύνσεις ηλεκτρονικού ταχυδρομείου χωρισμένοι σε ομάδες ανάλογα τα ενδιαφέροντα. Ο κάθε χρήστης μπορεί να στείλει μήνυμα σε κάποια ομάδα χρηστών που έχει κοινά ενδιαφέροντα με αυτόν. Τα μέλη της ομάδας αυτής μπορούν να το διαβάσουν και να απαντήσουν αν θέλουν σε αυτό. Η κάθε ομάδα ονομάζεται «ομάδα ειδήσεων» (newsgroup).

Peer – to –Peer (ή P2P). Είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα και συνδέει υπολογιστές χωρίς να υπάρχει κεντρικός server.

Search engine.Η μηχανή αναζήτησης δίνει τη δυνατότητα για εξερεύνηση στο Internet με λέξεις κλειδιά.

Spam. Αζήτητη αλληλογραφία που αποστέλλεται μαζικά μέσω του ηλεκτρονικού ταχυδρομείου, σε μια προσπάθεια προώθησης προϊόντων ή ιδεών.

Spyware. Λογισμικό κατασκοπίας το οποίο φορτώνεται κρυφά (με ύπουλο τρόπο) σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη.

Trojan Horse. Είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.

Virus (ιός). Ένας ιός υπολογιστών είναι ένα πρόγραμμα υπολογιστών που μπορεί να αντιγραφεί και να μολύνει έναν υπολογιστή χωρίς την άδεια ή τη γνώση του χρήστη.

Web. Ο παγκόσμιος ιστός ή αλλιώς το WWW (World Wide Web).

Web Browser. Ο φυλλομετρητής που μας βοηθά να ανοίγουμε σελίδες στο internet και να κάνουμε περιήγηση.

Worm. Είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη.

XML. Είναι μία γλώσσα σήμανσης, που περιέχει ένα σύνολο κανόνων για την ηλεκτρονική κωδικοποίηση κειμένων. Επιτρέπει το διαχωρισμού προγραμματισμού για τη διαχείριση περιεχομένου μιας σελίδας από τον προγραμματισμό για τη μορφοποίηση και τη διάταξη.

Ευαίσθητα, δεδομένα: Ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.

Ιομορφικό λογισμικό: Ένα πρόγραμμα, το οποίο δημιουργεί αντίγραφα του εαυτού του ενσωματώνοντας τα μέσα σε άλλα προγράμματα του υπολογιστικού συστήματος, με συνηθέστερο στόχο να εκμεταλλευτεί αδυναμίες του συστήματος. Αυτό γίνεται εν αγνοία του χρήστη.

Κοινωνία της Πληροφορίας: Κοινωνία της Πληροφορίας είναι η σύγχρονη κοινωνία, μια κοινωνία που οργανώνεται γύρω από την πληροφορία μέσω της τεχνολογίας και χωρίς χωροχρονικούς περιορισμούς, λειτουργεί ως οικονομικός πόρος για γνώση και για κάθε δραστηριότητα μας στην κοινωνία συμβάλλοντας στην εξέλιξη. Με αυτόν τον όρο περιγράφουμε το νέο περιβάλλον που αναπτύσσεται με άξονες τα δεδομένα, την πληροφορική και τις τηλεπικοινωνίες.

Κρυπτογραφία: Η κρυπτογραφία είναι ο κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει

μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι σε θέση να διαβάσει την πληροφορία εκτός από τα μέλη. Η διαμόρφωση των δεδομένων σε «ακατάληπτη» μορφή, ώστε να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των πληροφοριών.

Πληροφοριακό Σύστημα (ΠΣ): Ένα οργανωμένο σύνολο αλληλεπιδρώντων στοιχείων (άνθρωποι, δεδομένα, λογισμικό, υλικός εξοπλισμός, διαδικασίες), το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού.

Προσωπικά δεδομένα : Κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

Πρωτόκολλο SSL. Είναι το πρωτόκολλο που χρησιμοποιείται, για την ασφαλή μετάδοση και επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών, για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Συμμετρικά κλειδιά: Ψηφιακά κλειδιά που χρησιμοποιούνται στην συμμετρική κρυπτογραφία για την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων.

Ταυτοποίηση: Η συσχέτιση του χρήστη ενός ΠΣ με το πραγματικό φυσικό πρόσωπο.

Ψηφιακά κλειδιά: Τα συμμετρικά και ασύμμετρα κλειδιά που χρησιμοποιούνται στην κρυπτογραφία. Συνήθως είναι ομάδες bit το μήκος των οποίων εξαρτάται από τον κρυπτογραφικό αλγόριθμο που χρησιμοποιείται**.**

Ψηφιακά πιστοποιητικά: Είναι ηλεκτρονικά έγγραφα, ένα είδος ηλεκτρονικής ταυτότητας, που χρησιμοποιούνται για την αναγνώριση μιας οντότητας και την συσχέτισή της με ένα δημόσιο κλειδί.

Πηγές: 1. Ηλεκτρονική εγκυκλοπαίδεια Wikipedia

http://el.wikipedia.org/wiki/81%CE%B9%CE%B1

2. Παρούσα διπλωματική εργασία με αντίστοιχες παραπομπές

ΓΝΩΜΟΔΟΤΗΣΕΙΣ - ΕΝΤΥΠΑ

Οι γνωμοδοτήσεις που παρατίθενται είναι για τα έτη 2001-2011 και έχουν αντληθεί από τον δικτυακό τόπο της Αρχής [447].

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2001

Ανάλυση γενετικού υλικού για σκοπούς εξιχνίασης εγκλημάτων και ποινικής δίωξης	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 15/2001
Νομιμότητα έκδοσης Κάρτας Υγείας Αθλητή από την Ελληνική Ποδοσφαιρική Ομοσπονδία (ΕΠΟ)	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 19/2001
Σχετικά με την υποχρέωση ή μη ενημέρωσης της αστυνομίας και της υπηρεσίας αλλοδαπών και μετανάστευσης από τους διευθυντές ξενοδοχείων, παραθεριστικών κέντρων, κλινικών και θεραπευτηρίων για την άφιξη και αναχώρηση αλλοδαπών που φιλοξενούν.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 86/2001

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2002

Γνωμοδότηση για τη νομιμότητα διατήρησης των αρνητικών φωτογραφιών από τους φωτογράφους.	ΑΠΟΦΑΣΗ ΑΡ. 30/2002
Γνωμοδότηση παροχής στοιχείων βοηθηματούχων προς Ταμείο	ΑΠΟΦΑΣΗ ΑΡ. 31/2002
Νομιμότητα εγκατάστασης κλειστού κυκλώματος τηλεόρασης σε χώρο εργασίας από εργοδότη ο οποίος έχει υπόνοιες διάπραξης καθ' υποτροπήν υπεξαιρέσεων σε βάρος του από υπάλληλό του	ΓΝΩΜΟΔΟΤΗΣΗ 68/2002
Γνωμοδότηση για την αναγνώριση καλούντος συνδρομητή σε ISDN	ΑΠΟΦΑΣΗ ΑΡ. 71/2002
Γνωμοδότηση για τη διασταύρωση προσωπικών δεδομένων στο χώρο της σταθερής τηλεφωνίας	ΑΠΟΦΑΣΗ ΑΡ. 78/2002
Γνωμοδότηση σχετικά με ανακοίνωση προσωπικών δεδομένων συνδρομητών εταιρείας κινητής τηλεφωνίας σε αιτούντες τρίτους, εισαγγελείς, ανακριτικούς ή προανακριτικούς υπαλλήλους ή πολίτες	ΑΠΟΦΑΣΗ ΑΡ. 79/2002
Χρήση παράνομα συλλεγέντων αποδεικτικών μέσων από τα Μέσα Μαζικής Ενημέρωσης και ενώπιον των δικαστηρίων	ΓΝΩΜΟΔΟΤΗΣΗ 83/2002

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2003

Ικανοποίηση του δικαιώματος πρόσβασης συνδρομητών από εταιρείες παροχής τηλεπικοινωνιακών υπηρεσιών σε περιπτώσεις άρσης του απορρήτου	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2003
Χορήγηση στοιχείων των ασφαλισμένων και συνταξιούχων που περιέχονται στο αρχείο του ΤΕΒΕ, προς ιδιώτες ή Δημόσιες Αρχές	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 3/2003

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2004

Νομιμότητα κατάθεσης από το Υπουργείο Εθνικής Άμυνας στη Βουλή ατομικών φακέλων αξιωματικών που αποστρατεύθηκαν ή προήχθησαν και αιτιολογικών αποστρατείας στο πλαίσιο του κοινοβουλευτικού ελέγχου	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2004
Νομιμότητα κατάθεσης στη Βουλή στοιχείων που περιλαμβάνουν προσωπικά δεδομένα προσώπων που συνεργάζονται με το Υπουργείο Εθνικής Άμυνας ή με εξαρτώμενους από αυτό φορείς στο πλαίσιο κοινοβουλευτικού ελέγχου	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 2/2004
Νομιμότητα κατάθεσης από το Υπουργείο Δικαιοσύνης στη Βουλή στοιχείων που περιλαμβάνουν προσωπικά δεδομένα στο πλαίσιο κοινοβουλευτικού ελέγχου	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 3/2004

[447] http://www.dpa.gr/portal/page?_pageid=33,120923&_dad=portal&_schema=PORTAL#2012

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2005

Γνωμοδότηση για χορήγηση στοιχείων καταναλωτών ΔΕΗ σε Δήμους	ΑΠΟΦΑΣΗ ΑΡ. 20/2005
Γνωμοδότηση για τη νομιμότητα αρχείου του Υπουργείου Πολιτισμού	ΑΠΟΦΑΣΗ ΑΡ. 21/2005
Γνωμοδότηση της Αρχής σχετικά με τη δυνατότητα του υπευθύνου επεξεργασίας χορήγησης σε τρίτο στοιχείων (προσωπικών δεδομένων μη ευαίσθητου χαρακτήρα) που τηρεί στο αρχείο του	ΑΠΟΦΑΣΗ ΑΡ. 67/2005
Γνωμοδότηση της Αρχής σχετικά με την κατάρτιση από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης βάσης δεδομένων με καταλόγους ("λίστας αναμονής") ιατρών (υποψηφίων για τοποθέτηση προς απόκτηση ειδικότητας ή προς εκπλήρωση της υποχρεωτικής υπηρεσίας υπαίθρου) κατά Νοσοκομείο και ειδικότητα, που θα αναρτηθούν στο διαδίκτυο	ΑΠΟΦΑΣΗ ΑΡ. 69/2005

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2006

Χορήγηση εγγράφων που βρίσκονται στην κατοχή της ΕΥΕΠ	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2006
Δημοσίευση αποφάσεων - πράξεων του ΣτΕ στο διαδίκτυο	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 2/2006
Γνωμοδότηση της Αρχής για σύσταση και λειτουργία από την ΤΕΙΡΕΣΙΑΣ Α.Ε. αρχείου επιχειρήσεων των οποίων οι συμβάσεις για αποδοχή καρτών έχουν καταγγελθεί	ΑΠΟΦΑΣΗ ΑΡ. 6/2006

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2007

Επεξεργασία από το ΙΚΑ στοιχείων φορολογικής δήλωσης ασφαλισμένου	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2007
Γνωμοδότηση για το σύστημα Μ-TAXIS της Γενικής Γραμματείας Πληροφοριακών Συστημάτων	ΑΠΟΦΑΣΗ ΑΡ. 48/2007

Δεν υπάρχουν γνωμοδοτήσεις για το έτος 2008

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2009

Λειτουργία κλειστών κυκλωμάτων τηλεόρασης σε δημόσιους χώρους.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2009
Ανάλυση DNA και δημιουργία αρχείου γενετικών αποτυπωμάτων.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 2/2009
Έννομες συνέπειες εισαγγελικής παραγγελίας για τη χορήγηση δημοσίων εγγράφων.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 3/2009
Έκταση αρμοδιότητας της Αρχής επί αιτήσεων τρίτων σε δεδομένα προσωπικού χαρακτήρα.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 4/2009

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2010

Ανάρτηση νόμων, κανονιστικών και ατομικών πράξεων στο διαδίκτυο.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2010
Λειτουργία συστημάτων βιντεοεπιτήρησης από δημόσιες αρχές και ιδιώτες.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 2/2010
Καταχώριση και διαγραφή αλλοδαπών τρίτων χωρών από το Σύστημα Πληροφοριών Σένγκεν (ΣΠΣ) και τον Εθνικό Κατάλογο Ανεπιθύμητων Αλλοδαπών (ΕΚΑΝΑ).	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 3/2010
Ηλεκτρονική κάρτα αποδείξεων.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 4/2010

Περιγραφικός πίνακας γνωμοδοτήσεων της ΑΠΔΠΧ για το έτος 2011

Δημοσιοποίηση στο διαδίκτυο φορολογικών δεδομένων.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 1/2011
Δημοσιοποίηση από Δικηγορικούς Συλλόγους πειθαρχικών ποινών δικηγόρων.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 2/2011
Διαβίβαση προσωπικών δεδομένων μελών Δικηγορικού Συλλόγου σε τρίτους για δικαστική χρήση.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 3/2011
Δημοσιοποίηση στο διαδίκτυο στοιχείων οφειλετών ληξιπρόθεσμων οφειλών προς το Δημόσιο.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 4/2011
Ανάρτηση στο διαδίκτυο των δηλώσεων περιουσιακής κατάστασης πολιτικών προσώπων.	ΓΝΩΜΟΔΟΤΗΣΗ ΑΡ. 7/2011

Έντυπο Προσφυγής/Καταγγελίας

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Κηφισίας 1-3, Αμπελόκηποι, ΤΚ 115 23 Αθήνα **Internet Site: www.dpa.gr**
Τηλ.:210 6475 600, Fax:210 6475628

ΕΝΤΥΠΟ ΠΡΟΣΦΥΓΗΣ/ ΚΑΤΑΓΓΕΛΙΑΣ

1. Τύπος. Σημειώστε με Χ εάν πρόκειται για προσφυγή ή καταγγελία:

ΠΡΟΣΦΥΓΗ[1] ☐ **ΚΑΤΑΓΓΕΛΙΑ**[2] ☐

2. Στοιχεία προσφεύγοντος / καταγγέλλοντος

2.1. Επωνυμία/Ονοματεπώνυμο _____

_____

2.2. Οδός _____ 2.3. Αριθμός _____

2.4. Τ.Κ _____ 2.5. Πόλη _____

2.6. Χώρα _____

2.7. Τηλέφωνο/α επικοινωνίας _____

2.8. Φαξ _____

2.9. Ηλεκτρονική διεύθυνση _____

3. Κωδικός προηγούμενης υπόθεσης[3]

_____

4. Στοιχεία εκπροσώπου του προσφεύγοντος[4]

4.1. Επωνυμία/Ονοματεπώνυμο _____

_____

4.2. Οδός _____ 4.3. Αριθμός _____

4.4. Τ.Κ _____ 4.5. Πόλη _____

4.6. Χώρα _____

[1] Προσφυγή υποβάλλει μόνο το υποκείμενο της επεξεργασίας όταν θεωρεί ότι θίγεται από συγκεκριμένη επεξεργασία και υπό την προϋπόθεση ότι έχει ασκήσει προς τον υπεύθυνο της επεξεργασίας το δικαίωμα πρόσβασης ή/και αντίρρησης σύμφωνα με τα άρθρα 12 και 13 του Ν. 2472/97, όπου αυτά εφαρμόζονται..

[2] Καταγγελία υποβάλλει κάθε τρίτος (όχι το υποκείμενο των δεδομένων που θίγεται από τη συγκεκριμένη επεξεργασία) που επιθυμεί να αναφέρει στην Αρχή μία παράνομη επεξεργασία προσωπικών δεδομένων.

[3] Είναι ο κωδικός που λάβατε για προσφυγή/καταγγελία που υποβάλατε στο παρελθόν εφόσον είναι διαθέσιμος. Συμπληρώνεται σε περίπτωση που υποβάλλετε συμπληρωματικά στοιχεία για την παρακάτω προσφυγή/καταγγελία.

[4] Συμπληρώνεται μόνο όπου εφαρμόζεται, π.χ. όταν θιγόμενος είναι ανήλικο τέκνο σύμφωνα με τις διατάξεις του Αστικού Κώδικα, όταν η εκπροσώπηση ενώπιον της Αρχής έχει ανατεθεί σε πληρεξούσιο Δικηγόρο ή άλλο τρίτο πρόσωπο.

4.7. Τηλέφωνο/α επικοινωνίας _____

4.8. Φαξ _____

4.9. Ηλεκτρονική διεύθυνση _____

5. Κατά ποιου στρέφεται η προσφυγή / καταγγελία[5]

5.1. Επωνυμία/Ονοματεπώνυμο _____

_____

5.2. Οδός _____ 5.3. Αριθμός _____

5.4. Τ.Κ _____ 5.5. Πόλη _____

5.6. Χώρα _____

5.7. Τηλέφωνο/α επικοινωνίας _____

5.8. Φαξ _____

5.9. Ηλεκτρονική διεύθυνση _____

5.10. Ιστοσελίδα _____

5.11. Ονοματεπώνυμο εμπλεκόμενων ατόμων [6] _____

_____

6. Ποια η σχέση σας με τον καταγγελόμενο[7]

_____

[5] Συνήθως ο υπεύθυνος επεξεργασίας είναι κάποια Υπηρεσία ή Νομικό Πρόσωπο Ιδιωτικού ή Δημοσίου Δικαίου

[6] Αν γνωρίζετε, π.χ. όνομα υπαλλήλου, κλπ.

[7] Π.χ. εργαζόμενος, πελάτης, κλπ.

7. Αντικείμενο της προσφυγής/ καταγγελίας[8]

[8] Περιγράψτε τα περιστατικά που θεωρείτε ότι συνιστούν παράνομη επεξεργασία. Αναφέρετε ποια δεδομένα έχουν αποτελέσει αντικείμενο παράνομης επεξεργασίας, τι, που και πότε συνέβη, από ποιον –αναφέρετε τυχόν εμπλεκόμενα πρόσωπα-, πώς και πότε πληροφορηθήκατε την παραβίαση, οποιεσδήποτε άλλες σχετικές πληροφορίες.

8. Έγγραφα / στοιχεία που τεκμηριώνουν την προσφυγή / καταγγελία

8.1. Απαριθμείστε τα συνημμένα έγγραφα:

1
2
3
4
5
6

8.2. Αν έχετε αποστείλει αντίγραφα της αλληλογραφίας σας με άλλες Αρχές, υπηρεσίες ή οργανισμούς για το ίδιο θέμα, σημειώστε με Χ: ☐

9. Δήλωση

- Γνωρίζω ότι για την εξέταση της προσφυγής / καταγγελίας, το κείμενο αυτής θα γνωστοποιηθεί στον υπεύθυνο της επεξεργασίας ώστε να εκθέσει τις απόψεις του.
- Επισημαίνω ειδικώς τα στοιχεία που δεν επιθυμώ να γνωστοποιηθούν στον υπεύθυνο επεξεργασίας.
- Τα στοιχεία που αναφέρω στην προσφυγή / καταγγελία είναι αληθή.
- Γνωρίζω ότι η Αρχή δύναται να απευθύνει σύσταση προς τον υπεύθυνο επεξεργασίας ή να επιβάλει μόνο διοικητικές κυρώσεις. Ποινικές κυρώσεις ή αποζημίωση επιβάλλονται από τα αρμόδια δικαστήρια.

Ημερομηνία _____ Υπογραφή

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Κηφισίας 1-3, Αμπελόκηποι, ΤΚ 115 23 Αθήνα **Internet Site: www.dpa.gr**
Τηλ.:210 6475 601, Fax:210 6475628

ΟΔΗΓΙΕΣ ΓΙΑ ΤΗΝ ΣΥΜΠΛΗΡΩΣΗ ΤΟΥ ΕΝΤΥΠΟΥ ΚΑΤΑΓΓΕΛΙΑΣ/ΠΡΟΣΦΥΓΗΣ

1. Τύπος

Σημειώστε εδώ αν πρόκειται για προσφυγή ή καταγγελία, λαμβάνοντας υπόψη ότι:

- **Προσφυγή** υποβάλλει μόνο το υποκείμενο της επεξεργασίας όταν θεωρεί ότι θίγεται από συγκεκριμένη επεξεργασία και υπό την προϋπόθεση ότι έχει ασκήσει προς τον υπεύθυνο της επεξεργασίας το δικαίωμα πρόσβασης ή/και αντίρρησης σύμφωνα με τα άρθρα 12 και 13 του Ν. 2472/97, όπου αυτά εφαρμόζονται.

- **Καταγγελία** υποβάλλει κάθε τρίτος (όχι το υποκείμενο των δεδομένων που θίγεται από τη συγκεκριμένη επεξεργασία) που επιθυμεί να αναφέρει στην Αρχή μία παράνομη επεξεργασία προσωπικών δεδομένων.

2. Στοιχεία προσφεύγοντος/καταγγέλλοντος

Αναφέρατε τα ακριβή σας στοιχεία. Συμπληρώστε τα σχετικά πεδία με κεφαλαία γράμματα.

3. Κωδικός υπόθεσης:

Όταν υποβάλλετε μία καταγγελία ή προσφυγή στην Αρχή, δημιουργείται ένας μοναδικός κωδικός για την υπόθεση σας, τον οποίο μπορείτε να χρησιμοποιείτε σε κάθε σχετική επικοινωνία σας με την Αρχή.

Στο πεδίο αυτό συμπληράνετε τον κωδικό που λάβατε για προσφυγή/καταγγελία που υποβάλατε στο παρελθόν εφόσον είναι διαθέσιμος, στην περίπτωση που υποβάλλετε συμπληρωματικά στοιχεία για την παραπάνω προσφυγή/καταγγελία.

4. Στοιχεία εκπροσώπου του προσφεύγοντος:

Τα πεδία 4.1. – 4.9. συμπληρώνονται μόνο όπου εφαρμόζεται, π.χ. όταν θιγόμενος είναι ανήλικο τέκνο σύμφωνα με τις διατάξεις του Αστικού Κώδικα, όταν η εκπροσώπηση ενώπιον της Αρχής έχει ανατεθεί σε πληρεξούσιο Δικηγόρο ή άλλο τρίτο πρόσωπο. Αναφέρατε τα ακριβή στοιχεία του εκπροσώπου με κεφαλαία γράμματα.

Σε περίπτωση εκπροσώπησης από τρίτο πρόσωπο υποβάλλεται απαραιτήτως και το έγγραφο εξουσιοδότησης με βεβαίωση του γνησίου της υπογραφής του εξουσιοδοτούντος

5. Κατά ποιού στρέφεται η προσφυγή / καταγγελία

Αναφέρατε τα ακριβή στοιχεία του φυσικού ή νομικού προσώπου κατά του οποίου στρέφεται η προσφυγή /καταγγελία (συνήθως πρόκειται για κάποια Υπηρεσία ή Νομικό Πρόσωπο Ιδιωτικού ή Δημοσίου Δικαίου). Συμπληρώστε τα σχετικά πεδία με κεφαλαία γράμματα.

Ειδικά στο πεδίο 5.1.αναφέρατε στοιχεία εμπλεκόμενων προσώπων, αν γνωρίζετε, π.χ. όνομα υπαλλήλου, κλπ.

6. Ποια η σχέση σας με τον καταγγελόμενο

Αναφέρατε τη σχέση που σας συνδέει με τον καταγγελόμενο, π.χ. εργαζόμενος, πελάτης, κλπ.

7. Αντικείμενο προσφυγής

Στο πεδίο αυτό περιγράψτε με όσο το δυνατόν μεγαλύτερη ακρίβεια το αντικείμενο της προσφυγής/καταγγελίας. Περιγράψτε τα περιστατικά που θεωρείτε ότι συνιστούν παράνομη επεξεργασία. Αναφέρετε ποια δεδομένα έχουν αποτελέσει αντικείμενο παράνομης επεξεργασίας, τι, που και πότε συνέβη, από ποιόν –αναφέρετε τυχόν εμπλεκόμενα πρόσωπα-, πώς και πότε πληροφορηθήκατε την παραβίαση, οποιεσδήποτε άλλες σχετικές πληροφορίες.

Σε περίπτωση που πρόκειται για προσφυγή θα πρέπει να αναφέρετε εάν ασκήσατε προηγουμένως προς τον υπεύθυνο επεξεργασίας το δικαίωμα πρόσβασης ή/και αντίρρησης και να προσκομίσετε τα σχετικά στοιχεία (αντίγραφο της αίτησης πρόσβασης / των αντιρρήσεων, έγγραφο από το οποίο να προκύπτει η αποστολή της προς τον υπεύθυνο της επεξεργασίας, όπως σφραγίδα ταχυδρομείου, την απάντηση του υπεύθυνου της επεξεργασίας ή δήλωση ότι ο υπεύθυνος δεν απάντησε μέσα στην προθεσμία των 15 ημερών που τάσσει ο νόμος) και να αιτιολογήσετε τους λόγους για τους οποίους η τυχόν απάντηση του υπεύθυνου της επεξεργασίας δεν είναι ικανοποιητική.
Επισημαίνουμε ότι το δικαίωμα πρόσβασης αφορά στην πληροφόρηση του υποκειμένου των δεδομένων σχετικά με τα ζητήματα που αναφέρονται στο άρθρο 12 παρ. 2 Ν. 2472/97 (Να τα αναφέρουμε).
Το δικαίωμα αντίρρησης συνιστά εναντίωση του υποκειμένου των δεδομένων σε συγκεκριμένη επεξεργασία και περιέχει αίτημα προς τον υπεύθυνο επεξεργασίας για συγκεκριμένη ενέργεια, όπως διόρθωση των δεδομένων, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Σε περίπτωση που η αντίρρησή σας αφορά στην μη αποστολή διαφημίσεων μέσω ταχυδρομείου θα πρέπει προηγουμένως να εγγραφείτε στο σχετικό μητρώο που τηρεί η Αρχή.

8. Έγγραφα / στοιχεία που τεκμηριώνουν την προσφυγή / καταγγελία

Για την εξέταση της προσφυγής / καταγγελίας είναι απαραίτητη η υποβολή εγγράφων / στοιχείων που την τεκμηριώνουν. Τα έγγραφα θα πρέπει να υποβληθούν σε αντίγραφα, όχι πρωτότυπα. Η Αρχή δεν επιστρέφει τα έγγραφα.

Υποβάλετε μόνο έγγραφα που συνδέονται άμεσα με την προσφυγή / καταγγελία σας.
Εάν είναι απαραίτητη η αποστολή μεγάλου αριθμού εγγράφων ή σελίδων ενός εγγράφου σημειώστε τα σημεία που συνδέονται άμεσα με την προσφυγή σας.

Εάν υποβάλετε μεγάλο αριθμό συνημμένων εγγράφων που δεν αφορούν άμεσα την προσφυγή / καταγγελία η Αρχή δύναται να τα επιστρέψει και να σας ζητήσει να στείλετε μόνο τα σχετικά στοιχεία

ΔΗΛΩΣΗ ΑΙΤΗΣΗ

(Εγγραφής στο Μητρώο Προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ΄αποστάσεως)

ΕΠΙΘΕΤΟ

_____

ΟΝΟΜΑ

_____

ΟΝΟΜΑ ΠΑΤΡΟΣ

_____

ΕΠΑΓΓΕΛΜΑ

_____

ΔΙΕΥΘΥΝΣΗ

_____

ΤΑΧ. ΚΩΔΙΚΑΣ

_____

ΠΕΡΙΟΧΗ

_____

ΑΡΙΘΜΟΣ ΤΑΥΤΟΤΗΤΑΣ

_____

ΤΗΛΕΦΩΝΟ

_____

Προς την

Αρχή Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα
Κηφισίας 1-3, Αμπελόκηποι
ΤΚ 115 23
Αθήνα

Με την παρούσα δηλώνω σύμφωνα με την παράγραφο 3 αρθρ.13 του Νόμου 2472/97 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ΦΕΚ 50/τ.Α'/10-4-1997), ότι οποιουδήποτε είδους δεδομένα που με αφορούν δεν επιθυμώ να αποτελέσουν αντικείμενο επεξεργασίας από οποιονδήποτε, για λόγους προώθησης πωλήσεων αγαθών ή παροχής υπηρεσιών εξ' αποστάσεως.

Ως εκ τούτου, ζητώ να καταχωρηθούν τα στοιχεία μου στο σχετικό Μητρώο του εδαφίου δ', παράγραφο 4 του άρθρου 19 του Ν. 2472/1997 .

Αθήνα , _____

Ο Αιτών _____

Υπογραφή _____

Έντυπο 1.0

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Κηφισίας 1-3, Αμπελόκηποι, ΤΚ 115 23 Αθήνα **Internet Site: www.dpa.gr**
Τηλ.:210 6475 600, Fax:210 6475628

ΓΝΩΣΤΟΠΟΙΗΣΗ
ΤΗΡΗΣΗΣ ΑΡΧΕΙΟΥ / ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (ΜΕΡΟΣ Ι)
(Άρθρο 6 του Ν. 2472/97. Επέχει και θέση αίτησης αδείας αν τα δεδομένα είναι ευαίσθητα)

Οδηγίες: 1.Η ένδειξη "*" σημαίνει ότι συμπληρώνεται από την Υπηρεσία. 2. Όπου απαιτείται σημειώστε "Χ" στο αντίστοιχο τετράγωνο. 3. Πριν συμπληρώσετε το έντυπο, βεβαιωθείτε ότι το αρχείο δεν εμπίπτει στις κατηγορίες για τις οποίες η Αρχή έχει εκδώσει ειδικούς κανονισμούς ή διατάξεις.

Ι. Στοιχεία Πρωτοκόλλου :

***100. Αριθμός :** _____ ***101.Κωδικός Μητρώου Επεξεργασίας:** _____ ***102. Ημερομηνία :** _____

α. Κατηγορία γνωστοποίησης:

103. Αρχική γνωστοποίηση ☐ 104. Τροποποίηση γνωστοποίησης ☐ 105. Κατάργηση γνωστοποίησης ☐

106. Επέχει θέση αιτήσεως για χορήγηση άδειας επεξεργασίας ευαίσθητων δεδομένων (άρθρο 7 του Ν.2472/1997) ☐

ΙΙ. Στοιχεία υπεύθυνου επεξεργασίας[1] :

107. Επωνυμία επιχείρησης / Ονοματεπώνυμο :

108. Κύρια δραστηριότητα / Επάγγελμα: _____

109. Α.Φ.Μ [2]: Νομικό πρόσωπο _____ Φυσικό πρόσωπο: _____

110. Οδός: _____ 111. Αριθμός _____

112. Ταχ.Κώδικας: _____ 113. Πόλη : _____

114. Τηλέφωνο : _____ 115. Fax: _____

116. Ηλεκτρονική διεύθυνση : _____

α. Ο υπεύθυνος επεξεργασίας είναι:

117. Δημόσιο ☐ 118. Νομικό Πρόσωπο Δημοσίου Δικαίου, ΟΤΑ ☐ 119. Οργανισμός ευρύτερου Δημόσιου Τομέα ☐

120. Νομικό Πρόσωπο Ιδιωτικού Δικαίου κερδοσκοπικού χαρακτήρα ☐ 121. Χρηματοπιστωτικός οργανισμός ☐

122. Νομικό Πρόσωπο Ιδιωτικού Δικαίου μη κερδοσκοπικού χαρακτήρα ☐ 123. Φυσικό πρόσωπο ☐

124. Ένωση Προσώπων που δεν έχει νομική προσωπικότητα ☐

[1] *Προσοχή: Οι κωδικοί 107-116 πρέπει να συμπληρωθούν με κεφαλαία γράμματα.*
[2] Για τα νομικά πρόσωπα συμπληρώστε ολόκληρο το Α.Φ.Μ, ενώ για τα φυσικά πρόσωπα συμπληρώστε τα επτά (7) πρώτα ψηφία του Α.Φ.Μ