Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΟ ΔΙΑΔΙΚΤΥΟ** **SECURITY AND PRIVACY IN THE INTERNET TELECOMMUNICATIONS**
Ονοματεπώνυμο Φοιτητή	**ΙΩΑΝΝΑ ΚΟΤΣΙΚΟΝΑ**
Πατρώνυμο	**ΚΩΝΣΤΑΝΤΙΝΟΣ**
Αριθμός Μητρώου	**ΜΠΠΛ/ 10058**
Επιβλέπων	**ΣΙΝΑΝΙΩΤΗ ΑΡΙΣΤΕΑ**

Ημερομηνία Παράδοσης **Ιούλιος 2013**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	**(υπογραφή)**	**(υπογραφή)**
Όνομα Επώνυμο **Βαθμίδα**	**Όνομα Επώνυμο** **Βαθμίδα**	**Όνομα Επώνυμο** **Βαθμίδα**
Καθηγήτρια	**Καθηγητής**	**Λέκτορας**
Α.Σινανιώτη	**Χ.Δουληγέρης**	**Π.Κοτζανικολάου**

Ευχαριστίες

Στην διεκπεραίωση της διπλωματικής μου εργασίας είχα δίπλα μου ανθρώπους για τους οποίους νιώθω την ανάγκη να ευχαριστήσω για τις συμβουλές τους τις γνώμες τους και την βοήθεια που μου πρόσφεραν.

- Θερμές ευχαριστίες για την βοήθεια της και τις πολύτιμες υποδείξεις της, την καθοδήγηση της στην συγγραφή της εργασίας μου, στην κ. Σινανιώτη Αριστέα αλλά τον κ. Χ. Δουληγέρη , και γενικά όλους τους καθηγητές του μεταπτυχιακού προγράμματος για τις γνώσεις που μου μετέδωσαν καθ 'όλη την διάρκεια των σπουδών μου .

- Το Πανεπιστήμιο Πειραιώς , που μου έδωσε την δυνατότητα να πραγματοποιήσω το πρόγραμμα Μεταπτυχιακών σπουδών.
- Τους γονείς μου που με στηρίζουν σε όλη την πορεία της ζωής μου και των σπουδών μου.
- Τέλος, είμαι ιδιαιτέρως ευγνώμων στον φίλο μου Αλέξανδρο για την σπουδαία και σημαντική βοήθεια του αλλά και την υποστήριξη του και την υπομονή του.

Ένα μεγάλο ευχαριστώ σε όλους.

ΙΟΥΛΙΟΣ 2013
ΙΩΑΝΝΑ ΚΟΤΣΙΚΟΝΑ

«Η πληροφορία υπάρχει.

Δεν χρειάζεται να γίνει αντιληπτή για να υπάρξει.

Δεν χρειάζεται να γίνει κατανοητή για να υπάρξει. Δεν χρειάζεται νοημοσύνη για να ερμηνευτεί.

Δεν χρειάζεται να έχει ένα νόημα για να υπάρξει.

Υπάρχει.

Tom Stonien

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας διπλωματικής εργασίας είναι η εστίαση στα διαδικτυακά εγκλήματα και η προστασία των προσωπικών δεδομένων.

Το 1^{ο} κεφάλαιο ασχολείται με το διαδίκτυο και τα χαρακτηριστικά του

Το 2^{0} κεφάλαιο ασχολείται με την νομοθεσία στην προστασία των προσωπικών δεδομένων στην Ελλάδα

Το 3^{0} κεφάλαιο ασχολείται με τους πιο διαδεδομένους τρόπους των διαδικτυακών εγκλημάτων.

Το 4^{0} κεφάλαιο γίνεται αναφορά στους τρόπους με τους οποίους μπορεί ο κάθε χρήστης να προφυλαχθεί από τις επιθέσεις είτε με την χρήση λογισμικού είτε με διάφορες άλλες σημαντικές συμβουλές για την πλοήγηση στο διαδίκτυο.

ABSTRACT

The purpose of this thesis is the focus of online crimes and the protection of personal data.

The 1st chapter deals with the internet and features.

The 2st chapter deals with the legislation about the protection of individuals data.

The 3st chapter deals with most common ways of online crimes.

The 4st chapter refes to the ways in which each user can guard against attacks either using software or various other important tips for navigating the web.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

Προστασία προσωπικών δεδομένων

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

Βιβλιογραφία

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

1.1 Ιστορική Αναδρομή του Διαδικτύου

Το διαδίκτυο αναπτύχθηκε και εξελίχθηκε με ταχύτατους ρυθμούς μέσα σε λίγα χρόνια κατέχοντας κυρίαρχη θέση στην καθημερινότητα εκατομμυρίων ανθρώπων σε όλο τον κόσμο. Είναι λοιπόν, αξιοσημείωτο να παραταχθεί μια ιστορική αναδρομή του διαδικτύου. Το διαδίκτυο όπως το γνωρίζουμε σήμερα αποτελεί την εξέλιξη ενός πειραματικού δικτύου από τις ΗΠΑ κατά τη διάρκεια του ψυχρού πολέμου, που ονομάζεται Arpanet.

Τα τελευταία χρόνια το διαδίκτυο έχει εξαπλωθεί και έχει εξελιχθεί παρά πολύ και αποτελεί μια τεράστια πηγή δυνατοτήτων και δραστηριοτήτων. Ο καθημερινός χρήστης μέσω διαδικτύου μπορεί να ενημερωθεί για θέματα που τον αφορούν, να πραγματοποιήσει αγορές προϊόντων ή υπηρεσιών επίσης να συναντήσει εικονικά τους οικείους του και να πραγματοποιήσει μια πληθώρα δραστηριοτήτων και ενεργειών που παλαιότερα θα απαιτούνταν κόπος και χρόνος.

Το 1957 κατά τη διάρκεια του «ψυχρού πολέμου» η Σοβιετική ένωση έβαλε σε τροχιά τον πρώτο μη επανδρωμένο δορυφόρο [1]. Στην Αμερική προκλήθηκε ο φόβος πως δεν θα μπορούσαν να προστατευτούν από μια πιθανή πυρηνική επίθεση των Σοβιετικών και έτσι η κυβέρνηση αποφάσισε να δημιουργήσει την υπηρεσία ARPA[2] (Advanced Research Projects Agency)[3] με στόχο η συγκεκριμένη υπηρεσία να δημιουργήσει ένα είδος τεχνολογίας που να είχε την δυνατότητα να χρησιμοποιηθεί για στρατιωτικούς σκοπούς. Έτσι λοιπόν, η συγκεκριμένη υπηρεσία δημιούργησε ένα δίκτυο επικοινωνιών (το ARPAnet)[4] που σε περίπτωση πυρηνικού πολέμου δεν θα κατέρρεε, αλλά θα εξακολουθούσε να λειτουργεί ακόμα κι όταν θα ήταν άχρηστο το μεγαλύτερο μέρος των τηλεπικοινωνιών.

Ο Paul Baran ήταν ένας από τους υπεύθυνους επιστήμονες που του έπρεπε να δώσει λύση στο πρόβλημα του αμερικανικού στρατού φτιάχνοντας το κατάλληλο δίκτυο επικοινωνίας, που θα «άντεχε» σε πυρηνικές επιθέσεις. Έτσι λοιπόν, ο Paul Baran δημιούργησε ένα επικοινωνιακό σύστημα που θα ήταν κατάλληλο όχι μόνο για στρατιωτικούς σκοπούς. Ο ίδιος έλεγε από το 1962 «Είναι πλέον καιρός ν' αρχίσουμε να σκεφτόμαστε μια τεχνολογία η οποία να αφορά μια νέα και πιθανόν ανύπαρκτη μορφή επικοινωνίας».[5] Το σύστημα που έφτιαξε ο Baran

---

[1] Sputnik. Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα. Σελ.59

[2] Η υπηρεσία σήμερα είναι γνωστή και ως DARPA (Defense Advanced Research Projects Agency).

[3] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα. Σελ.59

[4] Η λέξη Arpanet προκύπτει από τα αρχικά της υπηρεσίας του αμερικανικού στρατού

[5] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα, σελ.60. Πολλά άρθρα του Baran εκείνης της εποχής υπάρχουν στο δικτυακό τόπο http://www.rand.org/publications/RM/baran.list.html

ήταν ένα δίκτυο[6] στο οποίο κάθε υπολογιστής θα συνδεόταν με πολλούς άλλους με στόχο να υπάρχουν αρκετοί διαφορετικοί τρόποι επικοινωνίας μεταξύ των δύο σημείων.

Το σύστημα που δημιούργησε ήταν ένα δίκτυο επικοινωνίας υπολογιστών χωρίς κεντρική δομή, κεντρικούς διακόπτες ή κεντρική διεύθυνση. Αυτό σημαίνει ότι έπρεπε να βρει ένα τρόπο που θα πηγαίνουν οι πληροφορίες(δεδομένα) από το ένα υπολογιστή στον άλλον που σε περίπτωση κάποιας «επίθεσης» σε ένα συγκεκριμένο σημείο του συστήματος δεν θα προκαλούσε ολοκληρωτική καταστροφή του συστήματος. Έτσι, η βασική μέθοδος που χρησιμοποίησε για να πετύχει τον παραπάνω στόχο ήταν η μέθοδος «διαμεταγωγής πακέτων» (packet switching)[7].

Αυτό που έκανε η μέθοδος της διαμεταγωγής πακέτων είναι πηγαίνοντας τα δεδομένα από τον ένα υπολογιστή στον άλλο να μπορούν να κόβονται σε πακέτα. Στη συνέχεια τα πακέτα αυτά ακολουθούσαν το καθένα διαφορετική πορεία μέχρι να φτάσουν στη σωστή «διεύθυνση» και όταν έφταναν εκεί έμπαιναν ξανά στη σωστή σειρά. Λόγω λοιπόν, του δεδομένου πως στο συγκεκριμένο σύστημα δεν υπήρχε κεντρικός έλεγχος αλλά ούτε σημεία ελέγχου, μέσα σε αυτό, σε περίπτωση «βλάβης» σε κάποιο σημείο του συστήματος, όλα τα υπόλοιπα σημεία θα είχαν την δυνατότητα να αποκτήσουν ξανά επαφή [8]. Με αυτό τον τρόπο ο Baran έλυσε το πρόβλημα καταστροφής ολόκληρου του συστήματος. Η έρευνά του, για την επίλυση του «σωστού» επικοινωνιακού δικτύου, οδήγησε στην δημιουργία του ARPAnet και ικανοποιούσε σε μεγάλο βαθμό την θεωρία του Licklider.

Ο Licklider οραματιζόταν ένα «Γαλαξιακό Δίκτυο» και προωθούσε την έννοια αυτή από το 1962 [9] Το δίκτυο αυτό του Licklider υποστήριζε ένα παγκόσμιο σύνολο υπολογιστών, όλοι συνδεδεμένοι μεταξύ τους και ο καθένας θα μπορούσε να έχει πρόσβαση σε πληροφορίες και προγράμματα καθώς και την γρήγορη ανταλλαγή αυτών.

Το 1969 το ARPAnet λειτούργησε για πρώτη φορά στο Πανεπιστήμιο της Καλιφόρνια του Λος Άντζελες (UCLA) [10] Αν και το ARPAnet αρχικά σχεδιάστηκε για στρατιωτικούς σκοπούς,

---

[6] Δίκτυο είναι ένα σύνολο υπολογιστών συνδεδεμένων μεταξύ τους ασύρματα ή ασύρματα που δίνει την δυνατότητα να διαμοιράζονται πληροφορίες ταυτόχρονα σε ένα μεγάλο σύνολο ανθρώπων

[7] Ο όρος ανήκει στον Άγγλο φυσικό D. W. Davies, ενώ το πρώτο άρθρο σχετικά με τη θεωρία της διαμεταγωγής πακέτων γράφτηκε από τον Leonard Kleinrock του MIT τον Ιούλιο του 1961 (Leiner et L.,2003). Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα, σελ.60.

[8] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 60

[9] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 61

[10] Παράλληλα, το αντίστοιχο δίκτυο είχε τεθεί σε πειραματική λειτουργία στο Εθνικό Εργαστήριο Φυσικής της Αγγλίας από το 1968 από τον D. W. Davies.

στη συνέχεια πάρθηκε η απόφαση πως η τεχνολογία που είχε το συγκεκριμένο δίκτυο ήταν ικανή να προάγει νέες μορφές επικοινωνίας για ανταλλαγή δεδομένων και ιδεών μεταξύ των πανεπιστημίων. Όσον αναφορά αυτή την άποψη ο Hamman υποστηρίζει ότι είναι λανθασμένη η ευρύτατη διαδεδομένη άποψη ότι το ARPAnet δημιουργήθηκε για να εξυπηρετεί στρατιωτικούς σκοπούς.

Το ARPAnet είχε ως αποστολή να μοιράζονται πληροφορίες μεταξύ τους τα πανεπιστήμια, τα ερευνητικά κέντρα και οι στρατιωτικοί για διάφορες εφαρμογές [11]Στα τέλη του 1969 το ARPAnet είχε καταφέρει και να συνδέσει τέσσερα πανεπιστήμια: το Standford, το πανεπιστήμιο της Καλιφόρνια Santa Barbara, της Γιούτας και της Καλιφόρνια Los Angeles [12].Οι βλέψεις για την δημιουργία ενός πρωτοκόλλου διασύνδεσης των δικτύων [13] που υπήρχαν ήδη εκείνη την εποχή, δεν ήταν αρκετός.

Έτσι, στράφηκαν ναι μεν στη δημιουργία πρωτοκόλλου διασύνδεσης αλλά με μια νέα παράμετρο να έχει δηλαδή το πρωτόκολλο δημιουργίας, την δυνατότητα να συνδέει και τα δίκτυα τα οποία μελλοντικά θα δημιουργούνταν. Το 1973 ο Vincent Cerf και ο Robert [14] είναι οι υπεύθυνοι για την επίτευξη της διασύνδεσης μεταξύ ανόμοιων δικτύων και τον ομοιόμορφο καταμερισμό δεδομένων από το ένα δίκτυο στο άλλο. Αυτό το κατάφεραν δημιουργώντας το TCP/IP(transmission control protocol-πρωτόκολλο ελέγχου μετάδοσης/ internet protocol, όπου η ονομασία του ήταν τα αρχικά των λέξεων). Το TCP/IP βασίζεται στην μέθοδο της διαμεταγωγής πακέτων δηλώνοντας ότι η μεταφορά των δεδομένων (εικόνες, λέξεις, κείμενα) γίνεται τμηματικά μέσω τηλεφωνικών γραμμών και υπολογιστών μέχρι να φτάσουν στο υπολογιστή του κάθε χρήστη [15] Στη συνέχεια τα δεδομένα χωρίζονται σε μικρότερα κομμάτια, έχοντας το κάθε κομμάτι έναν αριθμό και τους δίνεται η διεύθυνση για τον κατάλληλο υπολογιστή. Εκεί ο υπολογιστής τη στιγμή που θα λάβει τα δεδομένα θα κάνει επανασύνθεσή τους.

Τα δεδομένα δεν ακολουθούν ένα συγκεκριμένο δρόμο, ούτε στέλνονται με συγκεκριμένη σειρά. Κανένα από τα δύο παραπάνω δεν αποτελεί όμως πρόβλημα και αυτό γιατί το TCP είναι υπεύθυνο για τον έλεγχο και την σωστή διαχείριση των πακέτων ώστε να οδηγούνται στο προορισμό τους χωρίς λάθη και το IP είναι υπεύθυνο για τη μεταφορά των δεδομένων από το ένα μέρος στο άλλο κατά τα διάρκεια της διαδρομής τους. Έτσι κάθε υπολογιστής που είναι συνδεδεμένος στο Διαδίκτυο λειτουργεί το πρωτόκολλο TCP/IP και έχει μια ξεχωριστή-μοναδική διεύθυνση που τον ξεχωρίζει από όλους τους άλλους υπολογιστές που είναι συνδεδεμένοι. Επίσης έχει την δυνατότητα να στέλνει IP πακέτα σε όλους στο Διαδίκτυο.

---

[11] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα , σελ. 61.

[12] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 62

[13] Μέθοδος μεταφοράς πληροφοριών, σε μορφή πακέτων δεδομένων.

[14] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 63

[15] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ.64

Ανάμεσα στο 1972 και στο 1974 ορίστηκαν τα πρότυπα ορθής λειτουργίας των πρωτοκόλλων του διαδικτύου. Αυτά ήταν το Telnet που χρησιμοποιούνταν για σύνδεση εξ' αποστάσεως, το FTP (File Transfer Protocol) για την μεταφορά αρχείο μέσω Διαδικτύου και το SMTP (Simple Mail Transfer Protocol)[16] για τον καθορισμό πρότυπου λειτουργίας του ηλεκτρονικού ταχυδρομείου [17]..Το τελευταίο αυτό πρόγραμμα σχεδιάστηκε από τον Ray Tomlinson το 1971 [18].

Καθώς το ARPAnet «κέρδιζε» όλο και περισσότερο κόσμο αναπτύχθηκαν και άλλα δίκτυα όπως το CSNET το 1979, αρχικά του Computer Science Research Network (Δίκτυο έρευνας της Επιστήμης των Υπολογιστών), με στόχο την επικοινωνία μεταξύ των ερευνητικών κλάδων[19]. Ένα χρόνο αργότερα, το 1980 αυτά τα δύο δίκτυα συνεργάστηκαν και συνδέθηκαν μεταξύ τους χάρη στο κοινό πρωτόκολλο που χρησιμοποιούσαν το TCP/IP. Αυτό το «πάντρεμα» αποτέλεσε την αρχή του δικτύου των δικτύων το γνωστό σήμερα σε όλους Διαδίκτυο. Βασική αρχή του οποίου είναι η «ανοιχτή αρχιτεκτονική» [20], η δυνατότητα δηλαδή που προσφέρεται ώστε το κάθε δίκτυο να επικοινωνεί με οποιοδήποτε άλλο δίκτυο ανάλογα με τις ανάγκες και τον περιβάλλον του.

Το 1983 το ARPAnet λόγω του φόρτου του δικτύου γιατί πλέον σε αυτό είναι συνδεδεμένο εκατοντάδες πανεπιστήμια αναγκάζεται να χωριστεί σε δύο άλλα τμήματα: στο MILNET για στρατιωτικές επικοινωνίες και στο νέο ARPAnet το οποίο χρησιμοποιούσαν αποκλειστικά οι ακαδημαϊκοί για συνέχιση της έρευνας στη δικτύωση. Η συνεργασία ανάμεσα σε MILNET και ARPAnet κράτησε μέχρι το 1989 όπου το πρώτο διαχωρίστηκε τελείως από το ARPAnet. Πλέον το ARPAnet βρίσκεται κάτω από την επίβλεψη του National Science Foundation- NSF (Εθνικό Ίδρυμα Επιστημών)[21] των ΗΠΑ. Το ίδρυμα αυτό, παρατήρησε ότι το δίκτυο ήταν αργό για να είναι σε θέση να καλύπτει όλες τις επιστημονικές κοινότητες και τις έρευνές τους. Για αυτόν το λόγο το ίδρυμα NSF οδηγήθηκε στην δημιουργία του NSFNET,ένα δίκτυο ικανό να καλύπτει τις ανάγκες πουβδημιουργούνταν. Βαθμιαία, το NSFnet αντικατέστησε

---

[16] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 64.

[17] Το ηλεκτρονικό ταχυδρομείο είναι μια μέθοδος για την ψηφιακή ανταλλαγή (αποστολή και λήψη) μηνυμάτων μέσω διαδικτύου. Βλ. σελ. 79, Χρήστος Γουλτίδης, Ecdl 4 γρήγορα και απλά. Αθήνα 2004, Κλειδάριθμος.

[1818] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 64.

[19] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 64.

[20] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 65

[21] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 64

το ARPAnet ώσπου το τελευταίο σταμάτησε να λειτουργεί στις αρχές του 1990. Με το πέρασμα του χρόνου όλο και περισσότερες χώρες συνδέονται στο NSFNET ανάμεσα σε αυτές και η Ελλάδα το 1990. Το 1995 καταργείται επίσημα το NSFNET, έχοντας ήδη στη διάρκεια του χρόνου παραχωρήσει τμήματα του Διαδικτύου σε ιδιώτες.

Στις μέρες μας το διαδίκτυο δεν βρίσκεται υπό την ουσιαστική διοίκηση ούτε κάποιου προσώπου, ούτε κάποιου οργανισμού. Παρόλα αυτά όμως πρέπει να είναι κάποιος υπεύθυνος, ο οποίος να καθορίζει θέματα όπως την ονοματολογία, τις διευθύνσεις και την αρχιτεκτονική, καθώς επίσης, να διαβεβαιώνεται για την σωστή λειτουργία και την εξέλιξη του διαδικτύου. Ανάμεσα σε αυτούς τους υπεύθυνους είναι η Internet Society, ένας μη κερδοσκοπικός οργανισμός με σκοπό την ανταλλαγή πληροφοριών μέσω Διαδικτύου σε παγκόσμια κλίμακα, ο οποίος λαμβάνει τις τελικές αποφάσεις σε τεχνικά θέματα. Άλλα παραδείγματα τέτοιου είδους υπευθύνων είναι η Internet Activities Board Research-IAB Research, Internet Assigned Board-IAB, W3C. Λόγω της μεγάλης ανάπτυξης του Δικτύου, ήδη από το 1979 η ARPA είχε δημιουργήσει (κάποιον αντίστοιχο υπεύθυνο) την ICCB (Internet Configuration Control Board) για να ελέγχει την ανάπτυξή του.[22]

1.2 Τι είναι το Διαδίκτυο

Το διαδίκτυο, ή αλλιώς Internet στα αγγλικά, είναι το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο. Τι είναι όμως δίκτυο υπολογιστών; Είναι δύο ή περισσότεροι υπολογιστές συνδεδεμένοι μεταξύ τους αποτελούν ένα δίκτυο. Ένα δίκτυο δίνει την δυνατότητα στους χρήστες μεταξύ τους να επικοινωνούν να χρησιμοποιούν από απόσταση τις υπηρεσίες που προσφέρει ο καθένας υπολογιστής του δικτύου. Υπάρχουν τρία είδη ευρέως γνωστά όσον αναφορά των τρόπων που είναι τοποθετημένοι οι υπολογιστές σε ένα δίκτυο. Οι θέσεις αυτές είναι: ο Αστέρας (star) όπου υπάρχει ένας κεντρικός υπολογιστής στον οποίον συνδέονται οι υπόλοιποι υπολογιστές του δικτύου, ο Δακτύλιος (ring) όπου όλοι οι υπολογιστές είναι συνδεδεμένοι σε έναν πλήρη κλειστό δακτύλιο, ο Δίαυλος (bus) που όλοι οι υπολογιστές συνδέονται κατά μήκος ενός κεντρικού αγωγού.

Τα δίκτυα ανάλογα με το εύρος της περιοχής που μπορούν να καλύπτουν χωρίζονται: σε τοπικό δίκτυο (LAN) που έχει περιορισμένη γεωγραφική εμβέλεια, συνδέει δηλαδή υπολογιστές που βρίσκονται στον ίδιο ή γειτονικό κτίριο. Σε δίκτυο ευρείας περιοχής- WAN το οποίο συνδέει υπολογιστές που απέχουν μεταξύ τους μεγάλες αποστάσεις και βρίσκονται σε διαφορετικές πόλεις ή χώρες[23].

[22] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 65

[23] Γουλτίδης Χρήστος, ECDL4, Αθήνα 2004. Κλειδάριθμος σελ. 72

Το διαδίκτυο αποτελεί το μεγαλύτερο δίκτυο ευρείας περιοχής. Έτσι λοιπόν, έχουμε και εδώ υπολογιστές που είναι συνδεδεμένοι μεταξύ τους με τηλεφωνικές και άλλες γραμμές. Η μεταφορά δεδομένων στο Διαδίκτυο επιτρέπουν στους χρήστες να διαμοιράζονται μηνύματα και πληροφορίες που βασίζονται στην κοινή χρήση πρωτοκόλλου μεταφοράς δεδομένων του TCP/IP. Το Διαδίκτυο αποτελεί ουσιαστικά έναν τρόπο επικοινωνίας μεταξύ των χρηστών σε όλο τον πλανήτη που το χρησιμοποιούν, προσφέροντας απλόχερα τις υπηρεσίες του ανεξαρτήτως χώρου και χρόνου. Το Διαδίκτυο αποτελείται από το υλικό-hardware (υπολογιστές, καλώδια κ.α.), λογισμικό- software (εφαρμογές και προγράμματα) και μπορεί να λειτουργήσει ορθά όταν αλλάζει ένα μέσο δικτύωσης.

Επιπλέον, το Διαδίκτυο προσφέρει υπηρεσίες επικοινωνίας όπου οι άνθρωποι μπορούν να χρησιμοποιήσουν για να έρθουν σε επαφή με τους φίλους και την οικογένεια που μπορεί να ζουν σε μια διαφορετική χώρα. Τέτοιες υπηρεσίες επικοινωνίας περιλαμβάνουν MSN ,Skype και το Yahoo. Το chat room είναι ένας άλλος τρόπος για επικοινωνία μέσω της οποίας οι άνθρωποι έχουν την πιθανότητα να επικοινωνήσουν με άλλους ανθρώπους που δεν έχουν συναντήσει ποτέ πριν ή που ζουν στις διαφορετικές χώρες. Τα ηλεκτρονικά ταχυδρομεία (e-mails) είναι μια άλλη μορφή για επικοινωνία με την οικογένεια και τους φίλους και έχουν αντικαταστήσει τώρα τις παραδοσιακές χειρόγραφες επιστολές. Οι κοινωνικές περιοχές δικτύωσης (Social networking sites) είναι ιστοχώροι που προσφέρουν στους ανθρώπους την πιθανότητα να δημιουργήσουν ένα βιογραφικό τους, που να περιγράφει τις συμπάθειες και τις αντιπάθειες και τις προσδοκίες ενός προσώπου από άλλους ανθρώπους. Ο σκοπός αυτών των σελίδων είναι να επιτρέπουν στα μέλη τους να συναντήσουν άλλα μέλη για δημιουργία σχέσεων , φιλίες ή απλά τις απλές γνωριμίες. Τέλος, το Διαδίκτυο μπορεί να προσφέρει υπηρεσίες για κατέβασμα στον υπολογιστή.

1.3 Αρχιτεκτονική του Διαδικτύου

Η Αρχιτεκτονική ως θεωρητική γνώση και διαχρονική εμπειρία γίνεται εφαρμοσμένη επιστήμη. Με την εξέλιξη της βιομηχανικής επανάστασης σε τεχνολογική, πρώτα η πληροφορική και στη συνέχεια το διαδίκτυο αποτελούν βασικά εργαλεία εξυπηρέτησης των αναγκών αυτής της επιστήμης και κατ' επέκταση της ίδιας της κοινωνίας.

Το Διαδίκτυο (Internet) είναι μια (τεράστια) συλλογή συνεργαζόμενων δικτύων υπολογιστών. Το Διαδίκτυο σχεδιάστηκε και αναπτύχθηκε έτσι ώστε να εξασφαλίζει την αξιόπιστη επικοινωνία μεταξύ των ανομοιογενών συστημάτων που το απαρτίζουν.

Το Διαδίκτυο είναι απόγονος του ARPANET, ενός πειραματικού δικτύου μεταγωγής πακέτων, που χρηματοδότησε το Υπουργείο Άμυνας των ΗΠΑ το 1969. Στόχος τους ήταν η δημιουργία ενός δικτύου το οποίο θα μπορούσε αξιόπιστα να μεταφέρει πληροφορία από ένα άκρο του σε ένα άλλο άκρο ακόμα και όταν μερικοί κόμβοι του θέτονταν εκτός λειτουργίας. Στην αρχική του υλοποίηση, το ARPANET συνέδεε τέσσερα απομακρυσμένα συστήματα.

Το ARPANET εξαπλώθηκε με γοργούς ρυθμούς, συμπεριέλαβε πλήθος κόμβων από την ακαδημαϊκή και ερευνητική κοινότητα, αλλά σύντομα αντιμετώπισε το πρόβλημα της ανομοιογένειας των συνδεδεμένων συστημάτων. Το 1982 υιοθέτησε ένα σύνολο κανόνων επικοινωνίας, που έγιναν γνωστοί ως η ομάδα πρωτοκόλλων TCP/IP, διασυνδέοντας έτσι μια μεγάλη ποικιλία συστημάτων και εφαρμογών.

Το 1985 δημιουργήθηκε το NSFNET, το οποίο διέθετε ένα πολύ γρήγορο (για την εποχή του) δίκτυο κορμού και εξυπηρετούσε την ακαδημαϊκή και ερευνητική κοινότητα των ΗΠΑ. Πολύ σύντομα πλήθος πανεπιστημίων, ερευνητικών κέντρων και οργανισμών από όλο τον κόσμο συνδέθηκαν στο NSFNET, σχηματίζοντας έτσι ένα παγκόσμιο διαδίκτυο.

Η αρχιτεκτονική των δικτύων TCP/IP: Οι λειτουργίες των δικτύων TCP/IP οργανώνονται σε τέσσερα επίπεδα. Ονομάζοντάς τα από το χαμηλότερο επίπεδο προς το υψηλότερο, αυτά είναι τα επίπεδα Πρόσβασης Δικτύου, Δικτύου, Μεταφοράς και Εφαρμογής.

Η αρχιτεκτονική του Διαδικτύου, ή αλλιώς η αρχιτεκτονική των δικτύων TCP/IP, απεικονίζεται στο Σχήμα, όπου παρατηρούμε ότι τα πρωτόκολλα επικοινωνίας οργανώνονται σε τέσσερα επίπεδα.

- ***Επίπεδο Πρόσβασης Δικτύου***

Στο χαμηλότερο επίπεδο αυτής της αρχιτεκτονικής, το οποίο καλούμε Επίπεδο Πρόσβασης Δικτύου βρίσκονται εκείνα τα πρωτόκολλα επικοινωνίας που έχουν ως κύρια λειτουργία την μετάδοση πακέτων μεταξύ συγκεκριμένων κόμβων του δικτύου.

Οι κόμβοι επικοινωνούν μεταξύ τους είτε με σύνδεσμο σημείου με σημείο είτε μέσω κάποιου συνδέσμου πολλαπλής πρόσβασης. Μια μεγάλη ποικιλία πρωτοκόλλων έχουν αναπτυχθεί και χρησιμοποιούνται ευρέως για τη μετάδοση πακέτων πάνω από τους συνδέσμους(π.χ., Ethernet, Token Ring, FDDI, PPP κ.ά.). Συνήθως αυτά τα πρωτόκολλα υλοποιούνται με τη συνεργατική λειτουργία ενός τμήματος υλικού (π.χ. ο προσαρμογέας δικτύου) και ενός τμήματος λογισμικού (π.χ. ο αντίστοιχος «οδηγός» του προσαρμογέα δικτύου).

Σύμφωνα με τα παραπάνω, μπορούμε, σε γενικές γραμμές, να αντιστοιχίσουμε το Επίπεδο Πρόσβασης Δικτύου με τα δύο χαμηλότερα επίπεδα του μοντέλου αναφοράς OSI (Φυσικό και Επίπεδο Σύνδεσης Δεδομένων).

- ***Επίπεδο Δικτύου***

Στο Επίπεδο Δικτύου αυτής της αρχιτεκτονικής βρίσκεται μόνο το πρωτόκολλο IP (Internet Protocol), το οποίο ελέγχει τη διευθυνσιοδότηση των κόμβων του δικτύου και τη δρομολόγηση των πακέτων. Το IP, ωστόσο, δεν μπορεί να εγγυηθεί ότι θα παραδώσει όλα τα πακέτα δεδομένων στον προορισμό τους ή ότι θα τα παραδώσει με τη σωστή σειρά.

Με το πρωτόκολλο IP κατέστη δυνατή η διασύνδεση πολλών διαφορετικών δικτυακών τεχνολογιών και η ενοποίησή τους σε ένα λογικό διαδίκτυο. Για παράδειγμα, στο Διαδίκτυο μπορεί να συνδεθεί κάποιος είτε από το σπίτι του, μέσω του παραδοσιακού τηλεφωνικού δικτύου (PSTN) ή του δικτύου ISDN, είτε μέσω του τοπικού δικτύου του γραφείου του και της αντίστοιχης μόνιμης ζεύξης είτε από την παραλία, το βουνό, ή καθ'οδόν με τη χρήση ασύρματων συστημάτων τηλεπικοινωνιών (π.χ., το δίκτυο κινητής τηλεφωνίας). Όλοι αυτοί οι χρήστες, παρ' όλο που χρησιμοποιούν διαφορετικές τεχνολογίες πρόσβασης, έχουν ως κοινό χαρακτηριστικό τη χρήση του πρωτοκόλλου IP.

- ***Επίπεδο Μεταφοράς***

Στο Επίπεδο Μεταφοράς αυτής της αρχιτεκτονικής βρίσκονται τα πρωτόκολλα TCP (Transmission Control Protocol – πρωτόκολλο ελέγχου μετάδοσης) και UDP (User Datagram Protocol – πρωτόκολλο αυτοδύναμων πακέτων χρήστη), τα οποία ελέγχουν την ανταλλαγή των πακέτων μεταξύ των τερματικών κόμβων, ρυθμίζοντας έτσι την από άκρο σε άκρο επικοινωνία.

Το πρωτόκολλο UDP παραδίδει ένα πακέτο στον προορισμό του, διενεργώντας μόνο έναν απλό έλεγχο για να διαπιστωθεί αν το πακέτο έχει υποστεί αλλοίωση κατά τη μεταφορά του μέσω του δικτύου. Αν έχει φθαρεί, τότε απορρίπτεται, αλλιώς προωθείται για περαιτέρω επεξεργασία.

Αντίθετα, το πρωτόκολλο TCP διενεργεί πιο σύνθετους ελέγχους σφαλμάτων. Συγκεκριμένα, εάν ένα πακέτο διαπιστωθεί ότι έχει φθαρεί, τότε ζητείται από τον αποστολέα κόμβο η επανεκπομπή του πακέτου. Επιπλέον, το πρωτόκολλο TCP διενεργεί και έλεγχο ροής των πακέτων, φροντίζοντας να μειώσει το ρυθμό μεταφοράς τους σε καταστάσεις συμφόρησης του δικτύου και μέχρις ότου αυτές εξομαλυνθούν.

Από τα παραπάνω παρατηρούμε ότι στα δίκτυα TCP/IP οι σημαντικές λειτουργίες ελέγχου σφαλμάτων και ελέγχου ροής διενεργούνται στους τερματικούς κόμβους του δικτύου, απαλλάσσοντας έτσι τους ενδιάμεσους κόμβους από πολύπλοκες και δαπανηρές λειτουργίες. Αυτό είναι συμβατό με μια βασική σχεδιαστική αρχή στα δίκτυα υπολογιστών, σύμφωνα με την οποία «δεν πρέπει να ζητάμε από το δίκτυο να κάνει κάτι που μπορούμε να το κάνουμε μόνοι μας».

- ***Επίπεδο Μεταφοράς***

Πάνω από το Επίπεδο Μεταφοράς βρίσκεται μια μεγάλη ποικιλία πρωτοκόλλων εφαρμογής, όπως τα FTP (File Transfer Protocol – πρωτόκολλο μεταφοράς αρχείου), TFTP (Trivial File Transfer Protocol – τετριμμένο πρωτόκολλο μεταφοράς αρχείου), SMTP (Simple Mail Transfer Protocol – απλό πρωτόκολλο μεταφοράς ταχυδρομείου), HTTP (HyperText Transfer Protocol – πρωτόκολλο μεταφοράς υπερκειμένου), TELNET (πρωτόκολλο πρόσβασης σε απομακρυσμένο υπολογιστή), RTP (Real – time Transfer Protocol – πρωτόκολλο μεταφοράς πραγματικού χρόνου), SNMP (Simple Network Management Protocol – απλό πρωτόκολλο διαχείρισης δικτύου), DNS (Domain Name System – σύστημα ονομασίας περιοχών), NFS (Network File System – δικτυακό σύστημα αρχείων), κ.ά.

Η κύρια λειτουργία αυτών των πρωτοκόλλων εφαρμογής είναι η εξασφάλιση της διαλειτουργικότητας των αντίστοιχων εφαρμογών. Για να μπορέσουμε να κατανοήσουμε τη διαφορά μεταξύ του πρωτοκόλλου εφαρμογής και της εφαρμογής, ας θεωρήσουμε τα εργαλεία λογισμικού που χρησιμοποιούνται για ανάγνωση ιστοσελίδων που υπάρχουν διαθέσιμα στο εμπόριο (π.χ., το Netscape Communicator, το MS –Internet Explorer, το Mosaic κ.ά.). Όλες αυτές οι εφαρμογές συμμορφώνονται στους
κανόνες του πρωτοκόλλου εφαρμογής HTTP. Συνέπεια αυτού είναι το γεγονός ότι μπορούμε να χρησιμοποιήσουμε όλα ανεξαιρέτως τα προγράμματα περιήγησης για να προσπελάσουμε τις ιστοσελίδες κάποιου ηλεκτρονικού τόπου στο Διαδίκτυο.

Τα περισσότερα πρωτόκολλα εφαρμογής χρησιμοποιούν τις υπηρεσίες του TCP για την επικοινωνία τους με τα ομότιμα πρωτόκολλα (π.χ., FTP, SMTP, HTTP, TELNET,RTP). Αρκετά πρωτόκολλα εφαρμογής χρησιμοποιούν το UDP (π.χ., TFTP, SNMP, NFS), ενώ υπάρχουν και μερικά πρωτόκολλα που χρησιμοποιούν και το TCP και το UDP (π.χ., DNS).

Τέλος, σε γενικές γραμμές, θα μπορούσαμε να αντιστοιχίσουμε το Επίπεδο Εφαρμογής στη αρχιτεκτονική των δικτύων TCP/IP με τα τρία υψηλότερα επίπεδα του μοντέλου αναφοράς OSI (Συνόδου, Παρουσίασης και Εφαρμογής).[24]

1.4 Οι υπηρεσίες του Διαδικτύου

Το Διαδίκτυο παρομοιάζεται με **υπερλεωφόρο των πληροφοριών (super-highway)**.Καθημερινά διακινούνται πλήθος δεδομένων , με οποιαδήποτε μορφή , φέρνοντάς μας κοντά σε ένα τεράστιο αριθμό πηγών πληροφόρησης. Κείμενα , εικόνες, ήχοι, μουσικές και βίντεο συνυπάρχουν σε μια εκπληκτικά μεγάλη συλλογή από ψηφιακά έγγραφα. Τα ψηφιακά αυτά έγγραφα ονομάζονται ιστοσελίδες και βρίσκονται αποθηκευμένα σε διάφορους υπολογιστές ανά τον κόσμο. Όλες οι ιστοσελίδες μαζί συγκροτούν μια από τις πιο σημαντικές υπηρεσίες του Διαδικτύου : τον **Παγκόσμιο Ιστό(World Wide Web-WWW)**[25].

[24] https://sites.google.com/site/eisagogestadiktyaypologiston1/architektonike-diktyou/architektonike-diadiktyou

[25] http://hermes.di.uoa.gr/exe_activities/diadiktio/12____.html

Ένας υπολογιστής του Διαδικτύου δεν είναι μόνο μια υπολογιστική μηχανή, αλλά και ένα μέσο που μας δίνει την δυνατότητα να επικοινωνούμε με την παγκόσμια κοινότητα. Το **Ηλεκτρονικό Ταχυδρομείο (e-mail)**, η **Συνομιλία (chat)**,η **Τηλεδιάσκεψη (Teleconference)**, και οι **Ομάδες Συζητήσεων (Newsgroups)** είναι μερικές από τις βασικότερες υπηρεσίες που μας παρέχει το Διαδίκτυο, ώστε να επικοινωνούμε με ανθρώπους από διάφορα μέρη του πλανήτη.

Ηλεκτρονικό Ταχυδρομείο: Είναι μια Υπηρεσία του Διαδικτύου, η οποία επιτρέπει τη συγγραφή, αποστολή, λήψη και αποθήκευση μηνυμάτων με χρήση ηλεκτρονικών συστημάτων τηλεπικοινωνιών. Γενικά ο όρος "ηλεκτρονικό ταχυδρομείο" αναφέρεται στο σύστημα ηλεκτρονικού ταχυδρομείου του Διαδικτύου που χρησιμοποιεί το Simple Mail Transfer Protocol πρωτόκολλο, σε δικτυακά συστήματα που βασίζονται σε άλλα πρωτόκολλα μεταφοράς μηνυμάτων, αλλά και σε διάφορα συστήματα μηνυμάτων σε μικρά δίκτυα, υπερυπολογιστές, κλπ που επιτρέπου στους χρήστες τους να στέλνουν μηνύματα μεταξύ τους για την υποστήριξη ομαδικής συνεργασίας.

Τα συστήματα σε τοπικά δίκτυα ή σε δίκτυα intranet είναι πιθανόν να βασίζονται σε ιδιωτικά πρωτόκολλα, που υποστηρίζονται από το συγκεκριμένο σύστημα, ή να είναι τα ίδια πρωτόκολλα που χρησιμοποιούνται στα δημόσια δίκτυα. Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται συχνά για τη μεταφορά ανεπιθύμητων μηνυμάτων σε μεγάλο όγκο (spam)), αλλά υπάρχουν προγράμματα που μπορούν να "φιλτράρουν" και να σταματήσουν ή να σβήσουν αυτόματα τα περισσότερα από αυτά. Το ηλεκτρονικό Ταχυδρομείο είναι πιο γρήγορο και με μηδαμινό κόστος σε σύγκριση με το παραδοσιακό ,για αυτό σε πολλές χώρες χρησιμοποιείται περισσότερο.

Συνομιλία: Η υπηρεσία αυτή ξεπερνά το εμπόδιο της απόστασης και μας φέρνει σε επαφή γρήγορα και άμεσα με φίλους μας σε όποιο μέρος του πλανήτη και αν βρίσκονται χωρίς να μετακινηθούμε. Αρκεί να συνδέσουμε τον υπολογιστή μας σε υπολογιστή Διαδικτύου που μας παρέχει αυτή την υπηρεσία.

Τηλεδιάσκεψη: Η υπηρεσία αυτή μοιάζει με τηλεφωνική συνομιλία με ταυτόχρονη μετάδοση της εικόνας μας. Αρκεί να είμαστε συνδεδεμένοι στο Διαδίκτυο και να διαθέτουμε το κατάλληλο λογισμικό, κάμερα, ηχεία και μικρόφωνο.

Ομάδα Συζήτησης: Κάνουμε εγγραφή σε μία ομάδα συζητήσεων και μας αποστέλλονται ηλετρονικά μηνύματα για το θέμα που μας ενδιαφέρει και στέλνουμε και εμείς την αποψή μας.

Πρωτόκολλο Μεταφοράς Αρχείων- File Transfer Protocol ,FTP: Η υπηρεσία για ανταλλαγή προγραμμάτων και δεδομένων μεταξύ υπολογιστών. Συνδεόμαστε με έναν υπολογιστή του Διαδικτύου που προσφέρει έναν κατάλογο από προγράμματα , παιχνίδια, ταινίες DVD, τραγούδια (σε μορφή MP3,Midi,..) επιλέγουμε αυτό που μας ενδιαφέρει και το μεταφέρουμε (download-κατεβάζουμε) στον υπολογιστή μας. Η δυνατότητα αυτή αλλάζει σιγά σιγά τον παραδοσιακό τρόπο με τον οποίο προμηθευόμαστε τραγούδια ή προγράμματα. Δεν είναι αναγκαίο να τα αναζητήσουμε σε κάποιο κατάστημα διότι οι ίδιοι οι δημιουργοί μας τα διαθέτουν μέσω Διαδικτύου.

Είναι από τις τελευταίες και πιο γρήγορα αναπτυσσόμενες υπηρεσίες του Διαδικτύου. Το *World Wide Web (WWW)* επιτρέπει την πρόσβαση και την ανάκτηση κάθε είδους πληροφορίας, μέσα από ένα σύνθετο περιβάλλον γραφικών, κειμένου και φωτογραφιών. Το WWW αποτελείται από υπολογιστές που διανείμουν την πληροφορία, τους servers και από υπολογιστές που αναζητούν πληροφορίες εκ μέρους των χρηστών, τους clients. Οι πρώτοι τρέχουν ειδικά προγράμματα που καλούνται *Web servers*, ενώ οι δεύτεροι τρέχουν τους *Web browsers*, client προγράμματα που διατίθενται δωρεάν από πολλές εταιρίες.

Η πληροφορία αποθηκεύεται στους Web servers (συνήθως ένας αφιερωμένος υπολογιστής ταυτίζεται με το λογισμικό που τρέχει) υπό μορφή ηλεκτρονικών σελίδων. Η γλώσσα που χρησιμοποιείται για την σύνταξη των σελίδων αυτών είναι η *HTML (Hyper Text Mail Language)*. Τα περιεχόμενα της μπορεί να είναι δεδομένα κειμένου, γραφικά, εικόνες, σύνδεσμοι και τώρα τελευταία με την ανάπτυξη της Java, αλληλεπιδραστικές διεργασίες *(interactive sessions)*. Επίσης, με την χρήση του πρωτοκόλλου MIME που αναφέραμε παραπάνω, μπορεί να προστεθεί στις σελίδες κινούμενη εικόνα, ήχος και κινούμενα γραφικά.

Η θέση μιας σελίδας στο Διαδίκτυο καθώς και το πρωτόκολλο που χρειάζεται για να την ανοίξει κάποιος προσδιορίζεται από το λεγόμενο *URL (Uniform Resource Locator)*. Το URL προσδιορίζει επιπλέον το όνομα του αρχείου και του καταλόγου στον Web server. Τα πρωτόκολλα που χρησιμοποιούνται για το άνοιγμα των ηλεκτρονικών σελίδων και γενικότερα για την επικοινωνία μεταξύ του Web server και του Web browser, είναι κυρίως το *HTTP (Hyper Text Transfer Protocol)*. 'Αλλά πρωτόκολλα που μπορούν να χρησιμοποιηθούν είναι το *FTP* και το *GOPHER*.

1.5 Παροχή υπηρεσιών μέσω Internet

Α) Ελευθερία κυκλοφορίας υπηρεσιών

Τα άρθρα 59 και 60 της Συνθήκης της Ευρωπαϊκής Ένωσης εγγυώνται την ελεύθερη κυκλοφορία υπηρεσιών στην επικράτεια της Ευρωπαϊκής Ένωσης. Κάθε παροχέας υπηρεσιών μπορεί ανεμπόδιστα να προσφέρει τις υπηρεσίες του σε οποιοδήποτε κράτος-μέλος της Ένωσης .Το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων, ήδη από το 1992, έκρινε ότι η εξάρτηση από ειδική άδεια της μεταφοράς τηλεοπτικών προγραμμάτων από ένα δίκτυο καλωδιακής τηλεόρασης σε άλλο που βρίσκεται σε άλλο κράτος-μέλος αντίκειται στο άρθρο 59 της Συνθήκης. Αυτό ισχύει ακόμα περισσότερο ως προς την διασυνοριακή μεταφορά δεδομένων μέσω του internet[26] .Στην ίδια κατεύθυνση κινείται και η Οδηγία 90/388/ΕΚ΄ για την απελευθέρωση των τηλεπικοινωνιακών υπηρεσιών που ορίζει , ότι αν χρειάζεται άδεια για την παροχή υπηρεσιών αυτού του είδους, θα πρέπει να δίνεται χωρίς διακρίσεις. Εξαιρέσεις μπορούν να προβλέπονται για λόγους δημόσιας τάξεως, ασφαλείας και υγείας. Για παράδειγμα είναι δυνατόν να προβλέπονται νομοθετικοί περιορισμοί στην πρόσβαση προσώπων που οργανώνουν μέσω του internet τυχερά παίγνια ή διακινούν πορνογραφικό υλικό ή διεγείρουν το ρατσιστικό μίσος κ.π.λ. Περιορισμοί μπορούν επίσης να προβλέπονται για την προστασία των καταναλωτών και την προστασία της πνευματικής ιδιοκτησίας, πάντα όμως υπό όρους της αρχής της αναλογικότητας και σύμφωνα με το άρθρο 10 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου.[27]

Β) Προστασία των καταναλωτών-χρηστών του Internet

Το Internet, ένα δίκτυο στο οποίο εκατομμύρια άνθρωποι απ ’όλον τον κόσμο έχουν πρόσβαση, αποτελεί έναν νέο χώρο εμπορικών συναλλαγών , όπου οι εταιρείες μπορούν να διεξάγουν ηλεκτρονικό εμπόριο με χαμηλό διαφημιστικό κόστος. Μέσω του Internet και στο πλαίσιο της συμβατικής ελευθερίας είναι δυνατή η πώληση προϊόντων και η παροχή υπηρεσιών. Η απουσία όμως αποδεικτικών εγγράφων θέτει σε δοκιμασία την εμπιστοσύνη του καταναλωτικού κοινού και γενικότερα την ασφάλεια των συναλλαγών. Το ηλεκτρονικό ταχυδρομείο (E-mail), ο «παγκόσμιος ιστός» (World Wide Web) αλλά και άλλοι τρόποι επικοινωνίας διευκολύνουν τη σύναψη συμβάσεων σε μεγάλο βαθμό. Ο χρήστης των υπηρεσιών που παρέχονται μέσω του Internet ενδέχεται να είναι και καταναλωτής. Συνεπώς, μπορεί να εφαρμοστεί και το δίκαιο προστασίας των καταναλωτών. Η Οδηγία 93/13/ΕΟΚ «για

[26] Βλέπε και την απόφαση του ΔΕΚ,16 Δεκεμβρίου 1992, επιτροπή κατά του Βελγίου, 211/91

[27] Βλέπε ΔΕΚ ,18 Ιουνίου 1991, ΕΡΤ Α.Ε κατά Δημοτικής Εταιρείας Πληροφόρησης 260/89, 1991, 2951.

τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές», η Οδηγία 85/374/ΕΟΚ «για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών-μελών σε θέματα ευθύνης λόγω ελαττωματικών προϊόντων» , η Οδηγία 85/577/ΕΟΚ «για την προστασία των καταναλωτών κατά την σύναψη συμβάσεων εκτός εμπορικού καταστήματος», η Οδηγία 84/450/ΕΟΚ «για την παραπλανητική διαφήμιση», οι οποίες ενσωματώθηκαν στο ελληνικό δίκαιο με το ν. 2251/1994[28], παρέχουν ένα ευρύτατο προστατευτικό πλαίσιο για τους καταναλωτές που συνάπτουν ένα ευρύτατο προστατευτικό πλαίσιο για τους καταναλωτές που συνάπτουν συμβάσεις μέσω του δικτύου του Internet.

Το άρθρο 4 παρ.6 του ν.2251/1994 απαγορεύει την χρησιμοποίηση ηλεκτρονικών μέσων επικοινωνίας για την υποβολή προτάσεως σύναψης σύμβασης χωρίς την συναίνεση του καταναλωτή.. Η συναίνεση είναι απαραίτητη και για την μετάδοση διαφημιστικού μηνύμστος απευθείας στον καταναλώτη μέσω του ηλεκτρονικού ταχυδρομείου ή άλλου τρόπου επικοινωνίας μέσω του Internet σύμφωνα με το άρθρο 9 παρ. 10. Ιδιαίτερη σημασία έχει επίσης το άρθρο 8 του ν.2251/1994 για την ευθύνη του παρέχοντος υπηρεσίες το οποίο εφαρμόζεται αφενός στην σχέση χρήστη και παροχέα πρόσβασης στο Internet και αφετέρου στην σχέση μεταξύ χρηστών του Internet. Το άρθρο 9 απαγορεύει την αθέμιτη και παραπλανητική διαφήμιση μέσω του δικτύου. Το ισχύον θεσμικό πλαίσιο όμως δεν ρυθμίζει θέματα σχετικά με την διαφήμιση προϊόντων καπνού, φαρμάκων και αλκοολούχων ποτών στο internet[29] .

Η απαγόρευση ή οι περιορισμοί στην διαφήμιση των προϊόντων αυτών ισχύουν μόνο για τις ραδιοτηλεοπτικές μεταδόσεις.

1.6 Ηλεκτρονικό εμπόριο

Η ραγδαία ανάπτυξη της τεχνολογίας έχει αναμφισβήτητα επιφέρει σημαντικές αλλαγές στις παραδοσιακές οικονομικές δραστηριότητες . Η παγκόσμια οικονομία μετακινείται από μια κατεξοχήν μεταβιομηχανική οικονομία των υπηρεσιών σε μια ψηφιακή οικονομία , που ανήκει στην κοινωνία της πληροφορίας, όπου πρωταγωνιστικό ρόλο διαδραματίζει το ηλεκτρονικό εμπόριο[30]. Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο, η άσκηση του οποίου πραγματοποιείται με ηλεκτρονικά μέσα και αφορά στην δυνατότητα σύναψης εμπορικών συναλλαγών μέσω τηλεπικοινωνιακών δικτύων και ιδίως μέσω του διαδικτύου[31].

[29] Βλέπε την οδηγία 89/522/ΕΟΚ «για τον συντονισμό ορισμένων νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών –μελών σχετικά με την άσκηση τηλεοπτικών δραστηριοτήτων «, η οποία ενσωματώθηκε στον ελληνικό δίκαιο με το ΠΔ 236/1992 και το νόμο 2328/1995 καθώς και τον Κανονισμό 3/1991 του Εθνικού Συμβουλίου Ραδιοτηλεόρασης (ΦΕΚ Β 538) για την «Δεοντολογία των ραδιοτηλεοπτικών διαφημίσεων». Βλέπε ακόμα και την Οδηγία 92/28/ΕΟΚ του Συμβουλίου της 31 Μαρτίου «για την διαφήμιση των φαρμάκων που προορίζονται για ανθρώπους» που ενσωματώθηκε στο ελληνικό δίκαιο με την ΥΑ Υ6α/776/1993(ΦΕΚ Β,536/20.7.1993)

[30] Το κείμενο απετέλεσε εισήγηση της κ.Αριστέας Σινανιώτη –Μαρούδη στο 1_0 Επιστημονικό Συνέδριο του Πανεπιστημίου Πελοποννήσου σε συνεργασία με την Ελληνική Εταιρεία Επιχειρησιακών Ερευνών, Τρίπολη 31.10.2002.

[31] «Ηλεκτρονικό Επιχειρείν» (e-businness) είναι η κάθε είδους επιχειρηματική δραστηριότητα που μπορεί να ολοκληρωθεί ηλεκτρονικά, μέσω εναλλακτικών ηλεκτρονικών καναλιών επικοινωνίας και ανταλλαγής πληροφοριών.

Το ηλεκτρονικό εμπόριο περικλείει ολόκληρο το φάσμα των οικονομικών δραστηριοτήτων που λαμβάνουν χώρα μεταξύ των επιχειρήσεων (Β 2 B:Businness to Businness) ή μεταξύ επιχειρήσεων και καταναλωτών (Β 2 C:Business to Consumer). Χωρίς αμφιβολία στην έννοια του ηλεκτρονικού εμπορίου περιλαμβάνονται ποικίλες δραστηριότητες , όπως η ηλεκτρονική μεταφορά κεφαλαίου, οι ηλεκτρονικές φορτωτικές , η διαφήμιση και προώθηση προϊόντων , καθώς και άλλες οικονομικές δραστηριότητες . Τέλος, το ηλεκτρονικό εμπόριο μπορεί να αφορά τόσο σε προϊόντα όσο και σε υπηρεσίες.

Άμεση συνέπεια των ανωτέρω εξελίξεων και της τεχνολογικής προόδου είναι ότι καθίσταται δυνατή η κατάρτιση των συμβάσεων της καθημερινής ζωής από απόσταση με αυτοματοποιημένο τρόπο, στο πλαίσιο της χρήσεως των ηλεκτρονικών υπολογιστών [32] και του διαδικτύου, με αποτέλεσμα να κρίνεται ανεπαρκές το παραδοσιακό εμπόριο. Αντίθετα, το ηλεκτρονικό εμπόριο φαίνεται ιδανικότερο να ανταποκριθεί στις σύγχρονες ανάγκες για συνεχή ανανέωση, ταχύτατους ρυθμούς και δυνατότητα διαρκούς προσαρμογής στις καθημερινές απαιτήσεις των ηλεκτρονικών συναλλαγών .

Λαμβάνοντας υπόψη τα ανωτέρω, γίνεται αντιληπτή η ιδιαίτερη σημασία του διαδικτύου για την άσκηση του ηλεκτρονικού εμπορίου. Για τον λόγο αυτό και η ελληνική νομοθεσία δεν μπορούσε να μην παρακολουθήσει τις νέες εξελίξεις. Ο Κώδικας Βιβλίων και Στοιχείων προσαρμόστηκε με το πδ 186/1992 (τροποποιημένο από το πδ 134/1996) και έλαβε υπόψη τα νέα δεδομένα , τα οποία καθιστούν απαραίτητη την χρήση των Η/Υ από εμπόρους για τις ηλεκτρονικές εμπορικές συναλλαγές τους. Διατάξεις αφορώσες στην σύνοψη ηλεκτρονικών εμπορικών συναλλαγών υπάρχουν σε διάφορους νόμους, στο ρυθμιστικό πεδίο των οποίων εμπίπτουν τομείς της οικονομικής ζωής. Παραδείγματα με τα άρθρα 26 παρ. 2 και 27 παρ. 4 του ν.2533/1997 , τα οποία εξισώνουν την ηλεκτρονική επικοινωνία της εταιρείας εκκαθάρισης συναλλαγών επί παραγώγων με την έγγραφη[33]. Παρόλη όμως την προσπάθεια που γίνεται σήμερα για την θέσπιση νομοθεσίας ικανής για την προστασία και ανάπτυξη του ηλεκτρονικού εμπορίου , εξακολουθούν να υφίστανται προβλήματα, τα οποία κατά κύριο λόγο πηγάζουν από τον χαρακτήρα του ίδιου του διαδικτύου ως παγκόσμιας αγοράς.

Στην προσπάθεια αυτή εισαγωγής αρχών για την διενέργεια του ηλεκτρονικού εμπορίου η Ευρωπαϊκή Ένωση εξέδωσε την Οδηγία 2000/31/ΕΚ « για ορισμένες πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά»

[32] Βλ.Αλεξανδρίδου, Το δίκαιο του ηλεκτρονικού , ελληνικό και κοινοτικό, 2004, παντού, Πιτσιρίκο, Σύγχρονα μέσα επικοινωνίας (τηλεομοιότυπο, τηλετύπημα, ηλεκτρονικό έγγραφο) για την κατάρτιση τυπικών δικαιοπραξιών ως ζήτημα της σχέσως εγγράφου τύπου και δικαιοπραξίας, 2002, σελ.1 επ.

[33] Βλ. Καράκωστα ,Δίκαιο και Internet ,Νομικά ζητήματα του Διαδικτύου , β έκδοση ,2003 , σελ 167

Το ηλεκτρονικό εμπόριο διακρίνεται κυρίως σε δύο κατηγορίες [34].

- *Βασικές κατηγορίες ηλεκτρονικού εμπορίου*.

Το ηλεκτρονικό εμπόριο διακρίνεται σε τέσσερις κατηγορίες , ανάλογα με τα μετέχοντα σ'αυτό μέρη.

Στην πρώτη κατηγορία τα συμβαλλόμενα μέρη είναι επιχειρήσεις. Συγκεκριμένα ,μία επιχείρηση χρησιμοποιεί το δίκτυο μιας άλλης (επιχείρησης B2B) ,προκειμένου να έρθει σε επαφή με τους πελάτες της ή να αυξήσει τον αριθμό των πελατών της. Σε αυτήν την κατηγορία του ηλεκτρονικού εμπορίου υπάγεται και η ηλεκτρονική ανταλλαγή δεδομένων [35]. Ευνόητο είναι πως για την επιτυχή έκβαση των εφαρμογών αυτής της κατηγορίας απαιτείται η συνεργασία και η εναρμόνιση των επιχειρήσεων- συμβαλλομένων μερών.

Στην δεύτερη κατηγορία συμβάλλονται η επιχείρηση από την μια πλευρά και ο καταναλωτής από την άλλη (B2C). Αποτελεί την πλέον συνήθη σήμερα εφαρμογή του ηλεκτρονικού εμπορίου . Εξάλλου οι καταναλωτές αποτελούν και τον κύριο στόχο των διαφόρων επιχειρήσεων . Ενημερώνονται για τα νέα προϊόντα και τις παρεχόμενες υπηρεσίες μέσα από τις ηλεκτρονικές σελίδες της κάθε επιχείρησης. Επιλέγουν και αγοράζουν χρησιμοποιώντας ψηφιακό χρήμα.

Στην Τρίτη κατηγορία τα μετέχοντα στο ηλεκτρονικό εμπόριο μέρη είναι η επιχείρηση και οι αρχές της Δημόσιας Διοίκησης (B2A:Business to Administration ή B2G: Business to Government). Τα τελευταία χρόνια έχει ενεργοποιηθεί ιδιαίτερα αυτός ο τομέας του ηλεκτρονικού εμπορίου. Σε αυτήν την κατηγορία υπάγονται όλες οι πραγματοποιούμενες μεταξύ των δύο αυτών μερών συναλλαγές , με σκοπό την άντληση και παροχή πληροφοριών ή ακόμη και την προώθηση απευθείας πληρωμών προς το δημόσιο[36] . Μεγάλη ανάπτυξη παρουσιάζει τα τελευταία χρόνια στην ΕΕ και η δημόσια ηλεκτρονική προμήθεια (public e-procurement). Πρόκειται για την απόκτηση εκ μέρους της δημόσιας διοίκησης αγαθών και υπηρεσιών με ηλεκτρονικά μέσα. Στην τέταρτη κατηγορία τα συμβαλλόμενα μέρη είναι η Δημόσια Διοίκηση και οι καταναλωτές. Στην κατηγορία αυτή ισχύουν τα προαναφερθέντα για την Τρίτη κατηγορία.

[34] Βλ. Καρακώστα , ο.π , σελ.165-166.

[35] Βλ.Δουκίδη /Θεμιστοκλέους /Δράκο/Παπαζαφειροπούλου, Ηλεκτρονικό εμπόριο , 1998 , σελ 20. Γ.Γεωργιάδη, Η σύναψη συμβάσεως μέσω του διαδικτύου , 2003, σελ 26-28, Ιγγλεζάκη , Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου , 2003 ,passim, ιδίως Εισαγωγή, σελ.19-23.

[36] Βλ.και Λαζαράκο, Ηλεκτρονικό εμπόριο, Δυνατότητες αξιοποίησης και νομικά προβλήματα, Συνήγορος 2000, 44-45

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

Το νομοθετικό Πλαίσιο της Προστασίας των Προσωπικών Δεδομένων στην Ελλάδα.

«Η πρόσβαση του πολίτη στην πληροφορία τελειώνει εκεί που αρχίζει η απαίτηση του αστού για προσωπική ζωή» Σπύρος Σημίτης

Εισαγωγή

Η αλματώδης εξέλιξη της τεχνολογίας και του διαδικτύου, είναι ένα επακόλουθο της ραγδαίας ανάπτυξης της πληροφορικής και των πληροφοριακών συστημάτων, με την ταυτόχρονη εξάπλωση σε παγκόσμιο επίπεδο του ηλεκτρονικού εμπορίου και σε συνδυασμό με την τεχνολογική πρόοδο και βελτίωση του τομέα των τηλεπικοινωνιών, καθιστούν επιτακτική την δημιουργία κατάλληλου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων , αλλά και της εν γένει οικογενειακής ζωής του ατόμου. Το διαδίκτυο , η μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο, είναι ανοιχτό τόσο στους καλόβουλους όσο και στους κακόβουλους επισκέπτες. Ο πληθυσμός του Internet αν και έχει δεχτεί κατά καιρούς πολλές παραβιάσεις και παρενοχλήσεις όσον αφορά την ασφάλεια των συστημάτων και την κλοπή δεδομένων , δεν έχει υιοθετήσει μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια, με αποτέλεσμα ολοένα και περισσότεροι χρήστες να βρίσκονται σε σύγχυση[37].

2.1 Η έννοια των προσωπικών δεδομένων και άλλες έννοιες του Ν.2472/1997

Οι ορισμοί των βασικών όρων που χρησιμοποιούνται στον ν.2472/97 περιλαμβάνονται στο άρθρο 2. Οι ορισμοί έχουν ως εξής: ως δεδομένα προσωπικού χαρακτήρα είναι οποιαδήποτε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων , ενώ στην έννοια αυτή δεν εμπίπτουν τα στατιστικής φύσεως συγκεντρωτικά στοιχεία[38]. Μια ιδιαίτερη κατηγορία προσωπικών δεδομένων είναι τα « ευαίσθητα δεδομένα», στα οποία συμπεριλαμβάνονται όσα αφορούν την φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις , την συμμετοχή σε ένωση , σωματείο και συνδικαλιστική οργάνωση , την υγεία, την κοινωνική πρόνοια και την ερωτική , καθώς και τα σχετικά με ποινικές διώξεις ή

[37] Βλ.Ιγγλεζάκη, Η προστασία των προσωπικών δεδομένων στο Διαδίκτυο-Ρυθμίσεις εθνικού και κοινοτικού δικαίου Επισκ. ΕΔ 2002 ,679 Σινανιώτη- Φαρσαρώτα, Ηλεκτρονική Τραπεζική σελ.367 επ.

[38] Βλ.άρθρο 2 περ. α'ν.2472/97

καταδίκες (περ. β'). Υποκείμενο των δεδομένων θεωρείται το φυσικό πρόσωπο , στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί , δηλ. μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόσταση (περ.γ'). Ως επεξεργασία δεδομένων προσωπικού χαρακτήρα νοείται κάθε εργασία ή σειρά εργασιών που πραγματοποιείται από το Δημόσιο ή από φυσικό πρόσωπο με ή χωρίς την βοήθεια αυτοματοποιημένων μεθόδων που πραγματοποιείται σε προσωπικά δεδομένα. Εξειδικευμένη αναφορά γίνεται στην διασύνδεση , η οποία αποτελεί μορφή επεξεργασίας που συνίσταται στην δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από άλλον ή άλλους υπεύθυνους επεξεργασίας ή που τηρούνται από τον ίδιο υπεύθυνο για άλλον σκοπό (περ.στ').

Η έννοια του αρχείου δεδομένων προσωπικού χαρακτήρα , το οποίο εννοείται ως το σύνολο δεδομένων προσωπικού χαρακτήρα , τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας (περ.ε'). Ο κύκλος των προσώπων ,στα οποία αναφέρονται οι ρυθμίσεις του νόμου περιλαμβάνονται:

- Τον υπεύθυνο επεξεργασίας ή οποιοδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας δεδομένων(περ. ζ')
- Τον εκτελούντα την επεξεργασία, ήτοι οποιονδήποτε επεξεργάζεται τα προσωπικά δεδομένα για λογαριασμό υπευθύνου επεξεργασίας(περ.η')
- Τον τρίτο, ήτοι κάθε φυσικό πρόσωπο ή νομικό πρόσωπο ή δημόσια αρχή ή οργανισμός – εκτός από το υποκείμενο των δεδομένων και τα προηγούμενα πρόσωπα – που ενεργεί υπό την άμεση εποπτεία ή για λογαριασμό του υπευθύνου επεξεργασίας(περ. θ') και τέλος,
- Τον αποδέκτη, ήτοι το φυσικό ή νομικό πρόσωπο ή δημόσια αρχή ή οργανισμό, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως για τρίτο ή όχι[39].

Επίσης, η συγκατάθεση του υποκειμένου των δεδομένων, είναι κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επιγνώσει, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για τον σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους

[39] Βλπ.Αραβαντινό, Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή, σελ 46 επ.

αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.[40]

2.2 Πεδίο εφαρμογής

Οι διατάξεις του ν.2472/1997 δεν εφαρμόζονται στην επεξεργασία δεδομένων η οποία πραγματοποιείται:

- ✓ από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών,
- ✓ από τις δικαστικές – εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ελευθερίας, της οικονομικής εκμετάλλευσης της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων[41].

Ο ν.2472/1997 βρίσκει εφαρμογή στην επεξεργασία δεδομένων με αυτοματοποιημένες και συμβατικές μεθόδους , τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα. Αντικείμενο ρύθμισης αποτελούν τα δεδομένα προσωπικού χαρακτήρα , ενώ εξαιρούνται που πληροφορίες που δεν αναφέρονται σε πρόσωπα. Οι ρυθμίσεις του νόμου αφορούν τα φυσικά πρόσωπα (άρθρο 1 και 2 περ.γ) , με συνέπεια να εξαιρούνται τα νομικά πρόσωπα από το πεδίο εφαρμογής. Ο νόμος ρυθμίζει την επεξεργασία δεδομένων τόσο με ηλεκτρονικά όσο και με συμβατικά μέσα, όπου εμπίπτει η μη αυτοματοποιημένη , δια χειρός επεξεργασία δεδομένων προσωπικού χαρακτήρα (άρθρο 3).[42]

Οι επιταγές του νόμου απευθύνονται στον υπεύθυνο επεξεργασίας . Σύμφωνα με τον ορισμό του ν.2472/1997 , ως υπεύθυνος επεξεργασίας νοείται οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα , όπως φυσικό ή νομικό πρόσωπο , δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

Αντικείμενο της προστασίας του ν.2472/1997 είναι τα φυσικά πρόσωπα , ενώ στο ν.3471/2006 διευρύνεται το υποκειμενικό πεδίο εφραμογής του, καθώς οι διατάξεις του νόμου βρίσκουν εφραμογή και στην περίπτωση όπου οι συνδρομητές είναι νομικό (και όχι μόνο φυσικό) πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.

[40] http://www.dpa.gr/

[41] Βλ προστασία προσωπικών δεδομένων στο ηλεκτρονικό εμπόριο κεφ 9 σελ 199

[42] http://www.dpa.gr

Βασικός κανόνας, είναι ότι η επεξεργασία δεδομένων επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει την συγκατάθεση του (άρθρο 5 ν.2472/1997) ή εφόσον συντρέχουν οι περιοριστικά αναφερόμενες στο νόμο περιπτώσεις:

Συγκεκριμένα , η επεξεργασία δεδομένων επιτρέπεται και χωρίς την συγκατάθεση του υποκειμένου των δεδομένων , όταν :

- 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.
- Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας , η οποία επιβάλλεται από το νόμο,
- Η επεξεργασία είναι αναγκαία για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου , εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει την συγκατάθεση του.
- Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφερόντος 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
- Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφερόντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει των δικαιωμάτων και συμφερόντων των προσώπων [43].

[44]Ο παρών νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον αυτή εκτελείται:

α) Από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο.

β) Από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους-Μέλους της Ευρωπαϊκής Ένωσης ή κράτους του Ευρωπαϊκού Οικονομικού Χώρου, αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην Ελληνική Επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην Ελληνική Επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν

[43] http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#3(προϋποθέσεις επεξεργασίας)

ιδιαίτερη ευθύνη του. Το αυτό ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινική δίωξη[45].

2.3 Το νομοθετικό πλαίσιο του Ν.3471/2006

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ 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).

Σύμφωνα με το άρθρο 3 ν.3471/2006 τα άρθρα 1-17 του νόμου αυτού εφαρμόζονται για την προστασία δεδομένων του προσωπικού χαρακτήρα στο πλαίσιο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών. Πάντως ο ν.2472/1997 εξακολουθεί να εφαρμόζεται όταν δεν υπάρχει ειδικότερη ρύθμιση του ν.3471/2006[46].

Κατευθυντήρια γραμμή για τον νομοθέτη αποτέλεσε τόσο το είδος των δεδομένων (δεδομένα κίνησης, δεδομένα μη αναγκαία για την επικοινωνία μέσω του Διαδικτύου) όσο και τα συστήματα απαγόρευσης επεξεργασίας, εκτός αν την επιτρέψει το υποκείμενο (**σύστημα opt-in**) ελευθερίας , εκτός αν υπάρξει απαγόρευση του υποκειμένου (**σύστημα opt out**) ή ακόμα επεξεργασίας και παρά την αντίθεση του υποκειμένου (**σύστημα no-opt**) με σχετικούς νομικούς περιορισμούς του παρόχου, του αποδέκτη της επικοινωνίας και τρίτων.

Όσον αφορά τα δεδομένα κίνησης , δηλαδή τα δεδομένα που είναι αναγκαία για την παροχή υπηρεσιών διαμέσου δικτύου είτε για νομικούς αποδεικτικούς λόγους είτε για καθαρά τεχνικούς[47] σύμφωνα με τις εφαρμοστέες διατάξεις πρέπει να γίνουν οι ακόλουθες διακρίσεις[48]:

- Απέναντι στον αποδέκτη της επικοινωνίας: Ως προς αυτόν ισχύει η απαγόρευση πρόσβασης εκτός αν την επιτρέψει το υποκείμενο **(opt –in**)[49], αλλά ειδικά ο πάροχος του δικτύου επιτρέπεται εν αμφιβολία να γνωστοποιεί τον αριθμό κλήσης , εκτός αν το απαγορεύσει το υποκείμενο **(opt –out**)[50]. Εντούτοις, αν ο αποδέκτης επικαλεσθεί, ακόμη και αναιτιολόγητα, κακόβουλη ή οχληρή κλήση, και μάλιστα όχι

[45] http://www.dpa.gr

[46] [46] http://www.eskozanis.gr

[47] Βλ.Χριστοδούλου Κώστα «Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία»

[48] Άρθρο 4 ν.3471/2006

[50] Άρθρο 8 ν. 3471/2006 της Οδηγίας 2002/58/ΕΚ

κατ'ανάγκη προερχόμενη από τον συγκεκριμένο καλούντα , επιτρέπεται ο παραμερισμός της απαγόρευσης του υποκειμένου (σύστημα no-opt)[51].

- Απέναντι στον πάροχο του δικτύου . Ο πάροχος του δικτύου δικαιούται να αποθηκεύει τα δεδομένα κίνησης είτε για λόγους τεχνικούς είτε για λόγους νομικής προστασίας , κατόπιν βέβαια ενημέρωσης του υποκειμένου ,το οποίο μπορεί να απαγορεύσει την αποθήκευση ανατρέποντας τη σύμβαση παροχής υπηρεσιών δικτύου.(**σύστημα opt-in**)[52].

Όσον αφορά τις λεγόμενες «υπηρεσίες προστιθέμενης αξίας» [53] ισχύει καταρχήν ένα κοινό πλέγμα νομικών ρυθμίσεων ως προς τον αποδέκτη , τον πάροχο και τους τρίτους , δηλ. το σύστημα opt-in , αλλά ως προς τους δυο τελευταίους ισχύουν ορισμένες εξαιρέσεις αναφορικά με την δημοσίευση σε δημόσιους τηλεφωνικούς καταλόγους και με την αδικαιολόγητη μη ζητηθείσα εμπορική επικοινωνία (spamming).

- Για τον αποδέκτη: Ειδικά η καταγραφή του περιεχομένου της συνδιαλέξεως από τον αποδέκτη της (συνομιλητή) ακόμη και όταν αυτό επιβάλλεται από θεμιτή ανάγκη δικαστικής προάσπισης των δικαιωμάτων του, ιδίως την απόδειξη των γεγονότων που τα στηρίζουν , μπορεί μεν να επιτρέπεται κατά το κοινοτικό δίκαιο απαγορεύεται [54] από σειρά διατάξεων της ελληνικής νομοθεσίας [55]. Η άρση της σύγκρουσης αυτής θα γίνει με τη στάθμιση συγκρουόμενων συμφερόντων, δηλ. αφενός μεν του φορέα των εκάστοτε προσωπικών δεδομένων στον διακυβεύοντα [56] , αφετέρου δε του υπευθύνου επεξεργασίας που προβαίνει σε καταγραφή τους και έχει δικαίωμα παροχής έννομης προστασίας.
- Έναντι του παρόχου και των τρίτων . Και έναντι του παρόχου και των τρίτων ισχύει το σύστημα opt-in (απαγόρευση, εκτός αν επιτρέψει το υποκείμενο της επεξεργασίας των μη αναγκαίων για την επικοινωνία διαμέσου διαδικτύου δεδομένων [57], αλλά με τις ακόλουθες εξαιρέσεις:

➢ Αναφορικά με τη δημοσίευση σε τηλεφωνικούς καταλόγους. Καταρχήν , ισχύει η απαγόρευση επεξεργασίας με την επιφύλαξη τυχόν συναίνεσης του υποκείμενου (συστήμα opt-in) , αλλά ειδικά ως προς ορισμένα στοιχεία επαρκής , (π.χ ονοματεπώνυμο, διεύθυνση) ισχύει εν μέρει σύστημα ελεύθερης επεξεργασίας, εκτός αν το απαγορεύσει το υποκείμενο (opt-out, δηλ. καταρχήν ελευθερία δημοσιοποίησης),

---

[51] Άρθρο 8 ν.3471/2006, άρθρο 10 Οδηγία 2002/58/ΕΚ

[52] Άρθρο 6 ν.3471/2006, άρθρο 6 Οδηγία 2002/58/ΕΚ

[53] Άρθρο 2 ν.3471/2006.

[54] Άρθρο 5 της Οδηγίας 2002/48/ΕΚ

[55] Άρθρο 4ν.3471/2006

[56] Σύνταγμα 9Α

[57] Άρθρο 4 ν.3471/2006

εφόσον πρόκειται για φυσικό πρόσωπο [58] και σύστημα no-opt, αν πρόκειται για νομικό πρόσωπο , το οποίο λόγω της αρχής της διαφάνειας [59], δεν δικαιούται να αρνηθεί την δημοσιότητα των στοιχείων της ταυτότητας του[60].

- Ως προς τη μη ζητηθείσα επικοινωνία (spamming).Πριν το άρθρο 16 ν.3917/2011 και εδώ ίσχυε καταρχήν το σύστημα της απαγόρευσης πρόσβασης στο υποκείμενο εκτός αν υπάρξει συναίνεση του (σύστημα opt-in). Εξαίρεση καθιερώνεται όταν τα στοιχεία επαφής έχουν ήδη αποκτηθεί νομικά στο πλαίσιο παρόμοιων δοσοληψιών[61], οπότε η άμεση ηλεκτρονική επικοινωνία επιτρεπόταν , εφόσον το υποκείμενο έχει ενημερωθεί για τους όρους των συμβάσεων εξ αποστάσεως για την δυνατότητα υπαναχώρησης του και παρά ταύτα δεν απέστη της επικοινωνίας[62].

Η ευθύνη του παραβάτη σε περίπτωση παράβασης της απαγόρευσης μη ζητηθείσης εμπορικής επωνυμίας προκύπτει από τις ΑΚ 57,914, 904. Επίσης η σύμβαση υπόκειται σε ανακοπή σύμφωνα με τις προαναφερθείσες διατάξεις. Των άρθρων 3 και ν. 2251/1994 και παρέχεται δικαίωμα διάθεσης του αποσταλέντος με όριο βέβαια την συνταγματική προστασία των Συντ.17 και Συντ 25.

2.4 Η Νέα ρύθμιση.

Με το άρθρο 16 ν.3917/2011 ενσωμάτωση της Οδηγίας 2006/24/ΕΚ της 15.3.2006 για την διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ . Σύμφωνα με το άρθρο 1

Ν. 3917/20011 ο παρών νόμος εφαρμόζεται σε δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του εγγεγραμμένου χρήστη. Δεν εφαρμόζονται στο περιεχόμενο των ηλεκτρονικών επικοινωνιών καθώς με την χρήση δικτύου ηλεκτρονικών επικοινωνιών [63] και συνεπώς για τους τομείς αυτούς ισχύει ο ν.3471/2006. Έγινε στο άρθρο 11 διαχωρισμός της νομικής μεταχείρισης της μη ζητηθείσης εμπορικής επικοινωνίας ανάλογα με το αν αυτή πραγματοποιείται διαμέσου ή χωρίς ανθρώπινη παρέμβαση.

Αν λοιπόν πραγματοποιείται χωρίς ανθρώπινη παρέμβαση εξακολουθεί να ισχύει το σλυστημα opt-in , δηλ. καταρχήν απαγόρευση πραγματοποίησης μη ζητηθείσας εμπορικής επικοινωνίας , εκτός αν ο συνδρομητής συγκατατέδει εκ των προτέρων ρητά [64].

---

[58] Άρθρο 10 ν.3471/2006 , άρθρο 12 Οδηγία 2002/58/ΕΚ

[59] Σύμφωνα με το άρθρο 6 της Οδηγίας 2001/31/ΕΚ για το ηλεκτρονικό εμπόριο , όπου εισάγεται η υποχρέωση παροχής πληροφοριών στις εμπορικές επικοινωνίες ,» εκτός από άλλες προϋποθέσεις που προβλέπονται από το κοινοτικό δίκαιο.

[60] Σκοπός ,επωνυμία , έδρα άρθρο 10 ν.3471/2006 άρθρο 12 και 4 Οδηγία 2002/58ΕΚ

[61] Άρθρο 11 ν.3471/2006

[62] Σχετικές είναι οι διατάξεις του άρθρου 3 ν.2251/1994 (δικαίωμα του καταναλωτή για υπαναχώρηση, επί συμβάσεως εκτός εμπορικού καταστήματος ή ανάκλησης της πρότασης του εντός 14 ημερολογιακών ημερών από την παραλαβή του εγγράφου της σύμβασης ή από τυχόν μεταγενέστερη παραλαβή του προϊόντος.

[63] Άρθρο 1 ν. 3917/2011

[64] Άρθρο 11 ν.3471 όπως τροπο. Με το άρθρο 16 ν.3471/2011.

Αν όμως η μη ζητηθείσα εμπορική επικοινωνία πραγματοποίειται με ανθρώπινη παρέμβαση , τότε δεν επιτρέπεται , εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα της διαθέσιμης στο κοινό υπηρεσίας ότι δεν επιθυμεί γενικά να δέχεται τέτοιες κλήσεις . Επομένως, εξ αντιδιαστολής προκύπτει ότι επιτρέπεται καταρχήν του spamming, εκτός αν έχει γίνει η πιο πάνω δήλωση άρνησης του από τον συνδρομητή (σύστημα opt-out).

Ορισμοί του ν.3471/2006 [65]

- ✓ «συνδρομητής»: είναι κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.
- ✓ «χρήστης»: είναι κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς, χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.
- ✓ «δεδομένα κίνησης»: είναι τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία[66].
- ✓ «επικοινωνία»: κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Δεν περιλαμβάνονται πληροφορίες που διαβιβάζονται ως τμήμα ραδιοτηλεοπτικών υπηρεσιών στο κοινό μέσω δικτύου ηλεκτρονικών επικοινωνιών, εκτός από τις περιπτώσεις κατά τις οποίες οι πληροφορίες μπορούν να αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει.
- ✓ «κλήση»: σύνδεση που πραγματοποιείται μέσω μίας διαθέσιμης στο κοινό τηλεφωνικής υπηρεσίας που επιτρέπει αμφίδρομη επικοινωνία σε πραγματικό χρόνο.
- ✓ «Υπηρεσία προστιθέμενης αξίας»: κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή δεδομένων θέσης πέραν εκείνων που απαιτούνται για τη μετάδοση μίας επικοινωνίας και τη χρέωση της.
- ✓ «Ηλεκτρονικό ταχυδρομείο»: κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη.
- ✓ «Υπηρεσίες ηλεκτρονικών επικοινωνιών»: οι υπηρεσίες που παρέχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των

[65] www.dpa.gr(νόμος 3471/2006)

[66] Το στοιχείο 4 αντικαταστάθηκε ως άνω με το άρθρο 168,παρ.1στοιχ.α' του Ν.4070/2012 (ΦΕΚ Α 82/2012)

υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και υπηρεσίες της Κοινωνίας της Πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του π.δ. 39/2001 (ΦΕΚ 28 Α'), και που δεν αφορούν, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών.

- ✓ «Δημόσιο δίκτυο επικοινωνιών»: το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.
- ✓ 11. «Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών»: οι υπηρεσίες ηλεκτρονικών επικοινωνιών που παρέχονται στο κοινό.

2.5 Κατασκοπευτικό λογισμικό και cookies

[67]Στον ν.3471/2006 ρυθμίζεται η χρήση των κατασκοπευτικών λογισμικών που αποτελούν σαφή απειλή για την ιδιωτική σφαίρα του χρήστη του Διαδικτύου. Συγκεκριμένα, προβλέπεται ότι απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών , κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων (άρθρο 4 και 5).

Ωστόσο, επιτρέπεται η τεχνικής φύσεως αποθήκευση ή προσβαση που έχει αποκλειστικό σκοπό την διαβίβαση μιας επικοινωνίας μέσω του δικτύου ή η οποία είναι αναγκαία για την παροχή υπηρεσίας που έχει ζητήσει ο χρήστης ή ο συνδρομητής σύμφαωνα με το άρθρο 4 , όταν εξυπηρετεί θεμιτούς σκοπούς και εφόσον παρέχονται σχετικές πληροφορίες στους χρήστες.

Η ρύθμιση αυτή αφορά τα αυτοεγκαθιστώμενα αρχεία « cookies», για τα οποία υιοθετείται ένα σύστημα “opt-out” , κατά το οποίο ο συνδρομητής ή ο χρήστης δύναται να δηλώσει τη μη συγκατάθεση του, αλλά μόνο εκ των υστέρων.

2.6 Διατήρηση Δεδομένων- Οδηγία 2006/24/ΕΚ

[68]Για την καταπολέμηση της εγκληματικότητας και του οργανωμένου εγκλήματος εκδόθηκε η Οδηγία 2006/24/ΕΚ ,η οδηγία αυτή εισάγει την υποχρέωση των κρατών μελών να θεσπίσουν μέτρα ώστε να διασφαλισθεί ότι τα δεδομένα κίνησης και θέσης διατηρούνται από τους παροχείς διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για χρονικό διάστημα από έξι μήνες έως 2 έτη. Το αντικείμενο της Οδηγίας είναι η εναρμόνιση των διατάξεων των κρατών μελών όσον αφορά την διατήρηση δεδομένων κίνησης και θέσης που υποχρεούνται οι παροχείς υπηρεσιών ηλεκτρονικών επικοινωνιών, τα οποία θα πρέπει να καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης , διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων . Η υποχρέωση διατήρησης δεν εκτείνεται στο περιεχόμενο των επικοινωνιών , για το οποίο εξακολουθούν να ισχύουν οι κείμενες διατάξεις.

[67] Προστασία προσωπικών δεδομένων στο Ηλεκτρονικό εμπόριο βλ σε 211 (Διατάξεις)

[68] Προστασία προσωπικών δεδομένων στο Ηλεκτρονικό εμπόριο βλ σελ 212

Οι κατηγορίες δεδομένων που διατηρούνται είναι οι εξής:

Α) δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας β) δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας γ) δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας , ώρας και διάρκειας της επικοινωνίας δ) δεδομένα αναγκαία για τον προσδιορισμό του είδους της επικοινωνίας ε) δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών , ή του φερόμενου ως εξοπλισμού επικοινωνίας τους και στ) δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας.

Ο χρόνος διατήρησης των δεδομένων κίνησης και θέσης , ανέρχεται σε χρονικό διάστημα όχι μικρότερο του εξαμήνου και όχι μεγαλύτερο της διετίας από την ημερομηνία της επικοινωνίας. Η οδηγία περιέχει ρυθμίσεις για την προστασία και την ασφάλεια των δεδομένων που διατηρούνται (άρθρο 7) , ενώ ακόμα προβλέπει ότι κάθε κράτος μέλος πρέπει να ορίσει μια ή περισσότερες δημόσιες αρχές με την αρμοδιότητα να ελέγχει την εφαρμογή των διατάξεων σχετικά με την ασφάλεια των δεδομένων (άρθρο 9). Παραπέρα, ορίζεται, ότι τα δεδομένα αυτά πρέπει να διατηρούνται κατά τέτοιο τρόπο ώστε να μπορούν να διαβιβασθούν κατόπιν σχετικού αιτήματος στις αρμόδιες αρχές χωρίς αδικαιολόγητη καθυστέρηση (άρθρο 8). Τα υποκείμενα των δεδομένων που υπόκεινται σε επεξεργασία δυνάμει των διατάξεων της οδηγίας διατηρούν τα δικαιώματα που τους παρέχει η οδηγία 95/46 και προς αυτό ορίζεται ότι το εθνικό δίκαιο πρέπει να εφαρμόσει σχετικά τις διατάξεις της οδηγίας σχετικά με τα ένδικα μέσα, την ευθύνη και τις κυρώσεις (άρθρο 13).

Τέλος, η οδηγία δεν περιέχει πρόβλεψη για την αποζημίωση των παροχέων διαθέσιμών στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιου δικτύου επικοινωνιών, όπως η πρόταση οδηγίας. Είναι σαφές ότι το κόστος από την διατήρηση δεδομένων θα επιβαρύνει σε σημαντικό βαθμό τους παροχείς, οι οποίοι θα πρέπει να βρουν τρόπους για την κάλυψη.

2.7 Αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.

- ✓ [69]Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει και ως προς την τήρηση των διατάξεων του παρόντος νόμου τις αρμοδιότητες που προβλέπονται από το ν. 2472/1997, όπως εκάστοτε ισχύει.
- ✓ Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) έχει ως προς την τήρηση των διατάξεων του παρόντος νόμου, που αναφέρονται σε αυτήν, τις αρμοδιότητες που προβλέπονται από το ν. 3115/2003, όπως εκάστοτε ισχύει.
- ✓ Στις περιπτώσεις στις οποίες προβλέπεται γνωμοδότηση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), αυτή γνωμοδοτεί μετά από αίτηση

συνδρομητή ή αίτημα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή και αυτεπαγγέλτως.

- ✓ Σε περίπτωση παράβασης των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου, για την τήρηση των οποίων αρμόδια είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αυτή επιβάλλει τις προβλεπόμενες από το άρθρο 21 του ν. 2472/1997 διοικητικές κυρώσεις. Σε περίπτωση παράβασης των διατάξεων του παρόντος νόμου, για την τήρηση των οποίων αρμόδια είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, αυτή επιβάλλει τις προβλεπόμενες από το άρθρο 11 του ν. 3115/2003 διοικητικές κυρώσεις. Οι πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών με τις οποίες επιβάλλονται οι διοικητικές κυρώσεις σε φορείς παροχής δημοσίου δικτύου ή/και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών υπηρεσιών γνωστοποιούνται στην Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).
- ✓ Με κοινή πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, ρυθμίζονται θέματα σχετικά με τις εργασίες που πραγματοποιούνται σε συστήματα των παροχών ηλεκτρονικών επικοινωνιών για το συσχετισμό των στοιχείων ταυτότητας των συνδρομητών τους με τα αντίστοιχα δεδομένα επικοινωνίας τους.[70]

2.8 Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα και η προστασία αυτών στο τηλεπικοινωνιακό τομέα [71] διέπεται βασικά από τις διατάξεις του ν.2472/1997 και του ν.3471/2006 και συμπληρώνεται και από άλλα φρονήματα.

1)Χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα

- ✓ Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.
- ✓ Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.
- ✓ Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
- ✓ 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.

---

[70] http://www.eskozanis.gr

[71] Βλ. Ιγγλεζάκη, εισαγωγή στο Δίκαιο Πληροφορικής .Αξίζει ακόμα να αναφερθεί ότι οι διατάξεις για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα δεν παρουσιάζουν αυτοτέλεια, αλλά εντάσσονται στο γενικότερο πλαίσιο των ρυθμίσεων του ν. 2472/1997ν οι διατάξεις του οποίου εφαρμόζονται για κάθε ζήτημα που δεν ρυθμίζεται ειδικότερα από τον νόμο, σύμφωνα με το άρθρο 3 του νόμου 3471/2006, σελ 198.

2) 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. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει την διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεγεί ή τύχει επεξεργασίας.

Προϋποθέσεις επεξεργασίας

1. Επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.

2. Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, 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.

3. Η Αρχή μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης.

Επεξεργασία ευαίσθητων δεδομένων

1. Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων.

2. Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής,* όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

α) Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη ή νόμος ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση.

β) Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

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.

δ) Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας 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.

ε) Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία είτε αα) για λόγους εθνικής ασφάλειας είτε ββ) για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας είτε γγ) για λόγους προστασίας της δημόσιας υγείας είτε δδ) για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.

στ) Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

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. 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.

3.Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

Εφ' όσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου, σύμφωνα με το άρθρο 6 του παρόντος νόμου, επέχει θέση αιτήσεως για τη χορήγηση άδειας. Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την απο4. Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

5. **Η άδεια περιέχει απαραιτήτως**:

α) Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο καθώς και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του.

β) Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο.

γ) Το είδος των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να περιληφθούν στο αρχείο.

δ) Το χρονικό διάστημα για το οποίο χορηγείται η άδεια.

ε) Τους τυχόν όρους και προϋποθέσεις που έχει επιβάλει η Αρχή για την ίδρυση και λειτουργία του αρχείου.

στ) Την υποχρέωση γνωστοποίησής του ή των αποδεκτών ευθύς ως εξατομικευτούν.

6. Αντίγραφο της άδειας καταχωρίζεται στο Μητρώο Αδειών που διατηρεί η Αρχή.

7. Κάθε μεταβολή των στοιχείων που αναφέρονται στην παράγραφο 5 γνωστοποιείται χωρίς καθυστέρηση στην Αρχή. Κάθε άλλη μεταβολή, πλην της διεύθυνσης του υπευθύνου ή του εκπροσώπου του, συνεπάγεται την έκδοση νέας άδειας, εφόσον συντρέχουν οι νόμιμες προϋποθέσεις.

Απόρρητο και ασφάλεια της επεξεργασίας

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του.

2. 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.

3. 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. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 ι' για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.

4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει 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.

2.9 Διάκριση των δεδομένων προσωπικού χαρακτήρα και ενισχυμένη προστασία των ευαίσθητων προσωπικών δεδομένων.

Στο άρθρο 2 του ν. 2472/1997 , αλλά και στο άρθρο 2 περ. α της Οδηγίας 95/46/ΕΚ δίδεται ο ορισμός των δεδομένων , σύμφωνα με τον οποίο ως «δεδομένα προσωπικού χαρακτήρα» θεωρούνται κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, και ως τέτοιο λογίζεται το πρόσωπο που μπορεί να προσδιοριστεί άμεσα ή έμμεσα, ιδίως βάσει του αριθμού της ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόσταση του από φυσική, βιολογική, ψυχολογική , οικονομική, πολιτιστική ή κοινωνική άποψη.

Σύμφωνα με τον ορισμό του άρθρου 8 της οδηγίας, η ειδική αυτή διάταξη έχει ως αντικείμενο την επεξεργασία δεδομένων προσωπικού χαρακτήρα που παρέχουν πληροφορίες για την φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα , τιε θρησκευτικές ή φιλοσοφικές πεποιθήσεις , την συμμετοχή σε συνδικαλιστικές οργανώσεις και την υγεία και την σεξουαλική ζωή. Ο Έλληνας νομοθέτης συμπεριέλαβε στο άρθρ. 2 περ. β'ν.2472/1997 έναν πανομοιότυπο ορισμό, με την προσθήκη των κατηγοριών δεδομένων που αφορούν την κοινωνική πρόνοια και τις ποινικές διώξεις και καταδίκες[72] . Ως ευαίσθητα δεδομένα χαρακτηρίζονται ,ακόμα, κατά την ελληνική νομοθεσία: α) τα δεδομένα με τους λήπτες και τα αρχεία των Δωρητών ανθρωπίνων ιστών και οργάνων[73] και β) οι δηλώσεις των αιτούντων άσυλο και τα στοιχεία των αιτήσεων αλλοδαπών[74].

[72] Βλ.άρθρ 8 κ 5 οδηγίας 95/46/ΕΚ.

[73] Βλ.άρθρο 9 ν.2737/1999

[74] Βλ.άρθρο 2 &12 π.δ 61/1999

2.10 Τα προσωπικά δεδομένα στο Διαδίκτυο

Ένας χρήστης του διαδικτύου για να έχει πρόσβαση σε κάποιες σελίδες ,θα πρέπει να δώσει τα προσωπικά του στοιχεία. Αυτή η πρακτική είναι εντελώς διαφορετική από την κατάσταση κατά την οποία οι πληροφορίες στέλνονται ταχυδρομικώς παρόλο που πάλι είναι γνωστά σε τρίτους , συνήθως εταιρείες, το όνομα και η διεύθυνση του υποκειμένου. Ωστόσο, στην σύγχρονη οικονομία η παρουσία η απουσία ανταγωνισμού παίζει τεράστιο ρόλο. Πολλές εταιρείες μπορούν να δώσουν πρόσβαση στην σελίδα τους χωρίς να ζητήσουν επιπλέον στοιχεία, ενώ άλλες μπορούν να ζητήσουν πρώτα την παροχή προσωπικών στοιχείων.

Παρόμοια, κάποιες εταιρείες μπορούν να στέλνουν spam (διαφημιστικά μηνύματα χωρίς την άδεια του χρήστη να λαμβάνει τέτοιου είδους αλληλογραφία), ενώ άλλες το αποφεύγουν. Για τους καταναλωτές είναι σκόπιμο να χρησιμοποιούν τεχνολογικά μέσα κατά αυτών των μηνυμάτων.

Ένα από τα πιο χαρακτηριστικά παραδείγματα που καταδεικνύουν ότι το διαδίκτυο κρύβει σοβαρές απειλές για την ιδιωτική ζωή είναι η έκδοση του βιβλίου των Dr.Gubbler και Gonod της ιατρικής και πολιτικής ιστορίας του Προέδρου της Γαλλικής Δημοκρατίας Francois Mitterand. Αν και τον Ιανουάριο του 1996 απαγορεύτηκε με ασφαλιστικά μέτρα η δημοσίευση του βιβλίου και επιδικάστηκε αποζημίωση στην χήρα και τα τέκνα του, το Δικαστήριο έκρινε ότι η διατήρηση αυτής της απαγόρευσης κάποια χρόνια αργότερα δεν μπορούσε να στηριχθεί στους ίδιους δικαιολογητικούς λόγου.[75]

Το βιβλίο με τίτλο ‘ Le grand secret’ ήταν προσβάσιμο στο διαδίκτυο λίγε μέρες αφότου η πώληση του στα βιβλιοπωλεία είχε απαγορευτεί. Το δικαίωμα της πληροφόρησης του κοινού από την μια μεριά παραβιάζει το δικαίωμα στην προσωπική ζωή του αρχηγού του κράτους και της οικογένειας από την άλλη. Ανάμεσα στα δύο υπάρχει μια λεπτή ισορροπία που εξετάζεται από το δικαστήριο ανάλογα με την περίπτωση. Όμως η παραβίαση της ιδιωτικότητας στο διαδίκτυο παρουσιάζεται οξυμμένη λόγω της ταυτόχρονης μεταβίβασης της πληροφορίας σε παγκόσμιο επίπεδο.[76]

Οι τέσσερις παράγοντες σηματοδοτούν τον διαρκώς αυξανόμενο κίνδυνο από την αλόγιστη χρήση συλλογών προσωπικών δεδομένων σήμερα.[77] Πρόκειται για την εξεφάνιση της

[75] ΕΔΔΑ αποφ 18.5.2004 υποθ 58148/2000 Plon Societe κατά της Γαλλίας σελ 438-9

[76] Suzan DionneBalz, Olivier Hance, Privacy and the Internet 1996 σελ 219-220.

[77] Ι.Καρακωστας , Δίκαιο και Internet 2001 σελ.142

ανωνυμίας, την εξαφάνιση του τυχαίου αφού τα προσωπικά δεδομένα συνδέονται ευθύς εξαρχής και την εμπορικοποίηση του ατόμου με την δευτερεύουσα χρήση των πληροφοριών.[78]

2.11 Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

Η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) είναι ένας νέος φορέας που λειτουργεί με βάση το Ν.3115/2003 με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών [79] .

Η ΑΔΑΕ είναι ανεξάρτητη Αρχή που απολαμβάνει διοικητικής αυτοτέλειας. Έδρα της ΑΔΑΕ είναι η Αθήνα , αλλά μπορεί με απόφαση της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της ΑΔΑΕ κοινοποιούνται στο Υπουργείο Δικαιοσύνης και στο τέλος κάθε χρόνου υποβάλλεται έκθεση των πεπραγμένων της στη Βουλή. Η ΑΔΑΕ υπόκεινται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και την διαδικασία που κάθε φορά προβλέπεται από τον κανονισμό της Βουλής. Η ΑΔΑΕ για την εκπλήρωση της αποστολής της έχει τις ακόλουθες αρμοδιότητες :

- Διενέργεια αυτεπάγγελτων ελέγχων σε επιχειρήσεις και υπηρεσίες που έχουν γενικό αντικείμενο την επικοινωνία.
- Κατάσχεση ψηφιακών πειστηρίων , καταστροφή στοιχείων που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου επικοινωνιών.
- Εξέταση καταγγελιών σχετικά με την προστασία των δικαιωμάτων των αιτούντων
- Συνεργασία με άλλες αρχές της χώρας και με αντίστοιχες αρχές άλλων κρατών , για θέματα ασφάλειας και επικοινωνιών.
- Έκδοση κανονισμού εσωτερικής λειτουργίας ο οποίος δημοσιεύεται στην εφημερίδα της Κυβερνήσεως.
- Έκδοση κανονιστικών πράξεων , μέσω των οποίων ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις αρμοδιότητες της Αρχής.
- Σύνταξη, μια φορά το χρόνο, έκθεσης πεπραγμένων , στην οποία περιγράφεται το έργο της Αρχής , διατυπώνονται παρατηρήσεις και προτείνονται νομοθετικές μεταβολές στον τομέα της διασφάλισης του απορρήτου των επικοινωνιών.

Το ηλεκτρονικό εμπόριο βασίζεται στην επικοινωνία των πελατών με τους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου. Για να γίνει μια ηλεκτρονική συναλλαγή, πρέπει πρώτα να επικοινωνήσει ο πελάτης με τον έμπορα, να δώσει τα προσωπικά του στοιχεία, τον αριθμό της πιστωτικής του κάρτας και να λάβει πληροφορίες σχετικές με την

[78] Ι.Καρακώστας, Δίκαιο και Internet 2001 sel.142.

[79] Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (2006)

συναλλαγή. Είναι προφανές , ότι η επικοινωνία αυτή πρέπει να είναι απόρρητη , αφού σε καμία περίπτωση τα προσωπικά του στοιχεία του πελάτη και ιδιαίτερα οι αριθμοί των πιστωτικών του καρτών δεν πρέπει να γνωστοποιούνται σε τρίτους. Όπως, αναφέρθηκε πιο πάνω ο σκοπός της ΑΔΑΕ είναι η προστασία του απόρρητου των επικοινωνιών.

Συνεπώς κάθε οργανισμός, ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την ΑΔΑΕ. Η ΑΔΑΕΙ έχει εκδώσει κάποιους κανονισμούς για την διασφάλιση του απορρήτου των επικοινωνιών και κάθε οργανισμός ηλεκτρονικού εμπορίου , σύμφωνα με τα παραπάνω , πρέπει να τους ακολουθεί. Η ΑΔΑΕΙ ελέγχει τους οργανισμούς ηλεκτρονικού εμπορίου για την τήρηση των κανόνων, και η ίδια ελέγχεται από το κράτος. Η ΑΔΑΕ έχει εκδώσει και δημοσιεύει

Στην εφημερίδα της κυβερνήσεως κανονισμούς ασφάλειας για το διαδίκτυο, την διασφάλιση απορρήτου τηλεπικοινωνιακής υποδομής , την κινητή και σταθερή τηλεφωνία, το θεσμικό πλαίσιο για την ασφάλεια , καθώς και την ασφάλεια για αυτόματες τραπεζικές συναλλαγές. Με δεδομένο ότι το μεγαλύτερο μέρος του ηλεκτρονικού εμπορίου πραγματοποιείται μέσω του διαδικτύου , κάθε οργανισμός ηλεκτρονικού εμπορίου πρέπει να συμμορφώνεται και να τηρεί τους κανονισμούς ασφάλειας για το διαδίκτυο. Συγκεκριμένα α, θα πρέπει να ακολουθεί τουλάχιστον τους κανονισμούς που περιγράφονται στην συνέχεια με λεπτομέρεια , οι οποίοι δημοσιεύθηκαν στις 26 Ιανουαρίου 2005 στην εφημερίδα της κυβερνήσεως.

2.12 Η κλοπή των προσωπικών δεδομένων με σκοπό τη διενέργεια απάτης

Η «απάτη ταυτότητας», δηλαδή η χρήση προσωπικών δεδομένων τρίτων προσώπων με σκοπό την διενέργεια απάτης αποτελεί συχνό φαινόμενο στον κόσμο του διαδικτύου. Στατιστικές του 2001 έδειξαν ότι κάθε χρόνο 500.000 άνθρωποι πέφτουν θύματα αυτής της ψυχολογικά καταστροφικής και πολυδάπανης εγκληματικής δραστηριότητας. Συγκεκριμένα, αυτό το είδος απάτης περιλαμβάνει την παράνομη χρήση τους για πλαστοπροσωπία σε εμπορικές κυρίως συναλλαγές. Το πιο χαρακτηριστικό παράδειγμα είναι η χρήση κινητού ή σταθερού τηλεφώνου, τραπεζική απάτη και πλαστά δάνεια.

Αν και η μεγαλύτερη οικονομική ζημιά πέφτει στους εκδότες των πιστωτικών καρτών και στις επιχειρήσεις, οι καταναλωτές ζημιώνονται καθόσον στους λογαριασμούς τους περιλαμβάνονται ψευδείς ή μη ακριβείς πληροφορίες. Αυτό μπορεί να οδηγήσει ακόμα και στην απόρριψη αιτήσεών τους για δανειοδότηση και έκδοση πιστωτικών καρτών. Η επίλυση τέτοιων

προβλημάτων μπορεί να εμπεριέχει και απώλεια σημαντικού χρόνου. Για τους παραπάνω λόγους μερικοί έχουν ονομάσει το αδίκημα αυτό ως «το αδίκημα της νέας χιλιετίας».[80]

Οι διατάξεις της παρούσας οδηγίας δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:

- η οποία πραγματοποιείται στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου, όπως οι δραστηριότητες που προβλέπονται στις διατάξεις των τίτλων V και VI της συνθήκης για την Ευρωπαϊκή Ένωση και, εν πάση περιπτώσει, στην επεξεργασία δεδομένων που αφορά τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης και της οικονομικής ευημερίας του, εφόσον η επεξεργασία αυτή συνδέεται με θέματα ασφάλειας του κράτους) και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου,

- η οποία πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων.

Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει δυνάμει της παρούσας οδηγίας σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον:

α) η επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Όταν ο ίδιος υπεύθυνος είναι εγκατεστημένος στο έδαφος περισσοτέρων του ενός κρατών μελών, πρέπει να λαμβάνει τα αναγκαία μέτρα ώστε να εξασφαλίζεται ότι κάθε εγκατάστασή του πληροί τις απαιτήσεις που προβλέπει η εφαρμοστέα εθνική νομοθεσία 7

β) ο υπεύθυνος δεν είναι εγκατεστημένος στο έδαφος του κράτους μέλους, αλλά σε τόπο όπου εφαρμόζεται η εθνική του νομοθεσία δυνάμει του δημοσίου διεθνούς δικαίου 7

γ) ο υπεύθυνος της επεξεργασίας δεν είναι εγκατεστημένος στο έδαφος της Κοινότητας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στο έδαφος του εν λόγω κράτους μέλους, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από το έδαφος της Ευρωπαϊκής Κοινότητας.

2. Στην περίπτωση που αναφέρεται στην παράγραφο 1 στοιχείο γ), ο υπεύθυνος της επεξεργασίας πρέπει να υποδείξει έναν αντιπρόσωπο εγκατεστημένο στο έδαφος του εν λόγω κράτους μέλους. Δεν θίγεται η τυχόν ανάληψη νομικών ενεργειών κατά του ιδίου του υπευθύνου της επεξεργασίας.

[80] Alan Charles Raul,Privacy and the Digital State Balancing public Information and Personal Privacy , Kluwer Academic Publishers,2001 σελ 1

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΗΣ ΝΟΜΙΜΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Τα κράτη μέλη προβλέπουν ότι επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται μόνον εάν:

- το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή
- είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων αιτήσει του ή
- είναι απαραίτητη για την τήρηση εκ του νόμου υποχρεώσεως του υπευθύνου της επεξεργασίας ή
- είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα ή
- είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση δημοσίας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας ή στον τρίτο στον οποίο ανακοινώνονται τα δεδομένα ή
- είναι απαραίτητη για την επίτευξη του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα, υπό τον όρο ότι δεν προέχει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο οποίο αναφέρονται τα δεδομένα που χρήζουν προστασίας δυνάμει του άρθρου 1 παράγραφος 1 της παρούσας οδηγίας.

Ενημέρωση σε περίπτωση συλλογής δεδομένων όχι από το πρόσωπο στο οποίο αναφέρονται

1. Όταν τα δεδομένα δεν έχουν συλλεγεί από το πρόσωπο το οποίο αφορούν, τα κράτη μέλη προβλέπουν ότι, ευθύς ως καταχωρηθούν τα δεδομένα ή, εάν προβλέπεται ανακοίνωσή τους σε τρίτους, το αργότερο κατά την πρώτη ανακοίνωσή τους, ο υπεύθυνος της επεξεργασίας ή ο εκπρόσωπός του πρέπει να παρέχει στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα τις εξής πληροφορίες, εκτός εάν το πρόσωπο αυτό έχει ήδη ενημερωθεί:

α) την ταυτότητα του υπευθύνου της επεξεργασίας και, ενδεχομένως, του εκπροσώπου του

β) τους σκοπούς της επεξεργασίας

γ) οποιαδήποτε περαιτέρω πληροφορία, όπως:

- τις κατηγορίες των σχετικών δεδομένων,

- τους αποδέκτες ή τις κατηγορίες αποδεκτών,

- την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα που το αφορούν και δικαιώματος διόρθωσής τους,

εφόσον οι πληροφορίες αυτές είναι αναγκαίες, λόγω των ειδικών συνθηκών υπό τις οποίες συλλέγονται τα δεδομένα, ώστε να εξασφαλίζεται θεμιτή επεξεργασία, έναντι του προσώπου στο οποίο αναφέρονται τα δεδομένα.

2. Οι διατάξεις της παραγράφου 1 δεν εφαρμόζονται όταν, ιδίως όσον αφορά την επεξεργασία για σκοπούς στατιστικούς ή ιστορικής ή επιστημονικής έρευνας, η ενημέρωση του ενδιαφερομένου αποδεικνύεται αδύνατη ή προϋποθέτει δυσανάλογες προσπάθειες ή εάν η καταχώρηση ή η ανακοίνωση επιβάλλεται ρητώς από το νόμο. Στις περιπτώσεις αυτές, τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις.

Εξαιρέσεις και περιορισμοί

1. Τα κράτη μέλη μπορούν να περιορίζουν με νομοθετικά μέτρα την εμβέλεια των υποχρεώσεων και δικαιωμάτων που προβλέπονται από τις διατάξεις του άρθρου 6 παράγραφος 1, του άρθρου 10, του άρθρου 11 παράγραφος 1 και των άρθρων 12 και 21, όταν ο περιορισμός αυτός απαιτείται για τη διαφύλαξη:

α) της ασφάλειας του κράτους

β) της άμυνας

γ) της δημόσιας ασφάλειας

δ) της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης παραβάσεων του ποινικού νόμου ή της δεοντολογίας των νομοθετικά κατοχυρωμένων επαγγελμάτων

ε) σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος κράτους μέλους ή της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων

στ) αποστολής ελέγχου, επιθεώρησης ή ρυθμιστικών καθηκόντων που συνδέονται, έστω και ευκαιριακά, με την άσκηση δημόσιας εξουσίας στις περιπτώσεις που αναφέρονται στα στοιχεία γ), δ) και ε) 7

ζ) της προστασίας του προσώπου στο οποίο αναφέρονται τα δεδομένα ή των δικαιωμάτων και ελευθεριών άλλων προσώπων.

2. Υπό την επιφύλαξη των προσφόρων νομικών εγγυήσεων, και ιδίως εκείνων που ορίζουν ότι τα δεδομένα δεν επιτρέπεται να χρησιμοποιηθούν για μέτρα ή αποφάσεις που ανάγονται σε συγκεκριμένα πρόσωπα, τα κράτη μέλη μπορούν, ιδίως στην περίπτωση που σαφώς ελλείπει κάθε κίνδυνος να θιγεί η ιδιωτική ζωή του προσώπου που αφορούν, να περιορίζουν νομοθετικώς τα δικαιώματα εκ του άρθρου 12 όταν η επεξεργασία δεδομένων γίνεται αποκλειστικά για επιστημονική έρευνα ή όταν αποθηκεύονται υπό μορφή στοιχείων προσωπικού χαρακτήρα επί διάστημα που δεν υπερβαίνει το αναγκαίο προς κατάρτιση στατιστικών και μόνο.

ΑΠΟΡΡΗΤΟ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Απόρρητο της επεξεργασίας

Κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου της επεξεργασίας ή του εκτελούντος την επεξεργασία, περιλαμβανομένου του ιδίου του εκτελούντος την επεξεργασία, και έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, μπορεί να τα επεξεργασθεί μόνο κατ' εντολή του υπευθύνου της επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το νόμο

Ασφάλεια της επεξεργασίας

1. Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσων δικτύου, και από κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Τα μέτρα αυτά πρέπει να εξασφαλίζουν, λαμβανομένης υπόψη της τεχνολογικής εξέλιξης και του κόστους εφαρμογής τους, επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας.

2. Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας οφείλει, σε περίπτωση επεξεργασίας για λογαριασμό του, να επιλέγει προς εκτέλεση της επεξεργασίας πρόσωπο το οποίο παρέχει επαρκείς εγγυήσεις όσον αφορά τα μέτρα τεχνικής ασφάλειας και οργάνωσης της επεξεργασίας και να εξασφαλίζει την τήρηση των μέτρων αυτών.

3. Η εκτέλεση επεξεργασίας μέσω άλλου προσώπου πρέπει να διέπεται από σύμβαση ή δικαιοπραξία που συνδέει τον εκτελούντα με τον υπεύθυνο της επεξεργασίας και προβλέπει ιδίως:

- ότι ο εκτελών την επεξεργασία ενεργεί μόνον κατ'εντολήν του υπευθύνου της επεξεργασίας,

- ότι οι υποχρεώσεις που προβλέπονται στην παράγραφο 1, όπως ορίζονται από τη νομοθεσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκτελών την επεξεργασία, βαρύνουν και τον εκτελούντα την επεξεργασία.

4. Για αποδεικτικούς λόγους, τα τμήματα της σύμβασης ή δικαιοπραξίας που αφορούν την προστασία των δεδομένων και τις απαιτήσεις σχετικά με τα μέτρα που προβλέπονται στην παράγραφο 1 καταρτίζονται εγγράφως ή σε άλλη ανάλογη μορφή.

2.13 Προστασία Προσωπικών Δεδομένων στην Ελλάδα

Στην Ελλάδα τα προσωπικά δεδομένα και η προσωπική ζωή προστατεύονται στο Σύνταγμα από τα άρθρα 2(1) περί σεβασμού της ανθρώπινης αξιοπρέπειας, 5 Σ περί προστασίας της προσωπικότητας , 5 Α Σ περί του δικαιώματος στην πληροφόρηση, 7 (2) Σ περί προσβολής ανθρώπινης αξιοπρέπειας , 9 Σ προστασίας της ιδιωτικής ζωής , 9 Α Σ περί προστασίας προσωπικών δεδομένων και 19 Σ προστασία της αλληλογραφίας. Στο ιδιωτικό δίκαιο προστατεύεται από τις διατάξεις 57-60 ΑΚ περί προσωπικότητας και 281 ΑΚ για την προστασία των χρηστών αλλά και 330, 914,919, 920 και 932 περί συμβατικής υποχρέωσης και αδικοπρακτικής ευθύνης.

Παράλληλα, προστατεύονται από τα άρθρα 361-5 και 367 του Ποινικού Κώδικα αλλά και το άρθρο 370 του Ν 1805/1988 σχετικά με την διάπραξη εγκλημάτων στον κυβερνοχώρο. Επίσης, βρίσκουν εφαρμογή οι νόμοι μέσων μαζικής ενημέρωσης 1730/1987, για την προστασία της ιδιωτικής ζωής από την ΕΡΤ, οι Ν 2238/1995 και Ν 2644/1998 αλλά και η ενσωματωμένη ευρωπαϊκή οδηγία 89/552, ο Ν 2225/1994 για την μυστικότητα στις τηλεπικοινωνίες όπως και ο Ν 2246/1994. Ο πιο σημαντικός νόμος για την προστασία προσωπικών δεδομένων είναι ο Ν 2472/1997 ο οποίος ενσωμάτωσε την οδηγία 95/46. Τέλος, προστατεύονται από τα άρθρα 13 και 14 του Ν 146/1914 περί αθέμιτου ανταγωνισμού για την προστασία σημάτων και διακριτικών γνωρισμάτων.

[81]Η νέα διάταξη του άρθρου 9 ΑΣ γειτονιάζει με το άρθρο 9 που αναγορεύει τον ιδιωτικό βίο σε απόλυτα απαραβίαστο συνταγματικό αγαθό και υποδηλώνει την προσέγγιση ενός νέου δικαιώματος ως αμυντικού δικαιώματος. Η νέα συνταγματική διάταξη καλύπτει κάθε δεδομένο και όχι μόνο τα απόρρητα και αποδεσμεύει την συνταγματική προστασία από την αναζήτηση του περιεχομένου της πληροφορίας.

[82]Η προστασία των προσωπικών δεδομένων στρέφεται όχι μόνο κατά κράτους αλλά και κατά των ιδιωτών εξασφαλίζοντας την τριτενέργεια του δικαιώματος. Πριν την κατοχύρωση του δικαιώματος στο Σύνταγμα η τριτενέργεια γινόταν δεκτή καθώς υπαγορευόταν από το διφυή χαρακτήρα των διατάξεων 2 παρ. 1 και 5 ως δικαιωμάτων αλλά και από την επεκτεινόμενη χρήση επεξεργασίας προσωπικών δεδομένων στον ιδιωτικό τομέα.[83]

Στην Ελλάδα βασικός νόμος προστασίας των προσωπικών δεδομένων είναι ο Ν 2472/1997 ο οποίος ενσωμάτωσε στην ελληνική έννομη τάξη την αντίστοιχη ευρωπαϊκή οδηγία. Βασικό δικαίωμα ενημέρωσης κατά το στάδιο συλλογής των δεδομένων από τον υπεύθυνο της επεξεργασίας και το δικαίωμα συγκατάθεσης του υποκειμένου[84].

---

[82] Λ.Μήτρου, Προστασία Προσωπικών Δεδομένων: Ένα νέο δικαίωμα το Νέο Σύνταγμα Πρακτικά Συνεδρίου για το Αναθεωρημένο Σύνταγμα του 2001 εκδ, Σάκκουλα 2001, σελ, 94.

[83] Λ.Μήτρου Προστασία Προσωπικών δεδομένων σελ.96-97

[84] Άρθρο 11Δικαίωμα ενημέρωσης

2.14 Κανονισμοί Α.Δ.Α.Ε.

[85]Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών έχει σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών.

Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαύει διοικητικής αυτοτέλειας. Έδρα της είναι η Αθήνα, μπορεί όμως με απόφασή της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της ΑΔΑΕ κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους υποβάλλεται Έκθεση των πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο. Η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον Κανονισμό της Βουλής.

Η ΑΔΑΕ για την εκπλήρωση της αποστολής της έχεις τις εξής αρμοδιότητες:

- Διενέργεια αυτεπάγγελτων ελέγχων σε επιχειρήσεις και υπηρεσίες που έχουν γενικό αντικείμενο την επικοινωνία.
- Κατάσχεση ψηφιακών πειστηρίων , καταστροφή στοιχείων που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών .

- Ο υπεύθυνος επεξεργασίας οφείλει , κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα , να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής στοιχεία

  Την ταυτότητα και την ταυτότητα του τυχόν εκπροσώπου

  Τον σκοπό της επεξεργασίας

  Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων

  Την ύπαρξη του δικαιώματος πρόσβασης
- Εάν για την συλλογή των δεδομένων προσωπικού χαρακτήρα ο υπεύθυνος επεξεργασίας ζητεί την συνδρομή του υποκειμένου, οφείλει να το ενημερώνει ειδικώς και εγγράφως για τα στοιχεία της παρ. 1 του παρόντος άρθρου καθώς και για τα δικαιώματα, σύμφωνα με τα άρθρα 11 έως και 13 του παρόντος νόμου., Με την αυτή ενημέρωση ο υπεύθυνος επεξεργασίας γνωστοποίει στο υποκείμενο εάν υποχρεούται ή όχι να παράσχει την συνδρομή του, με βάση ποιες διατάξεις, καθώς και για τις τυχόν συνέπειες της αρνήσεως του
- Εάν τα δεδομένα ανακοινώνονται σε τρίτους , το υποκείμενο ενημερώνεται για την ανακοίνωση πριν από αυτούς.
-

[85] Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) (2006), «Κανονισμός για την Διασφάλιση του Απορρήτου Δικτυακών Υποδομών»

- Εξέταση καταγγελιών σχετικά με την προστασία των δικαιωμάτων των αιτούντων
- Συνεργασία με άλλες αρχές της χώρας και με αντίστοιχες αρχές άλλων κρατών , για θέματα ασφάλειας επικοινωνιών
- Έκδοση κανονισμού εσωτερικής λειτουργίας ο οποίος δημοσιεύεται στην Εφημερίδα της Κυβερνήσεως.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

3.1 Ορισμός Εγκλήματος

[86]Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει πολλές επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

Ως έγκλημα μπορεί να νοηθεί κάθε ενέργεια που παρεκκλίνει από αποδεκτούς κοινωνικούς κανόνες. Σύμφωνα, με τον Γάλλο κοινωνιολόγο Durkheim “Το έγκλημα υπάρχει σε όλες τις κοινωνίες.[87] Δεν υπάρχει κοινωνία η οποία δεν αντιμετωπίζει το πρόβλημα της εγκληματικότητας. Εκείνο που αλλάζει είναι η μορφή του . Έτσι οι πράξεις που παίρνουν τον χαρακτηρισμό αυτό δεν είναι παντού οι ίδιες, θα υπάρχουν όμως παντού και πάντοτε άνθρωποι των οποίων η συμπεριφορά θα επισύρει ποινικές κυρώσεις σε βάρος τους. Άπλα, λοιπόν εκείνο το οποίο θα πρέπει να θεωρηθεί σαν κάτι το φυσιολογικό είναι η ύπαρξη της [88]εγκληματικότητας.»

[89]Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που

[88] Τσουραμάνης Χ.(2003) Σύγχρονα κοινωνικά προβλήματα .Η ελληνική πραγματικότητα. Αθήνα Παπαζήσης, σελ 110.

[89] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύο.

Υιοθετώντας μια τριπλή προσέγγιση (Αγγέλης, 2000) που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- ✓ μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
- ✓ μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- ✓ μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: [90] *e-crime, cybercrime, computer-crime, internet related crime και hitech-crime* είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι *ηλεκτρονικό έγκλημα*, *δικτυακό έγκλημα* και *έγκλημα του κυβερνοχώρου*. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

3.2 Η Συνθήκη της Βουδαπέστης

Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής[91]. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23.11.2001. Στη Συνθήκη της Βουδαπέστης, υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα Ηλεκτρονικά Εγκλήματα.

[91] http://www.e-crime.gr/crime.htm

3.3 Μορφές Κυβερνοεγκλήματος

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime... and Punishment?» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα κατηγορίες[92]:

- Παρεμπόδιση (κυβερνο)κυκλοφορίας,
- Τροποποίηση και Κλοπή δεδομένων,
- Εισβολή και Σαμποτάζ σε δίκτυο,
- Μη εξουσιοδοτημένη πρόσβαση,
- Διασπορά ιών,
- Υπόθαλψη αδικημάτων,
- Πλαστογραφία
- Απάτη. Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ

[92] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&lte

- ✓ ΑΠΆΤΕΣ ΜΈΣΩ ΔΙΑΔΙΚΤΎΟΥ
- ✓ ΠΑΙΔΙΚΉ ΠΟΡΝΟΓΡΑΦΊΑ
- ✓ CRACKING ΚΑΙ HACKING
- ✓ ΔΙΑΚΊΝΗΣΗ-ΠΕΙΡΑΤΕΊΑ ΛΟΓΙΣΜΙΚΟΎ
- ✓ ΠΙΣΤΩΤΙΚΈΣ ΚΆΡΤΕΣ
- ✓ ΔΙΑΚΊΝΗΣΗ ΝΑΡΚΩΤΙΚΏΝ
- ✓ ΈΓΚΛΗΜΑ ΣΤΑ CHAT ROOMS

Ελληνική νομοθεσία

Ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) και στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.

Στην ελληνική νομοθεσία όμως, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων[93].

Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τελεία αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Άρθρο 370Β

[93] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.

Άρθρο 370Γ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386[Α]

- Απάτη με υπολογιστή - Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

Νομοθεσία διαδικτυακών εγκλημάτων στην αλλοδαπή

[94]Στην Αγγλία από τον Φεβρουάριο του 2001, οι hacker, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες.

Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

3.4 Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

- Το έγκλημα στον [95]Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

- Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά...

- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.

- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.

- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (news groups) ή μέσα σε chat rooms.

- Οι "εγκληματίες του Κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα , αποστέλλουν ηλεκτρονικά μηνύματα(e-mail) με ψευδή στοιχεία.

[94] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&lte

[95] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&lte

- Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.

- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες..

- Η έρευνα απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι σπάνια.

- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», από ότι στον «κοινό» εγκληματικό χώρο.

3.5 Διαδικτυακά Εγκλήματα

Το έγκλημα είναι ένα αναπόσπαστο κομμάτι κάθε κοινωνίας και συμπεριφέρεται σαν ένας ζωντανός οργανισμός που διαρκώς μεταβάλλονται οι μορφές, τα μέσα διάπραξης καθώς και η νομοθεσία που το διέπει . Με διαφορετικό περιτύλιγμα αλλά και ουσία πολλές φορές, ανάλογα με τις πολιτικές , κοινωνικές, και ηθικές τάσεις κάθε εποχής έγκλημα , παραμένει παρόν, κινούμενο πάντα σε τρείς άξονες , τα απαραίτητα συστατικά στοιχεία του, αυτά που το ορίζουν. Ποια είναι αυτά όμως τα στοιχεία; Το εγκληματικό φαινόμενο εμφανίζεται στον κοινωνικό χώρο ως σύνθεση των παρακάτω στοιχείων που εμφανίζονται στον πίνακα[96];

Πίνακας: Βασικά στοιχεία του εγκλήματος

Κοινωνικό αγαθό	**Προσβολή κοινωνικού Αγαθού**	**Αντίδραση στην προσβολή**

[96] Μανωλεδάκης Ι.»Ποινικό Δίκαιο» , ζ΄ έκδοση , εκδόσεις Σακκούλα, 2005

Α) Υλικό αντικείμενο, φυσική ιδιότητα υλικού αντικειμένου ή κοινωνική ιδιότητα υλικού αντικειμένου + Β) Ουσιώδες συμφέρον ατομικό ή συλλογικό για την διατήρηση του.	Συμπεριφορά που θίγει την ύλη ή αναιρεί ή αλλοιώνει τις φυσικές ή κοινωνικές ιδιότητες των κοινωνικών αγαθών.	Οργανωμένη κοινωνική αντίδραση με προσβολή αγαθών του δράστη και έντονα στοιχεία αποδοκιμασίας και στιγματισμού.

Το εγκληματικό φαινόμενο αποτελεί ιστορικό, κοινωνικό φαινόμενο , καθώς ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Έτσι τα επιμέρους χαρακτηριστικά του (κοινωνικά αγαθά, έγκλημα, ποινή) έχουν και αυτά ιστορικότητα, δηλαδή σχετικότητα, διαφοροποιούμενα από τόπο σε τόπο και από εποχή σε εποχή [97] . Υπάρχουν άνθρωποι οι οποίοι παραβαίνουν τους κοινωνικούς κανόνες, αυτούς που θεσπίστηκαν τυπικά ή άτυπα προκειμένου να διαφυλαχθούν τα κοινωνικά αγαθά. Αποτέλεσμα της προσβολής αυτών των αγαθών είναι η επιβολή διαφόρων κυρώσεων στους παραβάτες.

Η επιβληθείσα κύρωση ή αλλιώς ποινή, θα μπορούσαμε να πούμε , ότι αποτελεί τον τρόπο αντίδρασης της κοινωνίας στο έγκλημα. Η αντίδραση, καθώς και το είδος της ποινής, απευθύνεται στον παραβάτη των κοινωνικών κανόνων και βρίσκονται πάντα σε στενή εξάρτηση με την εκάστοτε εποχή και πολιτισμό. Το έγκλημα είναι αναμενόμενο, στα πλαίσια της κοινωνικής πραγματικότητας. Είναι το εμφανές σύμπτωμα της κοινωνικής κρίσης, της διάρρηξης του κοινωνικού ιστού, το βαθύ σημάδι μιας κοινωνίας που γερνά [98].

Τα βασικά στοιχεία του εγκληματικού φαινομένου, κανόνας, έγκλημα, κύρωση συναποτελούν έναν αδιάσπαστο κύκλο. Εδώ είναι ξεκάθαρη η αλληλεξάρτηση των στοιχείων αν δεν υπήρχε έγκλημα δεν θα υφίστατο κύρωση. Η μη ύπαρξη κανόνα δεν καθιστά δυνατή την παράβαση του. Ο κανόνας δημιουργήθηκε για να οργανώσει και να προστατέψει τα κοινωνικά αγαθά (υλικά και άυλα) από κάθε προσβολή μέσα στα πλαίσια της κοινωνικής συμβίωσης. Έπειτα και αφού επέλθει η προσβολή του έννομου αγαθού (αυτού που προστατεύεται από τον κανόνα-νόμο) έρχεται η κύρωση(ποινή).Είναι με λίγα λόγια η κύρωση συνέπεια της παράβασης του κανόνα και δηλώνει προς αυτόν που επιβάλλεται ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία.

[97] Βλ. Πιπερόπουλος Γ.»κοινωνικά προβλήματα» εκδόσεις Ελληνικά Γράμματα, 1998

[98] Βλ.Πιπερόπουλος Γ.»κοινωνικά προβλήματα» εκδόσεις Ελληνικά Γράμματα, 1998

[99]Νέες μορφές εγκληματικών πράξεων δεν εμφανίζονται συχνά στην πορεία της ανθρώπινης ιστορίας. Ωστόσο, τον 21ο αιώνα με αφορμή την ανακάλυψη και τη χρήση του Διαδικτύου **ένα νέο είδος εγκλήματος άρχισε να εμφανίζεται και να λαμβάνει ανησυχητικές διαστάσεις**, το ονομαζόμενο διαδικτυακό έγκλημα (cybercrime- internet crime). Είναι γεγονός ότι ένας μεγάλος αριθμός ανθρώπων έχει πρόσβαση στο Διαδίκτυο μέσω του οποίου εκτελεί μια σειρά δραστηριοτήτων, όπως αγορά προϊόντων, ειδησεογραφική ενημέρωση, ανταλλαγή πληροφοριών, διαφήμιση, κ.τ.λ.

Η μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο, είναι το διαδίκτυο το οποίο είναι ανοιχτό τόσο στους καλόβουλους όσο και στους κακόβουλους επισκέπτες. Ο πληθυσμός του internet, αν και έχει δεχτεί κατά καιρούς πολλές παραβιάσεις και παρενοχλήσεις όσον αφορά την ασφάλεια των συστημάτων και την κλοπή δεδομένων, δεν έχει υιοθετήσει μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια με αποτέλεσμα ολοένα και περισσότεροι χρήστες να βρίσκονται σε σύγχυση. Η ανασφάλεια που συνδέεται με τη χρήση του Διαδικτύου φαίνεται από το γεγονός ότι **το 70% των ατόμων που χρησιμοποιεί το διαδίκτυο πιστεύει ότι είναι πιο πιθανό να πέσει θύμα διαδικτυακού εγκλήματος**(π.χ. κλοπή πιστωτικής κάρτας) από ότι κάποιας άλλης μορφής εγκλήματος (Reisig, et. al., 2009). Η διαδικτυακή παρενόχληση και η υποκλοπή προσωπικών είναι μια εξελισσόμενη «μόδα». Οι χρήστες του διαδικτύου πρέπει να είναι πολλοί προσεκτικοί στην ανάγνωση όλων των μηνυμάτων που εμφανίζονται στον υπολογιστή. Πολλές φορές κατά την πλοήγηση ανοίγουν , χωρίς να το προκαλέσει ο χρήστης, παράθυρα των οποίο το περιεχόμενο ποικίλει:

- Δωρεές.
- Διαφημίσεις.
- Κάλεσμα για παιχνίδια είτε κανονικά είτε τυχερά.

Η ενδεδειγμένη ενέργεια είναι να κλείσουν άμεσα αυτά τα παράθυρα.

Συμπερασματικά, πρόκειται για μια μορφή απάτης που δεν στοχεύει την «τσέπη» του θύματος καταναλωτή, αλλά στην κλοπή των προσωπικών του δεδομένων και την χρήση τους από τρίτους στο διαδίκτυο. Η απάτη αυτή εμφανίζεται κυρίως:

- Στην ηλεκτρονική αλληλογραφία (e-mail)
- Στην απόσπαση προσωπικών στοιχείων (ψάρεμα) (phishing)
- Στην ανακατεύθυνση του browser σε πλαστογραφημένες wb pages (Pharming)
- Στις ψεύτικες αγγελίες για την ανεύρεση εργασιακής απασχόλησης (Scam)
- Στις λίστες καταχωρίσεων (ιστολόγια) Blogs
- Στα κανάλια συζητήσεων (Chat room)
- Στο διαμοιρασμό αρχείων μέσα από το διαδίκτυο (File sharing)

[99] http://e-psychology.gr/forensic-psychology/434-internet-crimes

Κατερίνα Γερολύμπου

Μέτρα προστασίας

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι.

Κατά προτίμηση, ο χρήστης που εισέρχεται στο Διαδίκτυο από dial up σύνδεση θα πρέπει να κλείνει με κωδικό που θα προμηθευτεί από τον Ο.Τ.Ε τις εξερχόμενες διεθνείς κλήσεις, καθόσον υπάρχει ο κίνδυνος του dialer (κώδικας που συνδέει τον η/υ του χρήστη σε I.S.P της αλλοδαπής με αποτέλεσμα την υπερβολική τηλεφωνική χρέωση του). Επίσης, ο χρήστης θα πρέπει να έχει εγκαταστήσει προγράμματα για την προστασία από ιούς και ηλεκτρονικές επιθέσεις.

Κίνδυνοι για τα παιδιά

- [100]Τα παιδιά μπορούν να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο.
- Τα παιδιά μπορούν να έρθουν σε επαφή με αγνώστους που μπορούν να τα βλάψουν.
- Τα παιδιά υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο Διαδίκτυο.
- Τα παιδιά μπορούν να εθιστούν στη χρήση του Διαδικτύου και έτσι κινδυνεύουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις, τα παιχνίδια τους με φίλους.

Συμβουλές για τα παιδιά

- Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο Διαδίκτυο.
- Πάντα να μιλάτε στους γονείς σας ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο Διαδίκτυο και σας ανησυχούν ή σας φοβίζουν.
- Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνση σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνο σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο Διαδίκτυο ακόμη και αν σας το ζητήσουν.
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν.

[100] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

- Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συμφωνήσετε να συναντήσετε κάποιον/κάποια που γνωρίσατε στο Διαδίκτυο.
- Προσέχετε όταν μιλάτε διαμέσου chatroom ή e-mail. Διακόψτε τη συνομιλία όταν κάποιοι σας κάνουν να νιώθετε άβολα.
- Μην εμπιστεύεστε ότι διαβάζετε στο Διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.

Συμβουλές για τους γονείς

- Κρατήστε τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το Διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον Κυβερνοχώρο και μάθετε από αυτά.
- Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους.
- Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms (δωμάτια συνομιλίας), χωρίς την επίβλεψη σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του Διαδικτύου χωρίς να είστε και εσείς μαζί.
- Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.
- Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου.
- Συζητήστε με τα παιδιά σας για την ασφάλεια του Διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του Διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.
- Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο

3.6 Ασφαλής Αναζήτηση στο Διαδίκτυο

Η τεράστια δεξαμενή πληροφοριών και εργαλείων του Διαδικτύου είναι διάσπαρτη σε δισεκατομμύρια ιστοσελίδες που πρακτικά είναι αδύνατον να ερευνηθούν από τον χρήστη χωρίς τη βοήθεια εξειδικευμένων προγραμμάτων, όπως οι μηχανές αναζήτησης. Οι μηχανές αναζήτησης χρησιμοποιούν ειδικά προγράμματα, τις λεγόμενες αράχνες (spiders), τα οποία «χτενίζουν» τις ιστοσελίδες αναζητώντας τα κείμενα και τις διευθύνσεις τους. Τα κείμενα και οι διευθύνσεις τους συγκεντρώνονται και καταγράφονται. Με άλλα προγράμματα συγκεντρώνονται πληροφορίες από τα κείμενα, το είδος των οποίων ποικίλει από μηχανή σε μηχανή, και αποθηκεύονται σε βάσεις δεδομένων, ώστε να είναι εύκολο να ανακτηθούν[101].

[101] [101] http://www2.e-yliko.gr/htmls/safety/ssearch.aspx

- Ασφάλεια Στην ηλεκτρονική αλληλογραφία (E-mail)

[102] Η ηλεκτρονική αλληλογραφία είναι η πιο δημοφιλής από τις υπηρεσίες του Διαδικτύου. Είναι μια μορφή επικοινωνίας η οποία επιτρέπει στους χρήστες του Διαδικτύου που έχουν **ηλεκτρονική διεύθυνση** (**e-mail address**) να στείλουν ένα μήνυμα σε άλλους χρήστες, με τρόπο που μοιάζει με αυτόν του κλασικού ταχυδρομείου. Κάθε μήνυμα χαρακτηρίζεται από την ηλεκτρονική διεύθυνση του αποστολέα, το περιεχόμενο (που μπορεί να είναι απλό κείμενο, εικόνα, επισυναπτόμενο αρχείο κ.ά.), και την ηλεκτρονική διεύθυνση του παραλήπτη. Τα μηνύματα φυλάσσονται σε ηλεκτρονικά γραμματοκιβώτια (**mailboxes**) μέχρι την ανάκτησή τους.

Η αποστολή των μηνυμάτων γίνεται με χρήση ενός πρωτοκόλλου μεταφοράς πληροφορίας του Διαδικτύου, του **Simple Mail Transfer Protocol** (**SMTP**). Το πρωτόκολλο SMTP επιτρέπει την μεταφορά μηνυμάτων από έναν **Εξυπηρετητή Ηλεκτρονικού Ταχυδρομείου** (**Mail Server**) του Διαδικτύου σε έναν άλλον. Κάθε μήνυμα έχει μια **επικεφαλίδα** (**header**) που χρησιμοποιείται για την αναγνώριση της ηλεκτρονικής διεύθυνσης του παραλήπτη, την ηλεκτρονική διεύθυνση και το όνομα του αποστολέα, και λεπτομέρειες για τους κόμβους από τους οποίους θα περάσει το μήνυμα μέσα στο δίκτυο για να φτάσει στον προορισμό του.

Η ανάκτηση των μηνυμάτων από τον Εξυπηρετητή γίνεται με χρήση του πρωτοκόλλου **Post Office Protocol** (**POP**). Η έκδοση 3 του POP (POP3) χρησιμοποιείται από τα περισσότερα προγράμματα διαχείρισης της ηλεκτρονικής αλληλογραφίας, τους **e-mail Clients**. Ο e-mail Client δημιουργεί ένα γραμματοκιβώτιο (**Inbox**) στον υπολογιστή του χρήστη, και όταν αυτός συνδέεται με τον Εξυπηρετητή Ηλεκτρονικού Ταχυδρομείου, τα μηνύματά του μεταφέρονται στο γραμματοκιβώτιο. Η ηλεκτρονική αλληλογραφία αποτελεί το συνηθέστερο τρόπο για την μετάδοση των ιών στα αρχεία και στα λογισμικά των υπολογιστών

Μερικά από τα σημαντικότερα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

Α) Οι ιοί

Β) Η ενοχλητική αλληλογραφία(spam mail)

Γ) Τα μηνύματα απατηλού περιεχομένου (hoaxes-phising)

Α) Ιοί

Ο ιός υπολογιστή είναι ένα μικρό πρόγραμμα λογισμικού που εξαπλώνεται από έναν υπολογιστή σε έναν άλλο και παρεμβαίνει στη λειτουργία των υπολογιστών. Ένας ιός υπολογιστή μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν υπολογιστή, να χρησιμοποιήσει ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου για να μεταδώσει τον ιό σε άλλους υπολογιστές ή ακόμα και να διαγράψει όλα τα δεδομένα στο σκληρό δίσκο.

[102] http://www.cnc.uom.gr/

Οι ιοί υπολογιστών διαδίδονται πιο εύκολα από τα συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μέσω άμεσων μηνυμάτων. Επομένως, δεν πρέπει να ανοίγετε ποτέ ένα συνημμένο ηλεκτρονικού ταχυδρομείου εκτός εάν γνωρίζετε τον αποστολέα του μηνύματος ή εκτός εάν αναμένετε το συνημμένο ηλεκτρονικού ταχυδρομείου. Οι ιοί υπολογιστών μπορεί να είναι μεταμφιεσμένοι ως συνημμένες αστείες εικόνες, ευχετήριες κάρτες ή αρχεία ήχου και βίντεο. Οι ιοί υπολογιστών μεταδίδονται επίσης χρησιμοποιώντας στοιχεία λήψης στο Internet. Οι ιοί υπολογιστών μπορεί να κρύβονται σε πειρατικό λογισμικό ή σε άλλα αρχεία ή προγράμματα που μπορεί να κατεβάσετε.

Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του email. Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (στο outlook express επιλέξτε Προβολή->Διάταξη->απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»).

Οι χρήστες θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Ακολουθούν ορισμένες βασικές ενδείξεις σύμφωνα με τις οποίες ένας υπολογιστής μπορεί να έχει προσβληθεί:

- Ο υπολογιστής λειτουργεί πιο αργά από ό, τι συνήθως
- Η λειτουργία του υπολογιστή σταματάει ή κλειδώνει συχνά.
- Ο υπολογιστής παρουσιάζει σφάλματα και μετά κάνει επανεκκίνηση κάθε λίγα λεπτά.
- Ο υπολογιστής επανεκκινεί μόνος του.. Επίσης, ο υπολογιστής δεν λειτουργεί όπως συνήθως.
- Δεν είναι δυνατή η σωστή εκτύπωση..
- Υπάρχει διπλή επέκταση σε ένα συνημμένο που ανοίξατε πρόσφατα, όπως επέκταση .jpg, .vbs, .gif ή .exe.
- Ένα πρόγραμμα προστασίας από ιούς έχει απενεργοποιηθεί χωρίς λόγο. Επιπλέον, δεν είναι δυνατή η επανεκκίνηση του προγράμματος προστασίας από ιούς

B) Ενοχλητική αλληλογραφία (spam email)

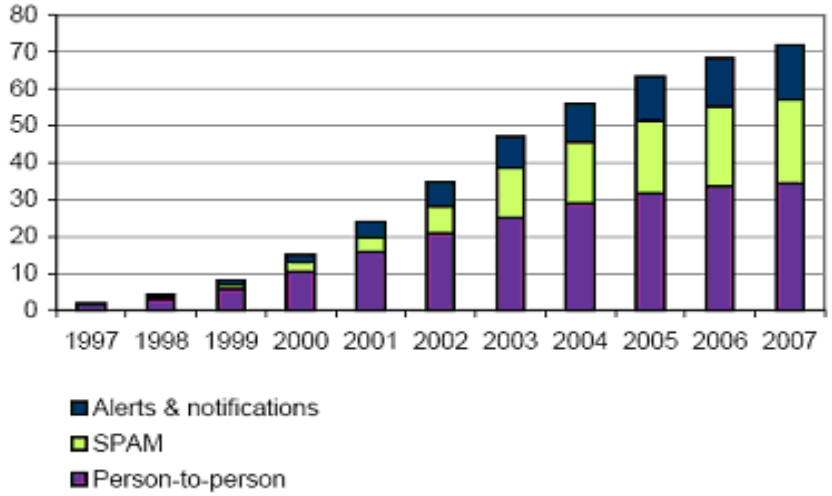
Η αποστολή και λήψη ηλεκτρονικής αλληλογραφίας (e-mail) αποτελεί ίσως την χρησιμότερη και πιο διαδεδομένη υπηρεσία του διαδικτύου. Κάθε χρήστης αυτής της υπηρεσίας αποκτά αργά ή γρήγορα την πρώτη του επαφή με το λεγόμενο «σπαμ» (spam). Πρόκειται συνήθως για μηνύματα εμπορικού περιεχομένου που στοχεύουν στη διαφήμιση κάποιου προϊόντος ή υπηρεσίας, τα οποία καταλήγουν στην ηλεκτρονική θυρίδα του παραλήπτη χωρίς ο τελευταίος να τα έχει ζητήσει ποτέ ή να γνωρίζει τον αποστολέα τους. Τα μηνύματα σπαμ, όμως, δεν περιορίζονται μόνο στην παρενοχλητική εμπορική επικοινωνία, καθώς πολλές φορές

διευκολύνουν απάτες, προσφέρουν πορνογραφικό υλικό ή εμπεριέχουν επικίνδυνα αρχεία, επιφυλάσσοντας δυσάρεστες εκπλήξεις και κινδύνους, ικανούς να ταλαιπωρήσουν τους έμπειρους χρήστες αλλά και να απογοητεύσουν τους νεόκοπους του κυβερνοχώρου[103].

ΤΟ ΜΕΛΛΟΝ ΤΟΥ SPAM

Η μέχρι σήμερα πορεία του φαινομένου δείχνει ότι το spam ετησίως αυξάνει και καταλαμβάνει ένα ιδιαίτερα μεγάλο ποσοστό της σημερινής ηλεκτρονικής αλληλογραφίας που κυμαίνεται από 20% έως και 70% σε κάποιες περιπτώσεις. Όσον αφορά το μέλλον του spam σύμφωνα με έρευνα της IDC η οποία αναπαριστάτε στο παρακάτω γράφημα το spam θα αυξάνεται σταδιακά αναλογικά με τον συνολικό αριθμό της ηλεκτρονικής αλληλογραφίας[104].

Αριθμός e-mails ανά ημέρα σε παγκόσμιο επίπεδο
(Διάφορες ειδοποιήσεις λαθών, Spam και προσωπική αλληλογραφία)



[103] http://e-pikaira.blogspot.

[104] http://www.no-spam.gr

Πολλά μηνύματα spam δεν είναι ούτε διαφήμιση, ούτε κάποιου είδους εμπορική πρόταση. Εκτός από την προσφορά αγαθών και υπηρεσιών, το spam μπορεί να περιλαμβάνει μεταξύ άλλων και τις ακόλουθες κατηγορίες:

- Μηνύματα πολιτικού περιεχομένου
- Οικονομικές απάτες
- Μηνύματα που προτρέπουν την προώθηση τους σε τρίτους (αλυσίδα)
- Μηνύματα που χρησιμοποιούνται για τη διάδοση κακόβουλου λογισμικού (malware)

Κίνδυνοι και τρόποι αυτοπροστασίας

Το spam δεν αποτελεί απλά ένα ενοχλητικό φαινόμενο, ικανό να καθυστερήσει ή και να εκνευρίσει το μέσο χρήστη του internet . Οι επιπτώσεις του γίνονται πολύ πιο κατανοητές όταν αποκτά περιεχόμενο ικανό να εξαπατήσει τον κοινό νου ή αρκετά επικίνδυνο για τη λειτουργία των ηλεκτρονικών υπολογιστών. Πολύ συχνά, λοιπόν, η μαζικές αποστολές e-mail εξυπηρετούν έμπειρους χάκερ προκειμένου να μεταδώσουν καταστρεπτικούς ιούς (Virus), προγράμματα-κατασκόπους (Spyware), δούρειους ίππους (Trojans), προγράμματα αυτόματης κλήσης (Diallers) κτλ. Τον ίδιο τρόπο χρησιμοποιούν επίσης και πολλά κυκλώματα που οργανώνουν ευφάνταστες απάτες και απευθύνονται σε χιλιάδες ανθρώπους με τη βοήθεια του διαδικτύου, προκειμένου να εκμεταλλευτούν την αφέλεια έστω και ενός. Το πιο χαρακτηριστικό παράδειγμα έως σήμερα αποτελεί η λεγόμενη απάτη του «νιγηριανού συνδέσμου» (Nigerian connection). Όταν πάλι στο πρόσωπο ενός κυβερνοπειρατή δεν απαντάται μόνο η ανάγκη επίδειξης γνώσης και υπεροχής αλλά υπερτερεί η ηθική ενός κοινού απατεώνα, οι συνέπειες για τον ανυποψίαστο χρήστη μπορεί να είναι απρόβλεπτες. Η υποκλοπή κωδικών τραπεζικών συναλλαγών ή αριθμών πιστωτικών καρτών αποτελούν την πιο ενδεικτική έκφραση του οικονομικού εγκλήματος στο διαδικτυακό περιβάλλον. Οι διαφορετικές αυτές μορφές κινδύνου της ψηφιακής πραγματικότητας, που υποβοηθούνται όλο και περισσότερο από τους μηχανισμούς του σπάμινγκ, χρήζουν εκτενέστερης ανάλυσης και θα αποτελέσουν αυτόνομο αντικείμενο της στήλης, ώστε να αποσαφηνιστούν κατά το δυνατόν οι πραγματικές τους διαστάσεις και να προκριθεί μια ψύχραιμη αντιμετώπιση.[105]

Κλείνοντας, είναι μάλλον χρήσιμη μια ανακεφαλαίωση, υπό μορφή πρακτικών οδηγιών για την αυτοπροστασία από το spam.

[105] http://e-pikaira.blogspot.

- Το σπαμ αφορά κάθε δικτυωμένο πολίτη. Δεν είναι πρόβλημα κάποιων άλλων.
- Αναγνωρίστε το σπαμ σε μηνύματα από άγνωστους αποστολείς και «υπερβολικά ελκυστικά» θέματα.
- Μην ανοίγετε τα μηνύματα σπαμ, απλά επιλέξτε διαγραφή.
- Μην απαντάτε σε μηνύματα σπαμ.
- Μην κάνετε κλικ σε ιστοσελίδες στις οποίες παραπέμπουν τα μηνύματα σπαμ.
- Μην προσπαθείτε να κάνετε “unsubscribe” ή “Opt out”.
- Προστατεύστε την ηλεκτρονική σας διεύθυνση από τη χρήση σε ύποπτους δικτυακούς τόπους, chat rooms, ομάδες συζήτησης κλπ.
- Δημιουργήστε επιπλέον ηλεκτρονικές διευθύνσεις μόνο για χρήση σε ιστοχώρους και υπηρεσίες που απαιτούν εγγραφή.
- Διαθέστε λίγο χρόνο για την επιλογή και τη ρύθμιση ενός φίλτρου ανεπιθύμητης αλληλογραφίας.

Το spam υποσκάπτει την εμπιστοσύνη των χρηστών ηλεκτρονικών υπηρεσιών και οδηγεί σε απώλεια χρόνου, πόρων και παραγωγικότητας, τόσο για τους ίδιους τους χρήστες, όσο και για τις επιχειρήσεις. Προβλήματα δημιουργεί επίσης και στους *Παρόχους Υπηρεσιών Διαδικτύου (ΠΥΔ)*, καθώς μπορεί να μειώσει την ποιότητα των παρεχόμενων υπηρεσιών και τον χρόνο απόκρισης του δικτύου τους, πλήττοντας έτσι τη διαθεσιμότητα και αξιοπιστία τους. Ενδεικτικά αναφέρεται ότι πάνω από το 70% των μηνυμάτων ηλεκτρονικού ταχυδρομείου σήμερα είναι spam.

Επιπλέον, τα μηνύματα spam, εκτός από ενοχλητικά, μπορεί να είναι προσβλητικά, απατηλά ή ακόμα και επικίνδυνου περιεχομένου. Για παράδειγμα αρκετά μηνύματα spam σήμερα διαφημίζουν πλαστά προϊόντα (π.χ. φαρμακευτικά προϊόντα ή προϊόντα λογισμικού) ως προϊόντα γνωστών εταιρειών, διαδίδουν παραπλανητικές ειδήσεις (όπως π.χ. σχετικά με τη "δύναμη" συγκεκριμένων μετοχών), ή/και προωθούν προϊόντα και υπηρεσίες σεξουαλικού ή/και πορνογραφικού χαρακτήρα.

Επίσης, τα μηνύματα spam χρησιμοποιούνται συχνά και ως μέσα μετάδοσης ιών ή άλλων επιβλαβών ή/και κατασκοπευτικών λογισμικών που σκοπεύουν στην "κατάληψη" του υπολογιστή του χρήστη (ή άλλως την μετατροπή του σε *zombie computer*) και την μετέπειτα χρήση του ως μέσο αποστολής νέων μηνυμάτων spam. Μεγάλη έκταση επίσης έχει πάρει το spam τύπου *phising* που στοχεύει στην παραπλάνηση των χρηστών και στην εκμαίευση

προσωπικών τους δεδομένων, συχνά με απώτερο σκοπό την απάτη και την απόσπαση χρηματικών ποσών μέσω τραπεζικών λογαριασμών.

[106]Το φαινόμενο του spamming είναι άμεσο συνδεδεμένο με την προσβολή των δεδομένων του προσωπικού χαρακτήρα καθώς η ηλεκτρονική διεύθυνση είναι από προσωπικό δεδομένο καθώς συνιστά μορφή ηλεκτρονικής υπογραφής. Ο ν.2472/1997 προβαίνει στην διάκριση των δεδομένων προσωπικού χαρακτήρα σε κοινά (απλά) και ευαίσθητα δεδομένα. Κοινά δεδομένα θεωρούνται οι πληροφορίες οι αναφερόμενες στο υποκείμενο των δεδομένων , δηλαδή στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα , ενώ ευαίσθητα θεωρούνται εκείνα που αφορούν την φυλετική ή εθνική προέλευση , στα πολιτικά φρονήματα, στις φυλετικές ή φιλοσοφικές πεποιθήσεις , στην συμμετοχή σε ένωση ,σωματείο και συνδικαλιστική οργάνωση , στην υγεία στην κοινωνική πρόνοια και στην ερωτική ζωή , καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες (άρθρο 8 της Οδηγίας 95/46/ΕΚ)

10 τρόποι να αποφύγετε το spam[107]:

1. Χρησιμοποιήστε το λιγότερο 2 ηλεκτρονικές διευθύνσεις (e-mail). Την μία θα πρέπει να την χρησιμοποιείτε αποκλειστικά και μόνο για την προσωπική σας αλληλογραφία, ενώ την δεύτερη (κοινόχρηστη) θα μπορείτε να την χρησιμοποιείτε σε δημόσια προσβάσιμες εφαρμογές, όπως για παράδειγμα καταχώρηση στοιχείων σε ομάδες συζητήσεων (forums), χώρους συζητήσεων (chat rooms), εγγραφές σε λίστες αλληλογραφίας κτλ
2. Μην δημοσιεύετε ποτέ το προσωπικό σας e-mail σε δημόσια προσβάσιμες εφαρμογές.
3. Χρησιμοποιείστε ως προσωπική σας διεύθυνση ένα συνδυασμό από το όνομα και το επίθετο σας αντί για απλά ονόματα που περιέχονται σε λεξικά π.χ. bill, mary. Οι αποστολείς spam χρησιμοποιούν συνδυασμούς ονομάτων, λέξεων και αριθμών για να δημιουργήσουν πιθανές διευθύνσεις.
4. Αν πρέπει οπωσδήποτε να κοινοποιήσετε το προσωπικό σας e-mail ηλεκτρονικά, καμουφλάρετε το, ώστε να δυσκολέψετε το έργο των spammers. Για παράδειγμα το Joe.Smith@yahoo.com, είναι εύκολο να βρεθεί από τις ειδικές μηχανές αναζήτησης (robots), όπως εύκολο είναι και το Joe.Smith at yahoo.com. Δοκιμάστε να το γράψετε Joe-dot-Smith-at-yahoo-dot-com. Επίσης αν πρέπει απαραίτητα να δημοσιεύσετε το προσωπικό σας e-mail σε κάποια ιστοσελίδα (το οποίο δεν συστήνεται), κάντε το ως αρχείο γραφικών ή εικόνα και όχι link.
5. Αντιμετωπίστε το «κοινόχρηστο» e-mail σας, ως προσωρινό. Οι πιθανότητες οι spammers να το βρουν είναι μεγάλες, συνεπώς μην διστάζετε να το αλλάζετε συχνά.
6. Να χρησιμοποιείτε πάντα το «κοινόχρηστο» e-mail για την καταχώρηση στοιχείων σε ομάδες συζητήσεων, χώρους συζητήσεων, για εγγραφή σε λίστες αλληλογραφίας. Επίσης θα μπορούσατε να χρησιμοποιείτε πολλές διαφορετικές «δημόσιες» (κοινόχρηστες) διευθύνσεις, ώστε να εντοπίσετε ποιες υπηρεσίες/ οργανισμοί, πωλούν διευθύνσεις σε spammers.
7. Μην απαντάτε ποτέ σε μηνύματα spam. Οι περισσότεροι spammers επαληθεύουν με τον τρόπο αυτό την λήψη της αλληλογραφίας και άρα την ύπαρξη της συγκεκριμένης

[106] Σινανίωτη-Μαρούδη /Φαρσαρώτα σελ.371 .ΔΕΕ 4/2001 σελ 377

[107] [107] http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=104

διεύθυνσης e-mail. Όσο περισσότερο απαντάτε, τόσο περισσότερη ανεπιθύμητη αλληλογραφία θα λαμβάνετε.

8. Μην επισκέπτεστε συνδέσμους με σκοπό την διαγραφή σας από μία λίστα στην οποία δεν θέλετε να ανήκετε, από ύποπτες/ αμφισβητήσιμες πηγές. Οι spammers στέλνουν τέτοια παραπλανητική αλληλογραφία, σε μία προσπάθεια να συλλέξουν ενεργές διευθύνσεις. Αν η διεύθυνση σας χαρακτηριστεί ως «ενεργή», θα αυξηθεί ο αριθμός των ανεπιθύμητων e-mail που λαμβάνετε.
9. Αν αντιληφθείτε πως το e-mail σας είναι γνωστό σε spammers, αλλάξτε το. Μπορεί να είναι άβολο/δύσκολο, αλλά είναι ένας τρόπος για να αποφύγετε το spam- έστω και για λίγο διάστημα.
10. Σιγουρευτείτε ότι το e-mail σας, φιλτράρεται από κατάλληλο λογισμικό anti-spam. Μπορείτε επίσης να εγκαταστήσετε στον υπολογιστή σας, κάποιο λογισμικό προστασίας από spam.

Γ) Μηνύματα απατηλού περιεχομένου (hoaxes)

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:

1.Προειδοποιητικά: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα

2.Συμπαράστασης: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται.

3.Εκφοβισμού: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου,

καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως. Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος.

Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

3.7 Προστασία προσωπικών δεδομένων

[108]Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού email . Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail , οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

- Στις ηλεκτρονικές συναλλαγές με τις τράπεζες (phishing)

[109]Το ηλεκτρονικό "ψάρεμα" (phishing) είναι ένα ιδιαίτερα δόλιο ηλεκτρονικό έγκλημα.Οι εγκληματίες δημιουργούν μια ψεύτικη τοποθεσία Web μιας υφιστάμενης τράπεζας ή μιας εταιρείας πιστωτικών καρτών. Στη συνέχεια, προσπαθούν να εξαπατήσουν τους ανθρώπους αποστέλλοντας μηνύματα ανεπιθύμητης αλληλογραφίας ή μηνύματα email σε συγκεκριμένους παραλήπτες, ελπίζοντας ότι θα σταθούν τυχεροί και θα καταφέρουν να εντοπίσουν πραγματικούς πελάτες της τράπεζας, της ηλεκτρονικής υπηρεσίας πώλησης ή της εταιρείας πιστωτικών καρτών που έχουν "καταλάβει".

Τα email αυτά μπορεί να είναι ιδιαίτερα πειστικά, όπως ένα μήνυμα από ένα ηλεκτρονικό κατάστημα το οποίο σας ενημερώνει ότι δεν έχει γίνει δεκτή η πιστωτική σας κάρτα ή ένα μήνυμα από την τράπεζά σας το οποίο σας ενημερώνει ότι έχει παρατηρηθεί μη εξουσιοδοτημένη χρήση ή ασυνήθιστη κίνηση στο λογαριασμό σας Τα μηνύματα αυτά συχνά περιέχουν λογότυπα, χρωματιστά μοτίβα, μότο εταιρειών ή μηνύματα διαφημιστικών

[108] http://www2.e-yliko.gr/htmls/safety/smail4.aspx

[109] http://www.toshiba.eu/security-center/se-gr/prevent-phishing.php

εκστρατειών τα οποία πιστοποιούν την αυθεντικότητά τους. Το μήνυμα σάς ζητά να κάνετε κλικ σε μια σύνδεση η οποία σας μεταφέρει στην ψεύτικη τοποθεσία Web. Στην τοποθεσία αυτή θα σας ζητηθεί να πληκτρολογήσετε προσωπικά στοιχεία τα οποία θα χρησιμοποιήσουν στη συνέχεια οι εγκληματίες για να καταχραστούν χρηματικά ποσά από εσάς ή για να διαπράξουν εγκλήματα κλοπής ταυτότητας.

*Πώς να διακρίνουμε μια απάτη ψαρέματος (*phishing);

Δεν είναι ασφαλές να εισάγετε προσωπικές ή οικονομικές πληροφορίες σε pop up windows (αναδυόμενα παράθυρα). Μια κοινή τεχνική ψαρέματος είναι το άνοιγμα ενός ψεύτικου αναδυόμενου παραθύρου όταν κάποιος κάνει κλίκ σε ένα ηλεκτρονικό μήνυμα ψαρέματος. Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεστε . Ακόμα και αν το αναδυόμενο παράθυρο φαίνεται πολύ επίσημο η διακηρύσσει πως είναι ασφαλές θα πρέπει να αποφεύγετε να εισάγετε ευαίσθητα προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελέγξετε την πιστοποίηση ελευθερίας.

Τι κάνουμε εάν πέσουμε θύμα απάτης με την πιστωτική μας κάρτα;

Όταν χρησιμοποιείτε πιστωτική κάρτα μπορεί να γίνετε ευάλωτοι σε πιθανή απάτη πληρώνοντας μέσω Διαδικτύου, και μέσω τηλεφώνου. Για αυτό κάθε φορά που πληρώνετε με πιστωτική κάρτα, οι επιχειρήσεις θα πρέπει να επιβεβαιώνουν τα στοιχεία του λογαριασμού σας πριν σας παρέχουν αγαθά και υπηρεσίες.

Δυστυχώς επειδή τα στοιχεία της πιστωτικής κάρτας αποθηκεύονται σε μεγάλους υπολογιστές , οι διακομιστές μπορεί να γίνουν στόχος χάκερ οι οποίοι αναζητούν τρόπους για να εισχωρήσουν στο σύστημα και να ανακτήσουν στοιχεία κατόπιν, θα τα χρησιμοποιήσουν για να διαπράξουν μια απάτη.

Πρέπει να ακολουθήσουμε τα επόμενα βήματα, εάν πιστεύουμε ότι έχουμε πέσει θύμα απάτης.

- ✓ Όσο ταχύτερα επικοινωνήστε με τις αρμόδιες αρχές , τόσο πιθανότερο είναι να μειώσετε την ζημιά που μπορεί να προκαλέσει ο απατεώνας με τα στοιχεία σας, την πιστωτική σας κάρτα και τον τραπεζικό σας λογαριασμό.
- ✓ Κλείστε όλους τους λογαριασμούς που επηρεάζονται
- ✓ Επικοινωνήστε με την πραγματική εταιρεία ή τον οργανισμό ένα πιστεύετε πως δώσατε ευαίσθητες πληροφορίες σε άγνωστη πηγή , η οποία προσποιήθηκε πως ήταν η πραγματική εταιρεία ή ο οργανισμός.
- ✓ Επικοινωνήστε με το τμήμα ασφάλειας ή απάτης κάθε τράπεζας ή πιστωτικού ιδρύματος με τον οποίο συνεργάζεσθε.
- ✓ Στην συνέχεια στείλτε μια επιστολή και κρατείστε και ένα αντίγραφο για εσάς.
- ✓ Όταν ανοίξετε νέους λογαριασμούς χρησιμοποιήστε νέους ισχυρούς κωδικούς πρόσβασης

- ✓ Αλλάξτε όλους κωδικούς πρόσβασης σε όλους τους διαδικτυακούς λογαριασμούς που χρησιμοποιείτε

Συμβουλές προστασίας από το ηλεκτρονικό ψάρεμα (Phishing)

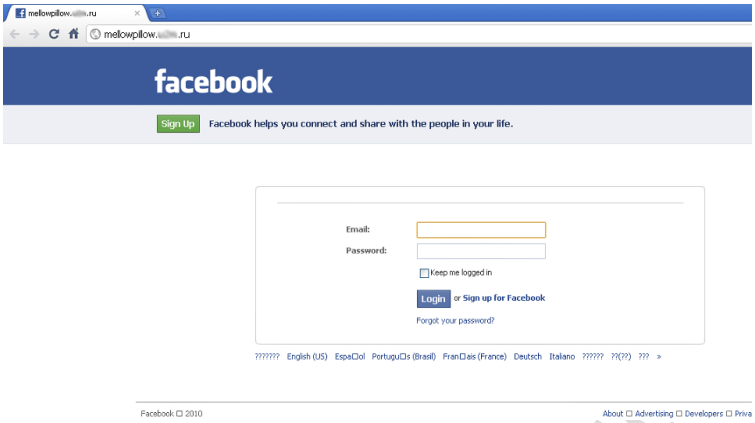
Σε κάθε εισαγωγή του χρήστη στο πληροφοριακό σύστημα της τράπεζας με την οποία συναλλάσσεται, ο ενδιαφερόμενος πρέπει να βεβαιώνεται ότι έχει συνδεθεί με τον πραγματικό δικτυακό τόπο (site) της τράπεζας. Αυτό γίνεται με το ψηφιακό πιστοποιητικό ασφαλείας που έχει προμηθευτεί η τράπεζα και το οποίο πιστοποιεί ότι τα προγράμματα που μεταφέρονται στο σταθμό του χρήστη είναι γνήσια που έχουν εκπονηθεί από την τράπεζα, γεγονός που επιβεβαιώνεται με την ύπαρξη των παραπάνω ψηφιακών πιστοποιητικών.

Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο στο κάτω μέρος της οθόνης για όσο χρονικό διάστημα ο χρήστης χρησιμοποιεί την εφαρμογή υποδεικνύει πως η τοποθεσία web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών του. Όμως , το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικό. Για να διασφαλίσετε την γνησιότητα του, κάντε διπλό κλικ, ώστε να διαπιστώσετε αν υπάρχει το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το ‘’Issued to” (εκδόθηκε για) θα πρέπει να αντιστοιχεί στο όνομα της τοποθεσίας. Εάν, το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως “spoofed” (πλαστή).

Ένα χρήσιμο παράδειγμα επίθεσης phishing μέσω Facebook

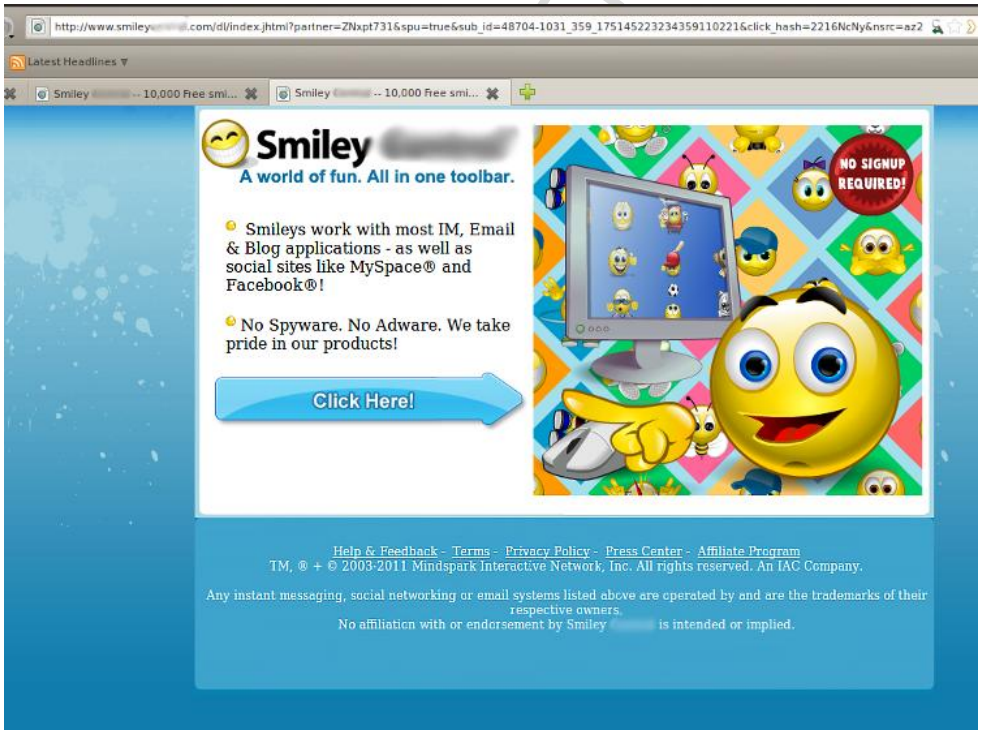
Μία νέα επίθεση μέσω του Facebook στοχεύει τους ανυποψίαστους χρήστες και αποστέλλει μηνύματα phishing μέσα από παραβιασμένους λογαριασμούς, με σκοπό οι χρήστες να τα ακολουθήσουν και να μεταφερθούν σε μια εικονική σελίδα του Facebook, ώστε να καταχωρίσουν τα στοιχεία του λογαριασμού τους.

Προσέξτε όμως την παρακάτω εικόνα και θα εντοπίσετε ότι στο link που εμφανίζεται επάνω δεν αναφέρεται πουθενά το Facebook.

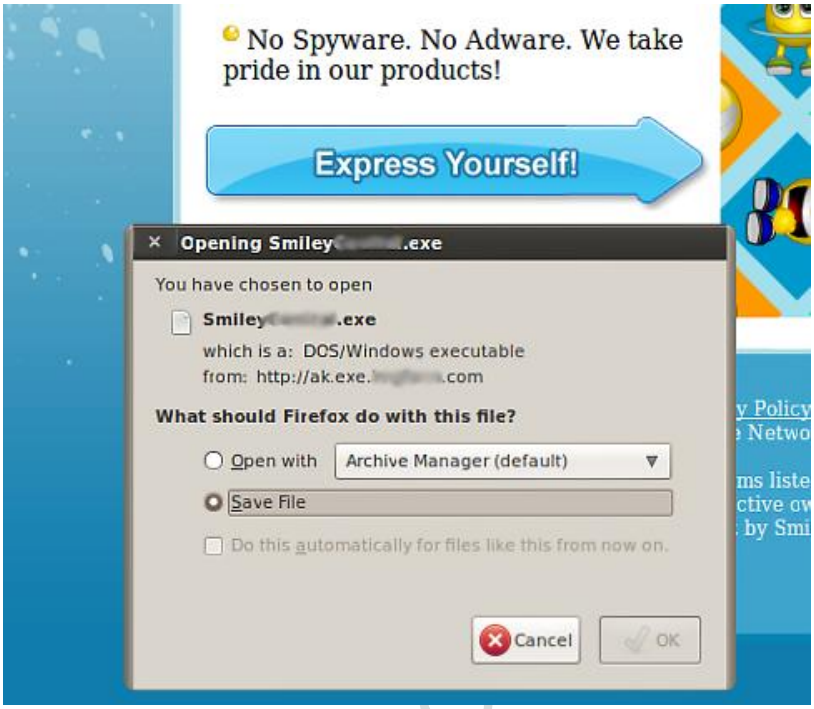


Στη συνέχεια καταχωρίσαμε τα στοιχεία ενός δοκιμαστικού λογαριασμού για να ελεγχθεί η συνέχεια. Το αποτέλεσμα ήταν η παρακάτω εικόνα

Στη συνέχεια όπως βλέπετε σας προσφέρουν κάποια συσκευή δωρεάν, και ποιος δεν τη θέλει; Εάν λοιπόν κάνετε κλικ επάνω στο 'Claim Now' θα μεταφερθείτε στην παρακάτω ιστοσελίδα



Εάν τώρα κάνετε κλικ στο κουμπί με το βέλος τότε θα εμφανιστεί το παρακάτω μήνυμα όπου θα σας ζητάει να μεταφορτώσετε ένα αρχείο.



Και εάν το μεταφορτώσετε τότε μόλις πληρώσατε με τον λογαριασμό σας ένα κακόβουλο λογισμικό που βρίσκεται τώρα στον υπολογιστή σας. Βέβαια στη συνέχεια το Facebook σας ενημερώνει για ύποπτη κίνηση στον λογαριασμό σας. Αυτό όμως δεν ισχύει, γιατί πάλι είναι παγίδα καθώς αν κάνετε κλικ στο 'I don't recognize' θα σας ζητηθεί να φτιάξετε νέο account για να επαναφέρετε τον λογαριασμό σας και φυσικά τα στοιχεία καταλήγουν στους επιτιθέμενους

- *Pharming*

[110]Η τεχνική του "**pharming**" αποτελεί μέθοδο εξαπάτησης μέσω του διαδικτύου παρόμοια με το "**phishing**" αλλά σαφώς πιο επικίνδυνη από αυτό. Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει κατά τέτοιο τρόπο, ώστε, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, ο συγκεκριμένος υπολογιστής τον "οδηγεί" μόνο σε πλαστές ιστοσελίδες. Ειδικότερα, αν πρόκειται για ιστοσελίδα τράπεζας, η προσπάθεια του θύματος να πραγματοποιήσει τις συναλλαγές του μέσω **on-line banking** καταλήγει στη μεταφορά των χρημάτων του στους δράστες (**Pharmers**).

[110] http://www.nomika-epilekta.gr/arthra/koinonika-arthra/phishing-and-pharming

Σοφία Δημητρακάκη

Είναι σαφές ότι η αύξηση των ωρών χρήσης του διαδικτύου πολλαπλασιάζει τον κίνδυνο εγκατάστασης προγραμμάτων που καθιστούν δυνατό το "**pharming**", το οποίο βαθμιαία εξελίσσεται σε μία από τις σοβαρότερες μορφές **εγκληματικότητας στο διαδίκτυο**.

Το pharming δηλ παραπλάνηση , η χρήση δηλαδή ψεύτικων ιστοσελίδων πιθανόν να θυμίζει τις απάτες ψαρέματος από ηλεκτρονικά μηνύματα, αφού μπορεί να κατευθύνετε σε μια ψεύτική ιστοσελίδα χωρίς να το γνωρίζετε.

Η μέθοδος "**pharming**" αποτελεί ένα είδος διείσδυσης μέσω του διαδικτύου, χωρίς τη συναίνεση του νόμιμου κατόχου των στοιχείων. Η μέθοδος αυτή, εφόσον είναι ολοφάνερο ότι τελείται με δόλο, συνιστά **παραβίαση απορρήτου** κατά το **άρθρο 370Γ § 2** του Ποινικού Κώδικα, σύμφωνα με το οποίο «όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον 29,00 € (…)».

Συμπερασματικά, οι ανωτέρω δύο μέθοδοι μπορούν να τιμωρηθούν, σύμφωνα με τις ισχύουσες διατάξεις του Ποινικού Κώδικα. Για την αντιμετώπιση τέτοιων φαινομένων κρίνεται απαραίτητη η λήψη τεχνικών μέτρων ασφαλείας, καθώς και η ευαισθητοποίηση των χρηστών του Ίντερνετ, ώστε να μην γίνονται εύκολα θύματα των **Phishers** και των **Pharmers**.

- *Email spoofing*

[111]Spoofing ονομάζουμε τη μέθοδο κατά την οποία ένας κακόβουλος χρήστης παραποιεί τη διεύθυνση του αποστολέα σε ένα ηλεκτρονικό μήνυμα που στέλνει ο ίδιος με απώτερο σκοπό να εκμαιεύσει πληροφορίες ή να αναγκάσει το θύμα να κάνει κάτι (όπως πχ να καταστρέψει κάποιο έγγραφο). Για παράδειγμα το πραγματικό μου email είναι pamal@microsoft.com αλλά τη στιγμή που στέλνω το μήνυμα, αλλάζω την email διεύθυνση μου σε kati.allo@kapou-allou.gov.

Spoofing (παραπλάνηση) είναι ο τρόπος που χρησιμοποιεί κάποιος για να αποκτήσει πρόσβαση σε ένα δίκτυο ή υπηρεσία δικτύου χωρίς να είναι νόμιμος χρήστης. Ο απλούστερος τρόπος να γίνει αυτό είναι γνωρίζοντας το όνομα χρήστη και τον κωδικό πρόσβασης ενός νόμιμου χρήστη. Μόλις αποκτήσει πρόσβαση ο μη νόμιμος χρήστης σε ένα δίκτυο, μπορεί έπειτα να αποκτήσει πρόσβαση και στα ιδιωτικά αρχεία ή τους πόρους. Παραπλάνηση μπορεί να υπάρξει και στα μηνύματα ηλεκτρονικού ταχυδρομείου που μπορούν να εμφανιστούν σαν να προέρχονται από έναν νόμιμο χρήστη.

Όσο περίεργο και αν φαίνεται αυτό δεν αποτελεί παραβίαση του SMTP Standard. Το πρωτόκολλο SMTP από τη φύση του δεν παρέχει κάποια ασφάλεια έτσι οποιοσδήποτε μπορεί να αλλάξει το πεδίο From: του ηλεκτρονικού του μηνύματος. Η πρακτική αυτή χρησιμοποιείτε συνήθως από κακόβουλα άτομα που θέλουν να εκμαιεύσουν πληροφορίες από ανυποψίαστους χρήστες (πχ κωδικούς ή κάποια απόρρητη πληροφορία).

[111] http://autoexec.gr/servers_servers_/f/23/t/103.aspx

την απλούστερη μορφή της επίθεσης, το κακόβουλο άτομο (από τώρα και στο εξής ο “cracker”) ανοίγει μία σύνδεση στην πόρτα επικοινωνίας του SMTP (tcp-25) server του θύματος και δίνει τις εξής εντολές:

[Cracker] telnet victims.mailserver.org

[Server] 220 victims.mailserver.org

[Cracker] helo otidipote.org

[Server] 250 victims.mailserver.org Hello otidipote.org [crackers ip sender], pleased to meet you

[Cracker] mail from:otidipote@otidipote.org

[Server] 250 otidipote@otidipote.org... Sender ok

[Cracker] rcpt to:victim@mailserver.org

[Server] 250 victim@mailserver.org... Recipient ok

[Cracker] data

[Server] 354 Enter mail, end with "." on a line by itself

[Cracker] From: your.boss@mailserver.org

[Cracker] To: victim@mailserver.org

[Cracker] Subject: Please send me the password

[Cracker] <μία κενή γραμμή>

[Cracker] Hello my employee. I forgot the password for our banking application and I’m abroad with no access to the corporate network. Please send me the password to my hotmail account at boss123@hotmail.com.

[Cracker] Thank you

[Cracker] <CR><LF>.<CR><LF> *(αυτή η ακολουθία ουσιαστικά είναι ένα enter (Carriage Return – Line Feed), μετά μία τελεία και μετά πάλι ένα enter. Δεν θα γράψετε τα CR κλπ αλλά απλά θα πατήσετε την παραπάνω ακολουθία πλήκτρων)*

[Server] 250 Message accepted for delivery

[112]Θα πρέπει να σημειώσουμε πως τα στοιχεία αποστολέα και παραλήπτη που βλέπουμε στον mail client μας (πχ Outlook 2003) είναι αυτά που μπήκαν μετά το κομμάτι DATA έτσι στο παραπάνω παράδειγμα βλέπουμε πως ο cracker άλλαξε το From: έτσι ώστε να φαίνεται σαν το

[112] http://autoexec.gr/servers_servers_/f/23/t/103.aspx

αφεντικό του θύματος. Όπως είναι λογικό, το email του recipient δεν μπορεί να είναι άσχετο. Δεν μπορούμε για παράδειγμα να κάνουμε spoofing στον mail server της Microsoft και σαν παραλήπτη να βάλουμε κάποιο χρήστη του οποίου το email τελειώνει σε @asxeto-domain.net.

Χρήσεις του Spoofing

- man-in-the-middle

Πρόκειται για παραβίαση ασφαλείας.Σε μια νόμιμη επικοινωνία μεταξύ δύο υπολογιστών παρεμβαίνει ένας τρίτος και δημιουργεί πρόβλημα. Κατόπιν ένας host παρεμβαίνει και ελέγχει τη ροή επικοινωνίας ή κλέβει κάποια στοιχεία που στέλνονται από κάποιον από τους συμμετέχοντες.

- routing redirect

Ο **routing redirect** μεταφέρει πληροφορίες από τον αρχικό host για κάποιους hacker host δηλαδή σε τρίτους hosts που σκοπό έχουν την παραβίαση του δικτύου.Συνήθως όταν υπάρχουν δυο router και επικοινωνούν με ένα υπολογιστή και έτσι επιλέγεται η μέγιστη διαδρομή για αποστολή δεδομένων μέσω ενός datagram που στέλνεται από ένα router.

- source routing

Σε ένα δίκτυο υπολογιστών το **source routing** επιτρέπει στον αποστολέα του πακέτου να καθορίζει εν μέρει ή πλήρως την πορεία του μέσα στο δίκτυο. Αντίθετα στα πρωτόκολλα που δεν έχουν την source routing οι routers του δικτύου καθορίζουν τη πορεία του πακέτου με βάση τον προορισμό αυτού.Το source routing επιτρέπει την ευκολότερη αντιμετώπιση προβλημάτων τη βελτίωση του traceroute και επιτρέπει σε ένα κόμβο να ανακαλύψει πιθανές διαδρομές προς ένα κεντρικό υπολογιστή.

- blind spoofing

Blind spoofing είναι ένας τύπος επίθεσης που χρησιμοποιεί ip spoofing .Οι επιτιθέμενοι χρησιμοποιούσαν μια μέθοδο οπού στέλνανε πολλά πακέτα σε μια μηχανή στόχο και έτσι υπολόγιζαν την ακολουθία των αριθμών,σήμερα όμως που τα λειτουργικά συστήματα εφαρμόζουν κάποια γεννήτρια τυχαίων αριθμών είναι δύσκολη η πρόβλεψη της ακολουθία των αριθμών.Το σύστημα αυτό λέγεται και τυφλή επίθεση-πλαστογράφηση.

- flooding

Το flooding αφορά τη πλημμύρα των πακέτων σε μια δικτύωση που δημιουργεί προβλήματα στη ροή των δεδομένων. Από τη μεριά μας μπορεί να προκαλέσει διαταραχή στη ροή που

κατεβαίνουν τα αρχεία από το δίκτυο, δηλαδή ροή αντίθετη της κανονικής με αποτέλεσμα την υπερχείλιση.[113]

[113] http://el.wikipedia.org/wiki/Spoofing

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

4. Μέσα προστασίας προσωπικών δεδομένων

4.1 Ασφάλεια Περιμέτρου

Πολλοί οργανισμοί ηλεκτρονικού εμπορίου έχουν συνδέσει τα εσωτερικά τους δίκτυα με το διαδίκτυο για την πραγματοποίηση των ηλεκτρονικών συναλλαγών, αλλά και για την λήψη χρήσιμών πληροφοριών από τον παγκόσμιο ιστό. Η σύνδεση όμως ενός συστήματος στο διαδίκτυο δίνει την δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Δηλαδή, οι χρήστες του ιδιόκτητου δικτύου μπορούν να έχουν πρόσβαση στο διαδίκτυο.

Ως περίμετρο Δικτύου, σύμφωνα με την ΑΔΑΕ ορίζονται «όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα»[114]. Σύμφωνα με την ΑΔΑΕ, κάθε οργανισμός που συνδέει το εσωτερικό του δικτύου με κάποιο δημόσιο δίκτυο π.χ το διαδίκτυο , θα πρέπει να εφαρμόζει μια πολιτική ασφάλειας περιμέτρου. Ο πρωταρχικός σκοπός της πολιτικής είναι να προστατεύσει τους διάφορους πόρους του οργανισμού από εισβολείς, δηλαδή να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του οργανισμού. Η ΑΔΑΕ υποχρεώνει κάθε πάροχο διαδικτύου, οπότε έμμεσα και κάθε οργανισμό ηλεκτρονικού εμπορίου, να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου με το διαδίκτυο και επιπλέον τον υποχρεώνει να χρησιμοποιεί συστήματα ανίχνευσης εισβολών για την ενίσχυση της προστασίας του δικτύου.

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

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

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

[114] Απόφαση 633^{A}/2005-ΦΕΚ Β/88/26.01.2005

4.2 Firewalls

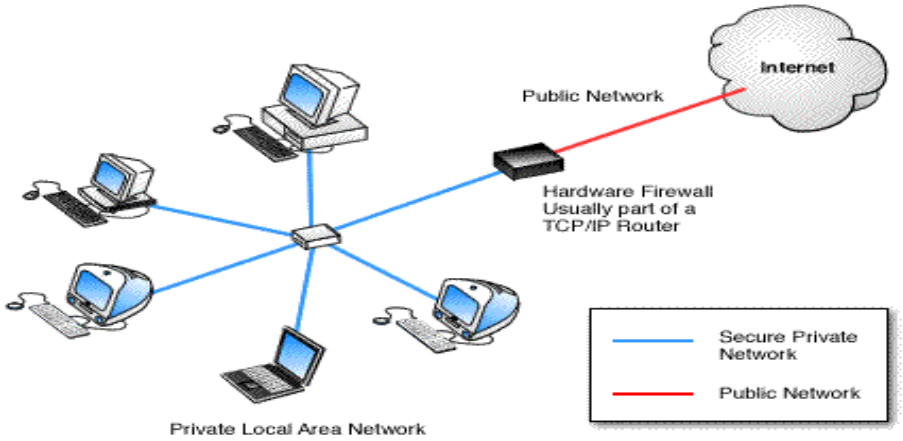
Η τεχνολογία του firewall εμφανίστηκε στα τέλη της δεκαετίας του 1980, όταν ακόμη το Internet ήταν σε πρώιμα στάδια. Εκείνη την εποχή είχαν παρατηρηθεί αρκετές "τρύπες" ασφαλείας στο Διαδίκτυο οπότε έπρεπε να βρεθεί μία λύση. Η λύση αυτή ήταν η δημιουργία της τεχνολογίας firewall.

[115]Το διαδίκτυο έχει καταστήσει μεγάλα ποσά πληροφοριών διαθέσιμα στον μέσο χρήστη υπολογιστών στο σπίτι, στην επιχείρηση και στην εκπαίδευση Για πολλούς ανθρώπους η απόκτηση πρόσβασης σε αυτές τις πληροφορίες δεν είναι πλέον μόνο ένα πλεονέκτημα είναι θεμελιώδης ανάγκη. Όμως , η σύνδεση ενός ιδιωτικού δικτύου, με το διαδίκτυο μπορεί να εκθέσει τα κρίσιμα ή εμπιστευτικά δεδομένα στην κακόβουλη επίθεση από οπουδήποτε στον κόσμο. Οι χρήστες που συνδέουν τους υπολογιστές τους με το διαδίκτυο πρέπει να γνωρίζουν αυτούς τους κινδύνους, τις επιπτώσεις τους και πώς να προστατεύσουν τα δεδομένα τους και τα κρίσιμα συστήματα τους. Τα Firewalls μπορούν να προστατεύσουν και τους μεμονωμένους υπολογιστές και τα εταιρικά δίκτυα από την εχθρική διείσδυση από το διαδίκτυο .

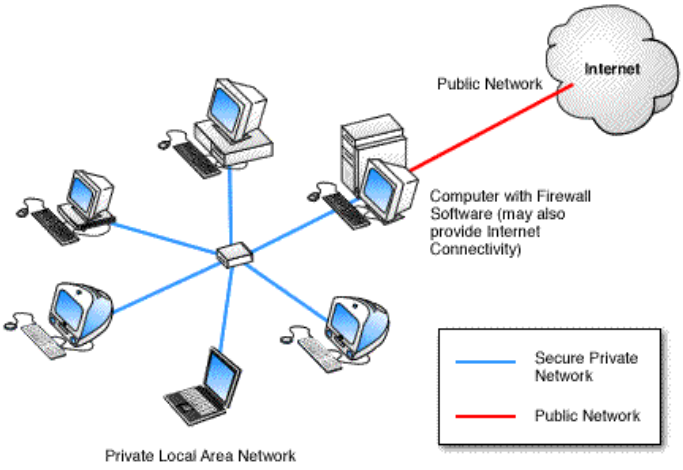
Ένα Firewall προστατεύει τους δικτυωμένους υπολογιστές από την σκόπιμη διείσδυση που θα μπορούσε να οδηγήσει σε συμβιβασμούς στην εμπιστευτικότητα (confidentiality) ή σε καταστροφή δεδομένων ή και άρνηση της υπηρεσίας (denial of service-DOS) . Μπορεί να είναι μια συσκευή υλικού (σχήμα 1) ή ένα πρόγραμμα λογισμικού (σχήμα 2) που τρέχει σε ασφαλή έναν host υπολογιστή. Σε κάθε περίπτωση, πρέπει να έχει τουλάχιστον δυο διεπαφές δικτύων, και μια για το δίκτυο στο οποίο εκτίθεται. Το Firewall τοποθετείται στο σημείο συνδέσεων ή στην πύλη μεταξύ των δύο δικτύων συνήθως ενός ιδιωτικού δικτύου και ενός δημοσίου δικτύου όπως το διαδίκτυο. Τα πρώτα firewalls ήταν απλά δρομολογητές . Ο όρος firewall προέρχεται από το γεγονός ότι με την κατάτμηση ενός δικτύου στα διαφορετικά φυσικά υποδίκτυα , περιορίζεται η ζημιά που θα μπορούσε να διαδοθεί από ένα υποδίκτυο στο άλλο λειτουργώντας όπως οι αντιπυρικές πόρτες (firedoors) ή αντιπυρικές ζώνες (firewalls).

[115] http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/Firewalls.pdf

Στο παρακάτω σχήμα φαίνεται ένα firewall που δημιουργείται από υλικό (hardware firewall) και το οποίο προστατεύει ένα τοπικό δίκτυο.



Σχήμα 1



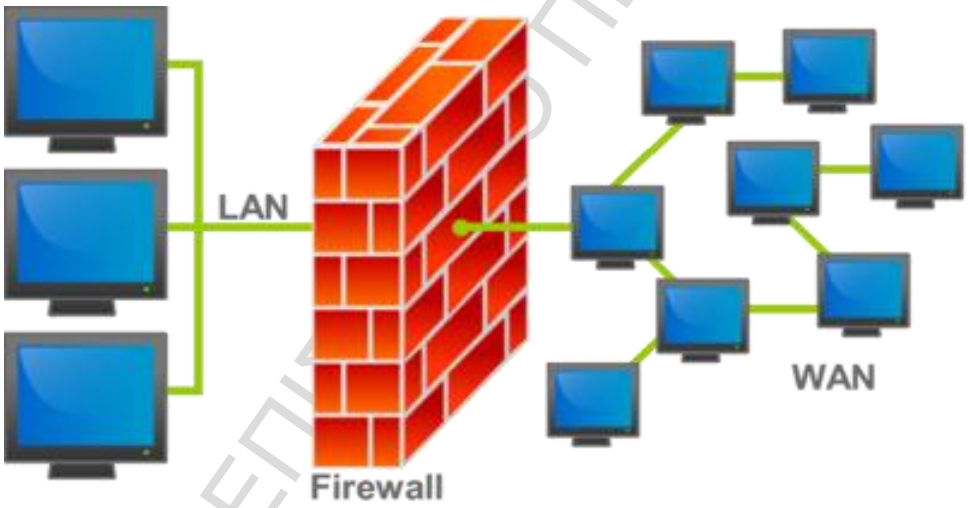
Σχήμα 2

[116]Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το

[116] http://el.wikipedia.org/wiki/Firewall

τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.



Μία τυπική διάταξη firewall.

Το firewall είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το ιδιόκτητο δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Λειτουργεί σαν μια πύλη από την οποία περνάει όλη η κίνηση δεδομένων από και προς το εξωτερικό δίκτυο. Στην πύλη εξετάζεται και αποφασίζεται αν θα επιτραπεί ή όχι η διέλευση των δεδομένων, σύμφωνα με την πολιτική ασφάλειας που εφαρμόζει ο οργανισμός του συστήματος. Το firewall δεν είναι

απλώς ένα σύνολο συνιστωσών λογισμικού ή υλικού , αλλά η τεχνική έκφραση μιας συγκεκριμένης στρατηγικής προστασίας των πόρων ενός οργανισμού.

Ένα firewall είναι ένας «τοίχος» ασφάλειας μεταξύ του μη ασφαλούς δημοσίου δικτύου και του ιδιόκτητου δικτύου που θεωρείται ασφαλές και αξιόπιστο. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν στο απέναντι δίκτυο. Ένα firewall δεν μπορεί να λειτουργήσει σωστά , ανεξαρτήτως του πως έχει σχεδιαστεί ή υλοποιηθεί , εάν δεν έχει καθοριστεί μια σαφής πολιτική ασφάλειας. Το firewall που λειτουργεί σωστά υλοποιεί και ενισχύει την πολιτική ασφάλειας που βρίσκεται κάθε φορά σε ισχύ και πρέπει να είναι συγκεκριμένη και σαφής. Το firewall αποτελεί την πρώτη γραμμή άμυνας του οργανισμού απέναντι στους επίδοξους εισβολείς, αλλά ποτέ την μοναδική.

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

- **Δυνατότητες των Firewalls**

Η λειτουργικότητα των firewalls εκτείνεται στα ακόλουθα:

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

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

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

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

- **Αδυναμίες των Firewalls**

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

Οι αδυναμίες των firewall είναι οι ακόλουθες:

- Το firewall δεν μπορεί να προστατεύσει από προγράμματα-ιούς. Τα firewalls δεν ασκούν σε βάθος έλεγχο των δεδομένων που εισέρχονται στο δίκτυο. Απλά εξετάζουν, τις διευθύνσεις και τις θύρες προέλευσης και προορισμού, για να καθορίσουν εάν επιτρέπεται η είσοδος στο εσωτερικό δίκτυο.
- Το firewall δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού. Οι εσωτερικοί χρήστες είναι σε θέση σε θέση να υποκλέψουν δεδομένα, να καταστρέψουν υλικό και λογισμικό, να τροποποιήσουν προγράμματα και γενικότερα να παραβιάσουν την πολιτική ασφάλεια του οργανισμού χωρίς καν να έρθουν σε επαφή με το firewall. Οι εσωτερικές απειλές απαιτούν εσωτερικά μέτρα ασφάλειας, όπως ασφάλεια σε επίπεδο ξενιστή υπολογιστή (host security).
- Το firewall δεν μπορεί να προστατεύσει τον οργανισμό απέναντι σε επιθέσεις συσχετιζόμενες με δεδομένα. Τέτοιου είδους επιθέσεις συμβαίνουν όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρετητές του οργανισμού, είτε διαμέσου του ηλεκτρονικού ταχυδρομείου , είτε διαμέσου της αντιγραφής από δισκέτα και εκτελούνται με σκοπό να εξαπολύσουν επίθεση εναντίον του συστήματος.
- Το firewall δεν μπορεί να προστατέψει τον οργανισμό από απειλές άγνωστου τύπου . Το firewall μπορεί να προστατέψει το δίκτυο μόνο από γνωστές απειλές που έχουν αντιμετωπιστεί στο παρελθόν , εφόσον διαθέτει την απαιτούμενη τεχνολογία.
- Το firewall δεν μπορεί να προστατέψει από συνδέσεις οι οποίες δεν διέρχονται από αυτό. Αν για παράδειγμα επιτρέπεται σε κάποιους έμπιστους χρήστες να έχουν πρόσβαση στο διαδίκτυο παρακάμπτοντας τους μηχανισμούς ασφάλειας του Firewall, τότε το firewall δεν μπορεί να προστατέψει τις συνδέσεις αυτές. Ένα firewall μπορεί να ελέγξει αποτελεσματικά την κίνηση που διέρχεται μέσα από αυτό.
- Τις εσωτερικές επιθέσεις.

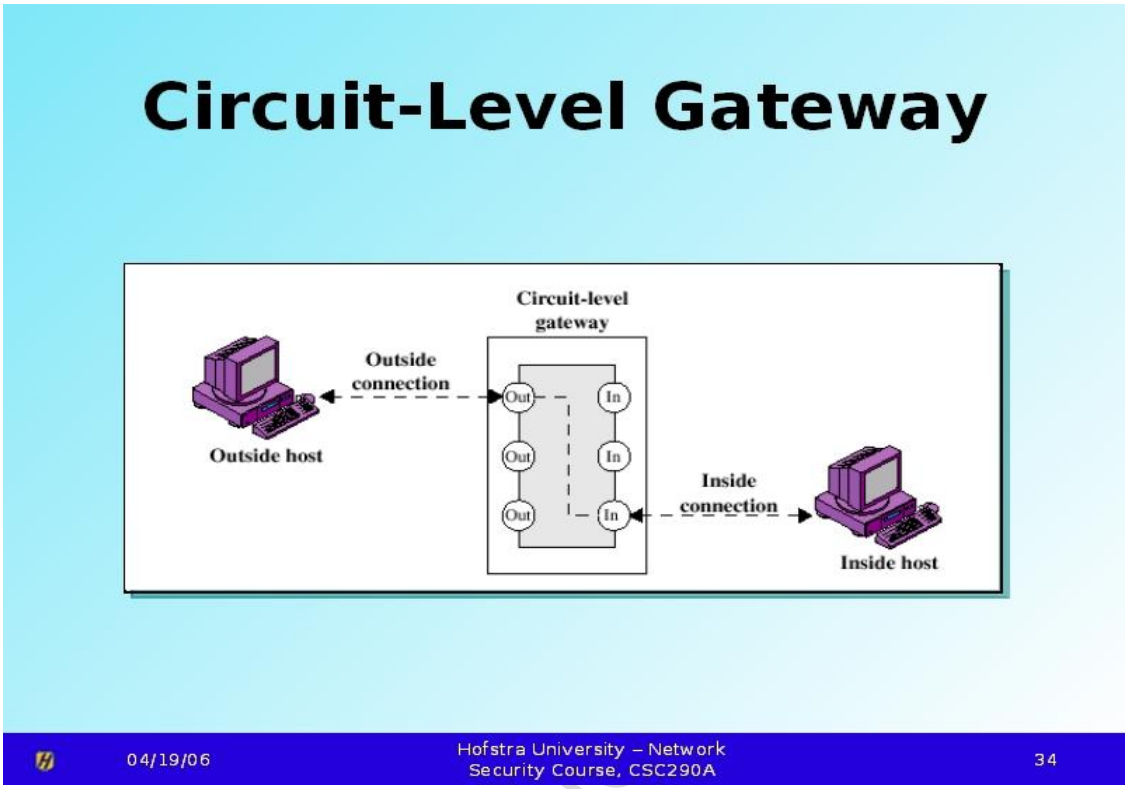
- Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του firewall. Είναι δυνατόν ένα firewall να ρυθμιστεί με πολύ αυστηρό τρόπο, με κίνδυνο να εμποδίσει την διαδικτύωση ή να προκαλεί την δυσαρέσκεια στους χρήστες , εξαιτίας των πολλών ελέγχων και της ελαττωμένης φιλικότητας και ευχρηστίας που εισάγει.

- **Τεχνικές Ασφαλείας με Firewalls**

Υπάρχουν τέσσερις βασικές τεχνικές ασφαλείας:

- Πύλες φιλτραρίσματος πακέτων(packet filtering gateways) ή δρομολογητές φιλτραρίσματος(screening routers)
- Πύλες κυκλωμάτων (circuit gateways)
- Πύλες εφαρμογών (application gateways)

Τα packet filtering gateways λειτουργούν στο επίπεδο δικτύου του μοντέλου OSI ή στο IP επίπεδο του μοντέλου TCP/IP. Είναι συνήθως μέρος ενός δρομολογητή. Σε ένα τέτοιο firewall κάθε πακέτο συγκρίνεται με ένα σύνολο κριτηρίων προτού να διαβιβαστεί. Ανάλογα με το πακέτο και τα κριτήρια, το Firewall μπορεί να απορρίψει το πακέτο , να το διαβιβάσει ή να στείλει ένα μήνυμα στο δημιουργό του. Οι κανόνες μπορούν να συμπεριλάβουν την διεύθυνση της πηγής (source address) και την διεύθυνση προορισμού IP(destination IP address) , το port της πηγής και προορισμού και το χρησιμοποιούμενο πρωτόκολλο. Το πλεονέκτημα αυτών των firewalls είναι το χαμηλότερο κόστος και το χαμηλότερο αντίκτυπο τους στην απόδοση του δικτύου. Οι περισσότεροι δρομολογητές υποστηρίζουν το φιλτράρισμα πακέτων . Ακόμα, και αν χρησιμοποιούνται firewalls, η εφαρμογή του πακετών στο επίπεδο δρομολογητών προσδίδει έναν αρχικό βαθμό ασφάλειας στο επίπεδο δικτύου (network layer). Αυτός ο τύπος firewall, λειτουργεί μόνο στο επίπεδο δικτύου και δεν υποστηρίζει ειδικούς περίπλοκους κανόνες ελέγχου. Οι Network Address Translation (NAT) routers προσφέρουν τα πλεονεκτήματα των packet filtering firewalls αλλά μπορούν επίσης να κρύψουν τις διευθύνσεις IP των υπολογιστών πίσω από το firewall, και να προσφέρουν ένα επίπεδο circuit –based φιλτραρίσματος.

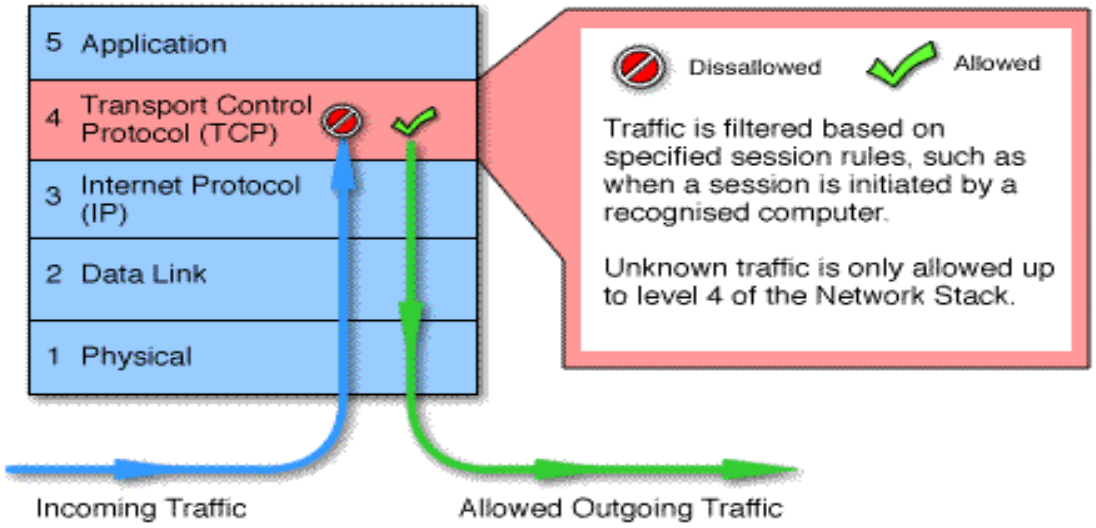


Αυτός ο τύπος φιλτραρίσματος των πακέτων δεν εξετάζει καθόλου εάν ένα πακέτο είναι μέρος ενός ρεύματος κυκλοφορίας δεδομένων (δεν αποθηκεύει καμία πληροφορία για την κατάσταση των διαφόρων συνδέσεων από το ένα δίκτυο στο άλλο - stateless packet filtering). Αντιθέτως, φιλτράρει κάθε πακέτο με βάση την πληροφορία που περιέχεται στο ίδιο το πακέτο (συνήθως χρησιμοποιεί έναν συνδυασμό πληροφοριών που αφορούν στη διεύθυνσης της πηγής και του προορισμού του πακέτου, το πρωτόκολλό που χρησιμοποιείται, και αν πρόκειται για TCP και UDP πρωτόκολλο, τον αριθμό του port).

Οι πύλες επιπέδου κυκλώματος circuit level gateway λειτουργούν στο επίπεδο συνόδου του πρότυπου OSI, ή το επίπεδο TCP του TCP/IP. Ελέγχουν το TCP handshaking [117] μεταξύ των πακέτων για να καθορίσουν εάν μια ζητούμενη σύνοδος είναι νόμιμη. Οι πληροφορίες που περνούν στον απομακρυσμένο υπολογιστή μέσω μιας πύλης επιπέδου κυκλώματος

[117] Ανταλλαγή δεδομένων του TCP πρωτοκόλου για επίτευξη της σύνδεσης.

(circuit gateway) εμφανίζονται να προέρχονται από την πύλη. Αυτό είναι χρήσιμο για την απόκρυψη των πληροφοριών που αφορούν προστατευμένα δίκτυα. Οι πύλες επιπέδου είναι σχεδόν ανέξοδες και έχουν το πλεονέκτημα της απόκρυψης πληροφοριών για το ιδιωτικό δίκτυο που προστατεύουν.



Σχήμα circuit level gateway

Ένας άλλος τύπος firewall είναι το ***proxy firewall*** ή αλλιώς ***(application level gateway)*** όπου κάθε πακέτο σταματά στο firewall. Το πακέτο έπειτα εξετάζεται και συγκρίνεται με τους κανόνες που διαμορφώνονται από το firewall. Εάν το πακέτο περάσει τις «εξετάσεις», επαναδημιουργείται και στέλνεται. Επειδή κάθε πακέτο καταστρέφεται και επαναδημιουργείται, υπάρχει η δυνατότητα να αποτρέψει το proxy firewall τις άγνωστες επιθέσεις που βασίζονται στις αδυναμίες του πρωτοκόλλου TCP/IP που δεν θα αποτρεπόταν από ένα packet filter firewall. Το μειονέκτημα είναι ότι για κάθε ξεχωριστή εφαρμογή-proxy θα πρέπει να γραφτεί για κάθε τύπο εφαρμογής που είναι proxy. Δηλαδή χρειαζόμαστε ένα proxy-HTTP για το web traffic, ένα proxy-FTP για τη μεταφορά αρχείων, κ.λ.π. Τα Application-proxy firewalls λειτουργούν στο επίπεδο 7 του προτύπου OSI, το επίπεδο εφαρμογών. Το μοντέλο του application proxy firewall προσφέρει έναν πολύ ανώτερο έλεγχο ασφάλειας διότι παρέχει πλήρη ενημερότητα σε επίπεδο εφαρμογών των συνδέσεων εξετάζοντας τα πάντα στη μέγιστη στρώση του πλήθους των πρωτοκόλλων. Ένα τέτοιο firewall μπορεί, για παράδειγμα, να ξεχωρίσει εύκολα τις σημαντικές εντολές εφαρμογών εφαρμόζοντας τις κατάλληλες πολιτικές για κάθε μία από αυτές. Τα proxy firewalls παρέχουν επίσης μία ενσωματωμένη proxy λειτουργία τερματίζοντας τη σύνδεση του πελάτη στο firewall και ξεκινώντας μία νέα σύνδεση στο εσωτερικό προστατευόμενο δίκτυο.

Πρόκειται δηλαδή για Υπηρεσίες πληρεξουσίου Οι πληρεξούσιοι επιπέδου εφαρμογής επιτρέπουν την πλήρη αποσύνδεση της ροής πρωτοκόλλων επιπέδου Δικτύου μέσω του Firewall και τον περιορισμό της κινήσεις μόνο σε πρωτοκόλλα υψηλότερου επιπέδου, όπως τα HTTP για υπηρεσίες Web,Ftp για αποστολή αρχείων και SMTP για email. Όταν γίνεται μια σύνδεση μέσω ενός πληρεξουσίου διακομιστή, ο πληρεξούσιος διακομιστής δέχεται την

σύνδεση, εξάγει το πρωτόκολλο υψηλού επιπέδου, όπως το HTPP, τα εξετάζει και παίρνει αποφάσεις για το περιεχόμενο του με βάση την πολιτική ασφαλείας που έχει καθορίσει

Από την άλλη τα stateful packet filters, παρακολουθούν τις συνδέσεις αλλά και άλλες πληροφορίες για τα στοιχεία των δικτύων που επεξεργάζονται. Ένα stateful firewall διαθέτει μια ή περισσότερες δομές δεδομένων, γνωστές ως state tables (πίνακες κατάστασης), στις οποίες αποθηκεύει πληροφορίες για τις συνδέσεις των δικτύων που ελέγχει. Αυτού του είδους firewalls μπορούν γενικά να παρέχουν ένα πιο σφιχτό επίπεδο ασφάλειας σε ένα δίκτυο, αν και είναι πιο σύνθετες στο σχεδιασμό αλλά και την εφαρμογή. Τα stateful packet filters firewalls βρίσκονται σε πολλές open-source λύσεις για firewall και διαμορφώνουν τη βασική τεχνολογία πίσω από πολλές λύσεις επιχειρηματικών firewalls. Τα stateful multiplayer Inspection firewalls, προσφέρουν έναν υψηλό επίπεδο ασφαλείας, καλή απόδοση και διαφάνεια στους τελικούς χρήστες. Παρ΄ ’όλα αυτά είναι ακριβά, και λόγω της πολυπλοκότητας τους, εάν δεν διαχειρίζονται από ικανό προσωπικό, είναι ενδεχομένως λιγότερο ασφαλή από τους απλούστερους Firewalls.

- **Λειτουργίες ενός Firewall**

Ένα firewall εξετάζει όλη την κυκλοφορία που δρομολογείται μεταξύ των δύο δικτύων για να διαπιστώσει εάν ικανοποιούνται ορισμένα κριτήρια. Εάν , ναι τότε η κυκλοφορία δρομολογείται μεταξύ των δικτύων , διαφορετικά διακόπτεται. Ένα firewall φιλτράρει την εισερχόμενη και την εξερχόμενη κυκλοφορία. Μπορεί επίσης να διαχειριστεί την δημόσια πρόσβαση στους ιδιωτικούς δικτυωμένους πόρους . Μπορεί να χρησιμοποιηθεί για να καταγράψει (log) όλες τις προσπάθειες για πρόσβαση στο ιδιωτικό δίκτυο και να ενεργοποιήσει συναγερμούς (alerts) όταν επιχειρείται εχθρική ή αναρμόδια πρόσβαση. Τα firewalls μπορούν να φιλτράρουν τα πακέτα βασιζόμενα στις διευθύνσεις της πηγής και του προορισμού καθώς και στα port number Τους. Μπορούν τα firewalls να φιλτράρουν συγκεκριμένους τύπους κυκλοφορίας δικτύων (protocol filtering) ως γνωστό φιλτράρισμα πρωτοκόλλου . Επειδή, η απόφαση μπορεί να διαβιβαστεί ή να απορριφθεί η κυκλοφορία εξαρτάται από το χρησιμοποιούμενο πρωτόκολλο π.χ HTPP, FTP ή Telnent. Επίσης, μπορούν να φιλτράρουν την κυκλοφορία από τις ιδιότητες ή την κατάσταση των πακέτων. Το firewall , προστατεύει διαφορετικά δίκτυα εντός του ίδιου οργανισμού . Μερικές φορές το firewall μπορεί να χρησιμοποιηθεί για να διαχωρίσει ένα τμήμα του δικτύου από κάποιο άλλο. Το Firewall έχει την δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης. Τα τελευταία χρόνια , το Iinternet αντιμετώπιζε πρόβλημα διαθέσιμων IP διευθύνσεων .Οι οργανισμοί που επιθυμούν να συνδεθούν με το INternet μπορεί να μην έχουν διαθέσιμες πραγματικές IP διευθύνσεις.

4.3 ΚΡΥΠΤΟΓΡΑΦΙΑ Το Α και το Ω της δικτυακής ασφάλειας

Ιστορική Αναδρομή

❖ **Πρώτη Περίοδος Κρυπτογραφίας (1900π.Χ-1900 μ.Χ)**

Κατά τη διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας, η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της μετάθεσης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» Σχήμα (2.1), ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στη στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

❖ ΔΕΥΤΕΡΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1900 Μ.Χ. – 1950 Μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά τη μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές».

Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma(εικόνα 3) αλλά και τον λιγότερο γνωστό Lorenz SZ40 και SZ42. Η μηχανή αυτή χρησιμοποιείται ως προσάρτημα στους τηλέτυπους που χρησιμοποιούνται για τις επικοινωνίες των υψηλότερων επιπέδων διοίκησης. Η χρήση της σταμάτησε το 1942, όταν οι άγγλοι κρυπταναλύτες, τον Ιανουάριο του ’42 , έσπασαν τον κώδικα της έπειτα από έναν λανθασμένο χειρισμό κάποιον γερμανού στρατιώτη ο τρόπος λειτουργίας των δύο αυτών μηχανών ήταν παρόμοιος . Λειτουργούσαν με ηλεκτρομηχανικούς ρότορες στους οποίους ο χειριστής έδινε μια αρχική τιμή (κλειδί) διαφορετική για κάθε μήνυμα , οι οποίοι άλλαξαν θέση μετά από την πληκτρολόγηση κάθε χαρακτήρα του προς κρυπτογράφηση κειμένου.

Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως στη Γερμανία Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζόταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου.

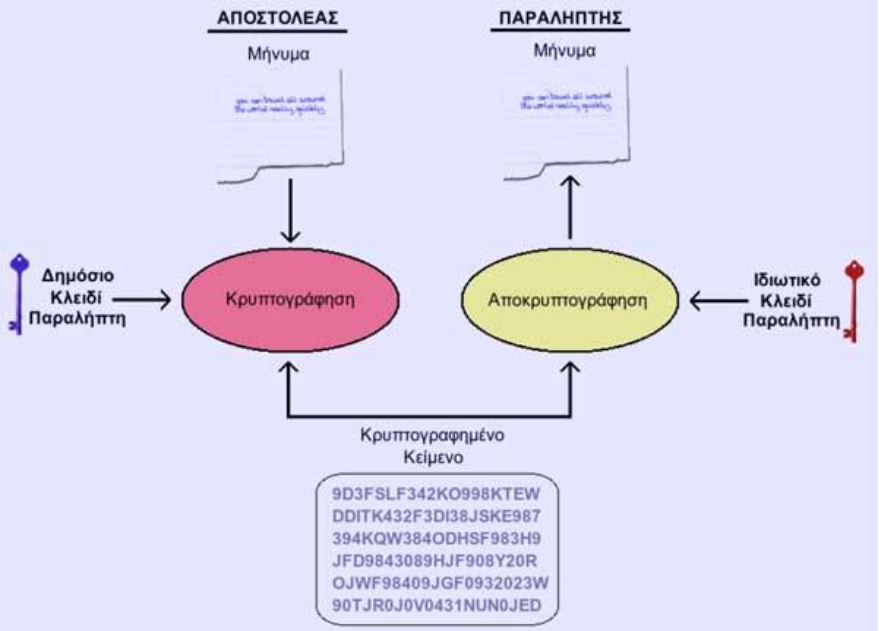
ΕΙΚΟΝΑ ENIGMA

❖ ΤΡΙΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1950 Μ.Χ. - ΣΗΜΕΡΑ)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο

πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (*Communication Theory of Secrecy Systems*) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (*Mathematical Theory of Communication*), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στη θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.



ΟΡΟΛΟΓΙΑ

Κρυπτογράφηση (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως 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 μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Αρχικό κείμενο (*plaintext*) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (*key*) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (*ciphertext*) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (*cryptanalysis*) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα

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 στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Η έννοια της κρυπτογραφίας

Η κρυπτογραφία είναι η επιστήμη και η ικανότητα να γράφεις με μυστικότητα κρατώντας τις πληροφορίες μυστικές. Η κρυπτογραφία , όταν αναφερόμαστε σε υπολογιστές , προστατεύει δεδομένα έναντι της αποκάλυψης αυτών χωρίς ‘άδεια. Μπορεί να αναγνωρίσει την ασφάλεια του χρήστη και φανερώνει την πλαστογραφία χωρίς άδεια . Η κρυπτογραφία είναι ένα αναπόφευκτο μέρος της μοντέρνας ασφάλειας υπολογιστών. Η κρυπτογράφηση είναι η βασική τεχνολογία που χρησιμοποιείται για να αποτρέψει την πρόσβαση μη εξουσιοδοτημένων χρηστών σε εμπιστευτικές πληροφορίες. Η κρυπτογράφηση μετατρέπει τα δεδομένα σε μια ακολουθία χαρακτήρων που δεν επιτρέπουν σε οποιονδήποτε να καταλάβει το περιεχόμενο τους. Μόνο εξουσιοδοτημένα άτομα μπορούν να τα επαναφέρουν στην αρχική τους μορφή με τη χρήση των κλειδιών κρυπτογράφησης.

Είναι ένα από τα αρνητικά στοιχεία του ανοιχτού χαρακτήρα του Διαδικτύου που συνδέεται με προβλήματα ασφάλειας και εμπιστευτικότητας. Η κρυπτογραφία, όπως προείπαμε είναι ένας από τους πιο σίγουρους τρόπους για να διασφαλίσει κανείς τον εμπιστευτικό του χαρακτήρα των μεταδιδόμενων πληροφοριών, την ασφαλή [πιστοποίηση συγκεκριμένων πληροφοριών , την προστασία εμπορικών και βιομηχανικών απορρήτων , την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας κ.πλ. και συνεπώς είναι απολύτως απαραίτητη στο Διαδίκτυο. Με τον όρο κρυπτογραφία [118] εννοούμε μια τεχνική , η οποία με την βοήθεια μαθηματικών αλγορίθμων καθιστά δυνατή την μετατροπή ενός προσιτού σε όλους κειμένου σε μια κωδικοποιημένη μορφή, την οποία δεν μπορεί να αποκωδικοποιήσει κανείς, αν δεν διαθέτει το μυστικό ειδικό κλειδί. Η κρυπτογραφία , δεν είναι νέα έννοια , καθώς σχετικές τεχνικές υπήρχαν ήδη από την αρχαιότητα, χρησιμοποιήθηκαν όμως κυρίως στο στρατιωτικό και διπλωματικό τομέα. Μ ε την ανάπτυξη του Διαδικτύου η κρυπτογραφία ξέφυγε οριστικά από τον περιορισμένο ρόλο της και τέθηκε πια στην υπηρεσία του ευρύτερου κοινού.

Το SSL (Secure Socket Layer) είναι ένα πρωτόκολλο για τη μεταφορά δεδομένων μεταξύ δύο συσκευών, που αναπτύχθηκε για να παρέχει ιδιωτικότητα και ακεραιότητα των πληροφοριών στο Internet. Το SSL διαχειρίζεται την εμπιστευτικότητα και την ακεραιότητα του καναλιού μετάδοσης με χρήση της κρυπτογράφησης των δεδομένων, καθώς και την αυθεντικοποίηση του εξυπηρετητή, αλλά και του πελάτη όταν είναι απαραίτητο.

Η κρυπτογραφία είναι μια διαδικασία που μπορεί να προστατέψει τις συναλλαγές σε ένα ανοικτό δίκτυο όπως είναι το Internet. Τα δεδομένα κρυπτογραφούνται με τη βοήθεια ενός κλειδιού. Το παραγόμενο μήνυμα (chiphertext) αποστέλλεται στον παραλήπτη και αποκρυπτογραφείται με ένα κλειδί που διαθέτει αυτός.

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Υπάρχουν διάφοροι τέτοιοι αλγόριθμοι δημοσιευμένοι και στη συνέχεια θα αναφερθούμε σε μερικούς που χρησιμοποιούνται πιο συχνά.

[118] Λάζο, σελ 175 επ.

Οι μέθοδοι κρυπτογραφίας που χρησιμοποιούνται περισσότερο είναι η Κρυπτογραφία Μυστικού Κλειδιού ή Συμμετρική Κρυπτογραφία και η Κρυπτογραφία Δημόσιου Κλειδιού ή Ασύμμετρη Κρυπτογραφία.

[119]Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω τον Κώστα και τη Βασιλική, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

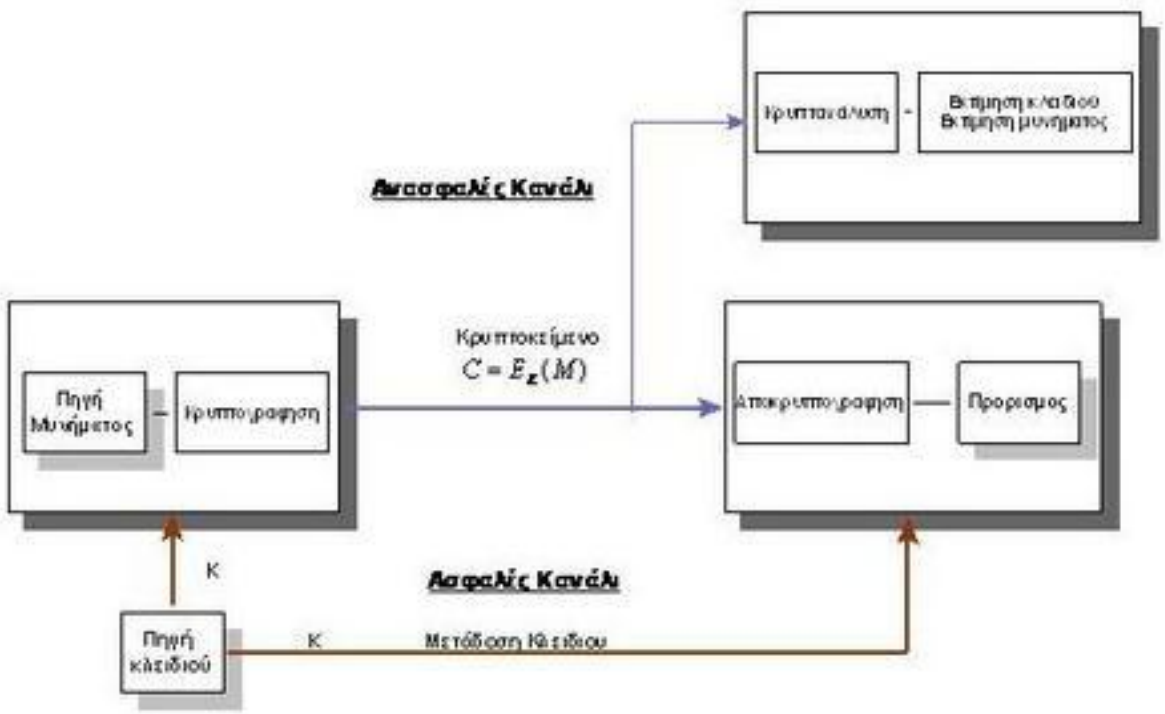
Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.

Το Σύστημα του Σχήματος λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους *n* από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις δύο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

119

http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1#.CE.92.CE.B1.CF.83.CE.B9.CE.BA.CE.AD.CF.82_.CE.AD.CE.BD.CE.BD.CE.BF.CE.B9.CE.B5.CF.82



Μοντέλο Τυπικού Κρυπτοσυστήματος

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες (Αντικειμενικοί σκοποί):

- *Εμπιστευτικότητα*: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- *Ακεραιότητα*: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- *Μη απάρνηση*: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- *Πιστοποίηση*: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών

5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

Βασικά θέματα προστασίας

Η διαδεδομένη χρήση του διαδικτύου σε εφαρμογές που περιλαμβάνουν επικοινωνίες ευαίσθητων δεδομένων εισάγει την ανάγκη για λύσεις στα προβλήματα ασφαλείας που υπάρχουν. Όλες οι επικοινωνίες μέσω του Internet χρησιμοποιούν το πρωτόκολλο Transmission Control Protocol/ Internet Protocol (TCP/IP). Το TCP/IP επιτρέπει να στέλνονται πληροφορίες από ένα Η/Υ σε ένα άλλο μέσω διαφόρων ενδιάμεσων Η/Ρ και δικτύων. Αυτό σημαίνει ότι τρίτα μέρη μπορούν να παρεμβληθούν στην επικοινωνία με τους εξής τρόπους:

- Υποκλέπτοντας (eavesdropping)
- Παραποιώντας (tampering)
- Παραπλανώντας(impersonation)
- Σε επίπεδο προσώπου(spoofing)
- Σε επίπεδο οργανισμού (misrepresentation)

Μια καλά σχεδιασμένη λύση σε αυτά τα προβλήματα αποτελεί η εκτεταμένη χρήση της κρυπτογραφίας που επιτρέπει για τις διακινούμενες πληροφορίες:

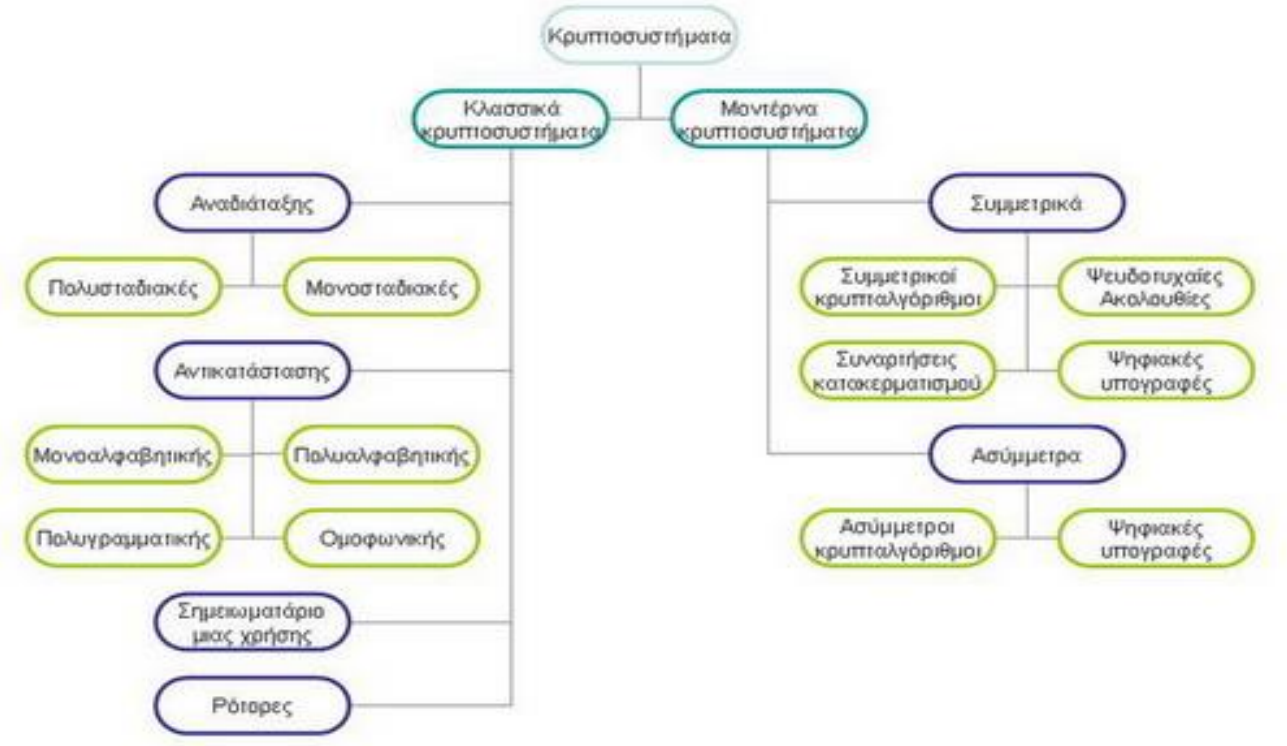
- Κρυπτογράφηση (encryption) και αποκρυπτογράφηση(decryption)
- Ανίχνευση αλλοιώσεων (tamper detection)
- Αυθεντικοποίηση του αποστολέα(authentication)

- Αδυναμία απάρνησης του αποστολέα(nonrepudiation)

Για την αντιμετώπιση αυτών των προβλημάτων αναπτύχθηκε η τεχνολογία των Υποδομών Δημοσίου Κλειδιού-ΥΔΚ. Μια ΥΔΚ αποτελεί μια υποδομή ασφάλειας που ενσωματώνει τεχνολογίες όπως η κρυπτογράφηση δημοσίου κλειδιού, ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές ώστε να διασφαλίζεται η εμπιστευτικότητα των διακινούμενων δεδομένων, αλλά και η ταυτοποίηση και η ιδιότητα της μη απάρνησης για τα συναλλασσόμενα μέρη. Η ανάπτυξη μιας ΥΔΚ βασίζεται κυρίως στην κρυπτογραφία δημοσίου κλειδιού.

- **Κατηγορίες Κρυπτοσυστημάτων**

Τα κρυπτοσυστήματα χωρίζονται σε κατηγορίες ανάλογα με τα κλειδιά και τον τρόπο κρυπτογράφησης των μηνυμάτων. Οι δυο μεγάλες κατηγορίες είναι τα κλασσικά κρυπτοσυστήματα και τα Μοντέρνα. Στα σύγχρονα συστήματα συνήθως υιοθετείται μια μέθοδος ασύμμετρου-συμμετρικού όπου χρησιμοποιείται ασύμμετρο σύστημα για την μεταφορά του κλειδιού και μετά συμμετρικού σύστημα για την μεταφορά και κρυπτογράφηση – αποκρυπτογράφηση των δεδομένων. Με αυτόν τον τρόπο εκμεταλλεύονται τα προτερήματα και των δύο συστημάτων.



Εικό. Μπλόκ ανάλυσης είδη κρυπτοσυστημάτων.

Επιπροσθέτως, οι κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων.:

- **Δέσμης(block ciphers):οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.**
- **Ροής(stream ciphers): οι οποίοι κρυπτογραφούν μια ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα..**

- **Κλασσικά Κρυπτοσυστήματα**

❖ **Αλγόριθμοι Κρυπτογράφησης Δεδομένων**

Η ασφάλεια δεδομένων αποτελεί σήμερα ένα από τα σημαντικότερα προβλήματα, που οι επιστήμονες της πληροφορικής πρέπει να αντιμετωπίσουν. Προσπάθειες προς αυτή την κατεύθυνση έχουν γίνει άλλες φορές με επιτυχία και άλλες χωρίς. Εδώ, θα παρουσιαστούν τρεις αλγόριθμοι, που αποτέλεσαν κάποιες πρώτες προσπάθειες για την κρυπτογράφηση δεδομένων. Αυτοί είναι οι:

α) **Αλγόριθμος του Καίσαρα (Caesar cipher)**

β) **Αλγόριθμος με κλειδί πίνακα**

γ) **Αλγόριθμος Vigenere (Vigenere cipher)**

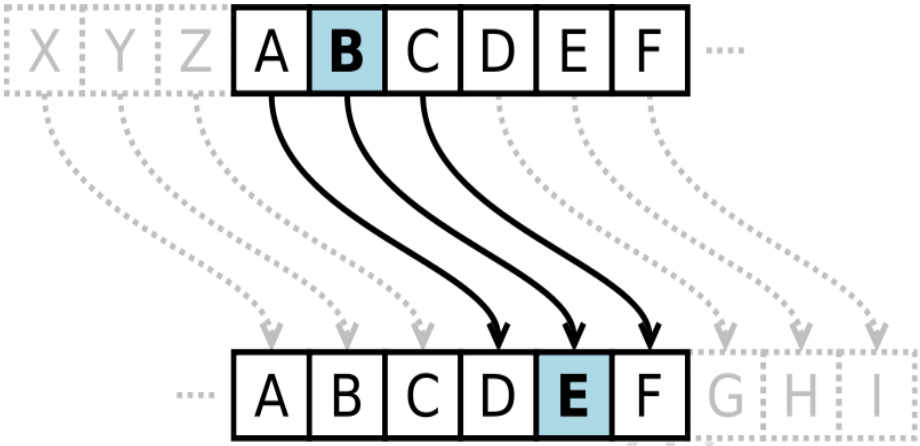
Ας δούμε τώρα πώς υλοποιείται κάθε αλγόριθμος :

Α) Κρυπτογράφηση με τον Αλγόριθμο του Καίσαρα

Ο **Κώδικας του Καίσαρα** είναι μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία. Είναι κώδικας αντικατάστασης στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο. Η μέθοδος πήρε το όνομά της από τον Ιούλιο Καίσαρα, ο οποίος την χρησιμοποιούσε στην προσωπική του αλληλογραφία.

Από τις παλιότερες μεθόδους κρυπτογράφησης είναι ο αλγόριθμος του Καίσαρα , όπου αν ένα γράμμα στο αρχικό κείμενο είναι το *Μ*ιοστό στο αλφάβητο ,αντικαθίσταται από το (*N+K*

)ιοστό γράμμα του αλφαβήτου , όπου *K* είναι ένας σταθερός ακέραιος (για τον αλγόριθμο του Καίσαρα *K=3*).



Για παράδειγμα, με μετατόπιση 3, το Α θα αντικαθιστούνταν από το Δ, το Β από το Ε, και ούτω καθεξής.

Παράδειγμα χρήσης του αλγορίθμου Caesar

Ο μετασχηματισμός μπορεί να αναπαρασταθεί με παράλληλη παράθεση δύο αλφαβήτων. Τα αλφάβητο κωδικοποίησης είναι το απλό αλφάβητο περιστρεμμένο δεξιά ή αριστερά κατά κάποιο αριθμό θέσεων. Για παράδειγμα ακολουθεί ένας κώδικας του Καίσαρα που χρησιμοποιεί αριστερή περιστροφή τριών θέσεων (η παράμετρος μετατόπισης, εδώ 3, χρησιμοποιείται ως κλειδί):

Απλό: ΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩ

Κώδικας: ΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓ

Όταν γίνεται κρυπτογράφηση, αναζητείται κάθε γράμμα της «απλής» γραμμής και γράφεται το αντίστοιχο γράμμα από την γραμμή του «κώδικα». Η αποκρυπτογράφηση γίνεται με την αντίστροφη φορά.

Κρυπτογραφημένο κείμενο: ΛΔΠΔΧΣΦ ΘΜΠΔΜ ΣΜ ΝΔΥΖΘΦ ΤΣΨ ΑΧΨΤΜΣΨΠΧΔΜ

Απλό κείμενο: θάνατος είναι οι κάργες που χτυπιούνται

Η κρυπτογράφηση μπορεί να αναπαρασταθεί με την χρήση αριθμητικής υπολοίπων αν πρώτα μετασχηματιστούν τα γράμματα σε αριθμούς, σύμφωνα με τον κανόνα, Α = 0, Β = 1,....

Ω = 23.[1] Η κρυπτογράφηση ενός γράμματος xμε μετατόπιση *n* μπορεί να περιγραφεί μαθηματικώς ως,[120]

$$E_n(x) = (x + n) \mod 24.$$

Η αποκρυπτογράφηση γίνεται αναλόγως,

$$D_n(x) = (x - n) \mod 24.$$

(Υπάρχουν διαφορετικοί ορισμοί για την πράξη modulo. Στα παραπάνω το αποτέλεσμα βρίσκεται στο εύρος 0...25. Ήτοι, αν *x+n* ή *x-n* δεν βρίσκονται στο εύρος 0...25, αφαιρείται ή προστίθεται 24.)

Η αντικατάσταση παραμένει η ίδια σε όλο το μήνυμα, έτσι ο κώδικας ταξινομείται ως μονοαλφαβητικής αντικατάστασης, σε αντίθεση με τους κώδικες πολυαλφαβητικής αντικατάστασης

Είναι άγνωστο το πόσο αποτελεσματικός ήταν ο κώδικας του Καίσαρα τον καιρό του, είναι όμως πιθανό ότι ήταν αρκετά ασφαλής, κυρίως επειδή οι περισσότεροι εχθροί του Καίσαρα ήταν αναλφάβητοι και οι υπόλοιποι θα υπέθεταν ότι τα μηνύματα ήταν γραμμένα σε μία άγνωστη ξένη γλώσσα.[121] Δεν υπάρχουν καταγραφές για τεχνικές λύσης κωδίκων απλής αντικατάστασης. Οι παλαιότερες σωζώμενες καταγραφές χρονολογούνται στον 9ο αιώνα στα έργα του άραβα Αλ Κιντί ο οποίος ανακάλυψε την μέθοδο ανάλυσης συχνοτήτων.[122]

Τον 19ο αιώνα, το τμήμα των προσωπικών διαφημίσεων των εφημερίδων χρησιμοποιούνταν για την ανταλλαγή κρυπτογραφημένων μηνυμάτων με απλούς κώδικες. Ο Ντέιβιντ Καν (1967) περιγράφει παραδείγματα εραστών που χρησιμοποιούσαν κρυπτογραφημένα με τον κώδικα του Καίσαρα μηνύματα για να επικοινωνήσουν μέσω των *The Times*.[123] Ακόμα και τόσο πρόσφατα όσο το 1915, ο κώδικας του Καίσαρα χρησιμοποιήθηκε από τον Ρωσικό στρατό σε αντικατάσταση πιο πολύπλοκων κωδίκων, οι οποίοι ήταν πολύ δύσκολοι για να εξοικειωθούν μαζί τους τα στρατεύματα. Επακόλουθο ήταν οι Γερμανοί και οι

---

[120] Wobst, Reinhard (2001). *Cryptology Unlocked*. Wiley. σελ. 19. ISBN 978-0-470-06064-3.

[121] ↑ Pieprzyk, Josef; Thomas Hardjono, Jennifer Seberry (2003). *Fundamentals of Computer Security*. Springer. σελ. 6. ISBN 3-540-43101-2.

[122] Singh, Simon (2000). *The Code Book*. Anchor. σελ. 14–20. ISBN 0-385-49532-3.

[123] Kahn, David (1967). *The Codebreakers*. σελ. 775–6. ISBN 978-0-684-83130-5).

Αυστριακοί κρυπταναλυτές να μην έχουν ιδιαίτερες δυσκολίες να αποκρυπτογραφήσουν τα μηνύματά τους.

Ο κώδικας του Καίσαρα μπορεί να βρεθεί σήμερα σε παιδικά παιχνίδια. Ένας κώδικας του Καίσαρα με μετατόπιση 13 χρησιμοποιείται από τον αλγόριθμο ROT13, μία απλή μέθοδο συσκότισης κειμένου που χρησιμοποιείται ευρέως στο Usenet για να συσκοτίζει το κείμενο (σε περιπτώσεις αστείων ή spoiler ιστοριών), αλλά δεν χρησιμοποιείται ως σοβαρή μέθοδος κρυπτογράφησης.

Ο κώδικας Vigenère χρησιμοποιεί τον κώδικα του Καίσαρα με διαφορετική μετατόπιση σε κάθε θέση του κειμένου. Η τιμή της μετατόπισης καθορίζεται από την χρήση μιας επαναλαμβανόμενης λέξης κλειδί. Αν η λέξη κλειδί είναι τόσο μεγάλη όσο το μήνυμα, επιλεγμένη τυχαία, και δεν χρησιμοποιηθεί ποτέ ξανά, τότε ο κώδικας είναι σημειωματάριο μίας χρήσης, και έχει αποδεικνύεται ότι δεν σπάει. Οι ιδανικές συνθήκες όμως είναι τόσο δύσκολο να ικανοποιηθούν που στην πράξη δεν γίνεται ποτέ. Λέξεις κλειδιά μικρότερες από το μύνημα εισάγουν κυκλικό μοτίβο το οποίο μπορεί να εντοπιστεί με στατιστικώς προηγμένη εκδοχή της ανάλυσης συχνοτήτων.[9]

Β) Κρυπτογράφηση με κλειδί πίνακα

Μια πολύ καλύτερη μέθοδος είναι να χρησιμοποιήσουμε ένα γενικό πίνακα που θα ορίζει την αλλαγή που πρέπει να γίνει : για κάθε γράμμα του κειμένου προς κρυπτογράφηση ,ο πίνακας λέει ποιο γράμμα να βάλουμε στο κρυπτογραφημένο κείμενο .Ο πίνακας που θα δίνει τις δικές μας αντιστοιχίες είναι ο παρακάτω (*key_arr*):

letters = [a b c d e f g h i j k l m n o p q r s t u v w x y z ! . , ?]

key_arr = [k o a p l n j b m e u f s q c t z w d y r i v h x g ? ! * ,]

Η υλοποίηση του αλγορίθμου είναι η ακόλουθη :

Βήμα 1 : Εισάγουμε το όνομα του αρχείου που θα επεξεργαστούμε καθώς και του αρχείου αποθήκευσης ή το κείμενο προς κρυπτογράφηση, αν η έξοδος γίνεται στην οθόνη.

Βήμα 2 : Διαβάζουμε έναν χαρακτήρα από το αρχείο εισόδου ή από το κείμενο που δώσαμε από το πληκτρολόγιο

Βήμα 3 : Αναζητούμε σειριακά το χαρακτήρα στον στον πίνακα letters.

Αν βρεθεί , γράφουμε στο αρχείο ή στην οθόνη το κωδικοποιημένο γράμμα που βρίσκεται στην αντίστοιχη θέση του πίνακα key arr. Αλλιώς πάμε στο Βήμα 4.

Βήμα 4 : Ελέγχουμε αν ο χαρακτήρας είναι η αλλαγή γραμμής ,το κενό ή αν είναι αριθμός και αντίστοιχα γράφουμε στο αρχείο εξόδου ή στην οθόνη την αλλαγή γραμμής, το κενό και αν είναι αριθμός τον γράφουμε αυξημένο κατά τρία.

Βήμα 5 : Αν έχουμε φτάσει στο τέλος του αρχείου ή αν βρήκαμε το χαρακτήρα τέλους των αλφαριθμητικών '\0'σταματάμε. Αλλιώς πάμε στο Βήμα 2.

Παράδειγμα για τον αλγόριθμο με κλειδί πίνακα

Ας δούμε πώς θα γίνει το μήνυμα που χρησιμοποιήσαμε στον αλγόριθμο του Καίσαρα με τον αλγόριθμο αυτό.

meet me at the park

Το κωδικοποιημένο μήνυμα θα είναι :

slly sl ky ybl tkwu

Αφού το m βρίσκεται στη 13η θέση του πίνακα letters θα αντικατασταθεί με το s που βρίσκεται στην 13η θέση του πίνακα key_arr. Ανάλογα θα αντικατασταθούν και τα υπόλοιπα γράμματα.

Αυτή είναι μια πολύ πιο ισχυρή μέθοδος από τη μέθοδο του Καίσαρα , καθώς ο κρυπταναλυτής θα πρέπει να δοκιμάσει πολλούς περισσότερους πίνακες (περίπου $27! > 10^{28}$) για να είναι σίγουρος ότι θα διαβάσει το μήνυμα. Πάντως , αλγόριθμοι "απλής αντικατάστασης" ,όπως αυτός , είναι εύκολο να σπάσουν λόγω της συχνότητας εμφάνισης γραμμάτων της γλώσσας . Για παράδειγμα , αφού το Ε είναι το πιο συχνό γράμμα σε αγγλικά κείμενα , ο κρυπταναλυτής μπορεί να κάνει μια καλή αρχή στο να διαβάσει το μήνυμα με το να ψάχνει για το γράμμα που εμφανίζεται συχνότερα στο κωδικοποιημένο κείμενο και να το αντικαθιστά με το Ε. Αν κι αυτή μπορεί να μην είναι η σωστή επιλογή ,είναι σαφώς καλύτερο από το να δοκιμάζεις και τα 26 γράμματα στην τύχη .

Ένας τρόπος για να κάνεις αυτό τον τύπο της επίθεσης πιο δύσκολο είναι να χρησιμοποιήσεις περισσότερους από έναν πίνακες . Ένα παράδειγμα αυτού του τύπου είναι ο αλγόριθμος Vigenere.

Γ) Αλγόριθμος κρυπτογράφησης Vigenere

Στον αλγόριθμο αυτό χρησιμοποιείται ένα μικρό επαναλαμβανόμενο κλειδί για να καθορίσει την τιμή του *K* για κάθε γράμμα .Σε κάθε βήμα , το γράμμα κλειδί προστίθεται στο γράμμα του κειμένου ώστε να μας δώσουν το κωδικοποιημένο γράμμα. Το κλειδί που χρησιμοποιήσαμε στον αλγόριθμό μας για την κρυπτογράφηση είναι :

key_table = [84 , 72 , 65 , 78 , 79 , 83] = ['T' , 'H' , 'A' , 'N' , 'O' , 'S']

Τα βήματα για την υλοποίηση του αλγορίθμου είναι τα ακόλουθα :

Βήμα 1 : Εισάγουμε το όνομα του αρχείου που θα επεξεργαστούμε καθώς και του αρχείου αποθήκευσης ή το κείμενο προς κρυπτογράφηση,αν η έξοδος γίνεται στην οθόνη και αρχικοποιούμε μετρητή i=o

Βήμα 2 : Διαβάζουμε έναν χαρακτήρα ***ch*** είτε από το αρχείο είτε από το αποθηκευμένο κείμενο που δώσαμε με το πληκτρολόγιο.

Βήμα 3 : Προσθέτουμε στον χαρακτήρα **ch** που διαβάσαμε τον αντίστοιχο αριθμό που βρίσκεται στην θέση ***key_table[i]*** και παίρνουμε έτσι το κωδικοποιημένο γράμμα , το οποίο είτε γράφουμε στο αρχείο εξόδου είτε εμφανίζουμε στην οθόνη.

Βήμα 4 : Αυξάνουμε το μετρητή i κατά ένα .Αν ο μετρητής είναι ίσος

με 6 τον μηδενίζουμε ,αφού θέλουμε να επαναλαμβάνεται

το κλειδί.

Βήμα 5 : Αν έχουμε φτάσει στο τέλος του αρχείου ή αν βρήκαμε το χαρακτήρα τέλους των αλφαριθμητικών '\0', σταματάμε.

Αλλιώς πάμε στο **Βήμα 2**.

Παράδειγμα για τον αλγόριθμο Vigenere

Ας δούμε πώς κωδικοποιείται το μήνυμα: meet me at the park

με τον αλγόριθμο Vigenere : A¦BoïHhÁBoHΌa´Y°EΏ

Στον αριθμό ASCII κάθε γράμματος προστίθεται ο αριθμός της θέσης του πίνακα-κλειδιού που τους αντιστοιχεί και το αποτέλεσμα είναι ένας νέος αριθμός ASCII που δείχνει ποιος χαρακτήρας θα εμφανιστεί.

Έτσι ,το m έχει ASCII 109 και του αντιστοιχεί η πρώτη θέση του πίνακα key_table ,δηλαδή το 84 .Επομένως ,το κωδικοποιημένο γράμμα είναι ο αριθμός ASCII 193.Ανάλογα κωδικοποιείται και το υπόλοιπο μήνυμα.

Βέβαια , δεν αρκεί μόνο να μπορείς να κρυπτογραφείς ένα κείμενο , χρειάζεται να μπορείς να το επαναφέρεις στην αρχική του μορφή ώστε να μπορεί να διαβαστεί από το δέκτη .Διαφορετικά , δε θα μπορέσουμε να επικοινωνήσουμε σωστά και η κωδικοποιημένη πληροφορία θα χαθεί . Για το λόγο αυτό ,παραθέτουμε στη συνέχεια τους αλγορίθμους αποκρυπτογράφησης των τριών παραπάνω αλγορίθμων κωδικοποίησης .

❖ ***Αποκρυπτογράφηση των Αλγορίθμων Κωδικοποίησης Δεδομένων***

Α) Αποκρυπτογράφηση του αλγορίθμου του Καίσαρα

Τα βήματα που θα ακολουθήσουμε είναι τα ίδια με της κρυπτογράφησης, αλλά τώρα για να μετατρέψουμε το κωδικοποιημένο σε κανονικό γράμμα δεν προσθέτουμε τον ακέραιο αριθμό *K =3* ,αλλά τον αφαιρούμε από κάθε γράμμα , το οποίο αποθηκεύουμε στο αρχείο εξόδου ή το εμφανίζουμε στην οθόνη.

Παράδειγμα αποκρυπτογράφησης του αλγορίθμου Caesar

Ας δούμε πώς θα αποκωδικοποιηθεί το μήνυμα

khoor wkhuh

που είχε κρυπτογραφηθεί με τον αλγόριθμο του Καίσαρα :

hello there

Έτσι ,το *k* μετατράπηκε σε *h* ,πήγαμε δηλαδή τρία γράμματα πίσω από το αρχικό γράμμα .Με τον ίδιο τρόπο , παίρνουμε το υπόλοιπο μήνυμα.

Β) Αποκρυπτογράφηση του αλγορίθμου με κλειδί πίνακα

Για την αποκρυπτογράφηση μηνυμάτων που χρησιμοποίησαν ως κλειδί πίνακα , το μόνο που αλλάζει από τον αλγόριθμο κρυπτογράφησης είναι ότι η αναζήτηση του χαρακτήρα που διαβάσαμε γίνεται στον πίνακα κλειδί ***key_arr*** και αν βρεθεί στη θέση ***I*** του πίνακα αυτού, αντικαθίσταται από το ***letters[I]*** για να πάρουμε το αποκωδικοποιημένο γράμμα. Επιπλέον,αν ο χαρακτήρας είναι ***αριθμός*** τον αποκωδικοποιούμε αφαιρώντας ***3***.

Παράδειγμα αποκρυπτογράφησης του αλγορίθμου με πίνακα ως κλειδί

Το κωδικοποιημένο μήνυμα είναι:

jmil sl 8 pcffkwd

και θα γίνει:

give me 5 dollars

Το ***j*** βρίσκεται στην ***έβδομη*** θέση του ***key_arr*** ,επομένως το αποκωδικοποιημένο γράμμα θα είναι το ***letters[7]*** ,που είναι το ***g***.

Από το ***8*** που είναι αριθμός ***αφαιρούμε 3*** και προκύπτει το ***5*** . Τα υπόλοιπα γράμματα προκύπτουν κατά ανάλογο τρόπο.

Γ) *Αποκρυπτογράφηση του αλγορίθμου Vigenere*

Για την αποκρυπτογράφηση των χαρακτήρων που διαβάζουμε από το αρχείο εισόδου, αφαιρούμε από τον κάθε χαρακτήρα τον αριθμό που βρίσκεται στη θέση ***key_table[i]*** ,(όπου ***i*** ένας μετρητής που αρχίζει από το μηδέν και μηδενίζεται όταν γίνει ίσος με το 6) κι έτσι παίρνουμε τον ASCII του αποκωδικοποιημένου χαρακτήρα.

Παράδειγμα αποκρυπτογράφησης του αλγορίθμου Vigenere

Το μήνυμα είναι το :

H¦nΘBlhΆBo

και μετά την αποκρυπτογράφηση γίνεται :

see you at 6

Έτσι ,αφαιρώντας από το ASCII του ***H*** το ***key_table[1]=84*** παίρνουμε το ***s*** .Ανάλογη διαδικασία γίνεται για κάθε γράμμα μέχρι να τελειώσει το αρχείο ή να βρούμε το τέλος του αλφαριθμητικού, αν η εισαγωγή γίνεται από την οθόνη.

Μοντέρνα κρυπτοσυστήματα

Τα μοντέρνα κρυπτοσυστήματα χωρίζονται με βάση τα κλειδιά σε:

- Μυστικού ή Συμμετρικού κλειδιού (symmetric key) χρησιμοποιούν το ίδιο μυστικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση

- Δημοσίου ή Ασύμμετρου κλειδιού (public or Asymmetric key) χρησιμοποιούν διαφορετικό κλειδί για κρυπτογράφηση (δημόσιο κλειδί παραλήπτη) και διαφορετικό για αποκρυπτογράφηση (προσωπικό κλειδί παραλήπτη).

ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί . Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων

Μοντέρνο συμμετρικό σύστημα

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- *Δέσμης (Block Ciphers)*, οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
- *Ροής (Stream Ciphers)*, οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα.

Συμμετρικοί Κρυπταλγόριθμοι Τμήματος (Block Ciphers)

- Data Encryption Standard
- 3-Way
- ,Blowfish,
- CAST ,
- CMEA ,
- Triple-DES,
- DEAL FEAL ,
- GOST
- ,IDEA ,
- LOKI ,
- Lucifer,
- MacGuffin,
- Twofish
- MARS ,
- MISTY ,
- MMB
- ,NewDES
- ,RC2,
- RC5 , RC6
- REDOC ,
- Rijndael ,
- Safer ,
- Serpent,SQUARE
- , Skipjack
- ,Tiny Encryption Algorithm

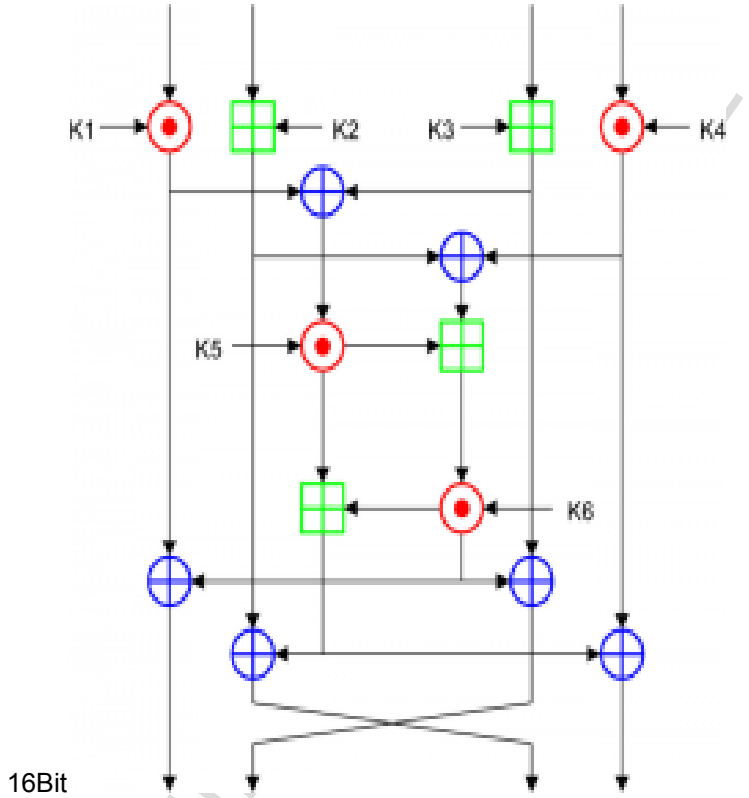
Συμμετρικοί Κρυπταλγόριθμοι ροής (Stream Ciphers) :

- ORYX ,RC4 , SEAL

Αξίζει να αναφερθούν κάποιες σημαντικές πληροφορίες για τους παρακάτω αλγόριθμους:

- Αλγόριθμος IDEA (International Data Encryption Algorithm)

Ο αλγόριθμος IDEA αποτελεί συμμετρικό κωδικοποιητή τμημάτων , που αναπτύχτηκε από τους X.Loi και j.Massey στο Swiss Federal institute of technology , το 1991.Ο idea χρησιμοποιεί block μεγέθους 64Bit και κλειδιά 128bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις . Ο IDEA διαφέρει από το DES τόσο στην συνάρτηση F, όσοκαι στην συνάρτηση παραγωγής των υποκλειδιών. Για την συνάρτηση F, ο IDEA δεν χρησιμοποιεί S-boxes αλλά στηρίζεται σε τρεις διαφορετικές μαθηματικές λειτουργίες την δυαδική πράξη XOR,την δυαδική πρόσθεση ακεραίαων των 16bit και το δυαδικό πολλαπλασιασμό ακεραίων των



Αλγόριθμος IDEA

- Αλγόριθμος Rijidael

Ο αλγόριθμος αυτός, έχει υιοθετηθεί πλέον ως ο αλγόριθμος AES, χαρακτηρίζεται

- ✓ Από απλότητα
- ✓ Από ευελιξία

- ✓ Από ανθεκτικότητα

Σε όλες τις γνωστές κρυπταναλυτικές επιθέσεις και υψηλή ταχύτητα λειτουργίας. Ο αλγόριθμος αυτός, δεν ακολουθεί την κλασσική δομή του Feistel, αλλά κάθε κύκλος λειτουργίας περιλαμβάνει τρεις όμοιους μετασχηματισμούς, με όρους ισότιμης αντιμετώπισης κάθε ξεχωριστού Bit,γνωστής ως επίπεδα.

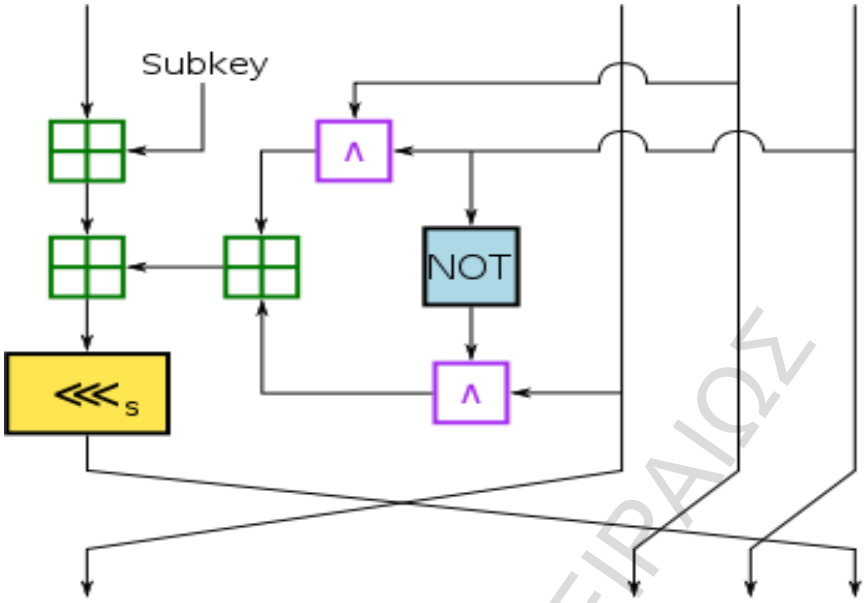
- ✓ Το επίπεδο γραμμικής ανάμιξης επιτυγχάνει υψηλή διάχυση σε πολλαπλούς κύκλους
- ✓ Το μη γραμμικό επίπεδο αφορά στην παράλληλη εφαρμογή S-boxes τα οποία εμφανίζουν εξαιρετικές μη γραμμικές ιδιότητες για το ενδεχόμενο χειρότερης περίπτωσης
- ✓ Το επίπεδο πρόσθεσης κλειδιού αφορά στην συσχέτιση των ενδιάμεσα προκύπτοντας αποτελέσματος με το υποκλειδί του κύκλου, με την πράξη XOR

Αλγόριθμος DES

Ο DES θεωρείται πλέον ανασφαλής για πολλές εφαρμογές. Αυτό οφείλεται κυρίως στο μικρό μέγεθος του κλειδιού του, που έχει μήκος 56 μπιτ. Τον Ιανουάριο του 1999 οι εταιρείες "Distributed.net" και "Electronic Frontier Foundation", κατόπιν συνεργασίας, “έσπασαν” δημοσίως ένα κλειδί του DES μέσα σε 22 ώρες και 15 λεπτά. Υπάρχουν, επίσης, ορισμένα αναλυτικά αποτελέσματα που καταδεικνύουν θεωρητικές αδυναμίες στον κρυπταλγόριθμο, αν και είναι ανέφικτο να υλοποιηθούν στην πράξη. Θεωρείται πως ο αλγόριθμος είναι πρακτικά ασφαλής υπό τη μορφή του τριπλού DES (triple DES), αν και υπάρχουν θεωρητικές αμφισβητήσεις. Τα τελευταία χρόνια ο κρυπταλγόριθμος DES έχει εκτοπιστεί από το Προηγμένο Πρότυπο Κρυπτογράφησης Στις 17 Μαρτίου του 1975 ο προτεινόμενος DES δημοσιεύθηκε στον Ομοσπονδιακό κατάλογο (Federal Register). Ζητήθηκαν δημόσια σχόλια και, στο έτος που ακολούθησε, δύο ανοικτά εργαστήρια κλήθηκαν για να συζητήσουν τα προτεινόμενα πρότυπα. Υπήρξε κριτική από διάφορα μέλη, ανάμεσα στους οποίους ήταν και οι πρωτοπόροι στην κρυπτογραφία δημοσίου κλειδιού Μάρτιν Χέλμαν (Martin Hellman) και Ουίτφιλντ Ντίφι (Whitfield Diffie), οι οποίοι ανέφεραν μικρότερο μήκος κλειδιού για τον DES καθώς και τα μυστήρια "S-boxes" ως στοιχεία ανάρμοστης παρέμβασης από την NSA.

Αλγόριθμος RC2-RC4

Ο αλγόριθμος RC2 και RC4 σχεδιάστηκαν από τον Ron Rivest παρέχουν ποικιλία ως προς το μέγεθος του κλειδιού κρυπτογράφησης.Οι δύοι αυτοί αλγόριθμοι θεωρούνται λίγο πιο γρήγοροι από τον DESκαι μπορούν να γίνουν ακόμα πιο ασφαλείς εάν επιλέξουμε μεγαλύτερο μήκος κλειδιού. Ο αλγόριθμος RC2 αποτελεί μια ομάδα κρυπτογράφησης και μπορεί να χρησιμοποιηθεί στην θέση του DES. Ο RC2 είναι ένα «ρεύμα» ψηφίων κρυπτογράφησης και θεωρείται περίπου 10 φορές πιο γρήγορος από τον DES.



Αλγόριθμος RC2

Αλγόριθμος RC5

Ο αλγόριθμος αυτός αναπτύχθηκε το 1994 από το R.Rivest. Σχεδιάστηκε για να υποστηρίζει τα ακόλουθα χαρακτηριστικά:

- Κατάλληλος για υλοποίηση σε υλικό ή λογισμικό,ο RC5 χρησιμοποιεί μόνο ασικές υπολογιστικές λειτουργίες , που συνήθως περιλαμβάνονται στους μικροεπεξεργαστές
- Ταχύς: προκειμένου α επιτευχθεί υψηλή ταχύτητα, ο RC5 είναι ένας απλός αλγόριθμος που βασίζεται στην λέξη (word)
- Προσαρμόσιμος σε επεξεργαστές διαφορετικών μήκων λέξης: ο αριθμός των δυαδικών ψηφίων σε μία λέξη αποτελεί παράμετρο του RC5, έτσι ώστε τα διαφορετικά μήκη λέξης παράγουν διαφορετικούς αλγόριθμους.
- Μεταβλητό μήκος γύρων : ο αριθμός των γύρων αποτελεί δεύτερη παράμετρο του RC5
- Απλός: η απλή δομή του RC5 υλοποιείται εύκολα και διευκολύνει τον υπολογισμό της ισχύος του αλγορίθμου
- Χαμηλή απαίτηση μνήμης: η χαμηλή απαίτηση μνήμης καθιστά τον αλγόριθμο RC5 κατάλληλο για αξιοποίηση σε έξυπνες κάρτες και άλλες συσκευές περιορισμένης μνήμης.

- Αλγόριθμος TRIPLE DES: βασίζεται στον DES αλγόριθμο κρυπτογραφεί μια ομάδα δεδομένων τρεις φορές με τρεία διαφορετικά κλειδιά. Έχει προταθεί σαν εναλλακτική λύση αντί του DES , γιατί υποστηρίζεται ότι τον τελευταίο καιρό έχει γίνει πιο εύκολο και πιο γρήγορο το ¨σπάσιμο¨ του DES αλγορίθμου.

- Αλγόριθμος RSA:

  ονομάστηκε έτσι από τους σχεδιαστές του rivest, Shamir και Adelman. Εϊναι ένας αλγόριθμος «δημοσίου κλειδιού» ο οποίος υποστηρίζει μια ποικιλία μήκους κλειδιών , καθλως επίσης πικιλία όσον αφορά το μέγεθος του σώματος του κειμένου προς κρυπτογράφηση . Το απλό block κειμένου πρέπει να είναι μικρότερο από το μήκος του κλειδιού. Το συνηθισμένο μήκους κλειδιού είναι 512 bits.

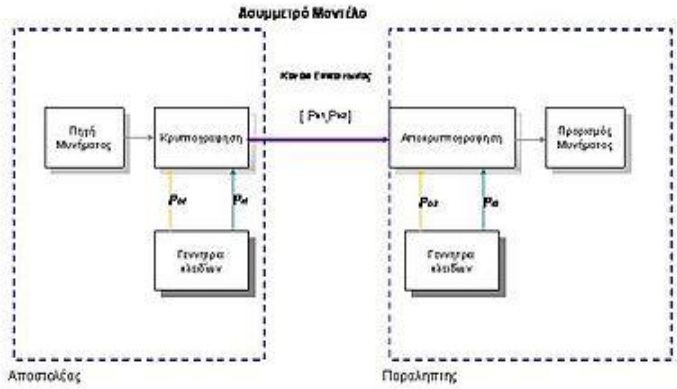
<u>Κρυπταναλυτικές επιθέσεις σε αλγορίθμους</u>

Υπάρχουν έξι βασικές κρυπταναλυτικές επιθέσεις, κατηγοριοποιημένες ανάλογα με την ικανότητα του αντιπάλου (πόρους-υπολογιστική ισχύ) και το επίπεδο πρόσβασης που έχει ο επιτιθέμενος:

1. Επίθεση βασισμένη στο κρυπτοκείμενο : Ο κρυπταναλυτής έχει στην διάθεση του Ν κρυπτομηνύματα με δεδομένη τη γνώση του αλγορίθμου. Σκοπός είναι να ανακαλύψει τα μηνύματα που περικλείουν τα κρυπτοκείμενα ή να εξαγάγει το κλειδί που χρησιμοποιήθηκε.
2. Επίθεση βασισμένη στην γνώση μηνυμάτων κρυπτοκειμένων : Ο κρυπταναλυτής έχει στην διάθεση του μερικά ζευγάρια (μηνυμάτων, κρυπτοκειμένων). Ο στόχος είναι η εξαγωγή του κλειδιού ή ενός αλγορίθμου για την αποκρυπτογράφηση νέων μηνυμάτων (προσεγγιστικός αλγόριθμος) με το ίδιο κλειδί.
3. Επίθεση βασισμένη στην επιλογή μηνυμάτων : Ο κρυπταναλυτής έχει καταφέρει να αποκτήσει πρόσβαση στη επιλογή του μηνύματος που θα κρυπτογραφηθεί. Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσεγγιστικού αλγορίθμου.
4. Προσαρμοσμένη επίθεση, βασισμένη στην επιλογή μηνυμάτων : Ο κρυπταναλυτής μπορεί να επιλέξει όχι μόνο μία συστάδα μηνυμάτων αλλά μπορεί να επιλέξει ποιο επόμενο μήνυμα θα κρυπτογραφηθεί(Κατάλληλη επιλογή ζευγαριών προσδίδει περισσότερη πιθανότητα για την τιμή του κλειδιού). Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσεγγιστικού αλγορίθμου.
5. Επίθεση βασισμένη στην επιλογή κρυπτοκειμένων: Ο κρυπταναλυτής μπορεί να επιλέξει κρυπτοκείμενα για αποκρυπτογράφηση (μελετά πώς συμπεριφέρεται ο αλγόριθμος στην αποκρυπτογράφηση) και έχει πρόσβαση στα αποκρυπτογραφημένα κείμενα.
6. Προσαρμοσμένη επίθεση βασισμένη στην επιλογή μηνυμάτων - κλειδιών: Ο κρυπταναλυτής επιλέγει μια σχέση μεταξύ του άγνωστου κλειδιού και του δικό του κλειδιού και βάση των συμπερασμάτων που βγάζει από την ανάλυση (Είσοδος/έξοδος) στο σύστημα - στόχο και στο δικό του αντίγραφο (Κρυπταλγόριθμος) προσεγγίζει, μετά από κάποιες δοκιμές, το σωστό κλειδί.

ΑΣΎΜΜΕΤΡΑ ΚΡΥΠΤΟΣΥΣΤΉΜΑΤΑ

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο .Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.



[124]Στην ασύμμετρη κρυπτογράφηση χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση : το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες :

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

Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο Η βασική αρχή αυτής της κρυπτογραφίας δημοσίου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman , ενώ

[124] STALLINGS W..,(2003) “Cryptography and Network Security :Principles and Practice”

το 1977 οι Rivest , Shamir και Adleman , βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτόσυστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού.

Προκειμένου, να επιτευχθεί η επικοινωνία με τον χρήστη ασύμμετρης κρυπτογραφίας , ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά. Κάθε χρήστης, λοιπόν, έχει στην κατοχή του ένα ζεύγος κλειδιών , το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται ενώ η ιδιωτική κλείδα κρατείται μυστική και δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και η επιβεβαιωμένη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους ώστε να μην είναι δυνατή ή σκόπιμη η πλαστοπροσωπία Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία , συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνον από τον ιδιοκτήτη του και δεν μεταδίδεται πότε. Όταν ένα μήνυμα έχει κρυπτογραφεί με το δημόσιο κλειδί κάποιου χρήστη , μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, για αυτό και η γνώση του δημοσίου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από την συμμετρική. Έχει όμως ένα μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποίει είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής. Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολή και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β , χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που «ακούει» την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνος που γνωρίζει την ιδιωτική κλείδα. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κτρυπτογραφία για να υπογράψει ένα μήνυμα τότε, πραγματοποιεί έναν υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού, καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα . Για να επαληθευτεί την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και τη υπογραφή. Ένα το αποτέλεσμα είναι θετικό , τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

Λίστα Ασύμμετρων Κρυπταλγορίθμων

- RSA
- Πρωτόκολλο Diffie-Hellman
- DSA
- Paillier
- Πρότυπο ElGamal - Υπογραφή ElGamal
- Κρυπτογραφία ελλειπτικών καμπυλών

Εφαρμογές της κρυπτογραφίας δημοσίου κλειδιού

4.4 Ψηφιακές υπογραφές

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

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

[125] http://www.eett.gr

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

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).

Δημιουργία ψηφιακής υπογραφής

Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.

2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

3.Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

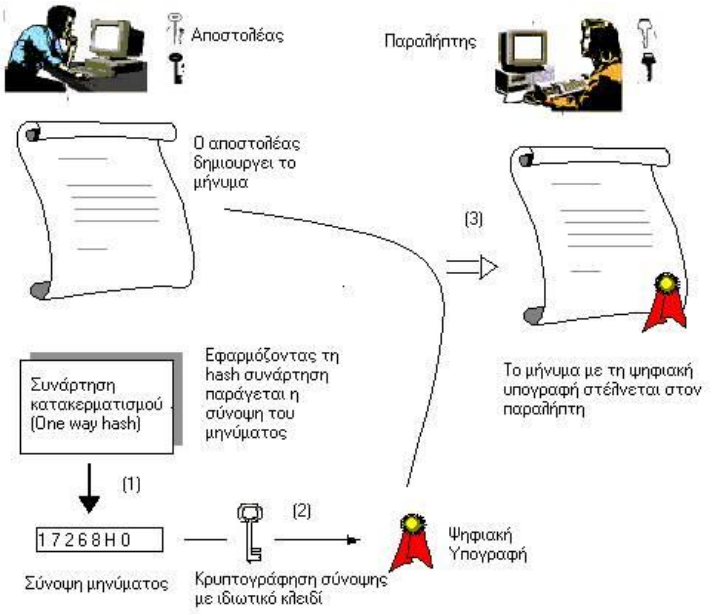
Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη

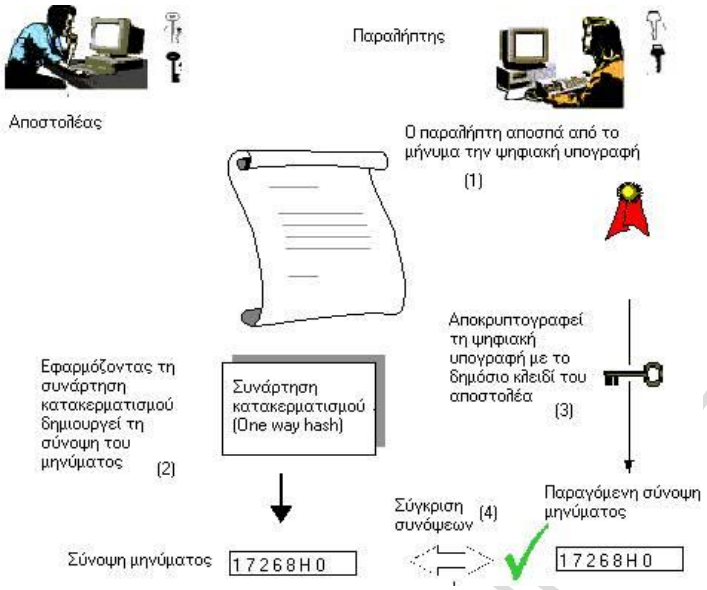
2.Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

3.Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.



Επαλήθευση ψηφιακής υπογραφής



Με τον όρο «ηλεκτρονική υπογραφή» δεν νοείται απλά η ηλεκτρονική αποτύπωση της ιδιόχειρης αλλά στην ουσία πρόκειται για «μια κλειδωμένη σύντμηση ενόςηλεκτρονικού κειμένου», η οποία θα μπορούσε να χαρακτηρισθεί και ως» δακτυλικό αποτύπωμα» αυτού [126].

Η ηλεκτρονική υπογραφή έχει ποικίλες μορφές, όπως π.χ. την βιομετρική υπογραφή, την τοποθέτηση πάνω σε ένα ηλεκτρονικό κείμενο μιας ιδιόχειρης υπογραφής με την χρήση scanner 'η άλλων μέσω. Δηλαδή, ο όρος « ηλεκτρονική υπογραφή» υπό ευρεία έννοια περιλαμβάνει ένα σύνολο μεθόδων, οι οποίες χρησιμοποιούνται προκειμένου να επιτελέσουν την ίδια εργασία με την ιδιόχειρη υπογραφή, δηλα΄δη σκοπούν να πιστοποιήσουν την ταυτότητα του υπογράφοντος. Μ ε άλλα λόγια , αποτελεί μια γενικότερηέννοια , στην οποία περιλαμβάνεται και η ειδική έννοια της ψηφιακής υπογραφής. Η ψηφιακή υπογραφή αποτεέι την πιο προηγμένη και ασφαλή μέθοδο αναγνώρισης της γνησιότητας του εκδότη ηλεκτρονικού εγγράφου, που δημιουργείται βάσει του ασύμμετρου κρυπτογραφικού συστήματος[127]

4.5 Ψηφιακά πιστοποιητικά

[128]Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο

[126] Βλ.Παπαθωμά-Μπέτεγκε ,ο.π. 1241 , Πιτσιρίκο , ο.π σελ.393-394 υποσημ. 26, Μανιώτη σελ. 43 Μαρίνο. ΤΟ internet και οι συνέπειες του κυρίως στον χώρο του δικαίου , Ελλ ΔΝ 39, 1, επ.7

[127] Βλ. Λιναρίτη, η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών μετά την ενσωμάτωση της Οδηγίας 99/93 τη ΕΕ στο ελληνικό δίκαιο με το ΠΔ 150/2001.

[128] http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#2

κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (μη αποποίηση).

[129]Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί.

Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

[130]Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.

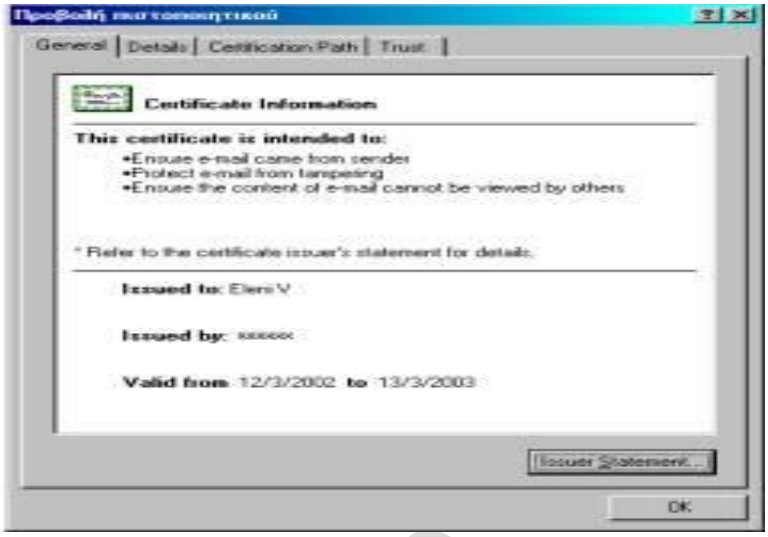
Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου

[129] http://www.eett.gr

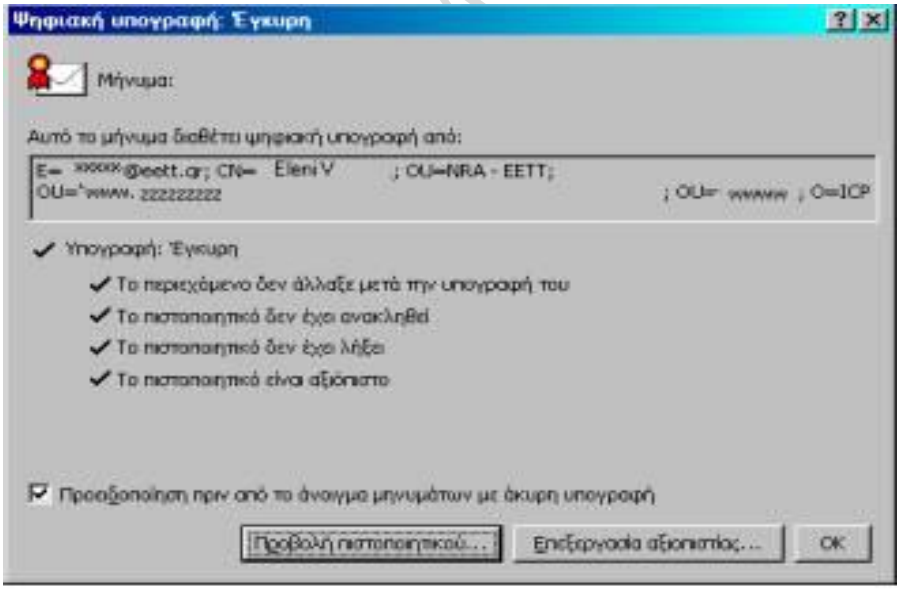
[130] http://www.eett.gr

Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Παράδειγμα προβολής πιστοποιητικού



Ένδειξη ψηφιακής υπογραφής σε μήνυμα με πιστοποιητικό



[131]Για να υπάρχει ασφάλεια στις εφαρμογές ηλεκτρονικού εμπορίου απαιτείται η ύπαρξη ενός ασφαλούς εξυπηρετητή διαδικτύου(web server). Ο εξυπηρετητής διαδικτύου πρέπει να προστατεύσει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης του πελάτη στον εξυπηρετητή του καταστήματος. Το SSL (Secure Socket Layer) είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκοσμίου Ιστού , το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft.

4.6 Το Νομικό πλαίσιο

Για την εγκυρότητα μιας καθημερινής συναλλαγής απαιτείται η υπογραφή του συναλλασσόμενου. Η υπογραφή σε ένα κείμενο, αποτελεί απόδειξη ότι το υπογράφον το περιεχόμενο του κειμένου πρόσωπο γνωρίζει, αναγνωρίζει, αποδέχεται το κείμενο αυτό. Ο υπογράφων δεν μπορεί να αρνηθεί το από αυτόν υπογεγραμμένο περιεχόμενο, εκτός από συγκεκριμένες περιπτώσεις εκδήλωσης παραβατικής συμπεριφοράς (πλαστογραφία, απάτη κ.λπ). Ένα υπογεγραμμένο κείμενο έχει νομική υπόσταση και επικυρώνει τη συναλλαγή.

Το Π.Δ. 150/2000 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν.

Επιπλέον, το προεδρικό Διάταγμα, εκτός των άλλων,

- καθόρισε τους όρους που πρέπει να ισχύουν σε ψηφιακά πιστοποιητικά για να θεωρούνται αναγνωρισμένα πιστοποιητικά και τους όρους που πρέπει να πληρούν οι Πάροχοι Υπηρεσιών Πιστοποίησης για να παρέχουν αναγνωρισμένα πιστοποιητικά.
- έθεσε τις αρχές λειτουργίας της εσωτερικής αγοράς όσον αφορά την παροχή υπηρεσιών πιστοποίησης
- έθεσε τις προϋποθέσεις νομικής αναγνώρισης εντός ΕΕ των αναγνωρισμένων πιστοποιητικών που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης εγκατεστημένους σε χώρες εκτός ΕΕ, και άλλες σχετικές προβλέψεις που αφορούν διεθνείς πτυχές.
- έθεσε το πλαίσιο της ευθύνης των Παρόχων Υπηρεσιών Πιστοποίησης
- ανέθεσε στην ΕΕΤΤ συγκεκριμένες αρμοδιότητες.

[131] http://www.kollas.gr/index.php?option=com_content&view=article&id=277:--ssl-secure-sockets-layer&catid=42:2011-02-23-07-53-15&Itemid=194

Οι αρμοδιότητες της ΕΕΤΤ όπως απορρέουν από το ΠΔ 150/2001, είναι επιγραμματικά οι εξής:

- Η παροχή Εθελοντικής Διαπίστευσης, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης, προκειμένου να επιτευχθεί βελτιωμένο επίπεδο παροχής υπηρεσιών πιστοποίησης. (άρθρο 4 παρ. 5 εδ.α) ή η ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού. Με την Εθελοντική Διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον Πάροχο Υπηρεσιών Πιστοποίησης.
- Η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το Παράρτημα ΙΙΙ του πδ. 150/2001 (εφόσον η ΕΕΤΤ αναθέσει τέτοια καθήκοντα σε άλλους φορείς) (άρθρο 4 παρ. 8).
- Η διαπίστωση της συμμόρφωσης των διατάξεων δημιουργίας υπογραφής (υλικού ή λογισμικού που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού για τη δημιουργία της ηλεκτρονικής υπογραφής) προς το Παράρτημα ΙΙΙ του Προεδρικού Διατάγματος 150/2001 (άρθρο 4 παρ. 2, εδ.α) ή ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού.
- Η επιβολή προστίμων σε Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι ενεργούν ως διαπιστευμένοι, χωρίς να είναι (άρθρο 4 παρ.9)
- Η ενημέρωση της Ευρωπαϊκής Επιτροπής για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και για τυχόν αλλαγές στις παραπάνω πληροφορίες (άρθρα 8 παρ. 2 και 3).

Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β/16-5-2002) ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.[132]

4.7 Το πρωτόκολλο SSL/TLS

Το **πρωτόκολλο SSL (Secure Sockets Layer)** αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

[132] http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES - Data Encryption Standard, DSA - Digital Signature Algorithm, KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4, RSA, SHA-1 - Secure Hash Algorithm, SKIPJACK, Triple-DES.

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. 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 θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.

3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.
4. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
7. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

SSL Handshake Protocol

Το SSL Handshake Protocol είναι το περισσότερο περίπλοκο πρωτόκολλο από τα χρησιμοποιούμενα στο SSL. Επιτρέπει σε server και σε client να:

- πιστοποιήσουν ο ένας την αυθεντικότητα του άλλου
- να διαπραγματευθούν για το ποιοι αλγόριθμοι κρυπτογράφησης και MAC θα χρησιμοποιηθούν
- διαπραγματεύονται για τα κρυπτογραφικά κλειδιά που θα χρησιμοποιηθούν

Παρακάτω θα δούμε τρεις διαφορετικές περιπτώσεις επικοινωνίας.

1. C → S : *Client_Hello*

2. S → C : Server_Hello

Certificate

Server_Key_Exchange

Certificate_Request

Server_Hello_Done

3. C → S : Certificate

Client_Key_Exchange

Certificate_Verify

Change_Cipher_Spec

Finished

4. S → C : Change_Cipher_Spec

Finished

Με το μήνυμα **client-hello** στέλνει ο client στον server μια λίστα με τους αλγόριθμους που υποστηρίζει και τα challenge-data που θα χρησιμοποιηθούν αργότερα για την πιστοποίηση της ταυτότητας του.

Το μήνυμα **server-hello** επιστρέφει στον client ένα αναγνωριστικό της σύνδεσης (connection-id), την επιλογή του server όσον αναφορά πακέτο των αλγόριθμων κρυπτογράφησης και συμπίεσης (που και οι δύο υποστηρίζουν) και το πιστοποιητικό του server που θα χρησιμοποιηθεί από τον client για την απόκτηση της δημόσιας κλείδας του server. Στην τελευταία έκδοση του

Το **client-master-key** και το master-key, που ανάλογα με το που βρίσκεται κάθε υπολογιστής, μπορεί να έχει δυο διαφορετικές μορφές. Για SSL εφαρμογές έξω από τις Ηνωμένες Πολιτείες, τα 88 bits του master-key μεταδίδονται μη κρυπτογραφημένα και κρυπτογραφούνται τα υπόλοιπα 40 bits με την δημόσια κλείδα του server. Αντίθετα για SSL εφαρμογές εντός των Ηνωμένων Πολιτειών, κρυπτογραφείται όλο το master-key και το clear-master-key είναι άδειο.

[133]Από αυτό το σημείο και μετά όλα τα μηνύματα κρυπτογραφούνται στο επίπεδο του SSL Record Protocol. Το master-key δεν χρησιμοποιείται άμεσα για κρυπτογράφηση, αλλά για την παραγωγή δύο ζευγάρια κλειδιών. Το ένα ζευγάρι ανήκει στον client και αποτελείται από το *client-write-key* που χρησιμοποιεί ο client για να κρυπτογραφήσει τα μηνύματα προς τον server και το *client-read-key* για να αποκρυπτογραφήσει ότι λαμβάνει από αυτόν. Το δεύτερο ζευγάρι ανήκει στον server και αποτελείται από το *server-write-key* για κρυπτογράφηση μηνυμάτων προς τον client και το *server-read-key* για αποκρυπτογράφηση των παραληφθέντων. Για την ακρίβεια, το client-write-key είναι το ίδιο με το server-read-key και το client-read-key είναι το ίδιο με το server-write-key.

Το **client-finish** περιέχει το αναγνωριστικό της σύνδεσης που αρχικά είχε σταλεί από τον server κρυπτογραφημένο με το client-write-key.

Το **server-verify** περιέχει τα challenge-data που είχε στείλει ο client στον server κατά την αρχή της σύνδεσης, κρυπτογραφημένα με το server-write-key. Η παραλαβή και αποκρυπτογράφηση αυτού του μηνύματος είναι το τελικό στάδιο για την επιβεβαίωση της ταυτότητας του server καθ' ότι μόνο ο αληθινός server θα μπορούσε να αποκρυπτογραφήσει με την ιδιωτική του κλείδα το master-key.

Τέλος, το μήνυμα **server-finish** τερματίζει το handshake. Περιέχει το session-id που χρησιμοποιείται σε επόμενες διαδικασίες handshake για την αποφυγή επανάληψης της φάσης επιλογής αλγορίθμων και ανταλλαγής του master-key. Το session-id αποθηκεύεται και από τους δύο και η προτεινόμενη διάρκεια ζωής είναι 100 δευτερόλεπτα. Έπειτα, αχρηστεύετε.

<u>ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ ΚΑΙ SMART CARDS</u>

Με την λεγόμενη « έξυπνη κάρτα» η ηλεκτρονικά αποθηκευμένη στην κάρτα αξία αγοράζεται από τον χρήστη και μειώνεται μετά από κάθε χρήση της για την πραγματοποίηση πληρωμών. Πέρα από την έξυπνη κάρτα « μέσο αποθήκευσης» μπορεί να είναι και η μνήμη ενός ηλεκτρονικού υπολογιστή. Πρόκειται για μορφές του λεγόμενου «ηλεκτρονικού χρήματος». Εδώ υπάγονται και οι προπληρωμένες κάρτες πολλαπλών χρήσεων και τα προπληρωμένα προϊόντα λογισμικού, εγκατεστημένα στην μνήμη ηλεκτρονικού υπολογιστή συνδεδεμένου με το διαδίκτυο (digital cash- ψηφιακά μετρητά)[134].

Ο συνδυασμός κωδικών πρόσβασης και έξυπνης κάρτας κερδίζει έδαφος , καθώς και οι περισσότεροι κατασκευαστές περιφερειακών (πληκτρολογίων κ.πλ.) ενσωματώνουν

[133] http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ssl.htm

[134] Βλ. Σιδηρόπουλο. Το δίκαιο του διαδικτύου , 2003 σελ. 25-26

αναγνώστες στα προϊόντα τους. Το ίδιο συμβαίνει και με τις συσκευές αναγνώρισης αποτυπωμάτων , καθώς όσο ασφαλής και αν είναι η smart card σε σχέση με το ψηφιακό πιστοποιητικό εγκυμονεί τον κίνδυνο απώλειας ή κλοπής κάτι που δεν συμβαίνει με τα ανθρώπινα αποτυπώματα. Αλλά φυσικά χαρακτηριστικά που χρησιμοποιούνται με την ταυτοποίηση, εκτός των αποτυπωμάτων , είναι η ίριδα

4.8 Το Πρωτόκολλο PEM

[135]Το πρωτόκολλο *Privacy-Enhanced Mail (PEM)* προβλέπει για αυτή την αδυναμία του ηλεκτρονικού ταχυδρομείου του Internet, προσθέτοντας την εφαρμογή των υπηρεσιών της απόρρητης συναλλαγής, της πιστοποίησης ταυτότητας, της ακεραιότητας των μηνυμάτων και την εξασφάλιση της μη αποκήρυξης της πηγής. Οι υπηρεσίες αυτές προσφέρονται μέσω της χρήσης απ' άκρη σ' άκρη κρυπτογράφησης μεταξύ του αποστολέα και του παραλήπτη. Δεν απαιτούνται ειδικές ικανότητες επεξεργασίας στα συστήματα MTS (Message Transfer System) και υποστηρίζεται η συνεργασία με άλλα ταχυδρομικά συστήματα μεταφοράς.

Οι προδιαγραφές του PEM διαχωρίζουν τρεις τύπους μηνυμάτων:

- μηνύματα **MIC-CLEAR** , που περιέχουν μια MIC υποστηρίζουν τις υπηρεσίες αυθεντικοποίησης μηνύματος , ακεραιότητας δεδομένων και μη αμφισβήτησης προέλευσης.
- **ENCRYPTED:** Αναπαριστά ένα PEM μήνυμα στο οποίο έχουν εφαρμοστεί οι υπηρεσίες της διαφύλαξης του απόρρητου της συναλλαγής, της εξασφάλισης της ακεραιότητας των δεδομένων, της πιστοποίησης ταυτότητας και της εξασφάλισης της μη αποκήρυξης της πηγής.
- **MIC-ONLY:** Αναπαριστά ένα PEM μήνυμα στο οποίο παρέχονται όλες οι προηγούμενες υπηρεσίες εκτός της διαφύλαξης του απόρρητου. Μόνο οι UAs που ενσωματώνουν το PEM μπορούν να παρουσιάσουν το μήνυμα για ανάγνωση.

[135] http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/pem.htm

Αποφάσεις Αρχές Προστασίας Δεδομένων είναι οι ακόλουθες:

Α)ΑΠΟΦΑΣΗ 83/2009

ΠΑΡΑΝΟΜΗ Η ΣΥΛΛΟΓΗ ΔΙΕΥΘΥΝΣΕΩΝ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΚΑΙ ΑΛΛΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΙΣΤΟΣΕΛΙΔΕΣ ΚΑΙ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΝΩΣΕΙΣ ΧΩΡΙΣ ΤΗΝ ΣΥΓΚΑΤΑΘΕΣΗ ΤΩΝ ΣΥΝΔΡΟΜΗΤΩΝ. ΗΛΕΚΤΡΟΝΙΚΟΥ .

1. Όπως ορίζεται στο άρθρο 4, παρ. 1, εδ. α' του Ν. 2472/1997 τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου αποτελούν δεδομένα προσωπικού χαρακτήρα, κατά την έννοια του άρθρου 2 στοιχ. α' του Ν. 2472/1997, όταν ανήκουν σε φυσικά πρόσωπα. Στην προκειμένη περίπτωση, όπως προκύπτει από το υπ' αριθμ. 1 εύρημα, πραγματοποιείται συλλογή διευθύνσεων από ιστοσελίδες, όπου το υποκείμενο των δεδομένων έχει ανακοινώσει τα στοιχεία του για τελείως διαφορετικό σκοπό, για παράδειγμα για την αποστολή μηνυμάτων επικοινωνίας για προσωπικούς σκοπούς ή για τη συμμετοχή του σε ομάδες συζήτησης. Το αυτόματο λογισμικό έχει ρυθμιστεί έτσι ώστε να μην κάνει καμία διάκριση των διευθύνσεων που συλλέγει με κριτήριο το σκοπό της δημοσίευσης τους, συλλέγοντας όλα τα στοιχεία τα οποία συναντά. Επομένως, οι διευθύνσεις ηλεκτρονικού

ταχυδρομείου, που συλλέγονται με τον τρόπο αυτό, δεν συλλέγονται με τρόπο θεμιτό και νόμιμο, για καθορισμένους και νόμιμους σκοπούς και δεν υφίστανται θεμιτή και νόμιμη επεξεργασία εν όψει των σκοπών αυτών, κατά παράβαση της προαναφερθείσας διάταξης του Ν. 2472/1997. Η άποψη αυτή ενισχύεται από το γεγονός ότι το έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα δεν υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα, καθώς προκαλείται σημαντική όχληση στους αποδέκτες των μηνυμάτων αλλά και πιθανά επιπρόσθετο κόστος από τη χρήση υπηρεσιών διαδικτύου για την ανάγνωση των μηνυμάτων. Έτσι, όσον αφορά στη συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου χωρίς τη συγκατάθεση του υποκείμενου, δεν μπορεί να έχει εφαρμογή η διάταξη του άρθρου 5, παρ. 2 ε' του Ν. 2472/1997. Επισημαίνεται ότι η Ομάδα Εργασίας του άρθρου 29 της οδηγίας 95/46/ΕΚ έχει παρουσιάσει, αναλυτικά, το σκεπτικό αυτό στο έγγραφο εργασίας υπ' αριθμ. 37/21.11.2000 (σελ. 37, 38 και 43, 44), ενώ παρόμοια παρουσίαση βρίσκεται και στο βιβλίο Regulating Spam, A European Perspective after the Adoption of the E-Privacy Directive (κεφάλαιο 4, Harvesting, σελίδες 67-79). Επομένως, το αρχείο που έχει δημιουργήσει η Calino, με την τεχνική που περιγράφεται στο εύρημα υπ' αριθμ. 1 του πορίσματος, παραβιάζει τις διατάξεις των άρθρων 4, 5 παρ. 2 του ν. 2472/1997 και τα στοιχεία του πρέπει να καταστραφούν. Καθώς το αρχείο αυτό έχει διαβιβασθεί σε απροσδιόριστο αριθμό πελατών της εταιρείας, είναι προς το συμφέρον των υποκειμένων της επεξεργασίας να ενημερωθούν όλοι όσοι αγόρασαν το αρχείο αυτό ώστε να προβούν σε διαγραφή των δεδομένων που έχουν συλλεγεί παράνομα. Η πλήρης άρση της παράβασης μπορεί να επιτευχθεί μόνο με τη διαγραφή των στοιχείων από όλα τα πωληθέντα αντίγραφα.

2. Όπως ορίζει το άρθρο 11 παρ. 1 του Ν. 2472/1997 «*Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία: α. την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του, β. τον σκοπό της επεξεργασίας, γ. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, δ. την ύπαρξη του δικαιώματος πρόσβασης.*». Όπως προκύπτει από το εύρημα υπ' αριθμ. 2, ο υπεύθυνος επεξεργασίας δεν φροντίζει σε κανένα σημείο για την παροχή ενημέρωσης προς τα υποκείμενα των δεδομένων κατά το στάδιο της συλλογής τους. Είναι αληθές ότι ο σκοπός που επιδιώκει η Calino, δηλαδή το οικονομικό συμφέρον για τη δημιουργία της εφαρμογής καταλόγου επαγγελματικών διευθύνσεων, συμβαδίζει καταρχήν με το επαγγελματικό συμφέρον των υποκειμένων για την ευχερέστερη αναζήτηση των στοιχείων τους από το κοινό. Έτσι, για τη χρήση των στοιχείων που λαμβάνονται από τους επαγγελματικούς φορείς και τις επαγγελματικές εκθέσεις δεν απαιτείται, σύμφωνα με το άρθρο 5 παρ. 2 στοιχ. ε' του Ν. 2472/1997, νέα συγκατάθεση των υποκειμένων των δεδομένων, αλλά αρκεί η προηγούμενη ενημέρωση αυτών σύμφωνα με τα οριζόμενα στο άρθρο 11 παρ. 1 του Ν. 2472/1997. Στην προκειμένη όμως περίπτωση, η ενημέρωση αυτή θα έπρεπε να είχε διενεργηθεί μέσω ατομικής επιστολής με την οποία να παρέχεται ικανό χρονικό διάστημα για την άσκηση του δικαιώματος αντίρρησης, καθώς τα στοιχεία διεύθυνσης είναι διαθέσιμα στην Calino και ο τρόπος αυτός αποτελεί τον προσφορότερο και ασφαλέστερο προκειμένου να ικανοποιηθούν τα δικαιώματα όλων των υποκειμένων της επεξεργασίας. Επομένως, κατά παράβαση του άρθρου 11 παρ. 1 του ν. 2472/97, έγινε συλλογή των παραπάνω στοιχείων από καταλόγους επαγγελματικών ενώσεων. Περαιτέρω παρατηρείται ότι οι διάφορες επαγγελματικές ενώσεις οφείλουν, κατά το στάδιο συλλογής των δεδομένων, να ενημερώνουν τα υποκείμενα για τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων. Η

Αρχή κρίνει ότι πρέπει με την επιμέλεια των εισηγητών της υποθέσεως να ενημερωθούν οι επαγγελματικές ενώσεις για την υποχρέωσή τους αυτή.

3. Στο άρθρο 10, παρ. 4 του Ν. 3471/2006 ορίζεται ότι «Τ*α δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται σε δημόσιο κατάλογο επιτρέπεται να υπόκεινται σε επεξεργασία μόνο για τους σκοπούς για τους οποίους έχουν συλλεγεί. Όταν τα δεδομένα αυτά διαβιβάζονται σε τρίτους, ο συνδρομητής θα πρέπει να ενημερώνεται, πριν από τη διαβίβαση, για αυτή τη δυνατότητα και για τον παραλήπτη ή για τις κατηγορίες των πιθανών παραληπτών, να έχει δε την ευκαιρία να αντιταχθεί στη διαβίβαση. Για τη χρησιμοποίηση των δεδομένων αυτών για άλλο σκοπό, είτε από τον φορέα είτε από τρίτο, απαιτείται εκ νέου η ρητή συγκατάθεση του συνδρομητή...*». Στην προκειμένη περίπτωση, όπως περιγράφεται στο υπ' αριθμ. 3 εύρημα του πορίσματος, η Calino συλλέγει προσωπικά δεδομένα από δημόσια προσβάσιμη πηγή, δηλαδή τον κατάλογο συνδρομητών του ΟΤΕ. Τα δεδομένα αυτά υπόκεινται σε επιπλέον επεξεργασία, καθώς συνδυάζονται με γεωγραφική πληροφορία, και δημοσιεύονται με τη μορφή του λογισμικού Hellas Navigator, δηλαδή με τη μορφή προηγμένου ηλεκτρονικού καταλόγου με χάρτη. Με τον τρόπο αυτό βελτιώνεται η ποιότητα των δεδομένων, καθώς είναι δυνατή η παροχή προηγμένων υπηρεσιών αναζήτησης προσωπικών δεδομένων. Η προηγμένη λειτουργία αναζήτησης συνίσταται στο γεγονός ότι ο χρήστης του εν λόγω λογισμικού δύναται να αναζητήσει τα στοιχεία συνδρομητών του ΟΤΕ και με βάση γεωγραφικά δεδομένα. Σε έναν απλό τηλεφωνικό κατάλογο θα μπορούσε να αναζητήσει τα στοιχεία του εκάστοτε συνδρομητή μόνο με βάση συγκεκριμένα στοιχεία (όνομα συνδρομητή, τηλέφωνο, διεύθυνση) και σε πιο περιορισμένη κλίμακα. Ο σκοπός που επιδιώκει ο υπεύθυνος επεξεργασίας, με την παροχή δυνατότητας γεωγραφικής αναζήτησης των προσωπικών δεδομένων όσων περιλαμβάνονται στους καταλόγους συνδρομητών, είναι η πώληση του ηλεκτρονικού καταλόγου για την πραγματοποίηση γεωγραφικά στοχευμένων διαφημιστικών ενεργειών από τον εκάστοτε αγοραστή. Ο εκάστοτε αγοραστής δύναται να δημιουργήσει στοχευμένες ομάδες διαφήμισης (πχ. όλοι οι ηλεκτρολόγοι μιας γεωγραφικής περιοχής) και να διαφημίσει τα προϊόντα του με βάση το είδος του αγοραστικού κοινού, το οποίο έχει επιλέξει. Συνεπώς, ο σκοπός της επεξεργασίας διαφοροποιείται από αυτόν ενός καταλόγου συνδρομητών και ως εκ τούτου, κατά παράβαση του άρθρου 10 παρ. 4 του ν. 3471/2006 η εταιρεία CALINO δημιούργησε αρχείο από τους συνδρομητές του ΟΤΕ.

4. Στο άρθρο 11 παρ. 1 του Ν. 3471/2006 αναφέρεται ότι «*η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς*». Από το διενεργηθέντα έλεγχο (εύρημα υπ' αριθμ. 4), έγινε σαφές ότι η Calino δεν εξασφαλίζει τη συγκατάθεση των συνδρομητών πριν την αποστολή των διαφημιστικών της μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου ή τηλεομοιοτυπίας. Η εταιρεία συμπεριλαμβάνει στο μήνυμα τρόπο

εναντίωσης στη συνέχιση της αποστολής διαφημιστικών μηνυμάτων, αλλά η ενέργεια αυτή δεν την απαλλάσσει από την υποχρέωση λήψης συγκατάθεσης των συνδρομητών. Η αποστολή πραγματοποιείται σε όλη τη λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεομοιοτυπίας και όχι μόνο σε όσους είχαν κάποια προηγούμενη συναλλαγή μαζί της, οπότε και θα ίσχυε η εξαίρεση της παρ. 3 του ανωτέρω άρθρου. Συνεπώς η Αρχή αποφαίνεται ότι η Calino παραβιάζει συστηματικά την προαναφερθείσα διάταξη, όπως τούτο επιβεβαιώνεται από τις προαναφερθείσες καταγγελίες.

5. Στο άρθρο 9 παρ. 2 του Ν. 2472/1997 ορίζεται ότι «*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..»*. Από το εύρημα υπ' αριθμ. 5 προκύπτει ότι η Calino πώλησε ηλεκτρονικά αρχεία με προσωπικά δεδομένα (ονόματα, διευθύνσεις και τηλέφωνα) σε κυβερνητική υπηρεσία των ΗΠΑ. Η ενέργεια αυτή αποτέλεσε διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρα εκτός Ευρωπαϊκής Ένωσης. Η εν λόγω διαβίβαση πραγματοποιήθηκε προς χώρα η οποία δεν περιλαμβάνεται σε αυτές, για τις οποίες η Ευρωπαϊκή Επιτροπή έχει αποφανθεί ότι εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας. Για τη διαβίβαση αυτή δεν είχε προηγηθεί γνωστοποίηση ή αίτηση για άδεια, ούτε, φυσικά, υπήρξε άδεια της Αρχής. Συνεπώς η διαβίβαση αυτή πραγματοποιήθηκε κατά παράβαση του προαναφερθέντος άρθρου.

6. Με δεδομένο ότι η εταιρεία CALINO υπέπεσε, κατά τα προαναφερόμενα, σε αυτοτελείς παραβάσεις διατάξεων της κείμενης νομοθεσίας, η Αρχή κρίνει ότι πρέπει να επιβληθούν αντίστοιχες κυρώσεις.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή

Επιβάλει στην εταιρεία CALINO Α.Ε., που αποτελεί τον υπεύθυνο επεξεργασίας για τις περιγραφόμενες στο πόρισμα διοικητικού ελέγχου επεξεργασίες, τις πιο κάτω διοικητικές κυρώσεις:

1. Πρόστιμο ποσού είκοσι πέντε χιλιάδων ευρώ (25.000) για την παραβίαση του άρθρου 4, παρ. 1, εδ. α' του Ν. 2472/1997 που συντελείται με την παράνομη επεξεργασία διευθύνσεων ηλεκτρονικού ταχυδρομείου. Επίσης, η Αρχή διατάσσει την καταστροφή του εν λόγω αρχείου και υποχρεώνει τον υπεύθυνο επεξεργασίας να ενημερώσει, εγγράφως, όλους τους πελάτες του ότι η τήρηση του αρχείου αυτού είναι παράνομη. Η καταστροφή του εν λόγω αρχείου από την Calino συνίσταται στην καταστροφή τόσο της λίστας διευθύνσεων ηλεκτρονικού ταχυδρομείου της Calino, οι οποίες δεν έχουν αποκτηθεί με νόμιμο τρόπο, όσο και στη διαγραφή όλων των διευθύνσεων ηλεκτρονικού ταχυδρομείου από το προϊόν Hellas Navigator. Ο υπεύθυνος επεξεργασίας οφείλει, εντός δεκαπέντε ημερών από τη λήψη της απόφασης, να προσκομίσει στην Αρχή κατάλογο με τους πελάτες που αγόρασαν τη λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου καθώς και αντίγραφο της επιστολής ενημέρωσης προς αυτούς.

2. Πρόστιμο ποσού πέντε χιλιάδων ευρώ (5.000) για την παραβίαση του άρθρου 11 παρ. 1 του Ν. 2472/1997 που αφορά στη μη παροχή ενημέρωσης προς τα υποκείμενα των δεδομένων για τη συλλογή που πραγματοποιείται από επαγγελματικές ενώσεις και επαγγελματικούς οδηγούς.

Η Αρχή κοινοποιεί την παρούσα απόφαση στις επαγγελματικές ενώσεις ενημερώνοντας τους κατ' αυτόν τον τρόπο ότι υποχρεούνται να ενημερώνουν τα μέλη τους (υποκείμενα των δεδομένων) για τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων που συλλέγουν από αυτά.

3. Προειδοποίηση για την παράβαση του άρθρου 10, παρ. 4 του Ν. 3471/2006. Η εταιρεία οφείλει να τροποποιήσει τον ηλεκτρονικό οδηγό που εκδίδει και να επιτρέπει τη γεωγραφική αναζήτηση μόνο σε όσους συνδρομητές τηλεφωνίας έχουν δώσει εκ νέου τη συγκατάθεση τους για χρήση των δεδομένων τους στο πλαίσιο της δυνατότητας γεωγραφικής αναζήτησης.

4. Πρόστιμο ποσού είκοσι πέντε χιλιάδων ευρώ (25.000) για την παραβίαση του άρθρου 11 παρ. 1 του Ν. 3471/2006 για την αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και τηλεομοιοτυπίας (FAX), χωρίς τη συγκατάθεση των συνδρομητών.

5. Πρόστιμο ποσού δέκα χιλιάδων ευρώ (10.000) για την παράβαση του άρθρου 9 παρ. 2 του Ν. 2472/1997 που συντελέστηκε με την παράνομη διαβίβαση δεδομένων σε χώρα εκτός Ε.Ε.

Β) ΑΠΟΦΑΣΗ 38/2008

ΠΑΡΑΝΟΜΗ Η ΣΥΛΛΟΓΗ ΔΙΕΥΘΥΝΣΕΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΚΑΙ ΑΛΛΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝΑΠΟ ΙΣΤΟΣΕΛΙΔΕΣ ΚΑΙ ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΕΝΩΣΕΙΣ ΧΩΡΙΣ ΣΥΓΚΑΤΑΘΕΣΗ ΤΩΝ ΣΥΝΔΡΟΜΗΤΩΝ.

Η Αρχή έλαβε υπόψη τα παρακάτω:

Υποβλήθηκε στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (με αρ. πρωτ. 3719, από 31/05/2006, όπως συμπληρώθηκε με το υπ' αρ. πρωτ. 4502, από 05/07/2006, έγγραφο) προσφυγή – καταγγελία των Α και Β, η οποία στρέφεται κατά της εταιρείας Microsoft Hellas ΑΕ, ως υπευθύνου επεξεργασίας, και κοινοποιήθηκε νομίμως στην εταιρεία αυτή. Σύμφωνα με την ως άνω προσφυγή – καταγγελία, η Microsoft Hellas ΑΕ προέβη σε αθέμιτη επεξεργασία δεδομένων προσωπικού χαρακτήρα, που αφορούν καθένα από τους προσφεύγοντες ατομικά και ως ομόρρυθμους εταίρους της εταιρείας με την επωνυμία «Χ *ΟΕ*», η οποία είχε έδρα, την περίοδο εκείνη, στην Καισαριανή. Η επίμαχη επεξεργασία συνίσταται – σύμφωνα με τα καταγγελλόμενα – στη δημοσιοποίηση στο Διαδίκτυο (Internet) στοιχείων, που αφορούν τη διενέργεια δικαστικών ενεργειών από τη Microsoft Hellas ΑΕ κατά των προσφευγόντων για «*πειρατεία λογισμικού*».

Η ύπαρξη της σχετικής ανακοίνωσης της Microsoft Hellas ΑΕ διαπιστώθηκε από διαδοχικές επισκέψεις, που διενήργησε έκτοτε ο εντεταλμένος ελεγκτής της Αρχής στη σχετική ιστοσελίδα της εταιρείας. Ειδικότερα, στο site της Microsoft Hellas ΑΕ (με είσοδο από το κεντρικό site της Microsoft.com και επιλογή χώρας) υπάρχει η ιστοσελίδα http://www.microsoft.com/hellas/piracy/news/default.mspx, όπου καταχωρούνται – κατά χρονολογική σειρά (έτος, μήνας) – ανακοινώσεις, που αφορούν τη διενέργεια δικαστικών ενεργειών κατά φυσικών προσώπων καθώς, επίσης, κατά νομικών προσώπων (που είναι κυρίως προσωπικές εταιρείες), από το έτος 2003 έως σήμερα για «*πειρατεία λογισμικού*» και «*βάσει των διατάξεων περί πνευματικής ιδιοκτησίας*», σύμφωνα με τη Microsoft Hellas ΑΕ. Στην ως άνω ιστοσελίδα, για το Μάρτιο 2006 αναφέρονταν τα ακόλουθα σε σχέση με τους προσφεύγοντες: «*Αθήνα, Μάρτιος 2006. Η Microsoft ανακοινώνει την έναρξη δικαστικών ενεργειών κατά της εταιρείας με την επωνυμία «Χ Ο.Ε.» και των ομορρύθμων εταίρων της Α και Β, βάσει των διατάξεων περί πνευματικής ιδιοκτησίας.* ******» . Ανοίγοντας την ιστοσελίδα ******* μπορούσε ο οποιοσδήποτε επισκέπτης του εν λόγω site να έχει πρόσβαση σε περισσότερες λεπτομέρειες σχετικά με την έναρξη δικαστικών ενεργειών κατά της εταιρείας των προσφευγόντων. Διαπιστώθηκε κατ' αυτό τον τρόπο ότι είναι δημοσιευμένες στην ιστοσελίδα http://www.microsoft.com/hellas/piracy/news/default.mspx του εν λόγω site, από το έτος 2003 και εντεύθεν, δεκάδες παρόμοιων ανακοινώσεων, που αφορούν πρωτίστως τη διενέργεια από τη Microsoft Hellas ΑΕ δικαστικών ενεργειών κατά φυσικών προσώπων, καθώς και κατά νομικών προσώπων (που είναι κυρίως προσωπικές εταιρείες), από το έτος 2003 έως σήμερα. Επίσης, πληροφορίες σχετικά με εξώδικους συμβιβασμούς μεταξύ της εν λόγω εταιρείας και άλλες εταιρείες (οι εκπρόσωποι των οποίων κατά κανόνα αναφέρονται ονομαστικά). Μέσω της εισόδου **** ο επισκέπτης έχει τη δυνατότητα να πληροφορηθεί, μεταξύ άλλων, το σύντομο ιστορικό της υπόθεσης και τις αστικές διώξεις, που έχουν κινηθεί. Υπάρχουν, επίσης, δημοσιευμένες ορισμένες δικαστικές αποφάσεις, οι οποίες έχουν εκδοθεί μετά από τη διενέργεια των προαναφερόμενων αστικών διώξεων. Εξάλλου, από δειγματοληπτικό έλεγχο, που διενήργησε ο εντεταλμένος ελεγκτής της Αρχής σε διάφορους διαδικτυακούς τόπους της εταιρείας Microsoft ανά την Ευρώπη, διαπιστώθηκε ότι μόνο στη Μ. Βρετανία η Microsoft προβαίνει στη δημοσίευση παρόμοιων ανακοινώσεων. Αντίθετα, σε άλλες χώρες (πχ. Γαλλία, Βέλγιο, Λουξεμβούργο, Γερμανία) η Microsoft περιορίζεται στις σχετικές ιστοσελίδες της στη δημοσίευση του υπάρχοντος νομικού πλαισίου και τεχνικών συμβουλών ή εργαλείων σχετικά με την «*πειρατεία λογισμικού*». Επιπλέον, διαπιστώθηκε ότι στην ιστοσελίδα http://www.microsoft.com/hellas/piracy/news/default.mspx η εταιρεία Microsoft Hellas ΑΕ δημοσιεύει πλέον και ανωνυμοποιημένες ειδήσεις νομικού περιεχομένου. Δηλαδή, σε κάποιες από τις υπάρχουσες υποθέσεις υπάρχουν ονομαστικές αναφορές, ενώ σε κάποιες άλλες όχι, προφανώς κατά την επιλογή της Microsoft Hellas ΑΕ.

Μετά από τις προαναφερόμενες διαπιστώσεις, ο εντεταλμένος ελεγκτής της Αρχής υπέδειξε στους προσφεύγοντες να ασκήσουν το κατά το άρθρο 13 του Ν. 2472/1997 δικαίωμα αντίρρησης έναντι της Microsoft Hellas ΑΕ, ως υπευθύνου επεξεργασίας. Το δικαίωμα αυτό ασκήθηκε πράγματι με την από 16/06/2006 εξώδικη πρόσκληση, που κοινοποιήθηκε στην Αρχή (με αρ. πρωτ. Γ/ΕΙΣ/4502/05.07.2006), και αίτημα για διαγραφή ολόκληρης της επίμαχης καταχώρισης από την ιστοσελίδα ****. Κοινοποιήθηκε, επίσης, στην Αρχή, με το ίδιο έγγραφο, η από 28/06/2006 εξώδικη απάντηση της Microsoft Hellas ΑΕ, σύμφωνα με την οποία η επίμαχη καταχώριση διεγράφη από την ως άνω ιστοσελίδα. Η διαγραφή αυτή διαπιστώθηκε από τον εντεταλμένο ελεγκτή της Αρχής. Διαπιστώθηκε, επίσης, η διαγραφή της σχετικής με τους προσφεύγοντες καταχώρισης από την ιστοσελίδα

http://www.microsoft.com/hellas/piracy/news/default.mspx, την οποία, ωστόσο, η Microsoft Hellas ΑΕ συνέχισε να τροφοδοτεί με πληροφορίες για άλλα φυσικά και νομικά πρόσωπα, σύμφωνα με τα προαναφερόμενα. Ο εντεταλμένος ελεγκτής της Αρχής προέβη σε επισκέψεις του site σε τακτά χρονικά διαστήματα και σε αντίστοιχες εκτυπώσεις του περιεχομένου του (30/06/2006, 29/09/2006, 21/02/2007, 15/05/2008).

Με βάση τα προαναφερόμενα, με το υπ' αρ. πρωτ. Γ/ΕΞ/4851/04.07.2007 έγγραφο της Αρχής, κλήθηκε η Microsoft Hellas ΑΕ να δώσει πλήρεις διευκρινίσεις σχετικά με τη δημοσίευση των προαναφερόμενων στοιχείων στο διαδικτυακό της τόπο. Πράγματι, υποβλήθηκε το υπ' αρ. πρωτ. Γ/ΕΙΣ/5325/20.07.2007 έγγραφο υπόμνημα της Microsoft Hellas ΑΕ, δια των πληρεξουσίων δικηγόρων της εν λόγω εταιρείας. Στο υπόμνημα αυτό η εν λόγω εταιρεία επιβεβαιώνει, καταρχάς, πλήρως τα προαναφερόμενα, σχετικά με τις επίμαχες πληροφορίες που αφορούν τους προσφεύγοντες και, παραθέτει, τους ισχυρισμούς της σχετικά με τις υπόλοιπες καταχωρίσεις του προαναφερόμενου site.

Στη συνέχεια, η Αρχή κάλεσε (με τα υπ' αρ. πρωτ. Γ/ΕΞ/2353/16.05.2008 και Γ/ΕΞ/2354/16.05.2008 έγγραφά της, αντίστοιχα) τους προσφεύγοντες Α και Β, όπως νομίμως εκπροσωπούνται, καθώς, επίσης, και την εταιρεία Microsoft Hellas ΑΕ, όπως νομίμως εκπροσωπείται, σε ακρόαση κατά τη συζήτηση της ως άνω προσφυγής από την Ολομέλεια της Αρχής, την 22/05/2008. Στη συνεδρίαση αυτή προσήλθαν ο Α, η Ιουλία Γαληνού, Δικηγόρος Αθηνών, ως πληρεξούσιος του Β, και ο Γεώργιος Μούκας, Δικηγόρος Αθηνών, ως πληρεξούσιος της εταιρείας Microsoft Hellas ΑΕ. Η Αρχή αποφάσισε την αναβολή της συζήτησης της παρούσας υπόθεσης για τη συνεδρίαση της Πέμπτης 05/06/2008, χωρίς νέα κλήση, προκειμένου να ενημερωθούν πληρέστερα τα μέλη της Αρχής για τα υπό κρίση ζητήματα και ανακοίνωσε την απόφασή της αυτή στους ως άνω κληθέντες. Επιπλέον, ζητήθηκε από τον πληρεξούσιο δικηγόρο της εταιρείας Microsoft Hellas ΑΕ να προσκομίσει στην επόμενη συνεδρίαση της Αρχής τις καταστάσεις ισολογισμού της εντολέως του εταιρείας των τελευταίων πέντε ετών.

Στη συνεδρίαση της 05/06/2008 προσήλθαν εκ νέου η Ιουλία Γαληνού, Δικηγόρος Αθηνών, ως πληρεξούσιος των Α και Β, και ο Γεώργιος Μούκας, Δικηγόρος Αθηνών, ως πληρεξούσιος της εταιρείας Microsoft Hellas ΑΕ, οι οποίοι ανέπτυξαν τους ισχυρισμούς τους ενώπιον της Ολομέλειας της Αρχής και απάντησαν σε σχετικές ερωτήσεις, που τους τέθηκαν. Εξάλλου, ο πληρεξούσιος δικηγόρος της εταιρείας Microsoft Hellas ΑΕ προσκόμισε στην Αρχή τις ως άνω ζητηθείσες καταστάσεις ισολογισμού της εντολέως του εταιρείας των τελευταίων πέντε ετών και ζήτησε και έλαβε προθεσμία (έως την 09/06/2008), προκειμένου να υποβάλει στην Αρχή υπόμνημα για την πληρέστερη ανάπτυξη των ισχυρισμών της εντολέως του εταιρείας. Πράγματι, το υπόμνημα αυτό υποβλήθηκε εμπροθέσμως στην Αρχή (με το υπ' αρ. πρωτ. Γ/ΕΙΣ/2822/09.06.2008 έγγραφο, καθώς, επίσης, και με τα συνημμένα σε αυτό έγγραφα).

Μετά από εξέταση των προαναφερόμενων στοιχείων, αφού αναγνώστηκαν τα πρακτικά των συνεδριάσεων της 22/05/2008 και 05/06/2008, άκουσε την πρόταση του εισηγητή και μετά από διεξοδική συζήτηση,

Η Αρχή, αφού έλαβε, ιδίως, υπόψη:

1) Τις διατάξεις του Συντάγματος, και, ιδίως, εκείνες των άρθρων 2 παρ. 1, 5, 9Α, 19 παρ. 3, 25, 101Α, και 106 παρ. 2,

2) Τις διατάξεις του Ν. 2472/1997 για την *Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*, που ενσωμάτωσε στην ελληνική έννομη τάξη εκείνες της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, *για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*, καθώς και τις διατάξεις της Οδηγίας αυτής,

3) Τις διατάξεις της Ευρωπαϊκής Σύμβασης για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ) του Συμβουλίου της Ευρώπης, η οποία κυρώθηκε εκ νέου με το ΝΔ 53 της 19/20.09.1974 (ΦΕΚ Α΄ 256), όπως αυτή ερμηνεύεται από τη νομολογία του Ευρωπαϊκού Δικαστηρίου για τα Δικαιώματα του Ανθρώπου (ΕΔΔΑ),

4) Τις διατάξεις της Σύμβασης 108 (1981) του Συμβουλίου της Ευρώπης *για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων*, η οποία κυρώθηκε με το Ν. 2068/1992 (ΦΕΚ Α΄ 118) και τέθηκε σε ισχύ ως προς την Ελλάδα την 01/12/1995 με την Ανακοίνωση Υπ. Εξωτερικών Φ.0546/4173 (ΦΕΚ Α΄ 207/1995),

5) Τη διάταξη του άρθρου 66Γ του Ν. 2121/1993 για την *Πνευματική ιδιοκτησία, τα συγγενικά δικαιώματα και πολιτιστικά θέματα*, η οποία ενσωματώνει στην ελληνική έννομη τάξη τις διατάξεις του άρθρου 15 της Οδηγίας 2004/48/ΕΚ *σχετικά με την επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας*, καθώς και τις διατάξεις της Οδηγίας αυτής,

Γ) ΑΠΟΦΑΣΗ 66/2010

Η Αρχή έλαβε υπόψη τα ακόλουθα:

Με το υπ' αρ. πρωτ. Γ/ΕΙΣ/3391/20-05-2010 έγγραφο οι κκ Α και Β υπέβαλαν καταγγελία στην Αρχή κατά της εταιρείας «Πάρκα Αναψυχής και Αθλητισμού ΑΕ» για παράνομη δημοσίευση φωτογραφιών τους στο διαδίκτυο. Οι καταγγέλλοντες συμμετείχαν σε δραστηριότητα rafting στις ../../2010. Στο έντυπο με τα στοιχεία συμμετοχής που συμπλήρωσαν δήλωσαν ότι δεν επιθυμούν τη χρήση των φωτογραφιών τους για εμπορικούς σκοπούς. Φωτογραφίες από την εκδήλωση οι οποίες τους απεικόνιζαν σε προσωπικές τους στιγμές (και μάλιστα κατά την προετοιμασία της δραστηριότητας) αναρτήθηκαν στο διαδικτυακό τόπο ……., προσβάσιμο μέσω υπερ-σύνδεσης από το διαδικτυακό τόπο της εταιρείας «Πάρκα Αναψυχής και Αθλητισμού ΑΕ». Κατά τους ισχυρισμούς του Α, τις φωτογραφίες είδε γνωστή του Α η οποία και ενημέρωσε τη σύζυγό του και στη συνέχεια ενημερώθηκε σχετικά και ο αρραβωνιαστικός της Β. Υπήρξαν επιπτώσεις τόσο στη σχέση της Β όσο και στο γάμο του Α.

Οι φωτογραφίες έμειναν αναρτημένες από τις ../../2010 μέχρι τις ../../2010 οπότε ο Α επικοινώνησε τηλεφωνικά με την εταιρεία και ζήτησε την αφαίρεση των φωτογραφιών αυτών από το διαδικτυακό τόπο, αίτημα το οποίο ικανοποιήθηκε.

Με το υπ' αρ. πρωτ Γ/ΕΞ/3391-1/04-06-2010 έγγραφο η Αρχή απευθύνθηκε στην «Πάρκα Αναψυχής και Αθλητισμού ΑΕ» ζητώντας διευκρινίσεις σχετικά με τα καταγγελλόμενα. Η «Πάρκα Αναψυχής και Αθλητισμού ΑΕ» απάντησε στην Αρχή με το υπ' αρ. πρωτ. Γ/ΕΙΣ/4028/25-06-2010 έγγραφο, στο οποίο ισχυρίζεται τα ακόλουθα:

Στο έντυπο δήλωσης συμμετοχής στη δραστηριότητα οι συμμετέχοντες δήλωναν εάν επιθυμούσαν ή όχι να χρησιμοποιηθούν οι φωτογραφίες στις οποίες απεικονίζονταν για εμπορικούς σκοπούς. Προκειμένου δε οι φωτογραφίες να καταχωρηθούν στο διαδικτυακό τόπο για αναμνηστικούς και μόνο λόγους, καθόλη τη διεξαγωγή της δραστηριότητας του rafting, η εταιρεία ενημέρωνε τους συμμετέχοντες με σχετικές πινακίδες που είχαν τοποθετηθεί σε εμφανή σημεία. Αν κάποιος από τους συμμετέχοντες δεν επιθυμούσε τη δημοσίευση φωτογραφιών στην ιστοσελίδα της διοργάνωσης τότε το δήλωνε είτε στο φωτογράφο είτε στο προσωπικό του γραφείου υποδοχής-πληροφοριών. Στην συγκεκριμένη υπόθεση, οι καταγγέλλοντες είχαν συμπληρώσει στην αίτηση συμμετοχής ότι δεν επιθυμούσαν οι φωτογραφίες τους να χρησιμοποιηθούν για εμπορικούς σκοπούς, γεγονός που έγινε σεβαστό με το να μην χρησιμοποιηθούν οι φωτογραφίες τους σε καμία ενέργεια προώθησης υπηρεσιών της εταιρείας. Η ανάρτηση των φωτογραφιών τους στο διαδίκτυο έγινε μόνο ως ενθύμιο από τη δραστηριότητα για τους ίδιους τους συμμετέχοντες, αφού οι καταγγέλλοντες δεν εξέφρασαν την αντίρρησή τους είτε στο φωτογράφο είτε στο προσωπικό του γραφείου υποδοχής-πληροφοριών.

Οι προσφεύγοντες Α και Β, καθώς και η «Πάρκα Αναψυχής και Αθλητισμού ΑΕ», ως υπεύθυνος επεξεργασίας, κλήθηκαν προς ακρόαση κατά τη συζήτηση της υπόθεσης ενώπιον της Αρχής στις 11/10/2010 με τις υπ' αριθμ πρωτ. Γ/ΕΞ/5656/27.09.2010, Γ/ΕΞ/5657/27.09.2010, και Γ/ΕΞ/5658/27.09.2010 κλήσεις αντίστοιχα, οι οποίες επιδόθηκαν νομίμως. Τον υπεύθυνο επεξεργασίας εκπροσώπησαν ο Γ και η δικηγόρος κ. Χαρίτου.

Μετά από εξέταση των προαναφερομένων στοιχείων, αφού άκουσε την πρόταση της εισηγήτριας, και κατόπιν διεξοδικής συζήτησης, η Αρχή

Σκέφτηκε σύμφωνα με τον νόμο

Οι φωτογραφίες αποτελούν δεδομένα προσωπικού χαρακτήρα, σύμφωνα με τα οριζόμενα στη διάταξη του άρθρου 2 στοιχ. α΄ του ν.2472/1997, στο μέτρο που από αυτές δύνανται να προσδιοριστούν, άμεσα ή έμμεσα, τα υποκείμενα των δεδομένων. Σύμφωνα με το άρθρο 5 του ίδιου νόμου, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.

Στη συγκεκριμένη περίπτωση υπήρξε παραβίαση του άρθρου 5 του ν.2472/1997 καθώς ο Α και η Β είχαν δηλώσει την αντίρρησή τους για την επεξεργασία των φωτογραφιών τους για εμπορικούς σκοπούς και δεν είχαν δώσει συγκατάθεση για καμία άλλη επεξεργασία φωτογραφιών. Η δημοσίευση φωτογραφιών συμμετασχόντων σε εκδηλώσεις της εταιρείας στο διαδίκτυο καθιστά τις εν λόγω φωτογραφίες προσβάσιμες από κάθε χρήστη του διαδικτύου, ενώ ο σύνδεσμος που παραπέμπει σε αυτές βρίσκεται στην κεντρική σελίδα της εταιρείας , όπου παρουσιάζονται υπηρεσίες της.

Κατά τον τρόπο αυτό οι φωτογραφίες χρησιμοποιούνται έμμεσα για εμπορική προώθηση υπηρεσιών, σκοπό για τον οποίο όχι μόνο δεν είχαν συγκατατεθεί αλλά είχαν σαφώς αντιταχθεί οι καταγγέλλοντες.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή επιβάλλει στον υπεύθυνο επεξεργασίας πρόστιμο ύψους χιλίων (1.000) ευρώ για τη διαπιστωθείσα παράνομη δημοσίευση φωτογραφιών στο διαδίκτυο των Α και Β.

Δ) ΑΠΟΦΑΣΗ 91/2009

Υπηρεσία εικονικής περιήγησης στους δρόμους ελληνικών περιοχών

Η Αρχή έλαβε υπόψη τα παρακάτω:

Εξ αφορμής της υπ' αρ. πρωτ. Γ/ΕΙΣ/1435/05-03-2009 αιτήσεως-καταγγελίας η Αρχή

διαπίστωσε ότι η εταιρεία ΚΑΠΟΥ Α.Ε. Γεωπληροφορικής

προβαίνει σε φωτογράφιση περιοχών της Αθήνας από κινητό συνεργείο της εταιρείας με ειδικώς εξοπλισμένο όχημα.

Σκοπός της φωτογράφισης είναι η παροχή υπηρεσίας εικονικής περιήγησης στους δρόμους ελληνικών περιοχών , την Θεσσαλονίκη, Αθήνα, και Τρίκαλα μέσω της ιστοσελίδας της εταιρείας www.kapou.gr.

Στην ιστοσελίδα της η εταιρεία ανέφερε ότι βρίσκεται στο στάδιο της ανάπτυξης ενός συστήματος αυτόματης τεχνητής απόκρυψης(‘θόλοση») προσώπων και πινακίδων αυτοκινήτων ώστε να είναι αδύνατη η αναγνώριση τους, και μέχρι να εφαρμοστεί το σύστημα αυτό, για λόγους προστασίας προσωπικών δεδομένων έχει μειώσει την ανάλυση των φωτογραφιών. Επιπλέον, σημειώνονταν ότι εάν κάποιος ενημερώσει ότι σε κάποια από τις φωτογραφίες απεικονίζεται ο ίδιος ή ο συγγενής του, το όχημα του ή η οικία του, τότε εντός 24 ωρών η φωτογραφία που θα αντικατασταθεί ή θα καλυφθεί τεχνητά το επίμαχο σημείο.

Με το υπ’ αρ. πρωτ. Γ/ΕΞ/1435-1/30-04-2009 έγγραφο προς την εταιρεία η Αρχή επιφυλάχθηκε να κρίνει τη νομιμότητα της προσφερόμενης υπηρεσίας αφού υποβληθεί η απαιτούμενη εκ του

νόμου γνωστοποίηση, επισημαίνοντας ταυτόχρονα να συγκεκριμένα μέτρα για την προστασία των προσωπικών δεδομένων που όφειλε να λάβει η εταιρεία καθώς και την υποχρέωσή της να διακόψει την παροχή της υπηρεσίας προς το κοινό μέχρι την πλήρωση όλων των ανωτέρω συνθηκών. Συνοπτικώς, η Αρχή θεώρησε για τους λόγους που θα εκτεθούν αναλυτικώς στο σκεπτικό της παρούσας ότι α) η συλλογή, αποθήκευση, δημοσίευση στο διαδίκτυο φωτογραφιών που απεικονίζουν πρόσωπα, πινακίδες οχημάτων και οικίες αποτελεί επεξεργασία προσωπικών δεδομένων, β) η επεξεργασία θα μπορούσε να είναι νόμιμη σύμφωνα με το άρθρο 5 παρ. 2 στοιχ. ε) Ν. 2472/1997 εφόσον λαμβάνονται συγκεκριμένα μέτρα για τα επιμέρους ζητήματα της θόλωσης των φωτογραφιών, της τήρησης των πρωτογενών δεδομένων, δηλαδή των δεδομένων που τηρούνται πριν την εφαρμογή της θόλωσης, της λήψης μέτρων για την τυχόν αποκάλυψη ευαίσθητων δεδομένων, της άσκησης των δικαιωμάτων πρόσβασης και αντίρρησης, τέλος, της ενημέρωσης των υποκειμένων των δεδομένων.

Η εταιρεία, στη συνέχεια, προέβη σε διακοπή της παροχής της υπηρεσίας στο κοινό, υπέβαλε την με αρ. πρωτ. ΓΝ/ΕΙΣ/507/11-05-2009 γνωστοποίηση επεξεργασίας προσωπικών δεδομένων, όπως τελικώς συμπληρώθηκε με το υπ. αρ.πρωτ ΓΝ/ΕΙΣ/1060/12-09-2009 έγγραφο, περιγραφή του πληροφοριακού συστήματος (αρ. πρωτ. ΓΝ/ΕΙΣ/514/12-05-2009) καθώς και πολιτική και σχέδιο Ασφαλείας (αρ. πρωτ. ΓΝ/ΕΙΣ/515/12-05-2009).

Σημειώνεται ότι η Αρχή εξέτασε προηγουμένως την με αρ. πρωτ. ΓΝ/ΕΙΣ/1205/22-12-2008 γνωστοποίηση επεξεργασίας που υπέβαλε η εταιρεία Google Inc. για την παρόμοια υπηρεσία “Street View” που προσφέρεται ήδη και σε πολλές πόλεις άλλων χωρών, από την οποία ζήτησε με το υπ. αριθμ. πρωτ.ΓΝ/ΕΞ/374/14-04-2009 έγγραφο διευκρινίσεις και μέτρα για την προστασία των προσωπικών δεδομένων.

Οι δύο αυτές υπηρεσίες, στο μέτρο που παρουσιάζουν κοινά χαρακτηριστικά, χρήζουν ενιαίας αντιμετώπισης. Για το σκοπό αυτό καθώς και για την ομοιόμορφη εφαρμογή της Οδηγίας στα κράτη μέλη της Ευρωπαϊκής Ένωσης λαμβάνονται υπόψη, κατά την εξέταση της παρούσας υπόθεσης, οι απόψεις της Ομάδας Εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ στην υπόθεση “Google – Street View”.

Η Αρχή, μετά από εξέταση όλων των παραπάνω στοιχείων, και κατόπιν διεξοδικής συζήτησης, αφού άκουσε τους εισηγητές,

ΣΚΕΦΤΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΝΟΜΟ

1. Η συγκεκριμένη υπηρεσία οδηγεί σε επεξεργασία προσωπικών δεδομένων κατά την έννοια του άρθρου 2 στοιχ. α), γ) και δ) Ν. 2472/1997, στο μέτρο που η φωτογράφιση των δρόμων συμπεριλαμβάνει και εικόνες προσώπων, πινακίδων οχημάτων και οικιών, δηλαδή πληροφοριών που αναφέρονται αμέσως ή εμμέσως σε φυσικά πρόσωπα και χαρακτηρίζουν την υπόστασή τους από διάφορες απόψεις, εν προκειμένω ιδίως από φυσική, οικονομική ή κοινωνική άποψη. Εξάλλου, δεν πρόκειται για ανώνυμα δεδομένα αφού τα πρόσωπα ή στοιχεία των προσώπων που απεικονίζονται μπορεί να μην είναι γνωστά στον ίδιο τον υπεύθυνο επεξεργασίας ωστόσο παραμένει πιθανή η αναγνώρισή τους από χρήστες της υπηρεσίας με μέσα που ευλόγως μπορεί να χρησιμοποιηθούν από αυτούς ή και άλλους τρίτους (πβλ. σκ. 26 Οδηγίας 95/46/ΕΚ). Αυτό ισχύει και για τις οικίες στο μέτρο που με τη συνδυαστική χρήση διαδικτυακών εφαρμογών γεωγραφικών πληροφοριών (π.χ. Google Maps, Microsoft Virtual Bing Maps) και των στοιχείων που περιέχονται σε δημόσια προσβάσιμους καταλόγους, όπως των διευθύνσεων στους τηλεφωνικούς καταλόγους, μπορεί να εξακριβωθεί η ταυτότητα του ατόμου που διαμένει σε συγκεκριμένο κτήριο και κατ' επέκταση να συναχθούν ενδεχόμενα συμπεράσματα για την οικονομική και κοινωνική κατάστασή του. Σε κάθε όμως περίπτωση η απεικόνιση προσώπων, πινακίδων οχημάτων και οικιών δεν αποτελεί επέμβαση ίδιας έντασης. Το πρόσωπο ενός ατόμου, καθιστά τούτο άμεσα αναγνωρίσιμο και μάλιστα δίνει πληροφορίες για την παρουσία του σε συγκεκριμένο τόπο και υπό συγκεκριμένες συνθήκες, επιπλέον χωρίς καν να το γνωρίζει. Τούτο ισχύει εξίσου και για το όχημα του κατόχου, ο οποίος καθίσταται αναγνωρίσιμος μέσω της πινακίδας.

Αντιθέτως, η απεικόνιση των οικιών, οδηγεί μεν σε κάποια, όχι όμως με βεβαιότητα ακριβή, συμπεράσματα για τις συνθήκες διαβίωσης ενός ατόμου, ενώ άλλωστε οι εικόνες των οικιών ανήκουν σε δημόσιο χώρο και συνεπώς δεν δικαιολογείται το ίδιο επίπεδο προστασίας.

Ως επεξεργασία ορίζεται κάθε εργασία που εφαρμόζεται σε προσωπικά δεδομένα από τη συλλογή μέχρι και την καταστροφή αυτών, με τη χρήση ή μη αυτόματοποιημένων μεθόδων. Εν προκειμένω τα προσωπικά δεδομένα υφίστανται επεξεργασία, αφού π.χ. η φωτογράφιση αξιολογείται ως συλλογή δεδομένων, η τήρηση των εικόνων προς το σκοπό παροχής της υπηρεσίας ως αποθήκευση, χρήση και τροποποίηση, τέλος, η δημοσίευση στο διαδίκτυο ως διάδοση ή διαβίβαση (πβλ. και ΔΕΚ, Απόφαση της 6ης Νοεμβρίου 2003, C-101/01 - Lindqvist, σκ. 25-27).

Η διάδοση των εικόνων αυτών μέσω του διαδικτύου ενέχει ιδιαίτερους κινδύνους αφού τα σχετικά δεδομένα είναι προσβάσιμα σε κάθε ενδιαφερόμενο χρήστη χωρίς κανένα χρονικό ή τοπικό περιορισμό, εκτός και αν ο ίδιος ο πάροχος της υπηρεσίας για άλλους λόγους αποσύρει τις εικόνες, αναστείλει ή καταργήσει την υπηρεσία, ενώ επιπλέον στους εγγενείς κινδύνους του διαδικτύου συγκαταλέγεται η δυνατότητα άντλησης και συνδυασμού προσωπικών δεδομένων μέσω διάφορων διαδικτυακών υπηρεσιών.

Τέλος, η εταιρεία ΚΑΠΟΥ Α.Ε. Γεωπληροφορικής είναι κατά την έννοια του άρθρου 2 στοιχ. ζ) Ν. 2472/1997 υπεύθυνος επεξεργασίας ως προς τη συγκεκριμένη υπηρεσία αφού αυτή ορίζει το σκοπό και τον τρόπο της επεξεργασίας των προσωπικών δεδομένων.

2. Το σύννομο της επεξεργασίας των προαναφερθέντων απλών προσωπικών δεδομένων θα πρέπει να κριθεί με βάση τη διάταξη του άρθρου 5 παρ. 2 στοιχ. ε) Ν. 2472/1997 στο μέτρο που προηγούμενη συγκατάθεση για την απεικόνιση ή μη ενός ατόμου ή άλλων στοιχείων, προσδιοριστικών του ατόμου, δεν είναι δυνατή και ούτε συντρέχει άλλος λόγος επεξεργασίας

από όσους αναφέρονται στο άρθρο 5 του ιδίου νόμου. Η διάταξη του άρθρου 5 παρ. 2 στοιχ. ε) ορίζει ότι η επεξεργασία επιτρέπεται, εφόσον είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας 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. Ως έννομο συμφέρον θεωρείται καταρχήν και η ανάπτυξη οικονομικής δραστηριότητας, ως ιδιαίτερη έκφραση του ατομικού δικαιώματος στην ελεύθερη ανάπτυξη της προσωπικότητας (άρθρο 5 παρ. 1 Συντάγματος). Η παροχή της συγκεκριμένης υπηρεσίας αποτελεί συνεπώς έναν θεμιτό σκοπό με οφέλη μάλιστα και για τους χρήστες της υπηρεσίας, δηλαδή της δυνατότητας περιήγησης και εξοικείωσής τους με τόπους χωρίς να είναι απαραίτητη η μετάβαση σε αυτούς. Η επεξεργασία των προσωπικών δεδομένων που συνδέεται με την παροχή της υπηρεσίας αυτής θα πρέπει ωστόσο να είναι απολύτως αναγκαία ή έστω αναγκαία, όπως ορίζει το άρθρο 7 στοιχ. στ) της Οδηγίας 95/46/ΕΚ, δηλαδή να υπακούει στην αρχή της αναλογικότητας από την οποία απορρέει και η ειδικότερη αρχή της ελαχιστοποίησης των προσωπικών δεδομένων που υφίστανται επεξεργασία για την επίτευξη του συγκεκριμένου σκοπού. Για τη συγκεκριμενοποίηση της αναγκαιότητας της επεξεργασίας προς το σκοπό της παροχής της εν λόγω υπηρεσίας θα πρέπει να ληφθεί υπόψη ότι τα άτομα, των οποίων τα προσωπικά δεδομένα υφίστανται επεξεργασία, εν έχουν προηγούμενη συναλλακτική επαφή με τον υπεύθυνο επεξεργασίας που θα δικαιολογούσε την επεξεργασία αυτή. Θα πρέπει συνεπώς να τηρηθούν συγκεκριμένες προϋποθέσεις ώστε να ελαχιστοποιηθεί η επεξεργασία των προσωπικών δεδομένων και να διασφαλισθούν τα δικαιώματα των υποκειμένων των δεδομένων.

3. Όσον αφορά στην απεικόνιση προσώπων και πινακίδων οχημάτων θα πρέπει να εφαρμόζεται η τεχνική της “θόλωσης” πριν από τη παροχή της υπηρεσίας στο κοινό μέσω του διαδικτύου και μάλιστα με τρόπο ώστε να αποτρέπεται η αντίστροφη μηχανική (reverse engineering). Εφόσον δεν είναι δυνατή η αναγνώριση των προσώπων και των πινακίδων οχημάτων, τα σχετικά δεδομένα καθίστανται ανώνυμα για το χρήστη της υπηρεσίας. Η εταιρεία ΚΑΠΟΥ Α.Ε. Γεωπληροφορικής διαβεβαίωσε με τα έγγραφα υπομονήματα της ότι οι ήδη ληφθείσες φωτογραφίες έχουν υποστεί επεξεργασία με τη μέθοδο της γκαουσιανής θόλωσης, η οποία οδηγεί σε τεχνικώς μη αντιστρέψιμα αποτελέσματα. Η ίδια τεχνική θα εφαρμοσθεί και σε κάθε μελλοντική φωτογράφιση. Η θόλωση πραγματοποιείται αρχικά αυτοματοποιημένα, με την εφαρμογή ειδικού λογισμικού και στη συνέχεια με ανθρώπινη παρέμβαση, όπου ελέγχονται και βελτιώνονται τα αποτελέσματα της αυτοματοποιημένης θόλωσης.

4. Περαιτέρω, όσον αφορά στην απεικόνιση των οικιών, με δεδομένο ότι τούτη δεν αποτελεί ίσης έντασης επέμβαση στο δικαίωμα προστασίας των προσωπικών δεδομένων, η απεικόνισή τους στο διαδίκτυο δεν επιβάλλει την προηγούμενη θόλωση όλων των κτηρίων. Εξάλλου δεν πρόκειται πάντα για κτήρια που χρησιμοποιούνται ως κατοικίες και αντίστοιχη απαίτηση θα μείωνε δραστικώς τα ποιοτικά χαρακτηριστικά της παρεχόμενης υπηρεσίας.

5. Τέλος, όσον αφορά στην τήρηση των πρωτογενών δεδομένων αυτή θα πρέπει να δικαιολογείται με βάση το έννομο συμφέρον του υπευθύνου της επεξεργασίας, δηλαδή να συντρέχουν επαρκείς λόγοι για την τήρησή τους και μάλιστα σε σχέση με συγκεκριμένο χρονικό διάστημα, αναγκαίο για την επίτευξη του σκοπού επεξεργασίας. Επιπλέον, θα πρέπει να λαμβάνονται τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την προστασία αυτών των δεδομένων.

Η εταιρεία ΚΑΠΟΥ Α.Ε. Γεωπληροφορικής δήλωσε ότι η τήρηση των πρωτογενών δεδομένων είναι απαραίτητη για την ορθή εκτέλεση του προγράμματος θόλωσης, την πρόσθετη χειροκίνητη θόλωση όπου χρειάζεται, και την αντικατάσταση τυχόν προβληματικών απεικονίσεων ψευδώς θετικών ή αρνητικών σημείων. Επίσης, δήλωσε ότι τα πρωτογενή δεδομένα, δηλ. οι μη θολωμένες εικόνες, θα διαγράφονται το αργότερο μετά από έξι (6) μήνες από τη φωτογράφιση και με τη βελτιστοποίηση των τεχνικών θόλωσης ο χρόνος αυτός δύναται να μειωθεί στο μέλλον.

Επιπλέον τα πρωτογενή δεδομένα δεν θα διαβιβάζονται σε τρίτους. Ως προς τα τεχνικά και οργανωτικά μέτρα ασφαλείας η εταιρεία δήλωσε τα εξής: α) για την ελαχιστοποίηση του κινδύνου λήψης εικόνων που περιέχουν προσωπικά δεδομένα η φωτογράφιση θα πραγματοποιείται πολύ πρωινές ώρες και κατά προτίμηση αργίες,

β) το πληροφοριακό σύστημα με το πρωτογενές υλικό δεν είναι συνδεδεμένο στο διαδίκτυο, γ) πρόσβαση σε αυτό έχουν μόνο 3 εξουσιοδοτημένα άτομα ενώ απαιτείται χρήση κωδικού ασφαλείας, δ) υπάρχει εγκατεστημένο λογισμικό προστασίας από ιούς, ε) η κεντρική πόρτα των γραφείων της εταιρείας είναι ασφαλείας και στ) τα γραφεία βρίσκονται σε χώρο που διαθέτει υπηρεσία φύλαξης όλο το εικοσιτετράωρο. Η Αρχή κρίνει ότι η τήρηση των πρωτογενών δεδομένων προς το σκοπό της βελτίωσης των αποτελεσμάτων της θόλωσης σε σχέση με το χρονικό διάστημα των έξι μηνών και τα ανωτέρω μέτρα ασφάλειας σε σχέση με το μέγεθος του υπευθύνου επεξεργασίας πληρούν τις προϋποθέσεις των άρθρων 4 παρ. 1 στοιχ. β) και δ), 5 παρ. 2 στοιχ. ε) και 10 Ν. 2472/1997. Σε περίπτωση αύξησης του μεγέθους του υπευθύνου επεξεργασίας, τα οργανωτικά και τεχνικά μέτρα ασφάλειας θα πρέπει να αναθεωρηθούν ώστε να διασφαλίζεται η ελεγχόμενη πρόσβαση στα δεδομένα.

6. Η Αρχή όμως κρίνει ότι η επεξεργασία ευαίσθητων δεδομένων θα παραβίαζε την αρχή της αναλογικότητας σε σχέση με την παροχή της συγκεκριμένης υπηρεσίας και θα πρέπει να ληφθούν μέτρα για την αποφυγή λήψης και περαιτέρω επεξεργασίας εικόνων που ενδεχομένως αποκαλύπτουν ευαίσθητα δεδομένα των ατόμων, όπως σε σχέση με θρησκευτικούς χώρους, νοσηλευτήρια, οίκους ανοχής κλπ.. Ο υπεύθυνος επεξεργασίας δήλωσε ότι ως γενικό μέτρο που λαμβάνει για την ελαχιστοποίηση του κινδύνου είναι ο προγραμματισμός της φωτογράφισης πολύ πρωινές ώρες και κατά προτίμηση αργίες. Επιπλέον, σε περιπτώσεις χώρων που είναι αποκαλυπτικοί ευαίσθητων δεδομένων, θα προβαίνει αμέσως στη θόλωση προσώπων και πινακίδων οχημάτων και κατά προτεραιότητα σε διαγραφή του αντίστοιχου πρωτογενούς υλικού, δηλαδή ο χρόνος τήρησης ευαίσθητων πρωτογενών δεδομένων θα είναι συντομότερος. Επιπλέον, δεν θα πραγματοποιείται φωτογράφιση χώρων για τους οποίους υπάρχει σχετική εκ του νόμου απαγόρευση, όπως στρατοπέδων.

7. Ο υπεύθυνος επεξεργασίας θα πρέπει να ικανοποιεί με τρόπο πρόσφορο που προσιδιάζει στα χαρακτηριστικά της υπηρεσίας τα δικαιώματα των υποκειμένων των δεδομένων που προβλέπονται στο Ν. 2472/1997, δηλαδή τα δικαιώματα της πρόσβασης και αντίρρησης

σύμφωνα με τα οικεία άρθρα 12 και 13, αντιστοίχως. Στη συγκεκριμένη υπηρεσία το δικαίωμα πρόσβασης έχει σημασία ως προς την τήρηση των πρωτογενών δεδομένων αφού στις εικόνες που δημοσιεύονται στο διαδίκτυο η πρόσβαση είναι ελεύθερη για τον καθένα, και εν αμφιβολία τα προσωπικά δεδομένα που δημοσιεύονται θα έχουν προηγουμένως θολωθεί. Εξάλλου, το δικαίωμα πρόσβασης αποτελεί σε πολλές περιπτώσεις την αναγκαία προϋπόθεση για να ζητήσει το υποκείμενο των δεδομένων κατά περίπτωση τη διόρθωση, διαγραφή ή τη δέσμευση των δεδομένων σύμφωνα με το άρθρο 12 παρ. 2 στοιχ. ε) καθώς και να ασκήσει το δικαίωμα αντίρρησης σύμφωνα με το άρθρο 13. Για την αποτελεσματική προστασία του υποκειμένου των δεδομένων η Αρχή κρίνει ότι το δικαίωμα πρόσβασης πρέπει να ικανοποιείται ήδη κατά το στάδιο μετά τη φωτογράφιση συγκεκριμένης περιοχής και πριν τη δημοσίευση της υπηρεσίας στο διαδίκτυο, εφόσον όμως το υποκείμενο των δεδομένων δίδει επαρκή στοιχεία για τον εντοπισμό των δεδομένων που το αφορούν (εικόνες προσώπων, πινακίδων οχημάτων, οικιών).

Το δικαίωμα αντίρρησης αποκτά ιδιαίτερη σημασία ιδίως στις περιπτώσεις που μια επεξεργασία επιτρέπεται με βάση τις διατάξεις του άρθρου 5 παρ. 2 στοιχ. ε) και δ) Ν. 2472/1997, όπως εν προκειμένω βάσει του στοιχ. ε), διότι οι διατάξεις αυτές προϋποθέτουν στάθμιση αντίρροπων συμφερόντων (πβλ. σκ. 45 και άρθρο 14 στοιχ. α) Οδηγίας 95/46/ΕΚ). Συνεπώς, η καταρχήν νόμιμη επεξεργασία των πρωγενών δεδομένων επιτρέπει την άσκηση του δικαιώματος αντίρρησης ήδη κατά το στάδιο πριν τη δημοσίευση της υπηρεσίας στο διαδίκτυο και θα πρέπει, λαμβάνοντας υπόψη τα χαρακτηριστικά της υπηρεσίας και το σκοπό που επιδιώκει ο υπεύθυνος της επεξεργασίας, η υποβολή αντιρρήσεων να μπορεί να οδηγήσει στη διαγραφή ή στη θόλωση του επίμαχου δεδομένου.

Κατά το στάδιο μετά τη δημοσίευση της υπηρεσίας στο διαδίκτυο σε περίπτωση μη θόλωσης ή μη επαρκούς θόλωσης των εικόνων προσώπων ή πινακίδων οχημάτων θα πρέπει το υποκείμενο των δεδομένων αλλά και κάθε τρίτος να μπορεί να επισημαίνει το επίμαχο σημείο και η εταιρεία να προβαίνει ακολούθως σε θόλωση. Καθ' ό μέρος τη θόλωση μπορεί να ζητήσει και κάθε τρίτος, χρήστης της υπηρεσίας, δεν πρόκειται για γνήσιο δικαίωμα αντίρρησης αλλά, για μέτρο βελτίωσης του ποιοτικού ελέγχου της διαδικασίας επεξεργασίας προσωπικών δεδομένων. Ως προς τις οικίες το δικαίωμα αυτό αναγνωρίζεται για τους λόγους που αναφέρονται στα σημεία 1 και 4 της παρούσας μόνο στο υποκείμενο των δεδομένων.

Όσον αφορά ειδικά στις εικόνες προσώπου, σε περίπτωση που το ίδιο το υποκείμενο το ζητήσει ρητώς είτε πριν είτε μετά τη δημοσίευση της υπηρεσίας στο διαδίκτυο, θα πρέπει η διαγραφή ή θόλωση να καταλαμβάνει μεγαλύτερο μέρος απότο πρόσωπο, αφού ακόμη και από το σωματότυπο θα μπορούσε σε ορισμένες περιπτώσεις να αναγνωρισθεί το υποκείμενο των δεδομένων.

Ο υπεύθυνος επεξεργασίας δήλωσε ότι θα ικανοποιεί κατά τα προμνημονευθέντα τα δικαιώματα πρόσβασης και αντίρρησης. Ειδικότερα, οι αντιρρήσεις θα ικανοποιούνται μέσα σε μια εργάσιμη ημέρα. Όσον αφορά στις οικίες το υποκείμενο των δεδομένων θα πρέπει να υποβάλει στοιχεία που να αποδεικνύουν τη σχέση του με το ακίνητο ή να καλεί τον υπεύθυνο επεξεργασίας χωρίς

απόκρυψη αριθμού από σταθερό τηλέφωνο που είναι δηλωμένο για το ακίνητο. Τέλος, ο υπεύθυνος επεξεργασίας δήλωσε ότι τα εν λόγω δικαιώματα μπορούν να ασκηθούν με κάθε μέσο επικοινωνίας.

8. Το δικαίωμα ενημέρωσης και η αντίστοιχη υποχρέωση του υπευθύνου επεξεργασίας σύμφωνα με το άρθρο 11 Ν. 2472/1997 κατά το στάδιο της συλλογής των προσωπικών δεδομένων, εν προκειμένω της φωτογράφισης, αποτελεί θεμελιώδη οριοθέτηση για την νομιμοποίηση της επεξεργασίας καθόσον έτσι το υποκείμενο καθίσταται γνώστης της επεξεργασίας και δύναται να ασκήσει τα υπόλοιπα δικαιώματά του.

Η ενημέρωση θα πρέπει σύμφωνα με το άρθρο 11 παρ. 1 Ν. 2472/1997 να περιλαμβάνει όλα τα στοιχεία που αναφέρονται στη διάταξη αυτή και να πραγματοποιείται με τρόπο πρόσφορο και σαφή. Ειδικότερα, το άρθρο 3 παρ. 2 της κανονιστικής Απόφασης 1/1999 της Αρχής ορίζει ενδεικτικούς τρόπους για την επαρκή και απρόσκοπτη ενημέρωση. Η Αρχή δεν κρίνει ως επαρκή την ενημέρωση μόνο με τη σήμανση των οχημάτων που διέρχονται στους υπό φωτογράφιση δρόμους. Ο υπεύθυνος επεξεργασίας οφείλει να λάβει επιπρόσθετα μέτρα, ώστε να διασφαλίζεται η ενημέρωση ως προς όλα τα σημεία που αναφέρει η διάταξη του άρθρου 11 Ν. 2472/97.

Ως πρόσφοροι τρόποι προτείνονται η ενημέρωση δια του τύπου ή διαμέσου άλλων μέσων μαζικής ενημέρωσης. Η ενημέρωση δια του τύπου θα πρέπει να πραγματοποιείται σε μια καθημερινή πανελλήνιας μεγάλης κυκλοφορίας εφημερίδα της πρωτεύουσας και σε μια τοπική καθημερινή μεγάλης κυκλοφορίας εφημερίδα εκδιδόμενης στην έδρα της Γενικής Γραμματείας της Περιφέρειας, στα διοικητικά όρια της οποίας βρίσκονται οι εκάστοτε υπό φωτογράφιση δήμοι. Δεδομένου ότι στην υπό κρίση περίπτωση δεν απαιτείται λόγω αδυναμίας η προηγούμενη συγκατάθεση των υποκειμένων, η δημοσίευσητου σχετικού κειμένου σε εφημερίδες ευρείας κυκλοφορίας δεν αποτελεί, κατά συνδυαστική ερμηνεία των διατάξεων των παρ. 2 και 3 του άρθρου 3 της Κανονιστικής Πράξης 1/1999 της Αρχής, ενημέρωση δια του τύπου κατά την έννοια της παρ. 3 του άρθρου αυτού, αλλά ενημέρωση με κάθε πρόσφορο μέσο σύμφωνα με την παρ.2 και συνεπώς, δεν απαιτείται προηγούμενη άδεια της Αρχής. Σε κάθε περίπτωση η ενημέρωση θα πρέπει να πραγματοποιείτε και μέσω της ιστοσελίδας της εταιρείας, σε εμφανές σημείο αυτής. Στην ιστοσελίδα θα πρέπει να αναφέρονται οι περιοχές όπου πρόκειται να πραγματοποιηθεί η φωτογράφισηκαθώς και το προγραμματισμένο χρονικό διάστημα για κάθε περιοχή.

Το κείμενο της ενημέρωσης στα κύρια σημεία ενδείκνυται να διαμορφωθεί περίπου ως εξής:

«Η εταιρεία ΚΑΠΟΥ Α.Ε. ανακοινώνει ότι κατά το διάστημα από ..../..../.... έως ..../..../.... θα προβεί σε τρισδιάστατη χαρτογράφηση των δρόμων, πεζοδρόμων, πεζοδρομίων και προσόψεων του αντίστοιχου κτηριοδομικού ιστού των/ης πόλεων/ης ..... των/ου Νομών/ού ..... με αυτοκίνητο που θα φέρει ευδιάκριτα γνωρίσματα της εταιρείας μας και στην οροφή μία κάμερα. Σκοπός της χαρτογράφησης είναι η εικονική περιήγηση μέσω διαδικτύου. Η χαρτογράφηση γίνεται τις πρωινές ώρες και κυρίως αργίες ώστε να ελαχιστοποιείται η πιθανότητα αποτύπωσης προσωπικών δεδομένων. Τα πρόσωπα και οι πινακίδες οχημάτων θολώνονται επαρκώς, έτσι ώστε να μην είναι εφικτή η αναγνώριση και με τρόπο μη αντιστρέψιμο πριν την ανάρτηση της χαρτογραφημένης περιοχής στην ιστοσελίδα μας .

Τέλος επισημαίνεται ότι ο υπεύθυνος επεξεργασίας δήλωσε ότι πρόκειται να συμμορφωθεί με την υποχρέωση του άρθρου 11 Ν. 2472/1997.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή κρίνει ότι η παροχή υπηρεσίας εικονικής περιήγησης στους δρόμους ελληνικών περιοχών από την εταιρεία ΚΑΠΟΥ Α.Ε. Γεωπληροφορικής, ως υπεύθυνο επεξεργασίας, είναι σύμφωνη με τον Ν. 2472/1997, εφόσον ο υπεύθυνος επεξεργασίας τηρήσει τους όρους που αναφέρονται στο σκεπτικό της παρούσας.

Οδηγίες κατασκευής site σε php και mysql databases.

Στοιχεία site:

Url: www.mywebpage1.com

Email: contact@mywebpage1.com

Πρόσβαση στο webmail: webmail.lonex.com

Στοιχεία Πρόσβασης στο webmail: contact@mywebpage1.com password: mypage1

Οι ενέργειες για την κατασκευή του site, με χρονική σειρά:

1. Αγορά χώρου φιλοξενίας σε Linux Server με Apache που υποστηρίζει php 4/5, mysql databases (php admin) με περιβάλλον διαχείρισης Hespia Control Panel.
2. Κατοχύρωση του domainσύμφωνα με τις υποδείξεις του εξυπηρετητή (server).
3. Δημιουργία της database μέσω του περιβάλλοντος διαχείρισης του server.
4. Δημιουργία ftp account μέσω του περιβάλλοντος διαχείρισης του server.
5. Δημιουργία ενός mailbox τύπου webmail (contact@mywebpage1.com) μέσω του περιβάλλοντος διαχείρισης του server και ενεργοποίηση των αντίστοιχων antispam filter που μου παρέχει το περιβάλλον διαχείρισής του.
6. Δημιουργία php, css, xml, javascript και .htaccess αρχείων που περιλαμβάνει το site μέσω εφαρμογής Dreamweaver Macromedia. Σύνδεση των αρχείων php με τις βάσεις δεδομένων μέσω της λειτουργίας εντολής: mysql_connect(servername, username, password);
7. Επεξεργασία των φωτογραφιών με την εφαρμογή Adobe Photoshop και την περίληψή τους σε ειδικό φάκελο.
8. Ανέβασμα όλων των παραπάνω αρχείων μέσω του Dreamweaver στο root της τοποθεσίας μου στον server.
9. Ενσωμάτωση κώδικα από το google για τη λειτουργία του recaptcha στη φόρμα επικοινωνίας που συμβάλλει στην αποφυγή spam και την ασφάλεια του site.
10. Δοκιμή και λειτουργία του δικτυακού τόπου www.mywebpage1.com.

Βιβλιογραφία

ΕΛΛΗΝΙΚΗ

- **Κούρτη Ευαγγελία ,2003 Η επικοινωνία στο Διαδίκτυο**
- **Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ) (2006),»Κανονισμός για την Διασφάλιση του Απορρήτου Δικτυακών Υποδομών»**
- **Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) (2006) ,»Κανονισμός για την Ο όρος ανήκει στον Άγγλο φυσικό D. W. Davies, ενώ το πρώτο άρθρο σχετικά με τη θεωρία της διαμεταγωγής πακέτων γράφτηκε από τον Leonard Kleinrock του MIT τον Ιούλιο του 1961 (Leiner et L.,2003). Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα, σελ.60.**

[1]Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 60

- **Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα , σελ. 61**
- **Παράλληλα, το αντίστοιχο δίκτυο είχε τεθεί σε πειραματική λειτουργία στο Εθνικό Εργαστήριο Φυσικής της Αγγλίας από το 1968 από τον D. W. Davies.**

- **Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου.**
- **Συνήγορος του Πολίτη ενημέρωση του καταναλωτή για την προστασία από το ηλεκτρονικό έγκλημα , Αθήνα 2008**
- **Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα, σελ.60. Πολλά άρθρα του Baran εκείνης της εποχής υπάρχουν στο δικτυακό τόπο**
- **Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα , σελ. 61.**
- **[1] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα , σελ. 62**
- **[1] Μέθοδος μεταφοράς πληροφοριών, σε μορφή πακέτων δεδομένων.**
- **[1] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 63**
- **[1] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ.64**

- **Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 65**
- [1] **Γουλτίδης Χρήστος, ECDL4, Αθήνα 2004. Κλειδάριθμος σελ. 72**
- **Βλέπε και την απόφαση του ΔΕΚ,16 Δεκεμβρίου 1992, επιτροπή κατά του Βελγίου, 211/91**
- [1] **Βλέπε ΔΕΚ ,18 Ιουνίου 1991, ΕΡΤ Α.Ε κατά Δημοτικής Εταιρείας Πληροφόρησης 260/89, 1991, 2951.**
- **Βλ προστασία προσωπικών δεδομένων στο ηλεκτρονικό εμπόριο κεφ 9 σελ 199**
- **Βλ.Χριστοδούλου Κώστα «Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία»**
- **Προστασία προσωπικών δεδομένων στο Ηλεκτρονικό εμπόριο βλ σελ 212**
- **Βλ. Ιγγλεζάκη, εισαγωγή στο Δίκαιο Πληροφορικής .Αξίζει ακόμα να αναφερθεί ότι οι διατάξεις για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα δεν παρουσιάζουν αυτοτέλεια, αλλά εντάσσονται στο γενικότερο πλαίσιο των ρυθμίσεων του ν. 2472/1997ν οι διατάξεις του οποίου εφαρμόζονται για κάθε ζήτημα που δεν ρυθμίζεται ειδικότερα από τον νόμο, σύμφωνα με το άρθρο 3 του νόμου 3471/2006, σελ 198.**
- **Ι.Καρακωστας , Δίκαιο και Internet 2001 σελ.142**
- **Ι.Καρακώστας, Δίκαιο και Internet 2001 sel.142.**
- [1] **Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (2006)**
- **Σινανιώτη Μαρούδα Ηλεκτρονική Τραπεζική**
- **Ιγγλεζάκης Ιωάννης ευαίσθητα προσωπικά δεδομένα**
- **Χριστοδούλου Κωνσταντίνος 2004 Αστική ευθύνη του παρόχου δικτύου ως μεσάζοντος στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας ΔιΜΜΕ,350**

Διαδίκτυο

- http://conventions .coe.int
- http://www.rand.org/publications/RM/baran.list.html
- http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/periinternet.htm
- http://www.dpa.gr/
- www.adae.gr
- http://pki.grnet.gr
- Htpp://pandasecurity.com
- http://ec.europa.gr
- www.microsoft.com

- www.ibm.com
- www.secnews.gr

ΝΟΜΟΙ

- **Νόμος 2472/1997 –«Για την προστασία των προσωπικών δεδομένων στο διαδίκτυο»**
- **Νόμος 3471/2006- «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών**
- **Νόμος 3917/2011 « διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσιών δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με την λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους ή συναφείς διατάξεις.**