# Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

## Μεταπτυχιακή Διατριβή

| | |
|---|---|
| Τίτλος Διατριβής | **Τεχνικά Μέτρα και Νομικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων στο Διαδίκτυο** |
| Ονοματεπώνυμο Φοιτητή | **Μαζαράκης Γεώργιος** |
| Πατρώνυμο | **Παναγιώτης** |
| Αριθμός Μητρώου | **ΜΠΠΛ/ 08024** |
| Επιβλέπουσα | **Αριστέα Σινανιώτη** |

Ημερομηνία Παράδοσης **25 Μαΐου 2011**

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

**Τριμελής Εξεταστική Επιτροπή**

| (υπογραφή) | (υπογραφή) | (υπογραφή) |
|---|---|---|
| Αριστέα Σινανιώτη<br>Καθηγήτρια | Χρήστος Δουληγέρης<br>Καθηγητής | Δέσποινα Πολέμη<br>Επίκουρος Καθηγήτρια |

# Πίνακας Περιεχομένων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

# Πίνακας Εικόνων

## Περίληψη

Στην παρούσα εργασία μελετήθηκαν τόσο το υπάρχον περιβάλλον στο διαδίκτυο και οι δραστηριότητες που λαμβάνουν χώρα σε αυτό, όσο και η συσχέτιση που υπάρχει με την επεξεργασία προσωπικών δεδομένων.

Πράγματι για τις περισσότερες διεργασίες στο διαδίκτυο (ηλεκτρονικές πληρωμές, εγγραφές σε ιστοσελίδες, ιστορικό περιήγησης στο διαδίκτυο) περιλαμβάνονται πληροφορίες που θεωρούνται «προσωπικού χαρακτήρα», και άρα προκύπτει η ανάγκη προστασίας των πληροφοριών αυτών.

Για το λόγο αυτό μελετώνται οι κυριότεροι κίνδυνοι παραβίασης των προαναφερθέντων προσωπικών δεδομένων, καταλήγοντας έτσι στην περιγραφή και μελέτη των υπαρχόντων μέτρων προστασίας των προσωπικών δεδομένων. Αρχικά γίνεται μια εκτενής αναφορά στις τεχνολογικές προτάσεις και στις αναπτυχθείσες αρχιτεκτονικές για την προστασία των προσωπικών δεδομένων (πυρότοιχοι, κωδικοποίηση, πιστοποίηση ταυτότητας, ασφαλή κανάλια ηλεκτρονικής επικοινωνίας), ενώ στη συνέχεια γίνεται αναφορά στο νομοθετικό πλαίσιο το οποίο προστατεύει τα προσωπικά δεδομένα στο διαδίκτυο.

Πιο συγκεκριμένα στο πέμπτο κεφάλαιο παρουσιάζονται αναλυτικά τόσο οι ευρωπαϊκές οδηγίες που αφορούν την προστασία των προσωπικών δεδομένων, όσο και οι αντίστοιχοι νόμοι που έχουν ψηφιστεί στην Ελλάδα και έχουν εναρμονιστεί με τις προαναφερθείσες οδηγίες. Τέλος γίνεται και μια σύνοψη για την εξαγωγή συμπερασμάτων σχετικά με το υπάρχον πλαίσιο γύρω από τα προσωπικά δεδομένα, την επεξεργασία και την μετάδοσή τους, τόσο τεχνικά όσο και νομικά.

## Abstract

In the present both the current Internet environment and the activities taking place therein are studied, as well as and the relationship that exists with the processing of personal data.

Indeed, most processes on the Internet (electronic payments, subscriptions to web sites, web browsing history) require some kind of information considered "personal" and therefore it is necessary to protect such information.

For this reason the main risks of violation of the above data are studied, thus leading to a detailed review of existing measures to protect personal data. Starting from a report on technological architectures aiming data protection (firewalls, cryptography, authentication, secure electronic channels) we continue referring to the legislative framework to protect personal data online.

More specifically both the European directives concerning the protection of personal data and the corresponding laws have been passed in Greece harmonizing with the above instructions are presented in chapter five. Finally, there is a summary with the conclusions on the existing protection measures studied dealing with personal data processing and broadcasting, both technically and legally.

# 1 Εισαγωγή

## 1.1 Γενικά

Το διαδίκτυο (internet) μετράει πάνω από 40 χρόνια «ζωής». Σε αυτό το πλαίσιο είναι γενικά παραδεκτό ότι καμία τεχνολογία δεν έχει εξελιχθεί τόσο πολύ σε τόσο μικρό χρονικό διάστημα. Αξίζει χαρακτηριστικά να αναφερθεί ότι το 1996 ο αριθμός των χρηστών του internet έφτανε διεθνώς τα 60.000.000 ενώ μέχρι και το τέλος του 2010 οι χρήστες του διαδικτύου ξεπέρασαν το όριο των 2 δισεκατομμυρίων, με πρόβλεψη ότι μέχρι το τέλος του 2011, θα είναι δικτυωμένος ο μισός πληθυσμός της Γης και μέχρι το 2020 το 75% – 80% των κατοίκων του πλανήτη θα βρίσκονται πλέον online.[1] Νούμερα που κάνουν τα λόγια του Βίντον Σερφ[1] που θεωρείται πατέρας του διαδικτύου προφητικά, αφού όπως είχε πει χαρακτηριστικά το 1998 “η εξάπλωση του διαδικτύου είναι σαν ένα τσουνάμι που ξεκινά από ύψος μερικών εκατοστών και όταν πλησιάζει την ακτή έχει φτάσει τα 30 μέτρα και παρασύρει τα πάντα. Κάθε αντίσταση είναι μάταιη.”[3]. Ακόμη και στα τελευταία δεκαπέντε χρόνια περίπου, έχει αναδομηθεί, αρκετές φορές, τόσο τεχνολογικά όσο και λειτουργικά. Σε κάθε προηγμένο τεχνολογικά κράτος, οποιαδήποτε υπηρεσία, οργανισμός, εταιρία ή επιχείρηση χρησιμοποιεί τον υπολογιστή της και μέσω του διαδικτύου διαχειρίζεται έναν τεράστιο όγκο πληροφοριών που μέχρι πριν λίγα χρόνια φάνταζε αδιανόητο. Μπορούμε πλέον δικαιολογημένα να μιλάμε για εξάρτηση του κράτους από την πληροφορική [2]. “Εξ’ άλλου η αύξηση του αριθμού των συνδέσεων με το internet θεωρείται από τους ειδικούς κριτήριο ανάπτυξης μιας χώρας, όπως η αύξηση του ΑΕΠ ή του αριθμού των πτυχιούχων και τονίζεται ότι η διάδοση του internet είναι πλέον μια διαδικασία μη αναστρέψιμη”.[3] Τώρα οι δραστηριότητες στο διαδίκτυο περιλαμβάνουν μεταξύ άλλων, αγορές, τραπεζικές συναλλαγές, εργασία και επικοινωνία ανθρώπων online, αλλά και κοινοποίηση αυτού που κάνουμε ή αισθανόμαστε μια δεδομένη χρονική στιγμή (π.χ. facebook). Έχουμε τη δυνατότητα μέσα απ’ αυτό να διαβάζουμε, να ακούμε και να παρακολουθούμε τα πάντα.

Η εξάρτησή μας αυτή καθώς και το γεγονός ότι η χρήση των συστημάτων αυτών είναι προσιτή ακόμα και στο μέσο χρήστη, έχουν οδηγήσει σε μία ενισχυμένη πολυπλοκότητα όσον αφορά τη δομή τους αλλά και το κανονιστικό πλαίσιο στο οποίο κινούνται, δημιουργώντας αναπόφευκτα κενά ασφαλείας, που οφείλονται ή σε προγραμματιστικά σφάλματα, ή σε εσφαλμένες ρυθμίσεις από μέρους του χρήστη, ή τέλος σε αδυναμία των νόμων και των κανόνων να καλύψουν κάθε πτυχή του θέματος. Εξαιτίας του γεγονότος ότι οι υπολογιστές έχουν τη δυνατότητα να συγκεντρώνουν, να επεξεργάζονται και να μεταδίδουν πληροφορίες σε ασύλληπτες ταχύτητες για τα ανθρώπινα δεδομένα, είναι ταυτόχρονα και σε θέση να προσβάλλουν την προσωπικότητα, την ανεξαρτησία και γενικότερα την ελευθερία του ανθρώπου πολύ πιο εύκολα απ’ ότι τα παραδοσιακά μέσα.[2]

Το μεγαλύτερο ποσοστό χρηστών του διαδικτύου παρ’ ότι βομβαρδίζεται καθημερινά από μηνύματα που του προσφέρουν απλόχερα προστασία από κακόβουλη επίθεση, δυστυχώς βρίσκεται σε πλήρη σύγχυση όσον αφορά την ασφάλεια των δεδομένων του, μην έχοντας πλήρη γνώση των κινδύνων και των απειλών που διατρέχει, ενώ οι εταιρείες παροχής υπηρεσιών είτε πρόκειται για απλές υπηρεσίες ηλεκτρονικής αλληλογραφίας, είτε για πολυπλοκότερες όπως web banking και υποβολή φορολογικών δηλώσεων δεν τον προστατεύουν στο ακέραιο και παρέχουν μια εσφαλμένη αίσθηση ότι ασχολούνται αποτελεσματικά με την ασφάλεια των προσωπικών δεδομένων του.

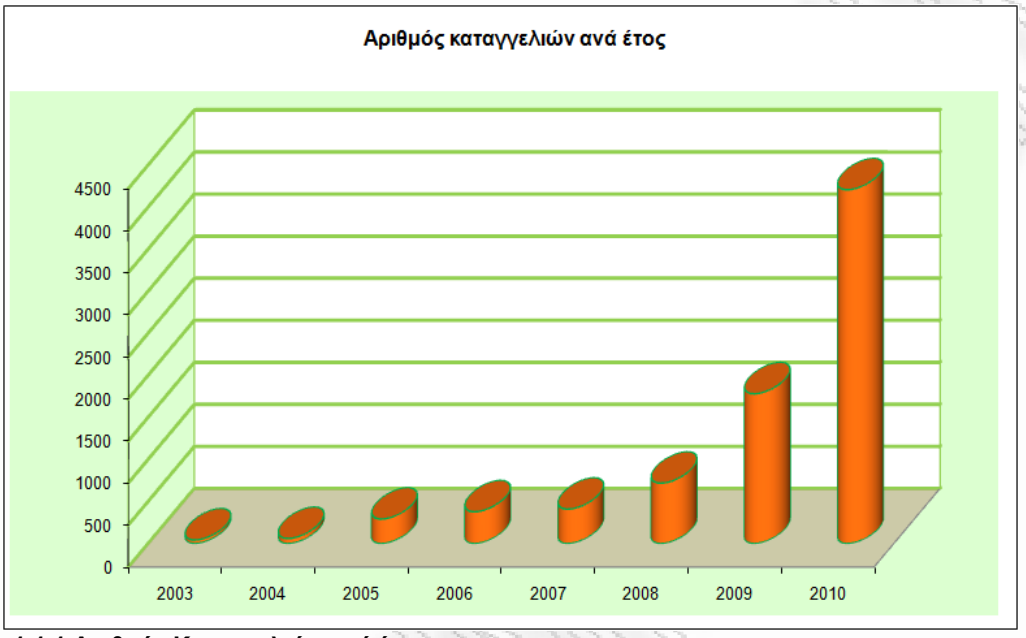
Μέρα με τη μέρα ο αριθμός των χρηστών του διαδικτύου, που πέφτει θύμα κάποιας ηλεκτρονικής απάτης όλο και αυξάνεται παρά το γεγονός ότι οι μέθοδοι και τα εργαλεία για την αποτροπή της συνεχώς βελτιώνονται. Αυτό αποδεικνύεται περίτρανα από τα στατιστικά στοιχεία που εξέδωσε η SafeLine[3] για το 2010. Ο αριθμός των καταγγελιών που έλαβε το 2010, έφτασε

[1] Δημιουργός του πρωτοκόλλου TCP/IP και σημερινός αντιπρόεδρος της Google

[2] Μαρίνος, Α. (2003). *Το διαδίκτυο*, Σάκκουλας Αντ. 25

[3] Η SafeLine ιδρύθηκε το 2003 από την Ελληνική Εταιρία Τηλεπικοινωνιών και Τηλεματικών Εφαρμογών (FORTHNET), το Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Internet (SAFENET), το Ίδρυμα Τεχνολογίας και Έρευνας - Ινστιτούτο Πληροφορικής (ΙΤΕ-ΙΠ) και το Ίδρυμα Μείζονος Ελληνισμού (ΙΜΕ). Είναι ανοικτή γραμμή καταγγελιών

τις 4204 (αύξηση 136,44% σε σχέση με το 2009) και αφορούσε παράνομο περιεχόμενο, ή παράνομες δραστηριότητες στο Διαδίκτυο (Εικόνα 1.1.1). Τα τελευταία 3 χρόνια οι καταγγελίες αυξήθηκαν κατά μέσο όρο κατά 1.250 ανά έτος, γεγονός που αντιστοιχεί σε ένα μέσο ετήσιο ρυθμό αύξησης των καταγγελιών της τάξης του 100%. [5]




**Εικόνα 1.1.1 Αριθμός Καταγγελιών ανά έτος**
**Πηγή:** [www.safeline.gr/Στατιστικά-Στοιχεία](www.safeline.gr/Στατιστικά-Στοιχεία)

Τους τελευταίους 6 μήνες οι καταγγελίες αφορούσαν κατά:(Εικόνα 1.1.2):
- 25% ρατσισμό ή ξενοφοβία
- 21% παραβίαση προσωπικών δεδομένων και υποκλοπή ταυτότητας
- 14% οικονομικές απάτες μέσω διαδικτυακών αγορών
- 10% εξύβριση ή συκοφαντική δυσφήμηση
- 6% παιδική πορνογραφία
- σε μικρότερο ποσοστό εγκλήματα όπως αποπλάνηση ανηλίκων (grooming)[4], phishing[5], ηλεκτρονικό εκφοβισμό (cyber bullying)[6], παραβίαση πνευματικής ιδιοκτησίας, παραβίαση του απορρήτου των επικοινωνιών και απειλή. [5]

Μια άλλη εξίσου σημαντική έρευνα που έγινε σε Ευρωπαϊκό επίπεδο από το Δίκτυο EU Kids Online network[7] δείχνει ότι το 9% των παιδιών ηλικίας 11-16 ετών έπεσαν θύματα

παράνομου περιεχομένου στο Διαδίκτυο και επίσημο μέλος του **INHOPE** (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου) από τις 18 Οκτωβρίου 2005.

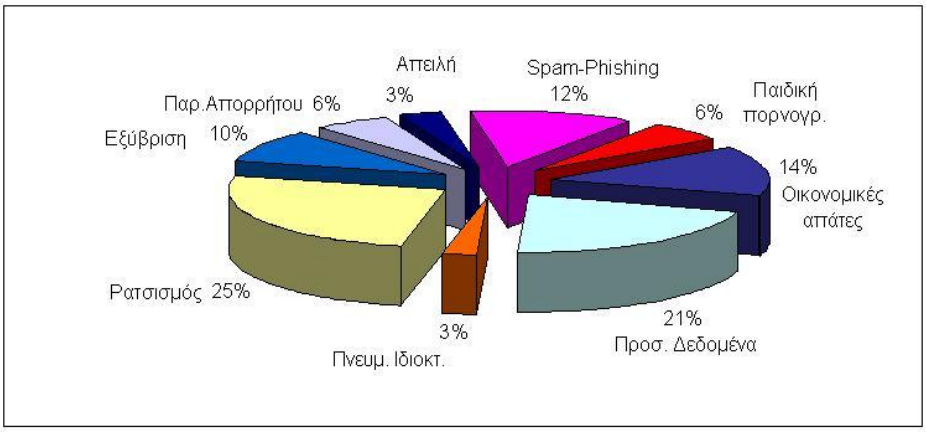
[4] Είναι η χρησιμοποίηση χώρων ανοικτής επικοινωνίας από παιδόφιλους που προσποιούνται ότι είναι έφηβοι, για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν.[4]

[5] Είναι παραλλαγή του αγγλικού «fishing» (ψάρεμα), και αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

[6] Αφορά τον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων με τη χρήση του διαδικτύου, των κινητών τηλεφώνων και άλλων ψηφιακών τεχνολογιών από ομηλίκους τους.

[7] Το EU Kids Online Network έχει στόχο τη διεξαγωγή συγκριτικών μελετών σε ευρωπαϊκό επίπεδο με θέμα τη χρήση του Διαδικτύου από παιδιά και εφήβους. Απαρτίζεται από ακαδημαϊκούς από 21 χώρες και τελεί υπό την αιγίδα του προγράμματος Safer Internet Plus 2006-2013 και την ακαδημαϊκή καθοδήγηση του London School of Economics (Dept of Mass Media and Communication). Στην έρευνα συμμετείχαν 25 χώρες (Αυστρία, Βέλγιο, Βουλγαρία, Γαλλία, Γερμανία, Δανία, Ελλάδα, Εσθονία, Ηνωμένο Βασίλειο, Ιρλανδία, Ισπανία, Ιταλία, Κύπρος, Λιθουανία, Ολλανδία, Ουγγαρία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβενία, Σουηδία, Τουρκία, Τσεχία και Φινλανδία) και η έρευνα πραγματοποιήθηκε στα σπίτια των παιδιών, σε μορφή δια ζώσης συνέντευξης. Συμπεριελάμβανε μια ενότητα για τις ευαίσθητες ερωτήσεις, την οποία συμπλήρωναν μόνα τους τα παιδιά έτσι ώστε να μην τους ακούσουν οι γονείς, άλλα μέλη της οικογένειας ή ο ίδιος ο ερευνητής.

παράνομης χρήσης των προσωπικών τους δεδομένων (7% παραβίαση κωδικών και 5% παραβίαση άλλων προσωπικών δεδομένων) ή θύματα οικονομικής απάτης (2%).[6]




**Εικόνα 1.1.2 Περιεχόμενο καταγγελιών**
**Πηγή: www.safeline.gr/Στατιστικά-Στοιχεία**

Τέλος ακόμη μια έρευνα που διεξήγαγε η εταιρία λογισμικού ασφαλείας ηλεκτρονικών υπολογιστών McAfee μεταξύ 200 στελεχών των τεχνολογιών πληροφορικής που εργάζονται για εταιρίες κοινής ωφελείας (φυσικού αερίου, ηλεκτρισμού και υδροδότησης) σε 14 χώρες, απέδειξε ότι 8 στους 10 δήλωσαν ότι τα δίκτυα τους αποτέλεσαν στόχο παράνομων εισβολέων κατά το έτος 2010 σε αντίθεση με το έτος 2009 που μόλις το 50% των ερωτηθέντων είχε δηλώσει πως είχαν πέσει θύμα επίθεσης. Πιθανότερη πηγή των επιθέσεων αυτών πιθανολογείται πως είναι η Κίνα, ακολουθούμενη από τη Ρωσία και τις ΗΠΑ.[15]

Περιστατικά υποκλοπών που έχουν σα στόχο τα προσωπικά δεδομένα υπάρχουν πάρα πολλά. Ένα από τα μεγαλύτερα περιστατικά στην ιστορία του Ίντερνετ και της πληροφορικής αποτελεί η πρόσφατη επίθεση στο δίκτυο της Sony Playstation μεταξύ 17ης και 19ης Απριλίου 2011, όπου υπήρξαν παραβιάσεις 70 εκατομμυρίων λογαριασμών χρηστών απ' όλο τον κόσμο, από τους οποίους εκλάπησαν ονόματα, διευθύνσεις, χώρες προέλευσης, email, ημερομηνίες γέννησης, κωδικοί πρόσβασης καθώς επίσης και στοιχεία πιστωτικών καρτών που είχαν χρησιμοποιηθεί κατά το παρελθόν για την αγορά παιχνιδιών, ταινιών και μουσικής. Επίσης άλλο ένα αντίστοιχο περιστατικό, που συνέβη τον Απρίλιο του 2011 ήταν η μαζική κλοπή δεδομένων δεκάδων εκατομμυρίων ονομάτων και διευθύνσεων e-mail μεγάλων αμερικανικών τραπεζών, ξενοδοχείων και καταστημάτων από τις βάσεις δεδομένων της αμερικανικής εταιρείας online marketing Epsilon, τα οποία θεωρείται πως σύντομα θα αρχίσουν (αν δεν έχουν αρχίσει ήδη) να χρησιμοποιούνται σε κυβερνοεγκληματικές δραστηριότητες.[15]

Τα νούμερα των ερευνών αυτών μιλάνε από μόνα τους και το συμπέρασμα που εξάγεται είναι ένα. Η προστασία του πολίτη από κάθε είδους απειλή στο διαδίκτυο είναι πλέον επιτακτική και οφείλει να γίνει είτε στο επίπεδο του διαδικτύου είτε στο επίπεδο του απλού χρήστη με σωστή ενημέρωση και κατάλληλη εκπαίδευση καθώς και με την ανάπτυξη κατάλληλων μηχανισμών που θα έχουν σα στόχο την αποτροπή ή έστω την ελαχιστοποίηση των ανεπιθύμητων παραβιάσεων ασφαλείας.

## 1.2 Σκοπός Εργασίας

Στα πλαίσια της εργασίας αυτής, αναγνωρίζοντας την αναγκαιότητα για παροχή εξασφαλισμένης προστασίας των προσωπικών δεδομένων κατά την διενέργεια συναλλαγών και γενικότερα υπηρεσιών επικοινωνίας μέσω του διαδικτύου, μελετήθηκαν τα υπάρχοντα σχήματα ασφαλείας σε δύο διαφορετικά επίπεδα. Αφενός γίνεται μια τεχνική προσέγγιση των τρόπων προστασίας των προσωπικών δεδομένων και αφετέρου αναλύονται διεξοδικά όλοι οι νόμοι που έχουν θεσπιστεί σε εθνικό αλλά και Ευρωπαϊκό επίπεδο μέσω των σχετικών οδηγιών του Ευρωπαϊκού Κοινοβουλίου.

Γίνεται, μία εκτενής παρουσίαση του περιβάλλοντος του διαδικτύου τόσο σε τεχνολογικό όσο και σε επίπεδο υπηρεσιών, ώστε να είναι εφικτή η κατανόηση των αναγκών που καθιστούν επιτακτική την προαναφερθείσα προστασία των δεδομένων προσωπικού χαρακτήρα και παράλληλα περιγράφονται και οι βασικές έννοιες σε νομικό επίπεδο.

## 1.3 Δομή Εργασίας

Η μεταπτυχιακή διατριβή αποτελείται από τρία μέρη. Στο μεν πρώτο μέρος γίνεται η τεχνική προσέγγιση του θέματος, στο δε δεύτερο η νομική και στο τρίτο και τελευταίο μέρος γίνεται η περιγραφή ανάπτυξης και υλοποίησης κάποιων μέτρων θωράκισης μιας ιστοσελίδας. Στο παρόν πρώτο κεφάλαιο γίνεται μια εισαγωγή στο αντικείμενο που πραγματεύεται η εργασία αυτή, παραθέτοντας κάποια στατιστικά στοιχεία χρήσης του διαδικτύου, που οδηγούν στη δικαιολόγηση της ανάγκης λήψης μέτρων προστασίας των προσωπικών δεδομένων ενώ το περιεχόμενο των υπολοίπων κεφαλαίων συνοψίζεται ως ακολούθως.

Στο δεύτερο κεφάλαιο γίνεται μια αναλυτική παρουσίαση των βασικών εννοιών που χρησιμοποιούνται στην εργασία αυτή, η κατανόηση των οποίων είναι απαραίτητη για τη ανάπτυξη των θεμάτων και την κατανόηση των όσων πρόκειται να αναλυθούν στη συνέχεια. Σε αυτό το πλαίσιο, πραγματοποιείται μια σύντομη ιστορική αναδρομή σχετικά με τον παγκόσμιο ιστό και τις ανάγκες για ασφάλεια, καθώς και μια συνοπτική παρουσίαση της έννοιας των προσωπικών δεδομένων. Επιπλέον, παρουσιάζονται τα βασικά χαρακτηριστικά και οι απαιτήσεις για την ασφάλεια ενός συστήματος.

Στο τρίτο κεφάλαιο παρουσιάζεται κατ' αρχάς ο λόγος ύπαρξης των πολιτικών ασφαλείας των δικτύων καθώς και οι βασικότεροι τομείς των ηλεκτρονικών επικοινωνιών που υφίστανται κάποια παραβίαση ασφαλείας. Στη συνέχεια γίνεται αναφορά στις κατηγορίες εισβολέων όπως διαμορφώνονται αυτή τη στιγμή στον χώρο της πληροφορικής όπως επίσης και στις βασικότερες και πιο διαδεδομένες επιθέσεις που λαμβάνουν χώρα σε περιβάλλοντα δικτύων μέχρι σήμερα. Τέλος γίνεται μια σύντομη αναφορά στις ενέργειες που θα πρέπει να προβεί κανείς, σε περίπτωση που θα πέσει θύμα κάποιας εκ των προαναφερομένων επιθέσεων.

Στο τέταρτο κεφάλαιο μελετώνται τα τεχνικά μέτρα προστασίας προσωπικών δεδομένων στο διαδίκτυο. Παρουσιάζονται τεχνικές προστασίας τόσο στο επίπεδο του εξυπηρετητή, όσο και στο επίπεδο του χρήστη. Πιο συγκεκριμένα, στο κεφάλαιο αυτό παρουσιάζονται οι πυρότοιχοι προστασίας, τα προγράμματα antivirus, τα συστήματα ανίχνευσης εισβολέων, η ασφάλεια της ηλεκτρονικής αλληλογραφίας, η κρυπτογράφηση, το πρωτόκολλο SSL όπως επίσης και οι ψηφιακές υπογραφές.

Στο πέμπτο κεφάλαιο γίνεται λόγος για την ιδιωτικότητα, όπως αυτή αναφέρεται παγκοσμίως και παρουσιάζεται αναλυτικά το νομοθετικό πλαίσιο που υποστηρίζει το θεμελιώδες δικαίωμα του ανθρώπου σχετικά με την ιδιωτικότητα και τα προσωπικά δεδομένα του, τόσο σε Ευρωπαϊκό όσο και σε εθνικό επίπεδο.

Στο έκτο κεφάλαιο γίνεται μια σύνοψη όσων παρουσιάστηκαν και εξάγονται τα σχετικά συμπεράσματα καταλήγοντας στο έβδομο κεφάλαιο όπου περιγράφονται αναλυτικά οι ενέργειες θωράκισης της ασφάλειας μιας ιστοσελίδας κατά την υλοποίησή της.

# 2 Προσωπικά Δεδομένα και Ασφάλεια στο Διαδίκτυο

## 2.1 Σύντομη Ιστορική αναδρομή

Ο αιώνας που διανύουμε δικαίως έχει χαρακτηριστεί ως ο αιώνας της πληροφορίας. Οι ραγδαίες εξελίξεις στον χώρο της τεχνολογίας τα τελευταία χρόνια έχουν οδηγήσει τόσο στην ανάπτυξη των πληροφοριακών συστημάτων που έχουν ως αντικείμενο την επεξεργασία και την επικοινωνία δεδομένων και πληροφοριών, όσο και του διαδικτύου, που είναι το κλειδί της ανάπτυξης νέων επιχειρησιακών μοντέλων όπως και νέου τρόπου διακίνησης γνώσης. Μέρα με τη μέρα το διαδίκτυο επεκτείνεται και δημιουργούνται νέες δυνατότητες που απαιτούν την ανταλλαγή όλο και περισσότερων δεδομένων.

Ο τομέας της πληροφορικής, έχει σημειώσει πολύ σημαντική πρόοδο μέσα σε πολύ μικρό χρονικό διάστημα. Ειδικά τις δύο τελευταίες δεκαετίες μπορούμε να πούμε ότι ο κόσμος των υπολογιστών έχει αλλάξει δραματικά. Βασικές δραστηριότητες που εκτελούσαμε μέχρι σήμερα όπως το να ακούμε μουσική, το να μαθαίνουμε τα νέα και κυρίως το να επικοινωνούμε μεταξύ μας έχουν αλλάξει άρδην. Μια πολύ σημαντική διαφοροποίηση του χτες με το σήμερα βρίσκεται στον τρόπο κατανομής της πληροφορίας στους υπολογιστές αλλά και στον τρόπο που αυτοί επικοινωνούν μεταξύ τους. Στα πρώτα στάδια ανάπτυξής τους, καταλάμβαναν πάρα πολύ μεγάλο χώρο και ήταν σε υψηλό βαθμό συγκεντρωμένοι, δούλευαν κατά κανόνα ανεξάρτητα και δεν είχαν οποιαδήποτε επικοινωνία με άλλα υπολογιστικά συστήματα.

Η ταχεία ανάπτυξη αυτής της τεχνολογίας, οδήγησε στο να μειωθεί χαρακτηριστικά ο χώρος που καταλάμβανε ένα υπολογιστικό σύστημα, με συνέπεια ο χώρος που χρησιμοποιούταν παλιότερα από έναν και μόνο υπολογιστή, να μετατραπεί σε χώρο που να μπορεί πλέον να φιλοξενήσει δεκάδες έως και εκατοντάδες ηλεκτρονικούς υπολογιστές ταυτόχρονα. Έτσι δημιουργήθηκε η ανάγκη για την υλοποίηση των δικτύων υπολογιστών, δηλαδή του φαινομένου κατά το οποίο δύο ή περισσότεροι διασυνδεδεμένοι υπολογιστές ανταλλάσσουν μεταξύ τους πληροφορίες. Τελικά η μεγάλη ανάπτυξη των δικτύων υπολογιστών αποτέλεσε σημαντικό κομμάτι της καθημερινότητας όλων μας, με κύριο εκφραστή το διαδίκτυο. Σήμερα το διαδίκτυο έχει δημιουργήσει παγκόσμια συνδεσιμότητα, ενώνοντας περισσότερους από 2 δισεκατομμύρια μεμονωμένους προσωπικούς υπολογιστές σ' όλο τον κόσμο αλλά και άλλου είδους συσκευές.

Η εξέλιξη αυτή έχει εισαγάγει νέους όρους στο προσκήνιο όπως το ηλεκτρονικό επιχειρείν γνωστό ως και e-business. Το ηλεκτρονικό επιχειρείν φαίνεται καθημερινά να κερδίζει έδαφος, στο χώρο των οικονομικών συναλλαγών. Οι παραδοσιακές εταιρείες διαπιστώνουν ότι με τη χρήση του internet μπορούν να πωλούν διάφορα προϊόντα, να συντονίζουν τους προμηθευτές τους, να οργανώνουν την παραγωγή τους και να κάνουν παραδόσεις στους πελάτες τους με μεγαλύτερη ευκολία απ' ότι παλαιότερα. Τα στατιστικά στοιχεία που εμφανίζονται κατά καιρούς παρουσιάζουν σαφείς ανοδικές τάσεις χρήσης του διαδικτύου ως μέσου αγοράς υπηρεσιών και καταναλωτικών αγαθών. Εξ' άλλου οι περισσότερο πετυχημένες επιχειρήσεις σήμερα είναι εκείνες που μπορούν να αποκτήσουν αλλά και να χρησιμοποιήσουν την πληροφορία πιο αποτελεσματικά από τις υπόλοιπες στον κλάδο τους.

Είναι προφανές ότι με την πάροδο του χρόνου το internet όπως και τα πιο μικρά δίκτυα θα χρησιμοποιούνται όλο και περισσότερο για την εξασφάλιση της παγκόσμιας συνδεσιμότητας, γεγονός που προσφέρει πάρα πολλά πλεονεκτήματα αλλά επιφυλάσσει και σημαντικούς κινδύνους οι οποίοι σχετίζονται ως επί τω πλείστον με την ασφάλεια των πληροφοριών που αυτά ανταλλάσσουν.

Πρέπει πάντα να έχουμε υπόψη, ότι η κάθε πληροφορία που αφορά κάποιο πρόσωπο ή οργανισμό, αποτελεί περιουσιακό στοιχείο και η κλοπή του, όπως και κάθε παράνομη εκμετάλλευσή του, παραβιάζει τους κανόνες προστασίας των προσωπικών δεδομένων και του δικαιώματος του ιδιωτικού βίου των πολιτών. Επομένως, είναι κάτι που οπωσδήποτε χρειάζεται επαρκή προστασία με ασφαλιστικές δικλείδες που να διασφαλίζουν υψηλό επίπεδο προστασίας.

Επομένως, η ασφάλεια των πληροφοριών καθίσταται βασική προτεραιότητα στην ανάπτυξη και λειτουργία κάθε υγιούς κοινωνίας έχοντας σαν απώτερο στόχο την προστασία του ίδιου του πολίτη. Η ανάγκη αυτή για προστασία της ιδιωτικής ζωής εξαιτίας της τεχνολογικής προόδου πρωτοεμφανίστηκε σχεδόν έναν αιώνα πριν [7] όταν κανείς ακόμα δεν είχε φανταστεί τις διαστάσεις που θα έπαιρνε η ανάπτυξη της τεχνολογίας της πληροφορικής. Στη συνέχεια, πρώτου παρουσιαστούν οι βασικές απαιτήσεις ασφάλειας σε ένα οποιοδήποτε πληροφοριακό σύστημα, πρέπει απαραιτήτως να γίνει μια αναφορά στην εννοιολογική σημασία κάποιων ορισμών που πρόκειται να χρησιμοποιηθούν στα επόμενα κεφάλαια, όπως και μια σύντομη αναφορά στα χαρακτηριστικά των προσωπικών δεδομένων στον χώρο του διαδικτύου.

## 2.2 Χρήσιμοι Ορισμοί

Όπως προαναφέρθηκε, προτού συνεχίσουμε στα επόμενα κεφάλαια, θα γίνει μία τυπική αναφορά σε κάποιους χρήσιμους ορισμούς όπως ακριβώς αναφέρονται στο Ν.2472/1997 [8]

α) <<Δεδομένα προσωπικού χαρακτήρα>>, κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

β) <<Ευαίσθητα προσωπικά δεδομένα>>, τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

γ) <<Υποκείμενο των δεδομένων>>, το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

δ) <<Επεξεργασία δεδομένων προσωπικού χαρακτήρα>>, κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση ή συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.

ε) <<Αρχείο δεδομένων προσωπικού χαρακτήρα>>, σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή μπορούν να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία τηρούνται είτε από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου, ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο.

στ) <<Διασύνδεση>>, μορφή επεξεργασίας που συνίσταται στη 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 επεξεργασίας για άλλο σκοπό.

ζ) <<Τρίτος>>, κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.

η) <<Αρχή>>, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

## 2.3 Προσωπικά δεδομένα και διαδίκτυο

Προσωπικά δεδομένα λοιπόν, θεωρούνται όλες εκείνες οι πληροφορίες που χαρακτηρίζουν ή προσδιορίζουν έναν άνθρωπο, όπως για παράδειγμα το όνομά του, η ηλικία του, η διεύθυνσή του, ο τόπος κατοικίας του, οι φωτογραφίες του και πολλά άλλα συναφούς περιεχομένου. Ένα φυσικό πρόσωπο διακινεί τέτοιου είδους πληροφορίες σε καθημερινή βάση στην ιδιωτική του ζωή. Ενδεικτικά, αναφέρω παρακάτω κάποιες συνήθεις περιπτώσεις χρήσης των προσωπικών μας δεδομένων στην καθημερινότητά μας όπως είναι για παράδειγμα, η εγγραφή μας σε κάποιο διαδικτυακό κατάστημα, η υποβολή μιας αίτησης μας σε κάποια δημόσια υπηρεσία, η αγορά κάποιου αεροπορικού εισιτηρίου, το άνοιγμα ενός τραπεζικού λογαριασμού ή η χρησιμοποίηση ιστοσελίδων κοινωνικής δικτύωσης όπως είναι το facebook, το οποίο έχει πλέον εισβάλλει στην προσωπική ζωή των περισσοτέρων νέων. Σε όλες τις παραπάνω περιπτώσεις βασική προϋπόθεση χρήσης των προσωπικών δεδομένων μας είναι η πρότερη εξασφάλιση της συγκατάθεσης μας. Αυτό σημαίνει δηλαδή ότι για να χρησιμοποιήσει κάποιος τα προσωπικά μας δεδομένα θα πρέπει να δηλώσουμε με σαφή τρόπο ότι συμφωνούμε σε κάτι τέτοιο αφού ενημερωθούμε πρώτα σχετικά με την ταυτότητα εκείνου που θέλει τα χρησιμοποιήσει, το λόγο που θέλει να τα χρησιμοποιήσει, ποια ακριβώς στοιχεία θα χρησιμοποιήσει και με ποιους θα τα μοιραστεί. Τα δεδομένα προσωπικού χαρακτήρα είναι δυνατόν να συγκεντρώνονται είτε άμεσα από κάποιο πρόσωπο είτε αυτόματα μέσω υπολογιστή σε κάποιες βάσεις δεδομένων. Σήμερα που ζούμε στην κοινωνία της πληροφορίας το πιο διαδεδομένο μέσο διάδοσης και ανταλλαγής της πληροφορίας είναι ο ηλεκτρονικός υπολογιστής που άλλοτε αποτελεί μέσο τέλεσης και άλλοτε στόχο μιας εγκληματικής δραστηριότητας. Ειδικότερα ο ηλεκτρονικός υπολογιστής μέσω του διαδικτύου επιτρέπει τη μετάδοση πληροφοριών μέσα σε δευτερόλεπτα και μάλιστα σε παγκόσμια κλίμακα.[9] Μέσω του διαδικτύου οδηγούμαστε ολοένα και περισσότερο προς τη μετατροπή των δεδομένων του φυσικού κόσμου σε ψηφιακή μορφή καθώς οποιαδήποτε υπηρεσία, φορέας ή οργανισμός τείνει να εξαφανίσει τον παραδοσιακό τρόπο καταχώρισης της πληροφορίας που ήταν ο χειρόγραφος, με πολύπλοκα πληροφοριακά συστήματα πολλές φορές διασυνδεδεμένα στο διαδίκτυο.

Η νέα αυτή κατάσταση πραγμάτων που δημιούργησε η ανάπτυξη και η κυριαρχία της επιστήμης της πληροφορικής οδήγησε στην εμφάνιση νέων μορφών εγκληματικότητας, οι οποίες ευνοούνται από το γεγονός ότι το νομικό καθεστώς που διέπει το διαδίκτυο είναι ακόμα ελλιπές. Αυτού του είδους η εγκληματικότητα δημιουργεί διάφορα προβλήματα από νομικής άποψης, καθώς δεν υπάρχει καθορισμένος τόπος τέλεσης εγκλήματος, δωσιδικία των δικαστηρίων ενώ πολλές φορές διεκδικούν εφαρμογή κανόνες δικαίου διαφορετικών έννομων τάξεων.[9] Βασικό χαρακτηριστικό αυτού του είδους εγκληματικότητας σε σχέση με άλλες μορφές εγκληματικότητας, είναι πρώτον η έλλειψη φυσικής επαφής του δράστη με το θύμα και δεύτερον η έλλειψη βίας. Για παράδειγμα όταν κάποιος υποκλέπτει προσωπικά δεδομένα από κάποιον υπολογιστή δεν χρειάζεται να εισβάλλει στην κατοικία του θύματος και να ασκήσει κάποιου είδους βία σ' αυτόν ή τον υπολογιστή του. Πολύ απλά μπορεί να εισέλθει στον ίδιο τον υπολογιστή σπάζοντας εξ' αποστάσεως τους κωδικούς πρόσβασης του, ή να τον καταστρέψει ολοσχερώς με την αποστολή ενός ιού, ενεργώντας υπό την άγνοια του θύματος που θα τον αποδεχτεί.[10] Άλλο ένα βασικό χαρακτηριστικό αυτής της εγκληματικότητας, είναι η διεθνής φύση της, εξαιτίας της διασύνδεσης των ηλεκτρονικών υπολογιστών σε παγκόσμιο επίπεδο. Η διεθνικότητα αυτή, γίνεται εύκολα αντιληπτή, αν αναλογιστεί κανείς ότι τ' αποτελέσματά της διάπραξης ενός διαδικτυακού εγκλήματος γίνονται ταυτόχρονα αισθητά σε διάφορους τόπους κάνοντας τον εντοπισμό του δράστη μία πάρα πολύ δύσκολη υπόθεση. Το γεγονός αυτό, όπως γίνεται αντιληπτό επιβάλλει την ανάγκη για διεθνή συνεργασία. Γι' αυτό το λόγο το Συμβούλιο της Ευρώπης έχοντας σα στόχο την προστασία της διεθνούς κοινότητας από τα διαδικτυακά εγκλήματα, στις 23 Νοεμβρίου του 2001 συνέταξε τη σύμβαση για την καταπολέμηση του Κυβερνοεγκλήματος[8] στηριζόμενο σε 3 κύριες κατευθύνσεις.

Πρώτον στη θεμελίωση κοινών ουσιαστικών και δικονομικών ποινικών αρχών, δεύτερον στη θέσπιση κατάλληλης νομοθεσίας από τα κράτη-μέλη και τρίτον στην επίτευξη Διεθνούς

[8] Τη σύμβαση υπέγραψαν 26 χώρες κράτη-μέλη του Συμβουλίου της Ευρώπης μεταξύ των οποίων και η Ελλάδα αλλά και 4 χώρες παρατηρητές (Καναδάς, Ιαπωνία, Νότιος Αφρική και Ηνωμένες Πολιτείες της Αμερικής)

δικαστικής συνεργασίας.[11] Περισσότερα όμως για τη σύμβαση αυτή θα δούμε στο 5$^{ο}$ κεφάλαιο όπου γίνεται εκτενέστερη αναφορά.

Στη συνέχεια γίνεται μια παρουσίαση των βασικών απαιτήσεων για την ασφάλεια ενός συστήματος, ώστε να εξασφαλίζεται, όσο αυτό είναι δυνατόν, η ιδιωτικότητα αλλά και η ασφάλεια.

## 2.4 Βασικές απαιτήσεις για την ασφάλεια ενός συστήματος

### 2.4.1 Ορισμός Πληροφοριακού συστήματος (Π.Σ) και Ασφάλεια

Πληροφοριακό σύστημα είναι ένα σύνολο αλληλεπιδρώντων στοιχείων το οποίο δέχεται δεδομένα, τα επεξεργάζεται και τελικά τα διανέμει υπό τη μορφή πληροφοριών στους διάφορους χρήστες που είναι συνδεδεμένοι με αυτό μέσω υπολογιστή ή άλλων μέσων. Τα αλληλεπιδρώντα αυτά στοιχεία είναι 5 στο σύνολό τους και είναι τα παρακάτω: ο άνθρωπος, το λογισμικό, το υλικό, οι διαδικασίες και τα δεδομένα. [12]

Εξαιτίας του πολύ σημαντικού ρόλου που παίζει ένα Π.Σ σε μια επιχείρηση είναι επόμενο να έχει την ανάγκη ασφάλειας και προστασίας, χωρίς βέβαια η ασφάλεια αυτή να στέκεται εμπόδιο στη ροή των πληροφοριών. Ως ασφάλεια Π.Σ ορίζεται [16] " Το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.". Σύμφωνα με αυτόν τον ορισμό νοείται η προστασία και των 5 αλληλεπιδρώντων στοιχείων που προαναφέρθηκαν αλλά και η προστασία ολόκληρου του Π.Σ από κάθε σκόπιμη ή τυχαία απειλή.

Σε αυτό το σημείο γίνεται φανερό πως η ασφάλεια Π.Σ είναι μία ευρύτερη έννοια από αυτή της ασφάλειας πληροφοριών, αφού η πληροφορία εμπεριέχεται μέσα στα στοιχεία ενός Π.Σ, χωρίς βέβαια αυτό να σημαίνει η ασφάλεια πληροφοριών μπορεί να αγνοήσει το Π.Σ αφού στα πλαίσια αυτού παράγεται και χρησιμοποιείται η πληροφορία.

### 2.4.2 Οι ιδιότητες της ασφάλειας

Η πληροφορία όπως είπαμε και παραπάνω αποτελεί πολύτιμο περιουσιακό στοιχείο και μάλιστα πάρα πολύ μεγάλης αξίας ανάλογα με τον τόπο και το χρόνο που γίνεται γνωστή, είτε αυτή αφορά ένα φυσικό πρόσωπο, είτε ένα δημόσιο οργανισμό είτε μια επιχείρηση. Αυτό που τη διαφοροποιεί σε σχέση με άλλα συμβατικά αγαθά που έχουν υλική υπόσταση είναι ότι παρ' ότι μπορεί να κλαπεί ή να παραποιηθεί, είναι δυνατόν να μην αφαιρεθεί από τον ιδιοκτήτη της αλλά ούτε και να διαπιστωθεί η παραποίησή της.[12] Εξαιτίας της χρησιμοποίησης ολοένα και πιο εξελιγμένων τεχνολογιών όπως είναι οι τεράστιες βάσεις δεδομένων και τα σύγχρονα δίκτυα, δημιουργείται συνεχώς μεγαλύτερη ανάγκη για διασφάλιση των πληροφοριών ώστε να μην διαταράσσεται η εύρυθμη λειτουργία μιας επιχείρησης ή ενός οργανισμού. Η ασφάλεια ενός δικτύου υπολογιστών σχετίζεται άμεσα με την ασφάλεια των πληροφοριών αφού το κύριο μέλημα της είναι να προστατέψει την πληροφορία που διακινείται ανάμεσα στους διασυνδεδεμένους χρήστες. Η ασφάλεια των πληροφοριών έχει να κάνει, με την προστασία της πληροφορίας, με την ολότητά της και με τις σχετικές με την ασφάλεια ιδιότητές της. Ως τέτοιες ιδιότητες θεωρούνται η ακεραιότητα (integrity), η εμπιστευτικότητα (confidentiality), η διαθεσιμότητα (availability) και η εγκυρότητα (validity) .[13]

Η **ακεραιότητα** αναφέρεται στη διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας όπως επίσης και στην αξιοπιστία των μεθόδων επεξεργασίας αυτής. Δηλαδή κάθε μη εξουσιοδοτημένη τροποποίηση της πληροφορίας θα πρέπει να αποτρέπεται, ενώ κάθε μετατροπή του περιεχομένου της θα πρέπει να γίνεται ελεγχόμενα και έπειτα από εξουσιοδότηση.

Η **εμπιστευτικότητα** αφορά την ασφάλιση της προσπέλασης της πληροφορίας μόνο από εξουσιοδοτημένους χρήστες. Αυτό σημαίνει ότι θα πρέπει να υπάρχει πρόληψη έτσι ώστε τα

δεδομένα που διακινούνται μεταξύ διασυνδεδεμένων υπολογιστών να είναι προσβάσιμα μονάχα από εξουσιοδοτημένους χρήστες.

Η **διαθεσιμότητα** έχει να κάνει με τη διασφάλιση διάθεσης, της πληροφορίας σε κάθε εξουσιοδοτημένο χρήστη όποτε αυτός το απαιτήσει. Αυτό πιο αναλυτικά σημαίνει ότι, οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων θα πρέπει να μπορούν να έχουν πρόσβαση στα δεδομένα και τις υπηρεσίες ενός δικτύου ανεξάρτητα από τις όποιες διαταραχές φυσικές ή τεχνητές προκύψουν. Σε ότι έχει να κάνει με την ασφάλεια, μας ενδιαφέρουν οι επιθέσεις άρνησης παροχής υπηρεσιών, οι οποίες έχουν σκοπό να παρεμποδίσουν την εξουσιοδοτημένη πρόσβαση στις πληροφορίες και στους πόρους του συστήματος ή να προκαλέσουν εσκεμμένη καθυστέρηση των λειτουργιών του.

Η **εγκυρότητα** έχει να κάνει με το κατά πόσο είναι πραγματική και επίκαιρη μία πληροφορία.

Πέρα απ' αυτές τις τέσσερις ιδιότητες, άλλοι ερευνητές υποστηρίζουν πως για την ασφάλεια των πληροφοριών απαιτείται ο ορισμός και άλλων ιδιοτήτων όπως η αυθεντικότητα (authenticity) που αφορά στην πιστοποίηση της προέλευσης του ιδιοκτήτη της πληροφορίας, η μοναδικότητα (uniqueness) που αφορά στην απαγόρευση επεξεργασίας και αναπαραγωγής της πληροφορίας χωρίς εξουσιοδότηση και τέλος η μη αποποίηση ευθύνης (non-repudiation) που σημαίνει ότι αυτοί που ανταλλάσσουν πληροφορίες μεταξύ τους δεν μπορούν να αρνηθούν την επεξεργασία, αποστολή ή λήψη μιας πληροφορίας λόγω του ότι υπάρχουν αποδεικτικά στοιχεία που επιβεβαιώνουν μία τέτοια ενέργεια. [14]

## 2.5 Τα προσωπικά δεδομένα των καταναλωτών απειλούνται στο Internet

Η Παγκόσμια Ομοσπονδία Καταναλωτών που αποτελείται από 263 Καταναλωτικούς Οργανισμούς, διεξήγαγε διεθνή έρευνα με θέμα την ασφάλεια των Ευρωπαϊκών και Αμερικανικών ιστοσελίδων και αποκάλυψε πρώτον ότι οι παραπάνω αποτυγχάνουν να εφαρμόσουν τα κριτήρια της προστασίας των προσωπικών δεδομένων και δεύτερον ότι οι καταναλωτές αγνοούν τις πιο βασικές αρχές της σωστής χρήσης του διαδικτύου. Η έρευνα αφορούσε 751 ιστοσελίδες που πωλούν προϊόντα και παρέχουν υπηρεσίες.

Η έρευνα της Διεθνούς Ομοσπονδίας Καταναλωτών αποκαλύπτει πως τα μέτρα που παίρνουν οι διάφορες Κυβερνήσεις για να προστατέψουν τα προσωπικά δεδομένα των καταναλωτών δεν είναι επαρκή και πιο συγκεκριμένα αναφέρει ότι: [17]

1) Πάνω από τα δύο τρίτα των ιστοσελίδων συλλέγουν κάποιες προσωπικές πληροφορίες και σχεδόν όλες αυτές οι ιστοσελίδες ζητούν τέτοιες λεπτομέρειες, ώστε να καθίσταται εύκολη η αναγνώριση και η επικοινωνία με τον επισκέπτη τους.

2) Η συντριπτική πλειοψηφία των ιστοσελίδων κατά την εγγραφή του χρήστη στην λίστα των διαφημιστικών email τους, μοιράζει τα στοιχεία του σε λίστες άλλων εταιριών με τις οποίες σχετίζεται, χωρίς να δίνει το περιθώριο επιλογής στον Καταναλωτή.

3) Παρά το γεγονός ότι υπάρχει αυστηρή Ευρωπαϊκή Νομοθεσία, που διέπει την προστασία των προσωπικών δεδομένων των χρηστών, η πλειοψηφία των ευρωπαϊκών ιστοσελίδων δεν ενημερώνει τους Καταναλωτές για την ακριβή χρήση των προσωπικών δεδομένων τους, ούτε ζητά την άδειά τους για το μοίρασμα των στοιχείων τους σε άλλες εταιρίες.

4) Μόνο το 10% των ιστοσελίδων, οι οποίες στοχεύουν στην πώληση προϊόντων σε παιδιά- καταναλωτές, ζητούν από αυτά να πάρουν την συγκατάθεση των γονέων τους, πριν δώσουν τα προσωπικά τους στοιχεία, ή έστω να ενημερώσουν τους γονείς τους μετά.

Συμπερασματικά θα αναφέρω τα λόγια που είπε η Κα Anna Fielder, διευθύντρια του γραφείου για τις αναπτυγμένες και τις μεταβατικές οικονομίες της Διεθνούς των Καταναλωτών, που είπε πως "παρ' ότι η προστασία των προσωπικών δεδομένων είναι αναγνωρισμένο ως βασικό ανθρώπινο δικαίωμα, πάρα πολλές εταιρίες συλλέγουν όχι απαραίτητες και πολύ προσωπικές πληροφορίες για τους πελάτες τους, με αποτέλεσμα οι καταναλωτές να μην έχουν τον έλεγχο των προσωπικών τους δεδομένων".[17] Πολύ σωστά έχει επισημανθεί λοιπόν πως

“από τη στιγμή που το άτομο αποφασίζει την αυτοέκθεσή του στην αγορά του Ίντερνετ, συναποφασίζει και τη διάθεση των εισφερομένων στο διαδίκτυο στοιχείων της προσωπικότητάς του σε κοινή χρήση” [18]

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

# 3 Ασφάλεια στα Δίκτυα Υπολογιστών

## 3.1 Γενικά

Όπως είναι ήδη φανερό οι διαφόρων ειδών επιθέσεις στα δίκτυα υπολογιστών με στόχο τα προσωπικά δεδομένα των καταναλωτών, παρουσιάζουν διαρκώς αυξητικές τάσεις, ως εκ τούτου η υιοθέτηση μιας ολοκληρωμένης πολιτικής ασφαλείας είναι ζωτικής σημασίας. Παρ' ότι τα μέσα και τα εργαλεία αντιμετώπισης των διαφόρων απειλών βελτιώνονται διαρκώς, παραδόξως αυξάνονται και οι επιτυχημένες επιθέσεις. Η ασφάλεια έρχεται να προστεθεί στις άλλες δύο απαραίτητες και βασικές προϋποθέσεις για τη σωστή λειτουργία μιας επιχείρησης ή δημόσιου οργανισμού που είναι η ποιότητα και η απόδοση. Η έννοια της ασφάλειας ενός δικτύου υπολογιστών έχει να κάνει με το κατά πόσο είναι ικανή μια επιχείρηση ή ένας οργανισμός να αποτρέψει μία ενδεχόμενη επίθεση που θα αποσκοπεί στην παράνομη χρήση των πόρων του ή την καταστροφή - παραποίηση των πληροφοριών που κατέχει. Για να μπορέσει να αντιμετωπισθεί μια τέτοια απειλή θα πρέπει να απαντηθούν ορισμένα ερωτήματα βήμα προς βήμα. Αρχικά πρέπει να διευκρινιστεί τι ακριβώς πρέπει να προστατευτεί, στη συνέχεια να εντοπισθούν οι κύριοι υπαίτιοι κινδύνων ασφαλείας, έπειτα να βρεθούν οι πιθανοί τρόποι παραβίασης της ασφάλειας του διαδικτύου και τέλος να καθοριστούν τα μέτρα και οι βασικές ενέργειες αντιμετώπισης των κινδύνων ασφαλείας.

Σε αυτό το κεφάλαιο, θα γίνει μια σύντομη παρουσίαση των χαρακτηριστικών που πρέπει να πληροί μία πολιτική ασφαλείας, όπως επίσης θα αναλυθούν και οι βασικές ενέργειες αντιμετώπισης των κινδύνων ασφαλείας. Σε αυτό το πλαίσιο, παρουσιάζονται καταρχήν οι σημαντικότεροι τομείς που απειλούνται, αλλά και οι βασικότεροι υπαίτιοι των παραβιάσεων ασφαλείας. Επίσης, γίνεται μια αναφορά σε όλους τους πιθανούς τρόπους παραβίασης της ασφάλειας στο διαδίκτυο που θέτουν σε κίνδυνο την ασφάλεια των δεδομένων του συστήματος.

## 3.2 Πολιτική Ασφαλείας Δικτύου (Network Security Policy)

Η πολιτική ασφαλείας κάποιου δικτύου θεσπίζει κάποιες βασικές οδηγίες που έχουν σαν στόχο τη διαφύλαξη των χρηστών του, του περιεχομένου του αλλά και γενικότερα ολόκληρου του δικτύου από κάθε είδους ζημία. Πιο συγκεκριμένα μεταξύ άλλων περιγράφει τα είδη των προσωπικών πληροφοριών που συλλέγονται, τον τρόπο με τον οποίο θα χρησιμοποιηθούν αλλά και το αν θα μοιραστούν ή όχι σε κάποιον τρίτο και για πόσο καιρό θα διατηρηθούν. Στην εκάστοτε πολιτική ασφαλείας που θα ακολουθείται, θα πρέπει να συνυπολογίζεται το κόστος των μέτρων ασφαλείας που θα λαμβάνονται, σε συνάρτηση με τα προβλήματα που θα προκαλούνται σε κάποιο σύστημα εξαιτίας κάποιου κενού ασφαλείας. Αυτό σημαίνει ότι θα πρέπει να υπάρχει μια εξισορρόπηση ανάμεσα στους δύο αυτούς παράγοντες, ώστε να μην παρεμποδίζεται η ευελιξία και η λειτουργικότητα του συστήματος αλλά και να είναι συγχρόνως και ασφαλές.[19] Για να έχει αξία μία πολιτική ασφαλείας θα πρέπει να πληροί κάποια βασικά χαρακτηριστικά όπως το να είναι πρακτικά εφαρμόσιμη από αυτόν που τη διαχειρίζεται, να είναι υλοποιήσιμη και τέλος να είναι σε θέση να καθορίσει τα όρια ευθύνης όλων όσων εμπλέκονται με αυτήν. Ο υπεύθυνος για τη σχεδίαση και ανάπτυξη μιας πολιτικής ασφαλείας κάποιου δικτύου θα πρέπει να λάβει υπόψη του κάποια πράγματα πριν προβεί στην υλοποίησή της.[20]

1) Να γνωρίζει σε γενικές γραμμές το ποιος και για ποιο λόγο θα μπορούσε να εξαπατήσει τα μέτρα ασφαλείας.

2) Να γνωρίζει πολύ καλά τα κενά ασφαλείας που θα έχει το λογισμικό πάνω στο οποίο θα στηρίζεται, όπως επίσης και τα αδύναμα σημεία του συστήματος που θα μπορούσαν κάλλιστα να αποτελέσουν σημεία εισόδου ενός κακόβουλου εισβολέα.

3) Να έχει προβλέψει δικλείδες ασφαλείας ώστε αν κάποιος εισχωρήσει σε κάποιο τμήμα του συστήματος, να μην έχει τη δυνατότητα να προχωρήσει παραπέρα.

4) Να έχει καθορίσει σαφώς τα δικαιώματα πρόσβασης κάθε χρήστη με τη χρήση διαφορετικών κωδικών λέξεων (passwords).

5) Να έχει προβλέψει συγκεκριμένο χρόνο και τρόπο συντήρησης του συστήματος.

6) Να παρέχει πληροφορίες στου χρήστες ή το προσωπικό για κάθε είδους παραβίαση και τέλος

7) Να φροντίσει η πολιτική ασφαλείας να συμβαδίζει με την εκάστοτε εθνική νομοθεσία, τους κανονισμούς και τις διεθνείς οδηγίες.

## 3.3 Βασικότεροι τομείς που επηρεάζονται από κενά ασφαλείας και οι αντίστοιχες απειλές τους

Ως απειλή ορίζεται «μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων ασφάλειας ενός πληροφοριακού συστήματος»[21] ή αλλιώς οποιαδήποτε κακόβουλη πράξη εκούσια ή ακούσια η οποία μπορεί να βλάψει κάποια λειτουργία ενός υπολογιστικού συστήματος. Μία ακούσια απειλή μπορεί να είναι ένα προγραμματιστικό ή σχεδιαστικό λάθος το οποίο είναι ικανό να προκαλέσει κενά ασφαλείας. Μερικές λειτουργίες που αποτελούν τους μεγαλύτερους αποδέκτες των κενών ασφαλείας και σχετίζονται με την παραβίαση των προσωπικών δεδομένων στο Διαδίκτυο μπορεί να είναι:

Το e-banking, το οποίο δίνει τη δυνατότητα στον κάθε χρήστη να μπορεί να διαχειρίζεται τους προσωπικούς του λογαριασμούς σαν να βρισκόταν στην τράπεζα. Η όλη λειτουργία υφίσταται την απειλή του να μεσολαβήσει κάποιος τρίτος και να υποκλέψει ευαίσθητα προσωπικά δεδομένα όπως είναι για παράδειγμα τα στοιχεία μιας πιστωτικής κάρτας.

Οι εμπορικές συναλλαγές, οι οποίες για να πραγματοποιηθούν θα πρέπει ο χρήστης να γνωστοποιήσει πρώτα κάποια από τα προσωπικά ή ευαίσθητα δεδομένα του στο διαδίκτυο, χωρίς να γνωρίζει αν αυτό που κάνει είναι ασφαλές ή όχι. Η απειλή σε αυτή την περίπτωση είναι ακριβώς ίδια με την προηγούμενη περίπτωση.

Η συγκέντρωση προσωπικών πληροφοριών σε μεγάλες βάσεις δεδομένων που είναι διασυνδεδεμένες στο Διαδίκτυο (π.χ εφορία). Η απειλή έχει να κάνει και με την κλοπή προσωπικών δεδομένων αλλά και με την προσβολή της εικόνας και της φήμης του οργανισμού ή της εταιρίας που θα προσβληθεί.

Τα κοινωνικά δίκτυα (π.χ facebook, twitter) τα οποία αποθηκεύουν τεράστιο όγκο προσωπικών πληροφοριών ελλοχεύουν τον κίνδυνο κλοπής των πληροφοριών αυτών με στόχο το ηλεκτρονικό φακέλωμα, δηλαδή τη δημιουργία προσωπικού αναλυτικού προφίλ, το οποίο μπορεί να χρησιμοποιηθεί από διάφορους δημόσιους ή ιδιωτικούς οργανισμούς προς όφελος τους.

Προγράμματα ανταλλαγής αρχείων, τα οποία λειτουργούν κάνοντας κοινόχρηστο ένα κομμάτι του σκληρού δίσκου κάποιου χρήστη, με αποτέλεσμα να μπορούν όλοι οι υπόλοιποι χρήστες του συγκεκριμένου προγράμματος να έχουν απευθείας πρόσβαση στον υπολογιστή πηγή και να μπορούν να κάνουν αντίγραφα αρχείων στο δικό τους υπολογιστή.

## 3.4 Εχθροί που αποτελούν απειλή για την ασφάλεια

Για να επιτευχθεί μία αποτελεσματική άμυνα έναντι οποιασδήποτε απειλής, θα πρέπει πρώτα να γίνει αναγνώριση και μελέτη του εχθρού σε ότι αφορά το υπόβαθρό του και τους σκοπούς του, έτσι ώστε να μπορέσει να μας δώσει χρήσιμες πληροφορίες για το είδος και το μέγεθος της απειλής που μπορεί να αποτελέσει. Έτσι οι εχθροί του διαδικτύου μπορούν να κατηγοριοποιηθούν με αύξουσα σειρά επικινδυνότητας ως εξής:[22]

- Ειδικοί Ασφαλείας
- Έφηβοι Εισβολείς
- Υποαπασχολούμενοι ενήλικες
- Εισβολείς λόγω ιδεολογίας
- Εγκληματίες (Criminals)
- Ανταγωνιστές (Competitors)

- Εσωτερικοί εχθροί

### 3.4.1 Ειδικοί Ασφαλείας

Οι ειδικοί ασφαλείας παρ' ότι έχουν τις απαραίτητες γνώσεις ώστε ν' αποτελέσουν σοβαρή απειλή για την ασφάλεια του διαδικτύου, παρ' όλα αυτά βρίσκονται στην πιο χαμηλή θέση όσον αφορά την κλίμακα επικινδυνότητας. Συνήθως οι λόγοι που τους αποτρέπουν από τέτοιου είδους ενέργειες είναι κυρίως ηθικοί αλλά και οικονομικοί. Ξέρουν ότι αν εργαστούν αντίστροφα, για τις εταιρίες δηλαδή που παρέχουν προστασία από κακόβουλες εισβολές, θα εξοικονομήσουν περισσότερα χρήματα απ' ότι αν προκαλούσαν ζημιές στο διαδίκτυο. Είναι συνήθως αυτοί που εντοπίζουν νέες μεθόδους εισβολής αλλά χρησιμοποιούν τη γνώση αυτή για να γράψουν και να θωρακίσουν το λογισμικό ακόμα περισσότερο.

### 3.4.2 Έφηβοι εισβολείς

Είναι αυτοί που βλέπουν την εισβολή σε ένα σύστημα ασφαλείας ως παιχνίδι και καλούν τους φίλους τους για να τους το δείξουν και να κάνουν πλάκα. Είναι συνήθως μαθητές ή φοιτητές και χρησιμοποιούν είτε τους δικούς τους υπολογιστές είτε τα δυνατά υπολογιστικά συστήματα της σχολής ή του πανεπιστημίου στο οποίο ανήκουν. Οι ζημιές που προκαλούν δεν είναι σημαντικές αλλά σίγουρα καταφέρνουν να σπαταλήσουν το χρόνο του προσωπικού ενός συστήματος μέχρι να καταλάβουν ποια είναι η ζημιά και να τη διορθώσουν. Είναι αυτοί που δημιουργούν τις βάσεις για να συνεχίσουν περαιτέρω οι υποαπασχολούμενοι ενήλικες.

### 3.4.3 Υποαπασχολούμενοι Ενήλικες

Αποτελούν τη συνέχεια των έφηβων εισβολέων που είτε για κάποιο λόγο δεν τελείωσαν το πανεπιστήμιο είτε δε θέλησαν να βρουν μία εργασία πλήρους απασχόλησης εξαιτίας της πολύωρης απασχόλησης τους με τον υπολογιστή. Συνήθως δεν έχουν κακή πρόθεση και ότι κάνουν το κάνουν μόνο και μόνο για να γίνουν γνωστοί στο χώρο των εισβολέων. Το βασικό τους κίνητρο είναι η επίδειξη και ο εντυπωσιασμός των άλλων.

### 3.4.4 Εισβολείς λόγω ιδεολογίας

Τα κίνητρά αυτού του είδους εισβολέων είναι συνήθως πολιτικά, περιβαλλοντικά ή εθνικά. Προσπαθούν η επίθεσή τους να γίνει ευρέως γνωστή είτε καταστρέφοντας και αλλοιώνοντας τις ιστοσελίδες των ιδεολογικών τους αντιπάλων είτε κάνοντας επιθέσεις άρνησης παροχής υπηρεσίας εναντίον τους. Πρόσφατα παράδειγμα τέτοιων εισβολέων έχουμε αρκετά. Χαρακτηριστική περίπτωση [23] αποτελεί η επίθεση στις ιστοσελίδες δύο μελών της κυβέρνησης που έκαναν άγνωστοι χάκερς, οι οποίοι κατάφεραν στη μεν πρώτη, να μπουν στην ιστοσελίδα της υφυπουργού Εξωτερικών Κ. Μαριλίζας Ξενογιαννακοπούλου και να παραποιήσουν την ομιλία της για τα ελληνοτουρκικά προσθέτοντας κάποιους υβριστικούς χαρακτηρισμούς για τον τούρκικο λαό και στη δε δεύτερη να μπουν στην ιστοσελίδα του υπουργού Δικαιοσύνης κ. Χάρη Καστανίδη και να αντικαταστήσουν την ελληνική σημαία με μία των Σκοπίων, η οποία κυμάτιζε για δύο ώρες. Άλλη μία παρόμοια επίθεση [24] δέχτηκαν πάνω από 100 κυπριακές ιστοσελίδες εταιριών, από Τούρκους χάκερς ως αντίποινα των επεισοδίων που σημειώθηκαν στον αγώνα μπάσκετ μεταξύ ΑΠΟΕΛ και της τουρκικής Πινάρ Καρσίκαγια αναρτώντας το έμβλημα της καλαθοσφαιρικής τους ομάδας καθώς και το μισοφέγγαρο πάνω στο έδαφος της Κυπριακής Δημοκρατίας.

### 3.4.5 Εγκληματίες (Criminals)

Το διαδίκτυο λόγω του εύρους του αλλά και της ανωνυμίας που παρέχει ήταν αδύνατο να μην αποτελέσει πόλο έλξης εγκληματιών. Πρόθεσή τους είναι καθαρά η υπεξαίρεση χρημάτων ή πληροφοριών που έχουν ως απώτερο σκοπό το χρήμα, μέσω κλοπής αριθμών πιστωτικών καρτών ή μέσω εισβολής στο μηχανισμό τραπεζικών συναλλαγών.

### 3.4.6 Ανταγωνιστές (Competitors)

Σε μια έντονη ανταγωνιστική κοινωνία όπως αυτή που ζούμε σήμερα, είναι πολύ πιθανό δύο ανταγωνίστριες εταιρίες να προβούν σε κατασκοπικές μεθόδους που θα έχουν σαν στόχο την υποκλοπή των διαφόρων επιχειρηματικών πλάνων ή την καταστροφή κάποιων πολύτιμων αρχείων ή βάσεων δεδομένων. Επιπλέον ο στόχος τους δεν είναι να κλέψουν άμεσα χρήματα αλλά να καταφέρουν να δημιουργήσουν κενά ασφαλείας στο σύστημα του αντιπάλου είτε για να θίξουν την αξιοπιστία του είτε για να έχουν ένα παράθυρο πρόσβασης στο σύστημά του, συνέχεια ανοιχτό.

### 3.4.7 Εσωτερικοί εχθροί

Στην κορυφή της κλίμακας επικινδυνότητας βρίσκονται οι εσωτερικοί εχθροί διότι αυτοί είναι που μπορούν να προκαλέσουν τα μεγαλύτερα κενά ασφαλείας σε κάποιο σύστημα. Ένας δυσαρεστημένος υπάλληλος μπορεί πολύ εύκολα να αποκτήσει πρόσβαση στις ευαίσθητες πληροφορίες ενός συστήματος και να τις χρησιμοποιήσει εναντίον του για να του κάνει κακό. Γι' αυτό το λόγο πέρα από τους τεχνικούς τρόπους διαφύλαξης της ασφάλειας (συσκευές προστασίας, μέσα καταγραφής των δραστηριοτήτων των χρηστών) θα πρέπει να υπάρχουν και καλές υπαλληλικές σχέσεις ώστε να μπορούν να αποφευχθούν απρόσμενες καταστάσεις.

## 3.5 Είδη Επιθέσεων δικτύων

Οι επιθέσεις που μπορεί να δεχτεί ένα δίκτυο είναι διαφόρων μορφών και κάθε μία εξ' αυτών έχει σα στόχο κάποια συγκεκριμένη υπηρεσία του δικτύου. Στη συνέχεια παραθέτονται ορισμένα βασικά χαρακτηριστικά των πιο διαδεδομένων τύπων επιθέσεων.[25][26]

- Επίθεση Άρνησης Παροχής Υπηρεσιών (Denial of Service)
- Διαμοιρασμένη Άρνηση Παροχής Υπηρεσιών (Distributed DoS)
- Πλαστογραφημένο E-mail (E-mail Spoofing)
- Επίθεση ωμής βίας (Brute – force attack)
- Επίθεση Επανάληψης (Replay Attack)
- Υπερχείλιση Καταχωρητή (Buffer Overflow)
- Επίθεση Ενδιάμεσου (Man in the middle attack)
- Κακόβουλος κώδικας (Malicious Code)

### 3.5.1 Επίθεση Άρνησης Υπηρεσιών (Denial of Service DoS)

Είναι μία από τις πιο γνωστές επιθέσεις που πραγματοποιείται σε χαμηλό επίπεδο. Σε αντίθεση με τα υπόλοιπα είδη επιθέσεων, ο επιτιθέμενος δεν προσπαθεί να εκμεταλλευτεί τα σχεδιαστικά λάθη και τις παραλείψεις των προγραμμάτων ή των πρωτοκόλλων για να διεισδύσει σε ένα δίκτυο αλλά αντιθέτως χρησιμοποιεί κάθε διαθέσιμο μέσο σε υπερβολικό βαθμό έτσι ώστε κανένας άλλος χρήστης να μην μπορεί να το χρησιμοποιήσει. Ο στόχος αυτού του είδους επίθεσης όπως φαίνεται και από το όνομα της, είναι να υπερφορτώσει το διακομιστή με σκοπό να τον θέσει εκτός λειτουργίας ή να μειώσει το μέγιστο δυνατό αριθμό πελατών που μπορεί να εξυπηρετήσει για ένα χρονικό διάστημα δεσμεύοντας όλους τους διαθέσιμους πόρους ή εξαντλώντας το διαθέσιμο εύρος ζώνης του δικτύου, εξαιτίας του τεράστιου όγκου πλαστών αιτήσεων που θα δεχτεί από τον επιτιθέμενο.

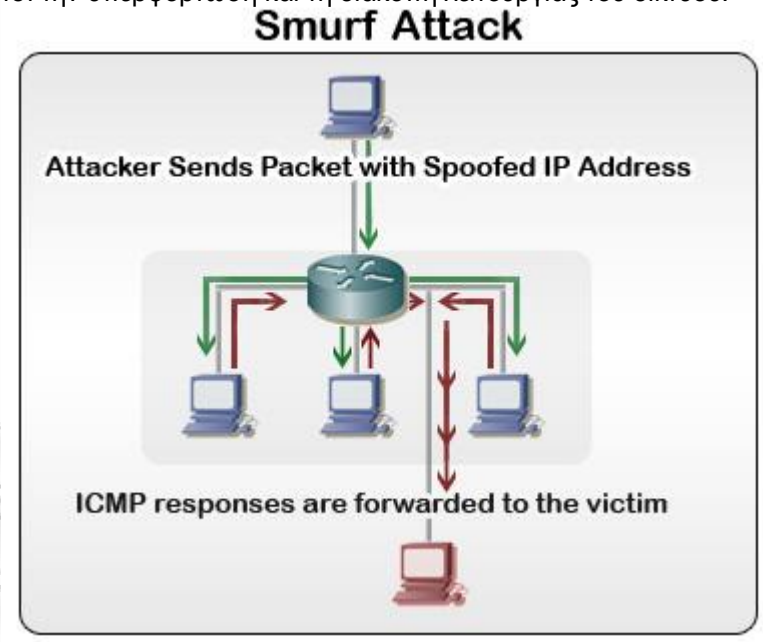
Σε αυτήν την κατηγορία επιθέσεων, οι 4 πιο γνωστές παραλλαγές είναι οι εξής: Ping of death, Smurf attack, SYN Flood attack και Teardrop attack.

Το ping του θανάτου (POD - Ping Of Death) ήταν η παλαιότερη (μέσα δεκαετίας 90) αλλά και πιο διαδεδομένη μορφή επίθεσης η οποία πραγματοποιούταν με την αποστολή

υπερβολικών κακοσχηματισμένων μηνυμάτων λαθών και ελέγχου (ping[9]). Ένα πακέτο ping είναι κανονικά μεγέθους 64 bytes ή 84 bytes εάν του προστεθεί και η κεφαλίδα που προσθέτει το πρωτόκολλο IP. Πακέτα λοιπόν που ήταν μεγαλύτερα από 64Kb ήταν ικανά να "κρεμάσουν" έναν υπολογιστή λόγω του ότι πολλοί ηλεκτρονικοί υπολογιστές δεν ήταν σε θέση να τα διαχειριστούν.


**Εικόνα 3.5.1.1 Ping of Death**
**Πηγή : http://www.seminartopicsonline.com/2010_07_01_archive.html**

Η smurf attack είναι μια μορφή επίθεσης που έχει σα στόχο το διακομιστή ενός δικτύου και πραγματοποιείται με την αποστολή ενός μεγάλου αριθμού άχρηστων πακέτων δεδομένων. Για να επιτευχθεί αυτή η επίθεση χρειάζεται ο αποστολέας, δηλαδή αυτός που κάνει την επίθεση, ο ενδιάμεσος, δηλαδή κάποιος υπολογιστής πελάτης και ο στόχος που στην προκειμένη περίπτωση είναι ο διακομιστής ενός δικτύου. Η λειτουργία αυτής της επίθεσης είναι απλή και έχει ως εξής. Ο επιτιθέμενος στέλνει μία εντολή ping στον ενδιάμεσο έχοντας βάλει όμως σαν διεύθυνση αποστολέα τη διεύθυνση του στόχου, έτσι όταν ο ενδιάμεσος χρειαστεί να απαντήσει στα ping του αποστολέα, οι απαντήσεις θα αποσταλούν όλες στο στόχο καθώς θα νομίζει πως αυτός είναι ο αποστολέας. Έτσι λοιπόν από τη στιγμή που όλα τα μηχανήματα ενός δικτύου έχουν την ίδια διεύθυνση εκπομπής και ο επιτιθέμενος στέλνει εκατοντάδες ή ακόμα και χιλιάδες ping δημιουργείται μία καταιγίδα άχρηστων πακέτων με στόχο το διακομιστή που προκαλούν έτσι την υπερφόρτωση και τη διακοπή λειτουργίας του δικτύου.

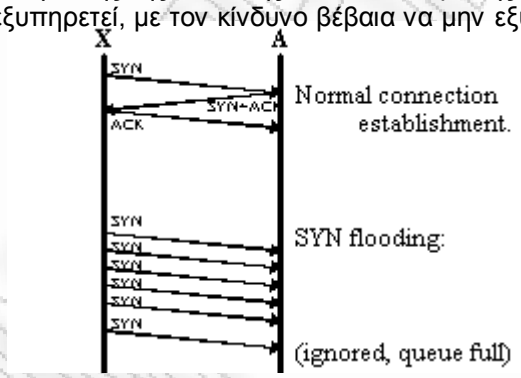



**Εικόνα 3.5.1.2 Smurf Attack**
**Πηγή: http://learn-networking.com/network-security/securing-cisco-routers-with-no-ip-directed-broadcast**

[9] Ping είναι η εντολή που χρησιμοποιείται για να καταλάβει ένας υπολογιστής αν κάποιος άλλος βρίσκεται on-line. Είναι ένα πακέτο μερικών bytes που αποστέλλεται στον άλλο υπολογιστή, ο οποίος αν του απαντήσει σημαίνει ότι είναι on-line.

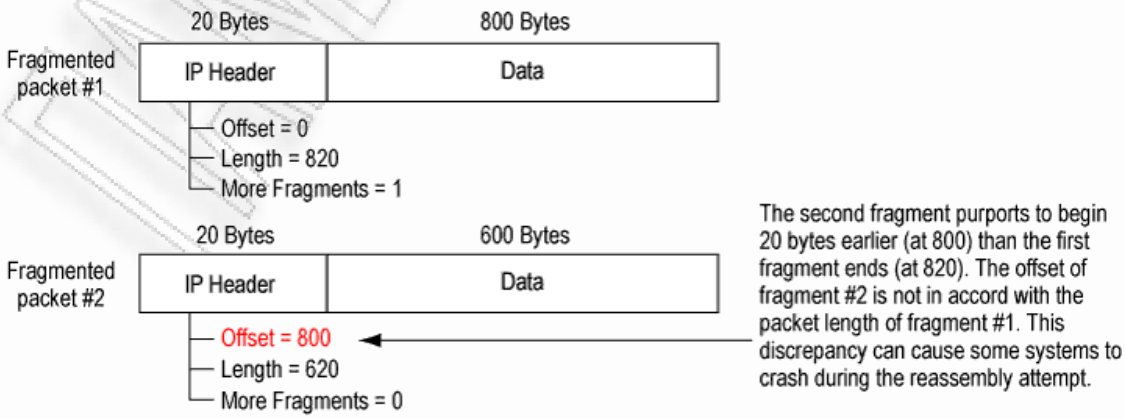
SYN Flood attack. Κατά την επικοινωνία μεταξύ δύο υπολογιστών χρησιμοποιείται η χειραψία 3 βημάτων όπου ο πελάτης αποστέλλει ένα πακέτο SYN στο διακομιστή, αυτός του απαντάει στέλνοντας πίσω μία επιβεβαίωση SYN-ACK και τέλος ο πελάτης του απαντάει με ένα ACK (acknowledge) μήνυμα οπότε και ολοκληρώνεται η μεταξύ τους σύνδεση και αρχίζει η μετάδοση των δεδομένων.

Στη SYN attack ο πελάτης δεν πραγματοποιεί ποτέ το τρίτο βήμα με αποτέλεσμα ο διακομιστής να είναι υποχρεωμένος να περιμένει για ένα μικρό χρονικό διάστημα το ACK μήνυμα. Στην περίπτωση που το ACK μήνυμα δε φτάσει ποτέ, τότε ο διακομιστής τερματίζει τη σύνδεση. Είναι δυνατό όμως ο επιτιθέμενος να στέλνει συνεχώς έναν αυξανόμενο αριθμό πακέτων SYN και να μη δίνει την πραγματική του ip ή να δίνει την ip του συστήματος στόχου με αποτέλεσμα να αναγκάσει το διακομιστή ή να περιμένει για πάντα μία απάντηση από μία ανύπαρκτη ip ή να αναγκάσει το σύστημα να πέσει σε μία ατελείωτη σειρά επεξεργασίας που και στις δύο περιπτώσεις είναι δυνατό να προκαλέσει κατάρρευση, πάγωμα ή επανεκκίνηση λειτουργίας. Η μόνη λύση για την αντιμετώπιση αυτής της επίθεσης είναι ο διακομιστής να βάζει όριο στον αριθμό των συνδέσεων που θα εξυπηρετεί, με τον κίνδυνο βέβαια να μην εξυπηρετεί και νόμιμους χρήστες του συστήματός του.




**Εικόνα 3.5.1.3 SYN Flood Attack**
**Πηγή : http://www.javvin.com/networksecurity/TCPSYNAttack.html**

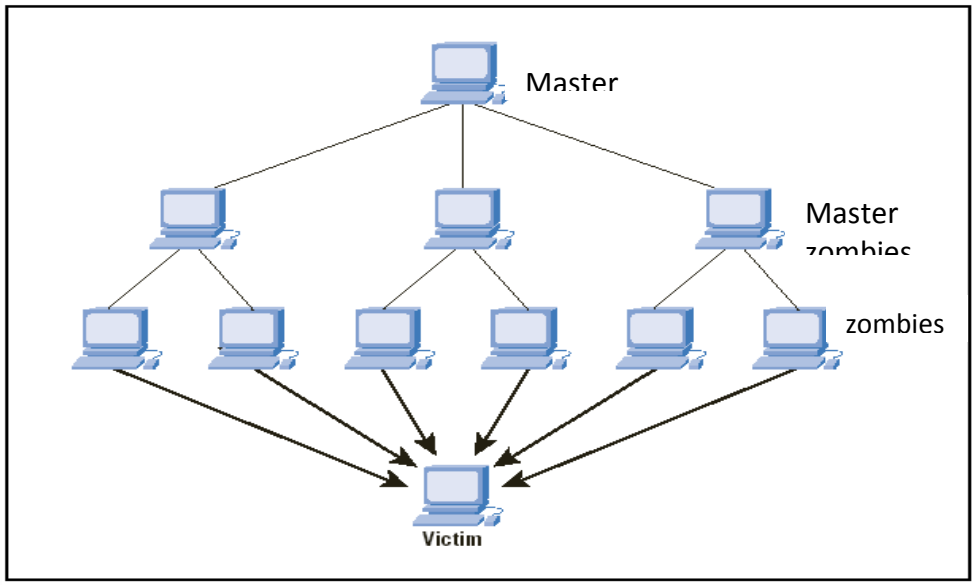
Η Teardrop, είναι το πιο πρόσφατο είδος επίθεσης και το πιο δύσκολο στην αντιμετώπισή του. Χρησιμοποιεί το πρωτόκολλο TCP/IP το οποίο χρησιμεύει στον τεμαχισμό και την επανασυναρμολόγηση των κομματιών ενός μεγάλου αρχείου που ταξιδεύει μέσα στο διαδίκτυο κατά την επικοινωνία δύο υπολογιστών. Τα κομμάτια αυτά περιλαμβάνουν κάποια πεδία που πληροφορούν τον παραλήπτη για το αν υπάρχει άλλο κομμάτι να περιμένει ή για το πώς να κάνει τη συναρμολόγηση όλων αυτών των κομματιών ή γενικότερα για το αν υπήρξε κανένα πρόβλημα κατά τη μεταφορά. Στην περίπτωση που θα διαπιστωθεί το οποιοδήποτε πρόβλημα ο παραλήπτης ενημερώνει τον αποστολέα να ξανακάνει τη μεταφορά των προβληματικών πακέτων. Ο επιτιθέμενος σε αυτή τη φάση εκμεταλλεύεται αυτό το γεγονός και χρησιμοποιώντας ένα πρόγραμμα που λέγεται teardrop στέλνει συνεχώς πακέτα με λανθασμένα στοιχεία με αποτέλεσμα να γεμίζει όλη η μνήμη του παραλήπτη ώστε να μην μπορεί να δέχεται άλλα πακέτα από κανέναν άλλο έως ότου καταρρεύσει ή κάνει επανεκκίνηση.



**Εικόνα 3.5.1.4 Teardrop**
**Πηγή:**[http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-security/understanding-teardrop-attacks.html](http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-security/understanding-teardrop-attacks.html)

### 3.5.2 Διαμοιρασμένη Άρνηση Παροχής Υπηρεσιών (Distributed DoS)

Ένα είδος διαδικτυακής επίθεσης που έχει σχεδόν τα ίδια αποτελέσματα με τις DoS επιθέσεις αλλά με τη διαφορά ότι χρησιμοποιεί την υπολογιστική ισχύ πολλών υπολογιστικών συστημάτων είναι αυτή της Διαμοιρασμένης Άρνησης Παροχής Υπηρεσιών (DDoS). Με την DDoS επίθεση επιδιώκεται η εξάντληση των πόρων που διαθέτει το θύμα. Για να πραγματοποιηθεί αυτή η επίθεση θα πρέπει αρχικά οι επιτιθέμενοι να φτιάξουν ένα δίκτυο υπολογιστών με το οποίο θα καταφέρουν να αποδυναμώσουν την παροχή υπηρεσιών στους νόμιμους χρήστες του δικτύου. Έπειτα θα πρέπει να εγκαταστήσουν το λογισμικό που θα χρησιμοποιήσουν σε όλους τους υπολογιστές (zombies) που θεωρούν ευάλωτους εξαιτίας των ελλιπών μέτρων ασφαλείας που εφαρμόζουν. Τα zombies γίνονται κοινωνοί της επίθεσης χωρίς καν να το γνωρίζουν, όπου και αυτά με τη σειρά τους ψάχνουν για νέα ευάλωτα συστήματα μέχρις ότου ο Master αποκτήσει υπό τον έλεγχό του όσα συστήματα zombie είναι αναγκαία για να κάνει την επίθεσή του. Η επίθεση ξεκινάει με την εντολή που δίνει ο Master στα zombies για την αποστολή μαζικών άχρηστων αιτήσεων προς το θύμα, πράγμα που το καθιστά ανίκανο να καταφέρει να ικανοποιήσει όλες αυτές τις αιτήσεις στο χρόνο που πρέπει, με αποτέλεσμα κάποια στιγμή να καταρρεύσει.




**Εικόνα 3.5.2.1 Distributed DoS**
**Πηγή:** [http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html)

### 3.5.3 E-mail Spoofing - Phishing

Είναι η μέθοδος κατά την οποία ο επιτιθέμενος παραποιεί ή αποκρύπτει την πραγματική ηλεκτρονική του διεύθυνση, προσποιούμενος κάποιον άλλο του οποίου το θύμα του έχει εμπιστοσύνη με τελικό σκοπό να τον παραπλανήσει ώστε ή να του αποσπάσει διάφορες πληροφορίες ή να τον αναγκάσει να κάνει κάτι που αυτός θέλει. Τέτοια πρακτική ακολουθούν συνήθως τα spam και phishing e-mails. Η αναγνώριση τέτοιων μηνυμάτων δεν είναι πάντα εύκολη υπόθεση αλλά οι συνήθεις μορφές τους είναι οι εξής:

- Το μήνυμα θα περιγράφει κάποιο σοβαρό πρόβλημα που θα αφορά για παράδειγμα το λογαριασμό του e-mail του χρήστη και θα τον προτρέπει να κάνει κλικ σε κάποιον

σύνδεσμο όπου θα πρέπει να συμπληρώσει τα στοιχεία του λογαριασμού του ώστε να μην ακυρωθεί.

- Πολύ πιθανό να δέχεται συγχαρητήρια κάποιος χρήστης για τη νίκη κάποιου λαχείου ή διαγωνισμού και να του ζητάει να επικοινωνήσει με τον αποστολέα για να παραλάβει τα κέρδη με απώτερο σκοπό όμως να του αποσπάσει απόρρητα στοιχεία για το άτομό του.
- Τα e-mails αυτά λανσάρονται συνήθως με το λογότυπο κάποιας γνωστής τράπεζας ή εταιρίας το οποίο δε διαφέρει σε τίποτα από τα πραγματικό, σε αντίθεση με τα στοιχεία επικοινωνίας τα οποία με μια απλή διασταύρωση με την αντίστοιχη πραγματική ιστοσελίδα μπορεί εύκολα να διαπιστώσει κανείς ότι είναι διαφορετικά.

Τα περισσότερα απ' αυτά τα μηνύματα στην προσπάθειά τους να τρομάξουν τον ανυποψίαστο παραλήπτη, τον απειλούν ότι αν δεν εκτελέσει άμεσα τις απαραίτητες ενέργειες που του υποδεικνύουν, θα προβούν σε ακύρωση του λογαριασμού του έτσι ώστε να μην μπορεί να τον χρησιμοποιήσει ποτέ ξανά, με απώτερο σκοπό φυσικά να μην του δώσουν περιθώριο να ελέγξει τη γνησιότητα του μηνύματος.

### 3.5.4 Επίθεση ωμής βίας (Brute – force attack)

Ένας από τους πιο διαδεδομένους τρόπους εύρεσης συνθηματικών λογαριασμού ενός χρήστη είναι η επίθεση ωμής βίας (brute force-attack). Η μέθοδος αυτή χρησιμοποιεί έτοιμες λίστες με ονόματα λογαριασμών και συνηθισμένων κωδικών πρόσβασης έτσι ώστε να μπορεί ο επιτιθέμενος συνδυάζοντάς τα, να μαντέψει τα συνθηματικά εισόδου κάποιου λογαριασμού. Αυτές οι λίστες είναι συνήθως αποκτήματα υποκλοπής από παραβιασμένους διακομιστές οι οποίες άπαξ και καταφέρουν να δώσουν πρόσβαση στον επιτιθέμενο, τότε του παρέχουν τα ίδια ακριβώς δικαιώματα χρήσης με τα δικαιώματα του χρήστη του οποίου παραβιάστηκε ο λογαριασμός.

### 3.5.5 Επίθεση Επανάληψης (Replay Attack)

Τέτοιου είδους επίθεση πραγματοποιείται όταν κάποιος τρίτος καταφέρει να καταγράψει την ανταλλαγή των δεδομένων που μεταφέρονται από τον πελάτη στο διακομιστή, ακόμα και αν τα δεδομένα αυτά είναι κρυπτογραφημένα και προσπαθήσει να επαναλάβει την εκπομπή σε κάποια άλλη στιγμή.

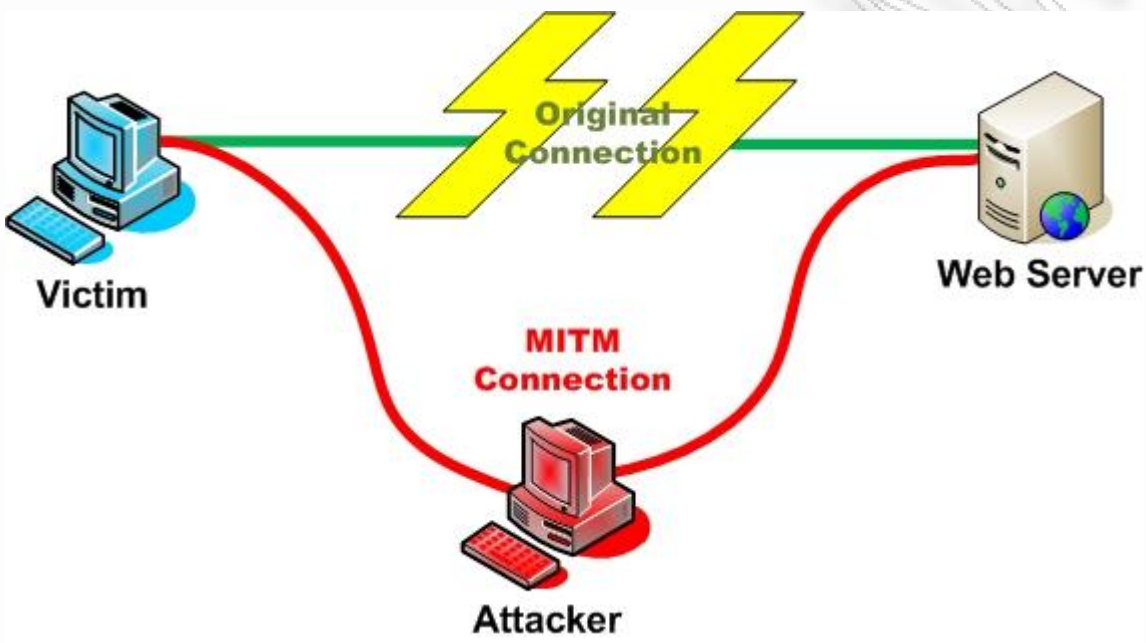
### 3.5.6 Υπερχείλιση Καταχωρητή (Buffer Overflow)

Ο στόχος αυτού του είδους επίθεσης είναι, να ωθήσει το λογισμικό στα όρια του μέχρι να σπάσει έτσι ώστε να μπορέσει αποκτήσει πρόσβαση στο σύστημα. Κατά την επίθεση αυτή θα πρέπει το buffer[10] μιας υπηρεσίας να είναι προκαθορισμένο και να μην προσαρμόζεται ανάλογα με το μέγεθος της πληροφορίας που αποθηκεύεται. Τέτοιου είδους υπηρεσίες χρησιμοποιούν συνήθως εφαρμογές γραμμένες σε C ή C++. Μια υπερχείλιση καταχωρητή δημιουργείται όταν μέσα σε ένα buffer βάλουμε ένα μήνυμα που έχει μεγαλύτερο αριθμό χαρακτήρων απ' αυτόν που χωράει. Στην περίπτωση που το κομμάτι που περισσεύει πέσει σε περιοχή μνήμης που έχει γραμμένη άλλη πληροφορία του ίδιου προγράμματος, τότε το κομμάτι αυτό αντικαθίσταται με τις νέες πληροφορίες και δημιουργείται κάποιο σφάλμα που είναι πολύ δύσκολο να λυθεί ενώ στην περίπτωση που το κομμάτι αυτό πέσει πάνω σε πληροφορία που είναι απαραίτητη για τη σωστή εκτέλεση του προγράμματος τότε υπάρχει καταπάτηση και ο επιτιθέμενος εκτελεί το δικό του κακόβουλο κώδικα για να πάρει τον πλήρη έλεγχο του συστήματος.

[10] Buffer είναι ένα συνεχόμενο κομμάτι μνήμης του υπολογιστή που αποθηκεύει προσωρινά πολλά στιγμιότυπα του ίδιου τύπου δεδομένων.

### 3.5.7 Επίθεση ενδιάμεσου (Man in the middle attack)

Η επίθεση του ενδιάμεσου είναι μία πολύ αποδοτική μορφή επίθεσης που έχει να κάνει μ' αυτό ακριβώς που υποδηλώνει και ο τίτλος της. Κατά την επικοινωνία δύο φιλικών μερών όπου πραγματοποιείται ανταλλαγή δεδομένων είναι δυνατόν να παρεμβληθεί κάποιος τρίτος, ο οποίος ή θα μπορεί απλά να κρυφακούει (eavesdropping) ή να παρεμποδίζει ή ακόμα και να τροποποιεί τα δεδομένα που ανταλλάσσονται μεταξύ των δύο αυτών μερών.




**Εικόνα 3.5.7.1 Man in the middle attack**

**Πηγή:** http://www.owasp.org/index.php/Man-in-the-middle_attack

### 3.5.8 Κακόβουλος Κώδικας (Malicious Code)

Ο κακόβουλος κώδικας (malicious code) είναι ένας όρος που δόθηκε για να ομαδοποιήσει όλα εκείνα τα προγράμματα που έχουν σαν αντικειμενικό σκοπό να βλάψουν ένα υπολογιστικό σύστημα. Είναι ικανά να προσβάλλουν την εμπιστευτικότητα, την ακεραιότητα αλλά και τη διαθεσιμότητα των συστημάτων αυτών και συνήθως οι βλάβες που μπορούν να προκαλέσουν είναι αντιστρόφως ανάλογες με το μέγεθός τους. Τα προγράμματα αυτά είναι δυνατόν να εισχωρήσουν σε κάποιο σύστημα είτε με τη συναίνεση του χρήστη είτε χωρίς αυτή. Τα βασικότερα είδη τέτοιων κακόβουλων προγραμμάτων είναι τα εξής:

- Οι Ιοί (Viruses)
- Τα σκουλήκια (Worms)
- Οι Δούρειοι Ίπποι (Trojan Horses)

#### 3.5.8.1 Οι Ιοί (Viruses)

Οι Ιοί εμφανίζονται για πρώτη φορά με τον εξής ορισμό: [28] "We define a computer "virus" as a program that can "infect" other programs by modifying them to include a possibly evolved copy of itself." που σημαίνει ότι "ιός είναι ένα πρόγραμμα που μπορεί να μολύνει άλλα προγράμματα τροποποιώντας τον κώδικά τους ώστε να περιλαμβάνουν μία έκδοση του εαυτού τους.". Οι Ιοί έχουν την ικανότητα να ενεργοποιούνται είτε αυτόματα σε κάποιον υπολογιστή είτε έπειτα από την παρέμβαση κάποιου χρήστη. Αυτό σημαίνει ότι ένας ιός μπορεί να εκτελεστεί είτε αυτόματα έπειτα από προγραμματισμό με βάση το ρολόι του υπολογιστή είτε ως πρόγραμμα από το

χρήστη. Τα κύρια μέσα διάδοσης των ιών είναι το ηλεκτρονικό ταχυδρομείο, τα φορητά μέσα αποθήκευσης δεδομένων και κυρίως το διαδίκτυο.

Η σειρά εμφάνισης κάποιων εκ των πιο γνωστών ιών των τελευταίων 40 χρόνων [29] έχει ως εξής: Ο πρώτος ιός έκανε την εμφάνισή του στο δίκτυο ARPANET[11] το 1970 και είχε την ονομασία Creeper, μεταφερόταν από σύστημα σε σύστημα μέσω του τερματικού και εμφάνιζε το μήνυμα "I'M THE CREEPER : CATCH ME IF YOY CAN ", ακολούθησε ο brain το 1980, που ήταν ο πρώτος ιός που έκανε την εμφάνισή του σε περιβάλλον MS-DOS, έπειτα ο "Michelangelo", το 1992 που ανάγκασε τις εταιρίες να φτιάξουν τα πρώτα antivirus προγράμματα, ο "Melissa" που ήταν ο πρώτος ιός που εμφανίστηκε μέσω mail το 1999, ο "I love you" που εξαπλώθηκε αστραπιαία το 2000 και ανάγκασε το Πεντάγωνο και τη CIA να ρίξουν τους mail servers τους όπως επίσης και να μολύνει 50 εκατομμύρια υπολογιστές μέσα σε 8 ημέρες, ο "Chernobyl" που διέγραφε το BIOS όταν η ημερομηνία του υπολογιστή έδειχνε 26 Απριλίου, ο "Sasser" ο οποίος κατάφερε κάνοντας επίθεση με τη μέθοδο της υπερχείλισης διακομιστή το 2004 να αναγκάσει το γαλλικό πρακτορείο ειδήσεων να κλείσει όλες του τις δορυφορικές επικοινωνίες για ώρες όπως και την αεροπορική εταιρία Delta Airlines να ακυρώσει έναν πάρα πολύ μεγάλο αριθμό υπερατλαντικών πτήσεων, ο "Scob" ο οποίος συνέλλεγε ευαίσθητα προσωπικά δεδομένα και τα έστελνε στη ρώσικη μαφία το 2004 και πολλοί άλλοι με παρόμοια περίπου λειτουργία.

Συμπερασματικά βλέποντας το παρελθόν και αναγνωρίζοντας το μέγεθος των ζημιών που μπορούν να προκαλέσουν οι ιοί, μπορούμε να πούμε ότι η προστασία του υπολογιστή μας δεν μπορεί να επιτευχθεί με κανένα είδους λογισμικό, όσο προσεχτικά φτιαγμένο κι αν είναι, παρά μόνο με τη γνώση και την προσεκτική χρήση του υπολογιστή μας.

### 3.5.8.2 Τα σκουλήκια (Worms)

Τα προγράμματα τύπου Worm δεν χρειάζεται να προσκολληθούν σε άλλα προγράμματα για να ενεργοποιηθούν αφού από μόνα τους ενσωματώνουν τον κώδικα που χρειάζονται για να πολλαπλασιαστούν και να μεταδοθούν σε άλλους υπολογιστές. Το σύνηθες αλλά και πιο αποτελεσματικό μέσο διάδοσης των σκουληκιών είναι τα δίκτυα υπολογιστών. Χαρακτηριστικά αξίζει να αναφέρουμε το σκουλήκι Code Red το οποίο αναπαρήγαγε τον εαυτό του πάνω από 250.000 φορές μέσα σε 9 ώρες τον Ιούλιο του 2001 και κατάφερε να μολύνει μέχρι και το διακομιστή του Λευκού Οίκου.

### 3.5.8.3 Οι Δούρειοι Ίπποι (Trojan Horses)

Απλά και μόνο, από την ονομασία τους καταλαβαίνει κανείς ότι αυτού του είδους οι ιοί για να δράσουν θα πρέπει να καμουφλαριστούν πίσω από άλλα προγράμματα για να μπορέσουν να εισχωρήσουν στο σύστημα κάποιου χρήστη. Αυτό πολύ απλά σημαίνει ότι όταν κάποιος χρήστης θα προσπαθήσει να εκτελέσει κάποιο χρήσιμο πρόγραμμα στον υπολογιστή του, τότε άθελά του θα εγκαταστήσει και έναν ιό τύπου Δούρειου Ίππου. Σε αντίθεση με τα άλλα είδη ιών για να αναπαραχθούν και να μεταδοθούν χρειάζονται ανθρώπινη παρέμβαση. Ένας Δούρειος Ίππος αποτελείται από δύο μέρη, τον πελάτη και το διακομιστή. Για να λειτουργήσει ο ιός θα πρέπει ο διακομιστής να εισέλθει στον υπολογιστή του θύματος και ο πελάτης να εγκατασταθεί στον επιτιθέμενο. Έπειτα το μόνο που χρειάζεται για να αποκτήσει πλήρη πρόσβαση ο εισβολέας στον υπολογιστή του θύματος είναι μία σύνδεση στο διαδίκτυο έτσι ώστε ο διακομιστής του υπολογιστή του θύματος να στείλει σήμα με την ip του, στον πελάτη του υπολογιστή του επιτιθέμενου για να γίνει η ζεύξη.

[11] Θεωρείται ο πρόγονος του σημερινού διαδικτύου . Ήταν ένα είδος δικτύου υπολογιστών γύρω στα τέλη της δεκαετίας του `60 που αρχικά συνέδεε 4 υπολογιστές (τρεις στην California και έναν στην Utah) .

## 3.6 Περιγραφή ενεργειών αντιμετώπισης κινδύνων ασφαλείας

Όλα όσα έχουν ειπωθεί μέχρι στιγμής και αφορούν στην ασφάλεια των προσωπικών δεδομένων κάποιου μεμονωμένου χρήστη ή κάποιας επιχείρησης ή οργανισμού, αποτελούν το υπόβαθρο για τη χάραξη μιας κοινής πολιτικής, που θα έχει σα μοναδικό στόχο την προστασία από κάθε είδους κακόβουλη ενέργεια. Η πολιτική αυτή θα πρέπει σε γενικές γραμμές να περιλαμβάνει κάποιες συγκεκριμένες ενέργειες, που είναι απαραίτητες για την όσο είναι ανθρωπίνως δυνατό, μείωση των πιθανοτήτων παραβίασης ασφαλείας. Οι ενέργειες αυτές πρέπει να εκτελούνται με τη σειρά που δίνονται και είναι οι εξής:

- Πρόληψη
- Ανίχνευση
- Αντίδραση - Αντιμετώπιση
- Αποκατάσταση – Ανάλυση επιπτώσεων

### 3.6.1 Προληπτικά μέτρα προστασίας

Τα προληπτικά μέτρα προστασίας αφορούν όλες εκείνες τις ενέργειες που πρέπει να εκτελούνται προτού καταφέρει να γίνει ορατή η οποιαδήποτε απειλή. Έτσι ο εκάστοτε χρήστης θα πρέπει:[94]

α) Να μην ανακοινώνει ποτέ και για κανένα λόγο στο διαδίκτυο, πληροφορίες που αφορούν, το υπολογιστικό σύστημα που διαθέτει, το λογισμικό που χρησιμοποιεί ή τα δικαιώματα χρηστών του συστήματος διότι πολύ απλά μ' αυτόν τον τρόπο βοηθάει τον επίδοξο εισβολέα να φτάσει πιο κοντά στο στόχο του. Μέχρι και η αποκάλυψη του e-mail του θα πρέπει να γίνεται αποκλειστικά και μόνο σε άτομα τα οποία θα γνωρίζει.

β) Στην περίπτωση δικτύου θα πρέπει ο διαχειριστής να περιορίζει κάθε χρήστη, αποκλειστικά και μόνο στα όρια των δικαιωμάτων που θα του έχει ορίσει.

γ) Όταν θα κάνει αγορές μέσω διαδικτύου θα πρέπει να είναι σε θέση να μπορεί να αναγνωρίσει πότε μία ιστοσελίδα είναι ασφαλής και πότε όχι.

δ) Να διαγράψει από τον υπολογιστή του οποιοδήποτε αρχείο ή πρόγραμμα έχει να χρησιμοποιηθεί πάρα πολύ καιρό διότι αυτό θα μπορούσε να αποτελέσει πιθανό σημείο εισόδου του επιτιθέμενου.

ε) Να εντοπίσει μέσω των μηχανών αναζήτησης το όνομά του και να το διαγράψει, από οποιονδήποτε κατάλογο του διαδικτύου δεν έχει επιλέξει να βρίσκεται.

στ) Να χρησιμοποιεί τα πιο ισχυρά αντιβιοτικά της αγοράς, τα οποία να μπορούν να κάνουν update σε καθημερινή βάση.

ζ) Να χρησιμοποιεί firewalls και μεθόδους κρυπτογράφησης κάθε φορά που είναι συνδεδεμένος στο διαδίκτυο.

η) Να διενεργεί συχνά τεστ στο σύστημά του που θα μπορούν να εντοπίζουν τυχόν αδυναμίες ασφαλείας.

θ) Να διαβάζει την πολιτική ασφαλείας κάθε ιστοτόπου που επισκέπτεται όταν πρόκειται να ανταλλάξει δεδομένα προσωπικού χαρακτήρα.

### 3.6.2 Ανίχνευση

Αφού ληφθούν όλα τα απαραίτητα μέτρα πρόληψης και ελαχιστοποιηθούν οι πιθανότητες αλλά και οι συνέπειες μιας επίθεσης, σειρά έχει η αναγνώριση του είδους της επίθεσης, η ανίχνευση του τρόπου εκδήλωσής της και τέλος η εύρεση του εισβολέα για τον αποκλεισμό του και την αποτροπή μελλοντικής του ενέργειας. Η αναγνώριση των συγκεκριμένων χαρακτηριστικών μιας επίθεσης είναι απαραίτητη προϋπόθεση προκειμένου να αντιμετωπιστεί πλήρως και όπως είναι λογικό η αντιμετώπισή της δυσκολεύει ακόμη περισσότερο, όσο αυξάνει η πολυπλοκότητα του περιστατικού.

### 3.6.3 Αντίδραση - Αντιμετώπιση

Με το τέλος του σταδίου της ανίχνευσης θα πρέπει να υλοποιηθούν πλέον όλες οι απαραίτητες ενέργειες για την αντιμετώπιση και ελαχιστοποίηση των συνεπειών της απειλής, εν τη γενέσει της. Η έγκαιρη αντιμετώπιση της επίθεσης, δίνει τη δυνατότητα στο διαχειριστή του δικτύου να προστατεύσει τα υπόλοιπα συστήματα που δεν θα έχουν προλάβει να χτυπηθούν από αυτήν και να περιορίσει όσο προλαβαίνει τη ζημιά που θα έχει προκληθεί. Τα μέτρα αυτά θα αναλυθούν διεξοδικά στο επόμενο κεφάλαιο.

### 3.6.4 Αποκατάσταση - Απολογισμός

Τέλος η αποκατάσταση και ο απολογισμός των επιπτώσεων είναι τα τελευταία στάδια αντιμετώπισης μιας επίθεσης που δίνουν τη δυνατότητα στο θύμα να εξακριβώσει το μέγεθος της ζημιάς που προκλήθηκε, να καταμετρήσει πόσες και ποιες πληροφορίες καταστράφηκαν αλλά και να αναγνωρίσει ποια είναι η τρέχουσα κατάσταση του υπολογιστικού του συστήματος ώστε να κάνει τις απαραίτητες ενέργειες για να το επαναφέρει όσο αυτό είναι εφικτό στην προτέρα του κατάσταση. Οι αποκατάσταση αυτή περιλαμβάνει τις παρακάτω ενέργειες [30]:

- Αποκατάσταση όσων αρχείων δεν καταστράφηκαν πλήρως.
- Επαναφορά όλων των λειτουργιών του συστήματος.
- Εύρεση και αποκατάσταση του κενού ασφαλείας που αποτέλεσε παράθυρο εισόδου για τον εισβολέα.
- Εντοπισμός και εύρεση των επιτιθεμένων με σκοπό να αποφευχθεί μελλοντική τους δράση.
- Αποκόμιση εμπειριών από τα λάθη και τις παραλείψεις που προκλήθηκαν όσον αφορά στην πολιτική ασφαλείας που ακολουθήθηκε με στόχο την απόκτηση γνώσεων για τη μη επανάληψη των ίδιων σφαλμάτων.

Αφού θα έχει πλέον αντιμετωπιστεί η επίθεση, κατά τη φάση του απολογισμού απαντώνται κάποια ερωτήματα και προκύπτουν κάποια συμπεράσματα, τα οποία θα μπορούσαν να αποτελέσουν πηγή βοήθειας για μελλοντική αποτροπή εισβολής. Παραδείγματα τέτοιων ερωτήσεων είναι: τί έφταιγε που η επίθεση ήταν επιτυχής; Ήταν δυνατόν να αποφευχθεί η καταστροφή; Θα μπορούσαν να γίνουν πιο σωστές ενέργειες για να αντιμετωπιστεί η κατάσταση; Οι απαντήσεις σε όλα αυτά τα ερωτήματα μπορούν να οδηγήσουν σε συμπεράσματα που μπορούν να αποβούν σωτήρια για την αποφυγή μελλοντικών κακόβουλων ενεργειών.

Στα πλαίσια του επόμενου κεφαλαίου αναλύονται τα μέτρα που θα πρέπει να ληφθούν για να αντιμετωπιστεί μια επιθετική ενέργεια με επιτυχία.

# 4 Τεχνικά Μέτρα Προστασίας

## 4.1 Γενικά

Στο προηγούμενο κεφάλαιο αναφέρθηκαν κάποια προληπτικά μέτρα προστασίας των ηλεκτρονικών συστημάτων όπως επίσης και οι ενέργειες αποκατάστασης μιας κακόβουλης επίθεσης που έχει σα στόχο την προσβολή της ακεραιότητας της ασφάλειας ενός υπολογιστικού συστήματος. Στο παρόν κεφάλαιο πρόκειται να αναλυθούν όλοι εκείνοι οι μηχανισμοί αλλά και οι τεχνικές αντιμετώπισης που χρησιμοποιούνται για την προστασία ενός ηλεκτρονικού συστήματος.

Στις μέρες μας λόγω του γεγονότος ότι πολλοί οργανισμοί αλλά και δημόσιες υπηρεσίες χρησιμοποιούν τοπικά δίκτυα, τα οποία τις περισσότερες φορές είναι συνδεδεμένα και με το διαδίκτυο, οι έννοιες ασφάλεια δικτύων και ασφάλεια ηλεκτρονικών συστημάτων τείνουν να συγκλίνουν, γι' αυτό το λόγο όταν θα αναφερόμαστε στην ασφάλεια ηλεκτρονικών συστημάτων θα εμπεριέχεται και η έννοια της ασφάλειας των δικτυωμένων ηλεκτρονικών συστημάτων.

Η ασφάλεια των επικοινωνιών μέσω διαδικτύου είναι υπόθεση τόσο των παρόχων διαδικτύου όσο και των χρηστών λόγω του ότι οι μεν επωφελούνται επιχειρηματικά και οι δε επωφελούνται από τις παρεχόμενες υπηρεσίες του διαδικτύου. Για την επίτευξη ικανοποιητικής ασφάλειας θα πρέπει να ληφθούν κάποια μέτρα τόσο σε επίπεδο φυσικής ασφάλειας, όσο και σε επίπεδο λογισμικού με σκοπό να αποτελέσουν τροχοπέδη στην οποιαδήποτε επίθεση θα έχει σα στόχο την παραβίαση ασφαλείας.

Η φυσική ασφάλεια στοχεύει πρώτον στην προστασία του συστήματος από μη εξουσιοδοτημένη φυσική πρόσβαση και δεύτερον στην ασφάλεια του υλικού ενός υπολογιστικού συστήματος [31] εξαιτίας της τρωτότητας των κυκλωμάτων και της τεχνολογίας κατασκευής του υλικού.

Κάποια σοβαρά μέτρα προστασίας κάθε εμπλεκομένου που πρέπει να λαμβάνονται κατά τη διάρκεια μιας ηλεκτρονικής επικοινωνίας σε επίπεδο λογισμικού αλλά και υλικού είναι τα εξής:

- Πυρότοιχοι Προστασίας (Firewalls)
- Προγράμματα Antivirus
- Συστήματα Ανίχνευσης εισβολέων (IDS)
- Ασφάλεια Ηλεκτρονικής Αλληλογραφίας (E-mail Security)
- Κρυπτογράφηση
- Πρωτόκολλα SSL
- Ψηφιακές Υπογραφές

## 4.2 Πυρότοιχοι Προστασίας (Firewalls)

Για να γίνει κατανοητός ο όρος firewall θα γίνει μία αναφορά στην αρχική χρησιμοποίηση της λέξης σύμφωνα με τον Schneier [32]. Ο πυρότοιχος λοιπόν ήταν ένας σιδερένιος τοίχος που βρισκόταν μεταξύ των βαγονιών των παλαιών τρένων που κινούνταν με κάρβουνο και του κλίβανου που έριχναν τα κάρβουνα οι μηχανοδηγοί για να κινηθεί το τρένο. Ο ρόλος του ήταν να προστατεύει τους επιβάτες από τη φωτιά που έπιανε η σκόνη του άνθρακα κατά τη μεταφορά του κάρβουνου στον κλίβανο. Τον όρο αυτόν τον δανείστηκε η πληροφορική για να περιγράψει το τοίχος ασφαλείας μεταξύ του διαδικτύου και ενός ιδιόκτητου δικτύου με απώτερο σκοπό την προστασία των δεδομένων που διακινούνται μεταξύ των δύο μερών.

Ο πυρότοιχος λειτουργεί σαν μια πύλη από την οποία πρέπει να περάσουν απαραιτήτως όλα τα δεδομένα που κινούνται από και προς το ιδιόκτητο δίκτυο, που σημαίνει ότι δεν ελέγχονται μόνο τα δεδομένα που εισέρχονται από το διαδίκτυο αλλά και τα προγράμματα που είναι ήδη εγκατεστημένα στον υπολογιστή μας και είτε στέλνουν δεδομένα προς τα έξω είτε ανοίγουν κάποιες οπές ασφαλείας, που θα επιτρέψουν στους επίδοξους hackers να εισέλθουν

στο σύστημά μας. Το αν θα περάσουν ή όχι τα δεδομένα αυτά, καθορίζεται τελικά από την πολιτική ασφαλείας που ορίζει ο εκάστοτε χρήστης ανάλογα με το επίπεδο ασφαλείας που θέλει να επιβάλλει.

Η ΑΔΑΕ [33] στην περίπτωση του παρόχου ορίζει το firewall ως απαραίτητη προϋπόθεση της πολιτικής ασφαλείας περιμέτρου και τον υποχρεώνει βάσει νόμου να χρησιμοποιεί τέτοια συστήματα 24 ώρες το 24ωρο, ασταμάτητα με μόνη διακοπή της λειτουργίας του, τη στιγμή της συντήρησης ή αναβάθμισης του, έπειτα από έγκαιρη ενημέρωση των χρηστών που θα συνοδεύεται με διακοπή της συνδεσιμότητας του δικτύου για όσο χρόνο χρειαστεί.

### 4.2.1 Δυνατότητες του Firewall

Οι δυνατότητες που έχει ένα σύστημα firewall είτε αυτό είναι τύπου λογισμικού είτε υλικού είναι οι εξής [34]:

- Αποτελεί το κέντρο αποφάσεων σε θέματα ασφαλείας, υλοποιώντας την πολιτική ασφαλείας που επιθυμεί ο κάθε χρήστης.
- Αποτρέπει την εισχώρηση ιών, σκουληκιών και δούρειων ίππων να εισχωρήσουν στο σύστημά.
- Απαγορεύει την ανεπιθύμητη πρόσβαση οποιουδήποτε δεν έχει πάρει άδεια να εισχωρήσει στο σύστημα.
- Παρουσιάζει αναλυτική καταγραφή όλων των κινήσεων δεδομένων που πραγματοποιούνται από και προς το δίκτυο.
- Έχει τη δυνατότητα να αποκρύψει την πραγματική διεύθυνση των υπολογιστών του δικτύου.

### 4.2.2 Αδυναμίες του Firewall

Έτσι όπως κάθε τι έχει τα πλεονεκτήματα και τα μειονεκτήματα του, έτσι και τα firewalls έχουν τις αδυναμίες τους και εάν δε ρυθμιστούν σωστά τότε μπορεί να αποδειχθούν άχρηστα. Κάποιες αδυναμίες που παρουσιάζουν είναι οι εξής:

- Δε μπορούν να διαγράψουν τους ιούς που θα καταφέρουν να εισχωρήσουν στο σύστημα.
- Δε μπορούν να αποτρέψουν κάποια επίθεση εκ των έσω, δηλαδή από τους εσωτερικούς χρήστες του δικτύου.
- Δε μπορούν να προστατέψουν ένα σύστημα από επιβλαβή προγράμματα τα οποία είτε δεν περνάνε μέσα απ' αυτό είτε έχει επιτρέψει ο ίδιος ο χρήστης τη διέλευσή τους.
- Δε μπορούν να προστατέψουν το σύστημα από απειλές που δεν έχουν κάνει έως τώρα την εμφάνισή τους.
- Πολλές φορές προκαλούν τη δυσαρέσκεια των χρηστών εξαιτίας των αυστηρών ρυθμίσεων ασφαλείας.

### 4.2.3 Αρχιτεκτονική των Firewalls

Η ασφάλεια που προσφέρει ένα firewall μπορεί να είναι είτε υπό μορφή λογισμικού για την περίπτωση οικιακού προσωπικού υπολογιστή είτε υπό μορφή υλικού για εταιρικά περιβάλλοντα. Οι τρόποι που υλοποιούνται είναι διάφοροι αλλά όλοι στηρίζονται στις αρχιτεκτονικές που αναλύονται παρακάτω.[35]

### 4.2.3.1 Συστήματα φίλτρου πακέτων

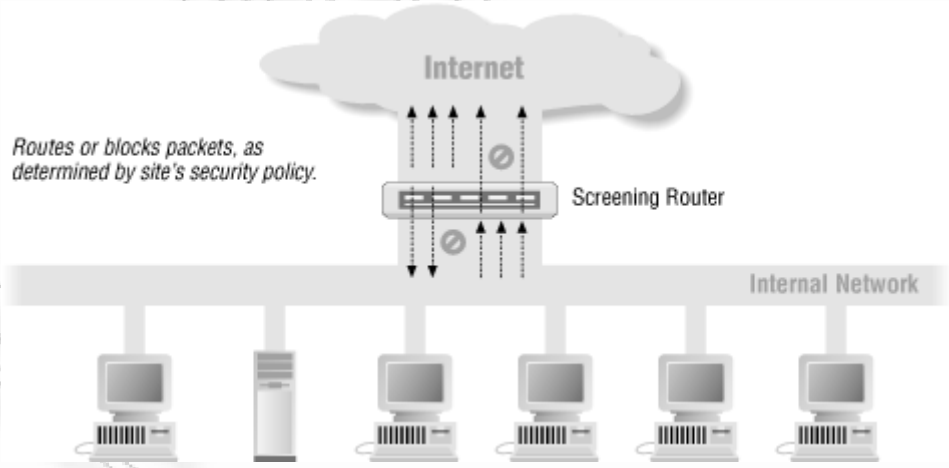
Τα συστήματα φίλτρου πακέτων [36], τα οποία είναι firewalls επιπέδου δικτύου, είναι δικτυακές συσκευές που ονομάζονται screening routers και επιτρέπουν ή εμποδίζουν την είσοδο και την έξοδο ip πακέτων σύμφωνα με την πολιτική ασφαλείας που έχει καθοριστεί από τον εκάστοτε οργανισμό . Η διαλογή των πακέτων αυτών δε γίνεται με βάση τα δεδομένα που μεταφέρουν αλλά με βάση τις πληροφορίες που είναι αποθηκευμένες στην επικεφαλίδα τους όπως:

- Την IP διεύθυνση του αποστολέα
- Την IP διεύθυνση του παραλήπτη
- Το είδος του πρωτοκόλλου που χρησιμοποιείται
- Το TCP ή UDP port του αποστολέα
- Το TCP ή UDP port του παραλήπτη

Η διαφορά τους σε σχέση με τους απλούς δρομολογητές, που απλά εξετάζουν εάν μπορούν να δρομολογήσουν ένα πακέτο προς τον παραλήπτη του, βρίσκεται στο ότι εξετάζουν επίσης και το αν πρέπει να το δρομολογήσουν, σύμφωνα πάντα με την προκαθορισθείσα πολιτική ασφαλείας.

Μερικά από τα πλεονεκτήματά τους είναι ότι εγκαθίστανται και διαμορφώνονται χωρίς ιδιαίτερη δυσκολία, είναι διαφανή προς τους χρήστες διότι δεν χρειάζεται ν' ασχοληθούν καθόλου με το τμήμα των δεδομένων των πακέτων, δεν δαπανούν μεγάλους υπολογιστικούς πόρους από τη CPU οπότε δε μειώνουν τη απόδοση του συστήματος και τέλος είναι πολύ οικονομικά σα λύση.

Τα μειονεκτήματα που παρουσιάζουν συνοψίζονται στα εξής: ο καθορισμός των κατάλληλων κανόνων φιλτραρίσματος είναι μια διαδικασία που κρύβει πολλούς κινδύνους αν δεν επιλεγεί σωστά και με τη σειρά που πρέπει, είναι λιγότερο ασφαλή από τα υπόλοιπα firewalls διότι δεν εξετάζουν καθόλου τα δεδομένα που διακινούνται, δεν αυθεντικοποιούν το χρήστη εκτός κι αν χρησιμοποιούν το πρωτόκολλο IPSP (IP Security Policy) το οποίο είναι σε θέση να απορρίπτει κάθε πακέτο IP το οποίο δεν είναι κατάλληλα πιστοποιημένο από μια έγκυρη επικεφαλίδα πιστοποίησης και τέλος δεν καταγράφουν τις λειτουργίες που εκτελούν με αποτέλεσμα να μην μπορούν να προσφέρουν μηχανισμούς ελέγχου και συναγερμού στο χρήστη από μία ενδεχόμενη παραβίαση .




**Εικόνα 4.2.3.1.1 Συστήματα Φίλτρου Πακέτων**
**Πηγή:** http://docstore.mik.ua/orelly/networking_2ndEd/fire/ch06_01.htm

### 4.2.3.2 Πύλες εφαρμογών (Application Gateways)

Οι πύλες εφαρμογών είναι γνωστές και ως application proxy ή application – level proxy [36]. Λειτουργούν στο επίπεδο εφαρμογής και έτσι έχουν πρόσβαση σε περισσότερες πληροφορίες απ' ότι τα προηγούμενα συστήματα που περιγράφτηκαν παραπάνω. Δρουν ως ενδιάμεσες διεργασίες μεταξύ του πελάτη που ζητάει μία υπηρεσία και του εξυπηρετητή που προσφέρει αυτή την υπηρεσία, έτσι ο πελάτης για να επικοινωνήσει με τον εξυπηρετητή πρέπει να διαπραγματευτεί πρώτα με τον proxy server, ο οποίος με τη σειρά του επικοινωνεί με τον εξυπηρετητή πίσω από το firewall και δρα εκ μέρους του πελάτη. Κατ' αυτόν τον τρόπο η πύλη εφαρμογών δρα ως εξυπηρετητής από τη σκοπιά του πελάτη και ως πελάτης από την πλευρά του εξυπηρετητή.

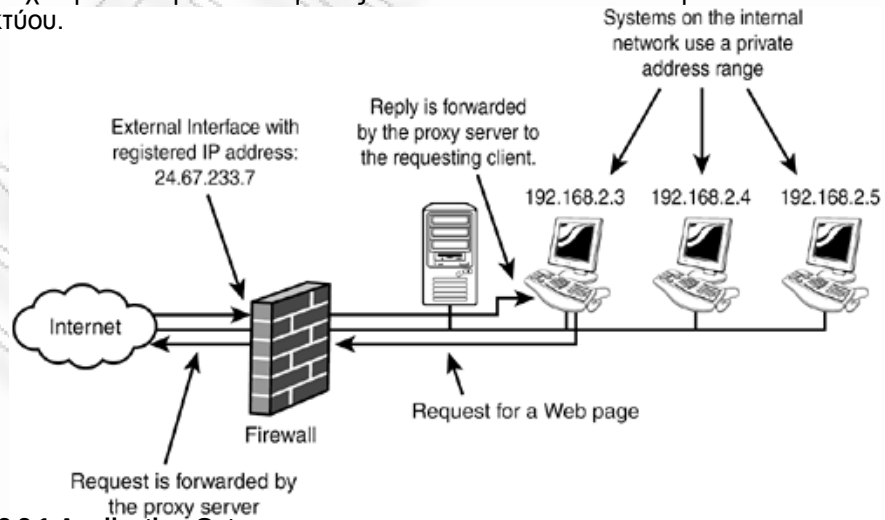
Πιο συγκεκριμένα η διαδικασία που ακολουθείται σε μία τέτοιου είδους σύνδεση είναι η εξής [37]:

Έστω ότι ένας πελάτης θέλει να στείλει κάποια αίτηση τύπου FTP ή Telnet σε έναν εξυπηρετητή χρησιμοποιώντας το πρωτόκολλο TCP/IP. Η αίτηση αυτή καταλήγει στην πύλη εφαρμογών. Η πύλη εφαρμογών βρίσκεται ως πρόγραμμα λογισμικού σε έναν υπολογιστή ο οποίος ονομάζεται υπολογιστής οχυρό (Bastion host) και ελέγχει την IP διεύθυνση του πελάτη ζητώντας του να αυθεντικοποιήσει τον εαυτό του με έναν κωδικό πρόσβασης. Αφού ολοκληρωθεί επιτυχώς η αυθεντικοποίηση του χρήστη, η πύλη λαμβάνει τα πακέτα που έστειλε ο χρήστης, τα ανοίγει, τα ελέγχει ως προς την ασφάλειά τους και αφού εξασφαλίσει ότι δεν μπορούν να προκαλέσουν κάποια βλάβη φτιάχνει καινούργια με το ίδιο ακριβώς περιεχόμενο και τα αποστέλλει στον εξυπηρετητή της εφαρμογής που ζητήθηκε εγκαθιστώντας μία καινούργια σύνδεση TCP/IP.Τα πλεονεκτήματα χρήσης των application gateways είναι τα εξής:[36]

- Παρέχουν μεγαλύτερη ασφάλεια αφού παρέχουν τη δυνατότητα αυθεντικοποίησης του χρήστη όπως και καλύτερο έλεγχο προσπέλασης.
- Παρέχουν καλύτερη καταγραφή των συμβάντων αφού επιτρέπουν την παρακολούθηση των ενεργειών και καταγραφή των γεγονότων.

Τα μειονεκτήματα που παρουσιάζουν είναι τα εξής:

- Είναι δυσκολότερα στην υλοποίηση.
- Επιτρέπουν την είσοδο μονάχα εκείνων των πρωτοκόλλων που έχουν proxy server. Για μια καινούργια υπηρεσία του διαδικτύου δηλαδή θα πρέπει να προστεθεί μια ξεχωριστή πληρεξούσια εφαρμογή.
- Δεν είναι πάντοτε διαφανή προς το χρήστη.
- Η ταχύτητα και η απόδοσή τους δεν είναι τόσο αποδοτική όσο αυτών του επιπέδου δικτύου.




**Εικόνα 4.2.3.2.1 Application Gateways**
**Πηγή:** http://www.brainbell.com/tutorials/Networking/Proxy_Servers.html

### 4.2.3.3 Υβριδικά Συστήματα Ασφαλείας

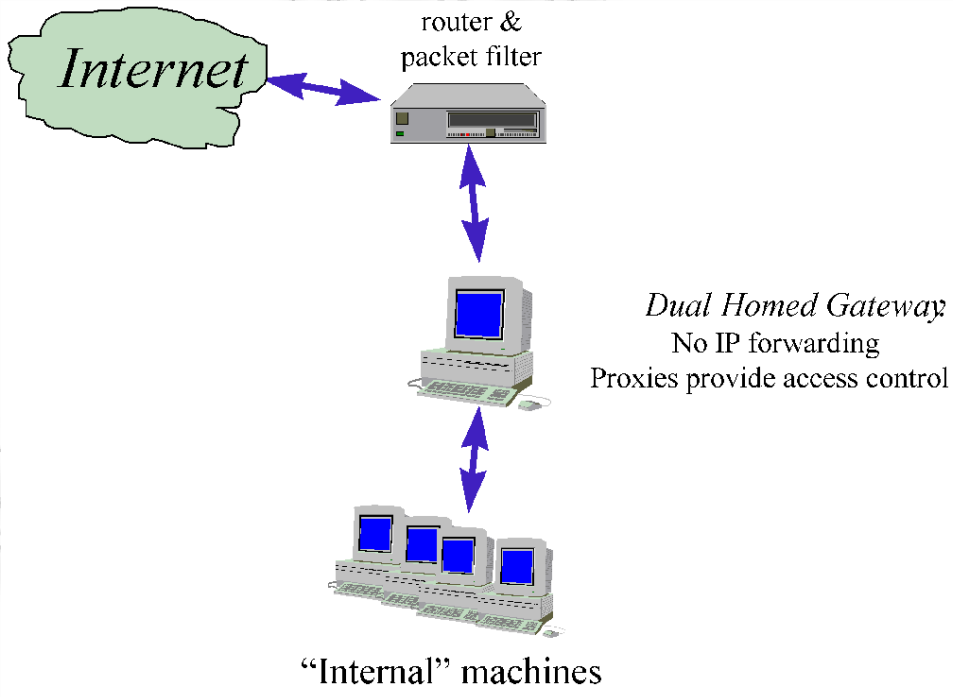
Τα υβριδικά συστήματα ασφαλείας είναι ένας συνδυασμός των δύο αρχιτεκτονικών που προαναφέρθηκαν και υλοποιούνται στην περίπτωση που κάποιος οργανισμός έχει ανάγκη την ασφάλεια που παρέχει το firewall επιπέδου εφαρμογής για κάποιες υπηρεσίες και την ταχύτητα ενός firewall επιπέδου δικτύου για κάποιες άλλες. Σε ένα υβριδικό σύστημα ασφαλείας τα εισερχόμενα πακέτα ελέγχονται πρώτα από το firewall επιπέδου δικτύου και στη συνέχεια είτε απορρίπτονται, είτε συνεχίζουν την πορεία τους προς τον προορισμό τους, είτε περνάνε από κάποιον proxy server για περαιτέρω έλεγχο.

Οι βασικότεροι τύποι τέτοιων συστημάτων ασφαλείας που απαντώνται σήμερα είναι τα Διπλοσυνδεδεμένα Φράγματα Ασφαλείας (Dual-Homed Firewalls), τα Φράγματα Ασφαλείας Υπολογιστή Διαλογής (Screened Host Gateway) και τα Φράγματα Ασφαλείας Υποδικτύου Διαλογής (Screened Subnet Firewalls) [38],[39]

#### 4.2.3.3.1 Διπλοσυνδεδεμένα Φράγματα Ασφαλείας (Dual-Homed Firewalls)

Τα διπλοσυνδεδεμένα firewalls αποτελούνται από έναν υπολογιστή οχυρό που έχει δύο διεπαφές δικτύου, μία με το εσωτερικό δίκτυο και μία με το εν δυνάμει εχθρικό δίκτυο που είναι ως επί το πλείστον το διαδίκτυο. Σε αυτήν την περίπτωση ο υπολογιστής ελέγχει όλα τα πακέτα που μετακινούνται μεταξύ των δύο δικτύων, τα οποία δεν επικοινωνούν άμεσα μεταξύ τους. Τοποθετείται επίσης και ένας δρομολογητής διαλογής μεταξύ του υπολογιστή – οχυρό και του διαδικτύου για να διασφαλίσει ότι τα πακέτα που έρχονται από το διαδίκτυο απευθύνονται με το σωστό τρόπο στον υπολογιστή – οχυρό. Ο bastion host τρέχει proxy servers που προωθούν τα πακέτα των εφαρμογών μεταξύ των δύο δικτύων, έτσι καμία υπηρεσία δεν περνάει από μέσα προς τα έξω και αντίστροφα, εκτός απ' αυτές για τις οποίες υπάρχουν proxy-servers.

Αποτελεί την πιο οικονομική λύση ανάμεσα στα υβριδικά συστήματα ασφαλείας αλλά αποτελεί σημείο δυνητικής αποτυχίας στο δίκτυο που σημαίνει ότι αν κάποιος εισβάλλει σ' αυτό τότε όλο το δίκτυο κινδυνεύει.

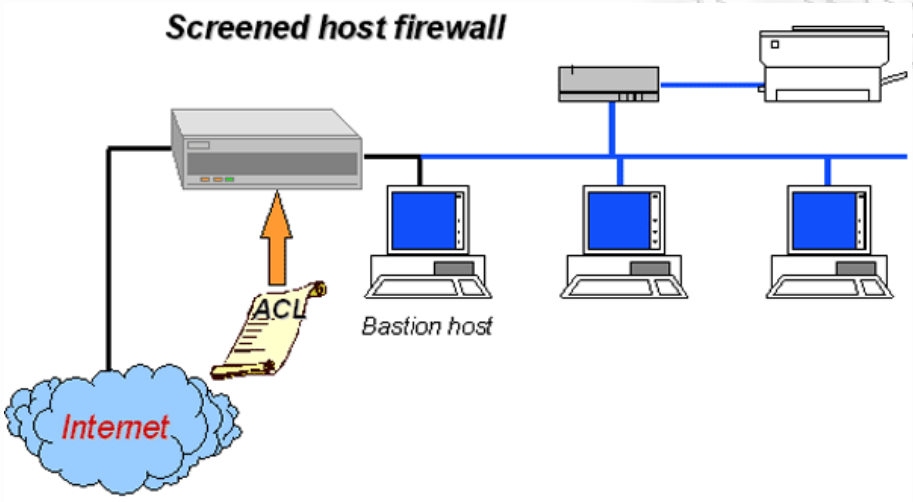



**Εικόνα 4.2.3.3.1.1 Dual Homed Firewalls**
**Πηγή : http://www.boran.com/security/it12-firewall.html**

#### 4.2.3.3.2 Φράγματα Ασφαλείας Υπολογιστή Διαλογής (Screened Host Gateway)

Η αρχιτεκτονική αυτή υλοποιείται όπως ακριβώς γίνεται και με τα διασυνδεδεμένα firewalls, με μόνη διαφορά ότι ο screening router δε στέλνει όλα τα εισερχόμενα πακέτα στον bastion host αλλά με κάποια παραμετροποίηση επιτρέπει τη δίοδο των πακέτων αυτών και προς τα άλλα συστήματα του εσωτερικού δικτύου, οπότε έχει τη δυνατότητα να επιτρέπει και τις υπηρεσίες για τις οποίες δεν υπάρχουν proxy servers να περνάνε στο εσωτερικό δίκτυο. Η προστασία του υπολογιστή – οχυρό από το εξωτερικό δίκτυο γίνεται από το δρομολογητή.

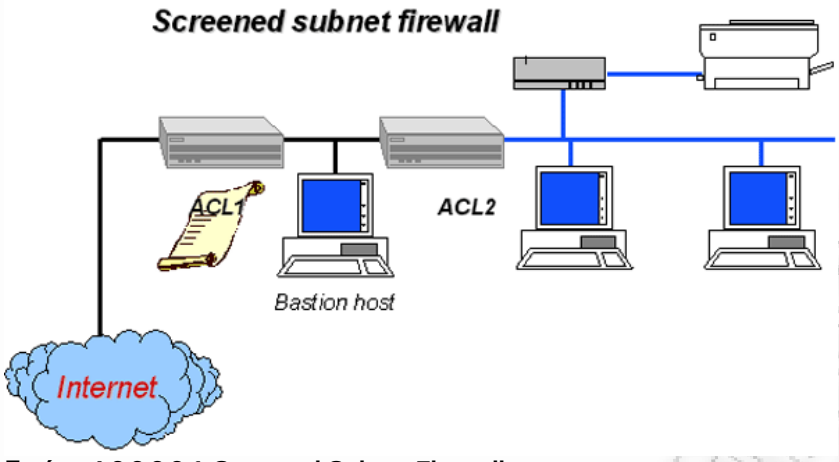
Αυτού του είδους η αρχιτεκτονική παρέχει μεγαλύτερη ασφάλεια από την προηγούμενη που περιγράφτηκε αλλά με σημαντικό μειονέκτημα το γεγονός ότι η ασφάλεια της εξαρτάται από δύο συσκευές που αν για κάποιο λόγο η μία από τις δύο παραβιαστεί τότε όλο το δίκτυο είναι δυνατόν να τεθεί σε κίνδυνο.




**Εικόνα: 4.2.3.3.2.1 Screened Host Gateway**
**Πηγή : http://www.isaca.org/Knowledge-Center/Standards/Pages/IS-Auditing-Procedure-P6-Firewalls1.aspx**

#### 4.2.3.3.3 Φράγματα Ασφαλείας Υποδικτύου Διαλογής (Screened Subnet Firewalls)

Η αρχιτεκτονική αυτή είναι η ασφαλέστερη που μπορεί να χρησιμοποιηθεί και υλοποιείται με τη χρήση δύο δρομολογητών διαλογής που περιβάλλουν τον υπολογιστή – οχυρό δημιουργώντας ένα εσωτερικό υποδίκτυο διαλογής ανάμεσα στο εσωτερικό και εξωτερικό δίκτυο το οποίο ονομάζεται «αποστρατικοποιημένη ζώνη» (DMZ – demilitarized zone). Με αυτόν τον τρόπο επιτυγχάνεται η ασφάλεια του bastion host που είναι μία από τις πιο ευπαθείς συσκευές του δικτύου αφού ο ένας δρομολογητής βρίσκεται μεταξύ του εσωτερικού υποδικτύου και του περιμετρικού υποδικτύου, ενώ ο άλλος βρίσκεται μεταξύ του περιμετρικού υποδικτύου και του εξωτερικού δικτύου. Όπως είναι εμφανές για να μπορέσει να εισβάλλει κάποιος στο εσωτερικό δίκτυο θα πρέπει να παραβιάσει και τις τρεις δικλείδες ασφαλείας.




**Εικόνα 4.2.3.3.3.1 Screened Subnet Firewalls**
**Πηγή : http://www.isaca.org/Knowledge-Center/Standards/Pages/IS-Auditing-Procedure-P6-Firewalls1.aspx**

### 4.2.4 Συμπεράσματα

Η φιλοσοφία των Firewalls έχει αποκτήσει τόσους υποστηρικτές, όσους και επικριτές με τους μεν να υποστηρίζουν ότι αποτελούν μία σίγουρη λύση για την ασφάλεια των δικτύων τους και τους δε να υποστηρίζουν ότι λόγω πολυπλοκότητας και τεχνογνωσίας αποτελούν περισσότερο πρόβλημα για τη λειτουργία των υπολογιστών τους και την εξάπλωση του διαδικτύου, παρά λύση. Η αλήθεια είναι όμως ότι από την πιο σοβαρή επιχείρηση ή δημόσιο οργανισμό μέχρι τον πιο απλό χρήστη η ασφάλεια των προσωπικών δεδομένων είναι πρωτεύουσας σημασίας και αδιαμφισβήτητα μια τεχνολογία firewall αποτελεί ένα πάρα πολύ καλό εφόδιο για την προστασία από κακόβουλες επιθέσεις τρίτων.

## 4.3 Προγράμματα Antivirus

Η απάντηση έναντι στο κακόβουλο λογισμικό έρχεται από τα προγράμματα antivirus, τα οποία έχουν δυο βασικές αποστολές. Πρώτον την ανίχνευση και δεύτερον την εξουδετέρωση των ιών. [40]

Όπως είδαμε και στο προηγούμενο κεφάλαιο οι ιοί ανάλογα με τον τρόπο δράσης τους ταξινομούνται σε κοινούς ιούς, σκουλήκια και δούρειους ίππους. Ο κώδικας καθ' ενός εξ' αυτών ονομάζεται αποτύπωμα του ιού και έχει κάποια συγκεκριμένα χαρακτηριστικά που τον χαρακτηρίζουν μοναδικά. Τα antivirus προγράμματα όταν κάνουν σάρωση ενός υπολογιστή για την εύρεση ιών εντοπίζουν αυτά τα αποτυπώματα και τα αντιπαραβάλουν μ' αυτά που έχουν αποθηκευμένα μέσα στη βάση δεδομένων τους. Όταν βρεθεί κάποιο ταίριασμα τότε ο χρήστης ειδοποιείται και καλείται να πάρει μία απόφαση που θα αφορά είτε στη διαγραφή (delete) του αρχείου που θα έχει μολυνθεί, είτε στην απομόνωσή του (quarantine) είτε στην επιδιόρθωσή του (repair, clean). Η σωστή σειρά ενεργειών εκ μέρους του χρήστη για να αποφύγει κάποια δυσλειτουργία του μολυσμένου προγράμματος είναι πρώτα να προσπαθήσει να επιδιορθώσει το μολυσμένο αρχείο, έπειτα να το απομονώσει και εάν δε μπορεί να τ' αποφύγει τελικά να το διαγράψει.

### 4.3.1 Δυνατότητες Προγραμμάτων Antivirus

Τα προγράμματα αυτά για να μπορέσουν να ανταπεξέλθουν στην ολοένα αυξανόμενη εφευρετικότητα των ιών για επιβίωση, πέρα από την ανίχνευση του χαρακτηριστικού τους κώδικα χρησιμοποιούν και κάποιες άλλες μεθόδους όπως την ευρετική ανάλυση, τον έλεγχο ακεραιότητας και τον έλεγχο συμπεριφοράς.

#### 4.3.1.1 Ευρετική Ανάλυση (Heuristic Analysis)

Η ευρετική ανάλυση είναι μία μέθοδος που έχει υιοθετηθεί από πολλά antivirus προγράμματα και έχει σα στόχο την εύρεση εντολών μέσα από τον κώδικά των αρχείων που θα ήταν πολύ πιθανό να αποτελούν τμήμα κακόβουλου κώδικα πριν ακόμα εκτελεστεί. Οι τεχνικές που χρησιμοποιεί είναι η εξομοίωση αρχείου (File Emulation), η ανάλυση αρχείου (File Analysis) και η γενική ανίχνευση υπογραφής (Generic Signature Detection).

#### 4.3.1.2 Έλεγχος Ακεραιότητας (Integrity Check)

Τα προηγμένα antivirus προγράμματα είναι δυνατόν να χρησιμοποιήσουν τον έλεγχο ακεραιότητας για να εντοπίσουν αν κάποιο αρχείο έχει μεταβάλει το άθροισμα ελέγχου του (checksum). Το checksum είναι ένας μοναδικός αριθμός που υπολογίζεται κατά την αποθήκευση ενός αρχείου στον υπολογιστή και ο μοναδικός τρόπος για να μεταβληθεί είναι να τροποποιηθεί το αρχείο είτε από επιτρεπτή ενέργεια είτε από ιό.

#### 4.3.1.3 Έλεγχος Συμπεριφοράς (Behaviour Blocking)

Αυτή η μέθοδος μοιάζει με την εξομοίωση αρχείου αλλά διαφέρει στο ότι δεν ελέγχεται ο κώδικας του αρχείου αλλά η συμπεριφορά του προγράμματος κατά την εκτέλεσή του. Συγκρίνοντας δηλαδή τη συμπεριφορά του με άλλες ύποπτες καταγεγραμμένες το antivirus πρόγραμμα προσπαθεί σε πραγματικό χρόνο να εκτελέσει την πολιτική ασφαλείας του χρήστη.

### 4.3.2 Συμπεράσματα

Τα antivirus προγράμματα σίγουρα από μόνα τους δεν μπορούν να προστατέψουν επαρκώς την ασφάλεια των υπολογιστικών συστημάτων αλλά εφαρμόζοντας μία πολιτική ορθής χρήσης και σε συνδυασμό με άλλα μέτρα προστασίας όπως τα firewalls που είδαμε παραπάνω μπορούν να δράσουν αποτελεσματικά. Η πολιτική ορθής χρήσης έχει να κάνει με την τακτική τους ενημέρωση (update), την αποφυγή ανοίγματος e-mails από άγνωστες πηγές, τον έλεγχο με πρόγραμμα antivirus κάθε μέσου που πρόκειται να χρησιμοποιηθεί και ειδικότερα τη διατήρηση της ψυχραιμίας διότι κάθε λάθος ενέργεια μπορεί να προκαλέσει ανεπανόρθωτη βλάβη στο υπολογιστικό μας σύστημα.

## 4.4 Συστήματα Ανίχνευσης Εισβολέων (IDS)

Ένα πολύ σημαντικό πρόβλημα που αντιμετωπίζουν οι διάφοροι οργανισμοί που απαρτίζονται από εσωτερικά δίκτυα, είναι ότι θέλουν να γνωρίζουν εάν κάποιος εισβολέας εισχώρησε στο δίκτυο τους. Έως ένα σημείο αυτό το πρόβλημα αντιμετωπίζεται από τα firewalls αλλά όχι ικανοποιητικά αφού υπάρχει η δυνατότητα εκ μέρους του εισβολέα να εξαφανίσει τα ίχνη που άφησε. Τη λύση σε αυτό το πρόβλημα έρχονται να δώσουν τα συστήματα ανίχνευσης εισβολέων (Intrusion Detection Systems, IDS), τα οποία επικουρικά σε συνδυασμό με άλλα μέτρα προστασίας αποτελούν μία καλή λύση προστασίας.[41]

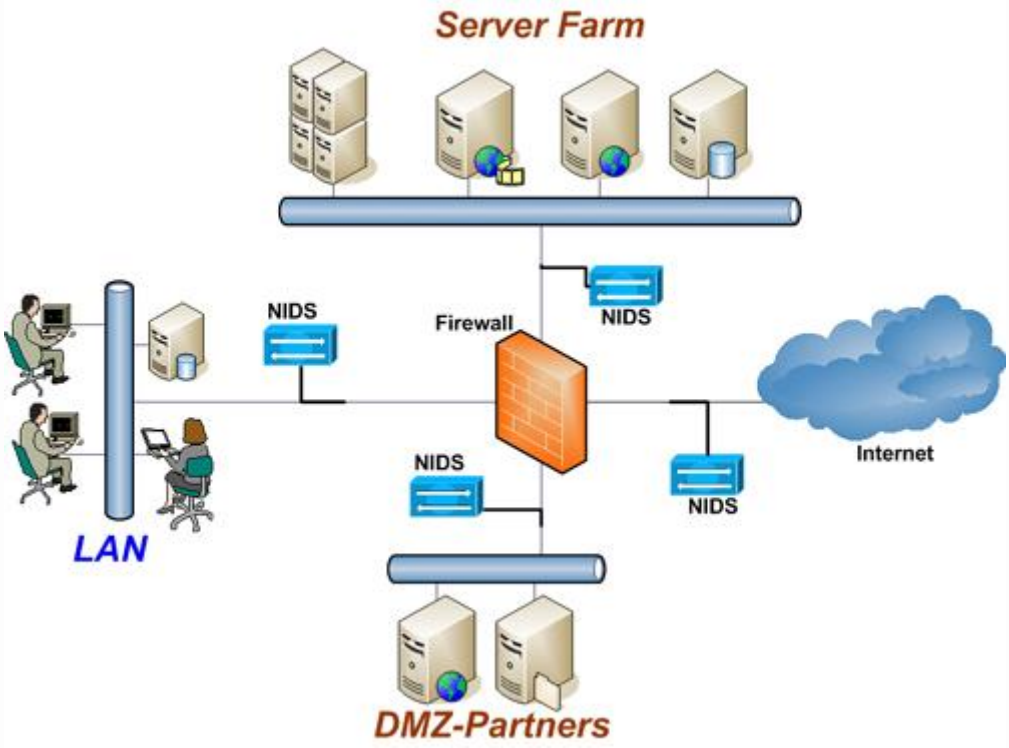
Τα IDS είναι σε μορφή λογισμικού και έχουν σα στόχο την ανάλυση των αρχείων καταγραφής ενός συστήματος, για τον εντοπισμό των ιχνών γνωστών επιθέσεων. Τα συστήματα αυτά μπορούν να κατηγοριοποιηθούν σε παθητικά (Passive) και ενεργητικά (Reactive) ανάλογα με τον τρόπο λειτουργίας τους, σε προσωπικά (host - based) και δικτυακά (NIDS) ανάλογα με το τι καλούνται να προστατέψουν και σε συστήματα ανίχνευσης ταυτότητας (Signatured Based) και συστήματα ανίχνευσης ανωμαλίας (Anomaly Based) ανάλογα με τον τρόπο ανίχνευσης της επίθεσης.[12]

[12] Scarfone, K and Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).*National Institute of Standards and Technology. Chapter 2. 1

Τα παθητικά συστήματα έχουν συνήθως ενημερωτικό χαρακτήρα αφού ανιχνεύουν και καταγράφουν τις αλλαγές που γίνονται στα συστήματα αρχείων για παράδειγμα, χωρίς να είναι σε θέση να τις αποτρέψουν ή να τις αντιμετωπίσουν. Αντιθέτως τα ενεργητικά συστήματα έχουν τη δυνατότητα να αντιμετωπίσουν κάποια απειλή δίνοντας κάποια εντολή για παράδειγμα στο firewall του συστήματος να μπλοκάρει κάποια κακόβουλη εισχώρηση.

Τα host – based συστήματα αφορούν μια συγκεκριμένη συσκευή, κάποιον router ή έναν server για παράδειγμα και παρακολουθούν αποκλειστικά τις επιθέσεις που γίνονται εις βάρος του, ενώ τα δικτυακά συστήματα εγκαθίστανται εντός του δικτύου και παρακολουθούν την εμφάνιση πιθανής επίθεσης όπως είναι η σάρωση θυρών ή η υπερχείλιση του καταχωρητή, σε ολόκληρο το δίκτυο.

Τα συστήματα ανίχνευσης ταυτότητας περιέχουν αποθηκευμένες βάσεις δεδομένων με τις υπογραφές των διαφόρων επιθέσεων κι έτσι όταν αντιληφθούν την εμφάνιση μιας ήδη γνωστής επίθεσης, σημαίνουν συναγερμό ενώ τα συστήματα ανίχνευσης ανωμαλιών στηρίζονται στη διαφορετικότητα των στοιχείων κίνησης ενός δικτύου που προκύπτουν από στατιστικές μετρήσεις σε σχέση με τα αρχικά καθορισθέντα από το διαχειριστή του συστήματος. Τέτοια στοιχεία μπορεί να είναι ο ρυθμός άφιξης και αναχώρησης των πακέτων, η αυξημένη κατανάλωση υπολογιστικών πόρων ή η συμμετρία της κίνησης από και προς το δίκτυο.




**Εικόνα 4.4.1 Συστήματα Ανίχνευσης Εισβολέων**
**Πηγή:** http://www.aecomp.com/ids.html

## 4.5 Ασφάλεια Ηλεκτρονικής Αλληλογραφίας (E-Mail Security)

Το e-mail όπως έχει ήδη αναφερθεί αποτέλεσε την πρώτη εφαρμογή του διαδικτύου που δέχτηκε τόσο μεγάλη απήχηση μέσα σε τόσο μικρό χρονικό διάστημα. Αποδέκτες αυτής της υπηρεσίας έγιναν πέρα από τους απλούς χρήστες και οι οργανωμένες επιχειρήσεις ανταλλάσσοντας εμπιστευτικές πληροφορίες δίχως να γνωρίζουν αν πληρούνται έστω οι ελάχιστες απαιτήσεις ασφαλείας. Ως εκ τούτου, το γεγονός αυτό την κατέστησε ως μία από τις πιο ευάλωτες υπηρεσίες του διαδικτύου που απαιτεί από μέρους του χρήστη ιδιαίτερη προσοχή.

Η εφαρμογή αυτή διατίθεται συνήθως δωρεάν από τους παρόχους ηλεκτρονικών συνδέσεων internet και δίνει τη δυνατότητα στο χρήστη να μπορεί να επισυνάψει οποιουδήποτε τύπου αρχείο μέσα στο κείμενο που θα συντάξει. Κατά την αποστολή ενός μηνύματος αλληλογραφίας από τον αποστολέα προς τον παραλήπτη, ξεκινάει το μήνυμα από τον υπολογιστή του αποστολέα και με τη βοήθεια των πρωτοκόλλων επικοινωνίας SMTP καταλήγει στο διακομιστή αλληλογραφίας (Mail Server) του παρόχου της ηλεκτρονικής σύνδεσης internet (Internet Service Provider ISP) και από εκεί καταλήγει στο διακομιστή αλληλογραφίας του ISP του παραλήπτη. Ο παραλήπτης σ' αυτό το σημείο με τη βοήθεια των πρωτοκόλλων POP (Post Office Protocol) ή IMAP (Internet Message Access Protocol) έχει τη δυνατότητα είτε να αποθηκεύσει την αλληλογραφία του στον υπολογιστή του μέσω κάποιας εφαρμογής είτε να τη διαγράψει απ' ευθείας.

### 4.5.1 Απειλές και τρόποι προστασίας ηλεκτρονικής αλληλογραφίας

Το μοναδικό επίπεδο ασφαλείας που προσφέρει αυτή η υπηρεσία είναι η ταυτοποίηση του χρήστη που πραγματοποιείται κατά την είσοδο του στον mail server με την εισαγωγή του ονόματος χρήστη (username) και τον κωδικό (password) του. Οι απειλές που μπορεί να δεχτεί όμως είναι αρκετές και σίγουρα δεν μπορούν να αποτραπούν από την μοναδική προστασία που παρέχεται κατά την είσοδο στον mail server.

Οι πιο κοινές απειλές που κάνουν την υπηρεσία αυτή ευάλωτη είναι οι εξής:

- Η υποκλοπή της ηλεκτρονικής αλληλογραφίας είτε μέσα από τον ηλεκτρονικό υπολογιστή του χρήστη με τη χρήση κακόβουλου λογισμικού είτε κατά τη μεταφορά της από τον αποστολέα στον παραλήπτη με τη χρήση λογισμικού υποκλοπής. Υποκλοπή μπορεί να γίνει είτε στο περιεχόμενο του μηνύματος είτε στα δεδομένα κίνησης όπως είναι η διεύθυνση του αποστολέα/παραλήπτη, η ημερομηνία αποστολής, το μέγεθος του μηνύματος κ.α. Το πρώτο είδος απειλής μπορεί να αντιμετωπιστεί με κάποιο πρόγραμμα antivirus ενώ το δεύτερο με κάποιο λογισμικό προστασίας δεδομένων (Data Loss Prevention software, DLP) που κυκλοφορεί στην αγορά. [48]
- Η πλαστοπροσωπία του αποστολέα ή κοινώς το email spoofing, όπως περιγράφτηκε σε προηγούμενο κεφάλαιο. Ο απλούστερος και καλύτερος τρόπος για να αποφευχθεί η οποιαδήποτε ζημιά είναι, ο παραλήπτης να μην προβεί σε καμία ενέργεια του ζητηθεί από το email αφαιρώντας το άμεσα από τα εισερχόμενά του με διαγραφή. Αυτό βέβαια, δεν αποτελεί ολοκληρωμένη λύση, γι' αυτό στην αντιμετώπιση του θα πρέπει να προστεθούν κανόνες δικαίου, καθώς και εφαρμογή ορισμένων προηγμένων τεχνικών.[44]
- Τα ενοχλητικά μηνύματα απατηλού περιεχομένου (hoaxes), τα οποία εξαιτίας της τεράστιας διάδοσής τους, επιβαρύνουν τους λογαριασμούς των χρηστών με ένα τεράστιο όγκο άχρηστων μηνυμάτων και θέτουν σε κοινή θέα πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου θέτοντας έτσι τους ιδιοκτήτες τους πιο εύκολα θύματα τέτοιου είδους ενοχλήσεως. Τα μηνύματα αυτά διακρίνονται σε προειδοποιητικά, λόγω του ότι προειδοποιούν το χρήστη για κάποια υποτιθέμενη απειλή (πχ ιό), συμπαράστασης λόγω του ότι παρουσιάζουν κάποια υποθετικά προβλήματα (πχ υγείας) τα οποία ζητούν άμεση κινητοποίηση και εκφοβισμού λόγω του ότι εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι κακό αν δεν προωθήσει το εισερχόμενο μήνυμα και σε άλλους χρήστες. Η λύση σ' αυτού του είδους την απειλή είναι η οριστική και άμεση διαγραφή τους από τη λίστα των εισερχομένων μηνυμάτων του παραλήπτη.[43]
- Η ενοχλητική αλληλογραφία (spam ή junk mail) η οποία έχει ως στόχο το βομβαρδισμό του χρήστη με άχρηστες και ανεπιθύμητες διαφημίσεις προϊόντων και υπηρεσιών. Τα μηνύματα αυτά απαγορεύονται από τις νομοθεσίες των περισσότερων κρατών διότι αποτελούν απειλή για τα προσωπικά δεδομένα του παραλήπτη. Η λύση για την αποτροπή λήψης ή διαγραφής τέτοιων μηνυμάτων, είναι η ενεργοποίηση των φίλτρων που παρέχονται μέσα στις εφαρμογές web mail.[43]
- Η μετάδοση ιών μέσω των συνημμένων αρχείων των ηλεκτρονικών μηνυμάτων, οι οποίοι είναι δυνατόν να μολύνουν τον υπολογιστή του παραλήπτη μόλις αυτός ανοίξει

το συνημμένο αρχείο. Σ' αυτήν την περίπτωση ο παραλήπτης δεν θα πρέπει να ανοίγει μηνύματα που προέρχονται από αποστολέα που δεν γνωρίζει ή και αν ακόμα τον γνωρίζει αλλά έχουν ύποπτο θέμα θα πρέπει να πρώτα να τα ελέγχει με την προεπισκόπηση.[43]

- Απειλή μπορεί να αποτελέσει επίσης το γεγονός ότι οι πάροχοι email εξαιτίας της πολιτικής αντιγράφου εφεδρείας (backup policy) που εφαρμόζουν είναι δυνατόν να πέσουν θύματα υποκλοπής αφού τα αντίγραφα αυτά δεν υφίστανται κανένα είδος κρυπτογράφησης. Η αντιμετώπιση αυτής της απειλής είναι υποχρέωση του παρόχου που οφείλει να ακολουθήσει την πολιτική ασφαλείας περιμέτρου που ορίζει η ΑΔΑΕ. [33].

## 4.6 Κρυπτογράφηση

### 4.6.1 Κρυπτογραφία – Κρυπτογράφηση – Κρυπτανάλυση

Η κρυπτογράφηση (encryption) αποτελεί μία έννοια ευρέως χρησιμοποιούμενη απ' όλα τα σύγχρονα συστήματα ασφαλείας ανά τον κόσμο και αναφέρεται στην τεχνική που χρησιμοποιείται, με τη βοήθεια κάποιων αλγορίθμων, για τη μετατροπή ενός συνόλου δεδομένων από αναγνώσιμη μορφή σε μη αναγνώσιμη, δίνοντας τη δυνατότητα ανάγνωσης μονάχα σε όσες οντότητες έχουν την κατάλληλη εξουσιοδότηση. Η αντίθετη διαδικασία ονομάζεται αποκρυπτογράφηση (decryption) ενώ ο κλάδος της επιστήμης που αποτελεί παρακλάδι της επιστήμης των μαθηματικών και της πληροφορικής και ασχολείται με τη μελέτη, χρήση και ανάπτυξη μεθόδων απόκρυψης πληροφοριών, ονομάζεται κρυπτογραφία (cryptography). Η κρυπτανάλυση (cryptanalysis), παρ' ότι έχει τον ίδιο στόχο με την αποκρυπτογράφηση, διαφέρει στο γεγονός ότι η προσπάθεια απόκτησης της αρχικής μη κωδικοποιημένης πληροφορίας γίνεται από μη εξουσιοδοτημένες οντότητες που δε γνωρίζουν τη μυστική πληροφορία που χρειάζεται για να γίνει η αποκρυπτογράφηση. Κρυπτογράφημα (ciphertext) ονομάζεται το αποτέλεσμα της κρυπτογράφησης.

### 4.6.2 Αναγκαιότητα Χρήσης Κρυπτογράφησης

Η κρυπτογράφηση αποτελεί μια πολύ παλιά υπόθεση [45] που έχει τις ρίζες της πριν από το 2000 π.Χ., όταν το ιερατείο των αρχαίων Αιγυπτίων χρησιμοποιούσε τα ιερογλυφικά για να κρυπτογραφήσει επιγραφές μέσα σε κατακόμβες και συνεχίζεται μέσα στους αιώνες παίρνοντας διάφορες μορφές συνεχώς πιο εξελιγμένες, χωρίς να μπορεί κανείς να φανταστεί μέχρι που θα καταλήξει.

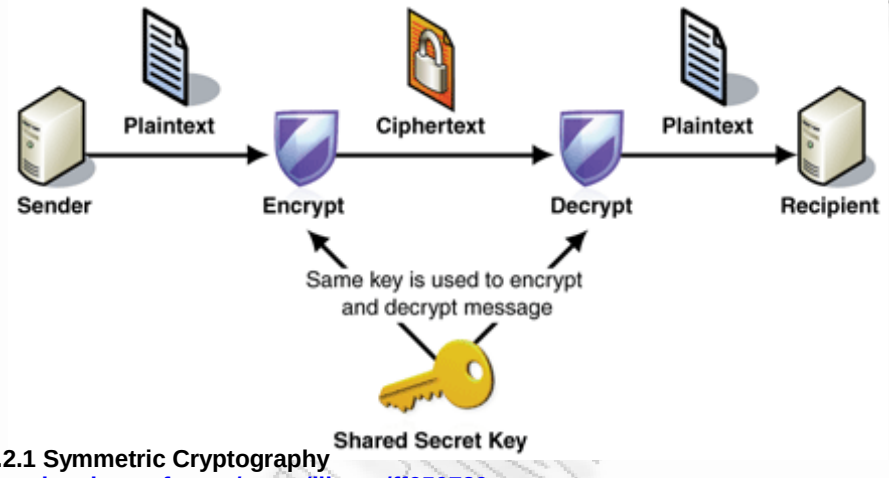
Η χρήση της κρυπτογράφησης σήμερα είναι δυνατόν να εφαρμοστεί από το επίπεδο του στρατού, για τη διαβίβαση άκρως απόρρητων πληροφοριών μέχρι το επίπεδο του απλού χρήστη για την αποστολή ενός mail μέσω διαδικτύου, που μπορεί να περιλαμβάνει εμπιστευτικές πληροφορίες. Οι εφαρμογές της κρυπτογράφησης είναι πολλές και μπορούν να αφορούν ασφαλείς δικτυακές επικοινωνίες, ασφαλή αποθήκευση αρχείων, ασφαλές ηλεκτρονικό εμπόριο ή ασφαλές ηλεκτρονικό ταχυδρομείο.

### 4.6.3 Μέθοδοι Κρυπτογράφησης

Οι βασικές μέθοδοι κρυπτογράφησης είναι δύο. Η συμμετρική (Symmetric Cryptography) και η ασύμμετρη κρυπτογράφηση ή αλλιώς κρυπτογράφηση δημοσίου κλειδιού (Public-Key Cryptography). Η βασική διαφορά ανάμεσα στις δύο αυτές μεθόδους εντοπίζεται στο σύνολο των κλειδιών που χρησιμοποιεί η κάθε μία απ' αυτές κατά την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων. [46]

### 4.6.3.1 Συμμετρική Κρυπτογράφηση (Symmetric Cryptography)

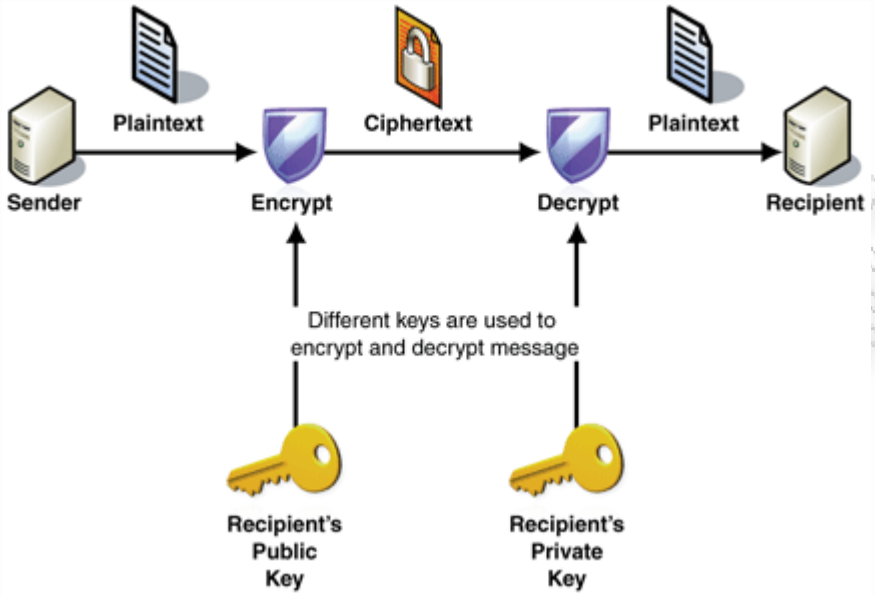
Στη συμμετρική κρυπτογράφηση χρησιμοποιείται ένα κοινό μυστικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση και έχει ως απαραίτητη προϋπόθεση το κλειδί αυτό να το γνωρίζουν αποκλειστικά και μόνο τα επικοινωνούντα μέρη. Η λέξη αποκλειστικά αποτελεί και το κύριο πρόβλημα αυτού του είδους κρυπτογράφησης αφού το μυστικό κλειδί θα πρέπει να μεταδοθεί από τον αποστολέα στον παραλήπτη του μηνύματος με κάποιον ασφαλή τρόπο, ο οποίος δεν μπορεί να είναι κανένας άλλος παρά μόνο η προσωπική συνάντηση. Επειδή αυτό όμως δεν είναι απόλυτα εφικτό, καθιστά τη μέθοδο αυτή αναποτελεσματική με πολλά κενά ασφαλείας. Οι πιο διαδεδομένοι συμμετρικοί αλγόριθμοι είναι ο Data Encryption Standard (DES), ο triple-DES, ο International Data Encryption Algorithm (IDEA) και η σειρά RC2, RC4, RC5.




**Εικόνα 4.6.2.2.1 Symmetric Cryptography**
**Πηγή:** http://msdn.microsoft.com/en-us/library/ff650720.aspx

### 4.6.3.2 Ασύμμετρη Κρυπτογράφηση (Public-Key Cryptography)

Κατά την ασύμμετρη κρυπτογράφηση χρησιμοποιείται ένα ζευγάρι ιδιωτικού και δημόσιου κλειδιού που εξασφαλίζει ότι τα δεδομένα που κρυπτογραφούνται με το ένα κλειδί μπορούν να αποκρυπτογραφηθούν αποκλειστικά και μόνο από το άλλο κλειδί του ζευγαριού. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα και μόνο κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού. Τα κλειδιά έχουν την ίδια φύση και μπορούν να χρησιμοποιηθούν εναλλάξ αλλά σε καμία περίπτωση το ένα δεν μπορεί προκύψει από το άλλο. Ένα «δημόσιο κλειδί» είναι μια σειρά από σύμβολα και αριθμούς και μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσει ένα μήνυμα έτσι ώστε μόνο ο ιδιοκτήτης του αντίστοιχου «ιδιωτικού κλειδιού» να μπορεί να το διαβάσει. Το ζευγάρι κλειδιών βασίζεται στους πρώτους αριθμούς και το μέγεθός τους εξασφαλίζει τη δυσκολία του να αποκρυπτογραφηθεί ένα μήνυμα. Το σημαντικό με τα ζευγάρια κλειδιών είναι ότι το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία οπότε μπορεί να μεταδίδεται χωρίς την ύπαρξη ασφάλειας ενώ το ιδιωτικό κλειδί θα πρέπει να χρησιμοποιείται μόνο από τον ιδιοκτήτη του και να μη μεταδίδεται ποτέ. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να αναζητήσει το δημόσιο κλειδί κάποιου χρήστη ή ακόμα και να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό. Αυτού του είδους η κρυπτογράφηση υπερτερεί έναντι της συμμετρικής κρυπτογράφησης στο θέμα της ασφάλειας, αφού δεν απαιτείται η ασφαλής μετάδοση κάποιου κλειδιού μέσω διαδικτύου αλλά μειονεκτεί στο θέμα της ταχύτητας αφού οι αλγόριθμοί που χρησιμοποιεί είναι πολύ βραδύτεροι εξαιτίας της αύξησης των διακινούμενων πακέτων μεταξύ των δύο επικοινωνούντων μερών.Οι πιο διαδεδομένοι ασύμμετροι αλγόριθμοι που χρησιμοποιούνται είναι ο Rivest-Shamir-Adleman (RSA), ο Diffie-Hellmann, ο ElGamal και ο Rabin.




**Εικόνα 4.6.3.2.1 Public-Key Cryptography**
**Πηγή : http://msdn.microsoft.com/en-us/library/ff650720.aspx**

### 4.6.3.2.1 Ιδιωτικό και Δημόσιο Κλειδί

Ας προσπαθήσουμε με τη βοήθεια ενός παραδείγματος να αναλύσουμε πρώτον τον τρόπο με τον οποίο πραγματοποιείται μία ασύμμετρη κρυπτογράφηση και δεύτερον το ρόλο που παίζουν τα κλειδιά σε όλη αυτή τη διαδικασία. Υποθέτουμε λοιπόν ότι θέλουμε να κάνουμε μία εμπορική συναλλαγή μέσω του διαδικτύου χρησιμοποιώντας την πιστωτική μας κάρτα όπου ως γνωστόν επιβάλλεται η ανταλλαγή των δεδομένων να είναι κρυπτογραφημένη. Για να επιτευχθεί λοιπόν η κρυπτογράφηση αυτών των δεδομένων, θα πρέπει να χρησιμοποιηθεί το δημόσιο κλειδί του διαδικτυακού μαγαζιού, που παρέχεται σ' εμάς, μέσω του πιστοποιητικού (βλέπε επόμενο κεφάλαιο) του ηλεκτρονικού καταστήματος. Σε πρώτη φάση με τη χρήση του δημοσίου κλειδιού του κρυπτογραφούνται τα δεδομένα που θα αποσταλούν από εμάς, οπότε παράγεται το κρυπτογραφημένο μήνυμα που θα ταξιδέψει μέσα στο διαδίκτυο. Έπειτα το διαδικτυακό μαγαζί θα αποκρυπτογραφήσει το μήνυμά μας χρησιμοποιώντας το ιδιωτικό κλειδί του και θα επανακτήσει τα αρχικά δεδομένα που του αποστείλαμε. Το γεγονός ότι, το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα ή το αρχείο το γνωρίζει μονάχα το ηλεκτρονικό κατάστημα, εξασφαλίζει ότι το μήνυμα ή το αρχείο δεν μπορεί να παρακολουθείται ή και να αλλοιώνεται από κάποιον τρίτο που δεν το κατέχει και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.[53]

### 4.6.3.2.2 Τρόπος Δημιουργίας Κλειδιών

Ποιος είναι όμως ο τρόπος που δημιουργούνται αυτά τα κλειδιά; Η δημιουργία αυτών των κλειδιών είναι εφικτή μέσω των προγραμμάτων κρυπτογράφησης όπου ειδικές συναρτήσεις δέχονται ως είσοδο ένα μεγάλο τυχαίο αριθμό ο οποίος προέρχεται από τυχαία δεδομένα που συλλέγονται από τη συμπεριφορά του χρήστη κατά τη διάρκεια χρήσης του υπολογιστή του όπως για παράδειγμα κινήσεις ποντικιού ή πλήκτρα του πληκτρολογίου που πατήθηκαν και στην έξοδο παράγουν το ζεύγος των κλειδιών [53]


**Εικόνα 4.6.3.2.2.1 Δημιουργία Κλειδιών**
**Πηγή:** http://www.nonpaper.net/security/ssl_asymmetric.html

### 4.6.3.3 Σύγκριση Συμμετρικών και Ασύμμετρων Μορφών Κρυπτογράφησης

Όπως αναφέρθηκε και παραπάνω η συμμετρική κρυπτογράφηση υπερτερεί σε ταχύτητα αλλά υπολείπεται σε θέματα ασφάλειας έναντι της ασύμμετρης κρυπτογράφησης.

Τα σημεία όπου εντοπίζεται η επιβάρυνση της ταχύτητας κατά τις ασύμμετρες κρυπτογραφήσεις είναι τα εξής:[47]

- Υπάρχει καθυστέρηση στη φάση της χειραψίας όπου δημιουργούνται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.
- Υπάρχει σημαντική καθυστέρηση κατά τη διάρκεια της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων με αποτέλεσμα οι υπολογιστικοί πόροι και ο χρόνος που δαπανώνται από το υπολογιστικό σύστημα να είναι μεγάλοι.
- Υπάρχει καθυστέρηση στη φάση της μετάδοσης των κρυπτογραφημένων δεδομένων, δεδομένου ότι αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Τα μειονεκτήματα της συμμετρικής κρυπτογράφησης που αφορούν σε θέματα ασφαλείας είναι τα εξής:

- Το γεγονός ότι για να διαβιβαστεί το μυστικό κλειδί θα πρέπει προηγουμένως να έχει υπάρξει αποκλειστική συνεννόηση μεταξύ των δύο μερών, η οποία σίγουρα δεν μπορεί να γίνει μέσω του διαδικτύου αφού θα είναι πολύ εύκολο να υποκλαπεί.
- Το γεγονός ότι δεν μπορούν να παρέχουν ψηφιακές υπογραφές, οι οποίες δεν μπορούν να αποκηρυχθούν από την πηγή τους.

Η επιλογή της μεθόδου κρυπτογράφησης που θα χρησιμοποιείται εξαρτάται κάθε φορά από διαφορετικούς παράγοντες. Η χρήση για παράδειγμα της συμμετρικής κρυπτογράφησης εντός κλειστού δικτύου που δε συνδέεται με το διαδίκτυο, όπου ο διαχειριστής του μπορεί να μοιράζει αποκλειστικά τα μυστικά κλειδιά, θα μπορούσε να είναι ιδανική λόγω εξοικονόμησης υπολογιστικών πόρων και καλύτερης απόδοσης συστήματος.

Η κρυπτογράφηση δημοσίου κλειδιού εφαρμόζεται κατά τη χρήση του πρωτοκόλλου SSL (Secure Socket Layer) όπως θα δούμε παρακάτω, ώστε να διασφαλίζεται η διαφάνεια στους τελικούς χρήστες. Οι παραπάνω λόγοι καθιστούν το πρωτόκολλο SSL χρήσιμο μονάχα στην περίπτωση όπου χρειάζεται πραγματικά ασφαλής σύνδεση όπως είναι η μετάδοση κωδικών ή αριθμών πιστωτικών καρτών.

### 4.6.4 Απόπειρες Κρυπτανάλυσης

Απόπειρα κρυπτανάλυσης ονομάζεται η επίθεση που μπορεί να γίνει εις βάρος ενός κρυπτογραφήματος. Οι κατηγορίες επιθέσεων είναι οι εξής[13]:

**Επίθεση κρυπτογραφήματος (ciphertext-only)**. Ο επιτιθέμενος γνωρίζει κομμάτι του κρυπτογραφήματος, το οποίο βρίσκεται στην κατοχή του έπειτα από υποκλοπή και προσπαθεί να ανακτήσει το αρχικό κείμενο ή να βρει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Σκοπός αυτής της επίθεσης είναι να βρεθούν διάφορα κλειδιά από τον επιτιθέμενο ώστε να μπορεί να τα χρησιμοποιεί σε μελλοντικές επιθέσεις.

**Επίθεση γνωστού κειμένου (known-plaintext attack)**. Ο επιτιθέμενος εκτός από κομμάτια του κρυπτογραφήματος έχει στην κατοχή του και τα αρχικά κείμενα από τα οποία προέρχονται τα κρυπτογραφήματα. Σκοπός αυτής της επίθεσης είναι να βρεθούν τα κλειδιά της κρυπτογράφησης ή ένας αλγόριθμος που θα μπορεί να παράγει παρόμοια αποτελέσματα ώστε να χρησιμοποιηθούν αντίστροφα.

**Επίθεση επιλεγμένου κειμένου (chosen-plaintext attack)**. Ο επιτιθέμενος σε αυτήν την περίπτωση έχει πρόσβαση σε κομμάτια του κρυπτογραφήματος και στα αντίστοιχα κείμενά τους, όπως επίσης και το πλεονέκτημα του να επιλέξει κάποιο δικό του κείμενο που θα κρυπτογραφήσει, στέλνοντας το σε έναν αλγόριθμο ώστε να παραχθεί νέο κωδικοποιημένο μήνυμα. Σκοπός αυτής της επίθεσης είναι η εύρεση διαφόρων κλειδιών που έχουν χρησιμοποιηθεί για την κρυπτογράφηση όπως επίσης και η φανέρωση περισσότερων πληροφοριών για τα κλειδιά αυτά.

**Επίθεση προσαρμόσιμου επιλεγμένου κειμένου (adaptive-chosenplaintext attack).** Σε αυτήν την περίπτωση ο επιτιθέμενος έχει τη δυνατότητα να πραγματοποιήσει την επίθεση με επιλεγμένο κείμενο αλλά και να τροποποιήσει την επιλογή του βασισμένος στα αποτελέσματα της προηγούμενης κρυπτογράφησης προκειμένου να εντοπίσει γρηγορότερα το κλειδί, με μια εξαντλητική αναζήτηση.

**Επίθεση επιλεγμένου κρυπτογραφήματος (chosen-ciphertext attack)**. Ο επιτιθέμενος μπορεί να επιλέξει τα κρυπτογραφήματα που θα αποκρυπτογραφήσει έχοντας σα στόχο να εντοπίσει το κλειδί αποκρυπτογράφησης ώστε αργότερα να μπορεί να αποκρυπτογραφεί χωρίς να γνωρίζει τον αλγόριθμο κρυπτογράφησης. Ο τύπος αυτός της επίθεσης είναι και ο πιο σημαντικός και εφαρμόζεται συνήθως σε αλγόριθμους δημοσίου κλειδιού.

**Επίθεση προσαρμόσιμου επιλεγμένου κρυπτογραφήματος (adaptive chosen-ciphertext)**. Είναι η αντίστοιχη επίθεση με την επίθεση προσαρμόσιμου επιλεγμένου κειμένου με τη διαφορά όμως ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο κρυπτογράφησης.

## 4.7 Πρωτόκολλο SSL

Τον Ιούλιο του 1994 η Netscape παρουσίασε το πρωτόκολλο Secure Socket Layer (SSL) αρχικά με την έκδοση v.1.0, έπειτα το Δεκέμβριο του 1994 λάνσαρε την έκδοση v.2.0, καταλήγοντας το Νοέμβριο του επόμενου έτους στην έκδοση v.3.0. Η τελευταία έκδοση αποτέλεσε και τη βάση για τη μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security) που χρησιμοποιείται ως επί το πλείστον σήμερα για τη διεκπεραίωση τραπεζικών συναλλαγών μέσω διαδικτύου και τείνει να αντικαταστήσει το SSL. Το SSL πρωτόκολλο χρησιμοποιεί ένα συνδυασμό κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού και σχεδιάστηκε για να προσφέρει ασφάλεια μεταξύ δύο μερών που επικοινωνούν μέσω διαδικτύου, γι' αυτό το λόγο χρησιμοποιείται κατά κόρον στο ηλεκτρονικό εμπόριο. Το πρωτόκολλο παρέχει κρυπτογράφηση των μεταδιδόμενων στοιχείων και χρησιμοποιεί έναν τρίτο φορέα, μια Αρχή έκδοσης πιστοποιητικών (CA), για να αναγνωρίσει το ένα ή και τα δύο άκρα που συναλλάσσονται μεταξύ τους. Ο σκοπός ενός πιστοποιητικού SSL είναι να παρέχει μία ισχυρή απόδειξη της ταυτότητας του ιστοχώρου που συνδέεται ένας χρήστης. Σκεφτείτε για

[13] Abhijit Das,C. E. Veni Madhavan. (2009). *Public- key cryptography: Theory and Practice.*Dorling Kindersley. India. 12-13

παράδειγμα πόση ανασφάλεια θα ένιωθε κανείς αν συνδεόταν με την ιστοσελίδα της τράπεζάς του για τη διεκπεραίωση κάποιου τραπεζικού του λογαριασμού και αντιλαμβανόταν κάποια στιγμή ότι δεν επικοινωνεί με αυτήν αλλά με κάποιον απατεώνα που θα προσπαθούσε να του αποσπάσει ευαίσθητες πληροφορίες ή ακόμα και χρήματα από το λογαριασμό του.

Ο σκοπός του πρωτοκόλλου αυτού είναι να εξασφαλίσει ότι τα στοιχεία που ανταλλάσσονται μεταξύ του φυλλομετρητή του υπολογιστή μας και της ιστοσελίδας που συνδεόμαστε είναι ασφαλή και δεν μπορούν να διαβαστούν ή να αποκρυπτογραφηθούν από έναν τρίτο που μπορεί να παρέμβει σ' αυτή την ανταλλαγή στοιχείων.

Είναι δυνατόν να υποστηρίξει ποικίλους μηχανισμούς κρυπτογράφησης και ψηφιακών υπογραφών και να εξασφαλίσει την ακεραιότητα των δεδομένων εφαρμόζοντας την τεχνική MAC (Message Authentication Codes) ώστε να μη μπορεί να γίνει καμία αλλοίωση της πληροφορίας χωρίς αυτό να γίνει αντιληπτό.

Πότε όμως είναι απαραίτητο να γίνεται χρήση αυτού του πρωτοκόλλου; Η απάντηση είναι, κάθε φορά που γίνεται διακίνηση ευαίσθητων ή μη, δεδομένων προσωπικού χαρακτήρα όπως είναι οι κωδικοί, τα ονόματα, οι διευθύνσεις, οι αριθμοί πιστωτικών καρτών και γενικότερα κάθε είδους πληροφορία που δεν θέλουμε να διαρρεύσει σε κανέναν άλλο παρά μόνο σ' αυτόν που απευθυνόμαστε.

Μία ασφαλής ιστοσελίδα του διαδικτύου που χρησιμοποιεί αυτό το πρωτόκολλο κατά την επικοινωνία της με το φυλλομετρητή του υπολογιστή μας, εμφανίζεται σε αυτόν με τη μορφή "https://" αντί για "http://" και χρησιμοποιεί την πόρτα 443 και όχι την προκαθορισμένη που είναι η 80. [49]

### 4.7.1 Τρόπος λειτουργίας του πρωτοκόλλου SSL

Κατά την πραγματοποίηση μιας σύνδεσης SSL όλες οι επικοινωνίες μεταξύ browser και server και αντίστροφα κρυπτογραφούνται μαζί με:

- το URL του ζητούμενου εγγράφου,
- το περιεχόμενο του ζητούμενου εγγράφου,
- το περιεχόμενο όλων των φορμών που υποβάλλονται,
- τα cookies που αποστέλλονται από τον browser στο server και αντίστροφα,
- τα περιεχόμενα του HTTP header.

Η μόνη πληροφορία που δεν κρυπτογραφείται είναι αυτή που μας δίνει πληροφορίες κίνησης όπως για παράδειγμα ότι ένας συγκεκριμένος server μιλάει με ένα συγκεκριμένο browser.

Για να κατανοήσουμε όμως τον ακριβή τρόπο με τον οποίο λειτουργεί το πρωτόκολλο αρκεί να προσέξουμε τα παρακάτω βήματα:[50]

Ο browser του client αιτείται μια ασφαλή σελίδα (συνήθως https://) και ταυτόχρονα πληροφορεί το server ποια έκδοση SSL χρησιμοποιεί, ποιους αλγόριθμους κρυπτογράφησης υποστηρίζει και γενικά οποιαδήποτε άλλη πληροφορία είναι απαραίτητη στο server για να ξεκινήσει μια σύνδεση SSL (Client hello).

Ο server δέχεται το αίτημα και απαντάει ποια έκδοση SSL και ποιον αλγόριθμο κρυπτογράφησης επέλεξε να χρησιμοποιήσει (Server hello).

Ο server στέλνει το ψηφιακό πιστοποιητικό του, το οποίο τον πιστοποιεί στον client.

Ο server ζητάει (προαιρετικά) το πιστοποιητικό του client για να τον πιστοποιήσει.

Ο client στην περίπτωση που ζητηθεί το πιστοποιητικό του, το στέλνει αλλιώς προχωράει στο επόμενο βήμα.

Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν παρουσιαστεί κάποιο πρόβλημα κατά την πιστοποίηση και αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL

ακυρώνεται. Εάν η πιστοποίηση του server όμως πραγματοποιηθεί χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.

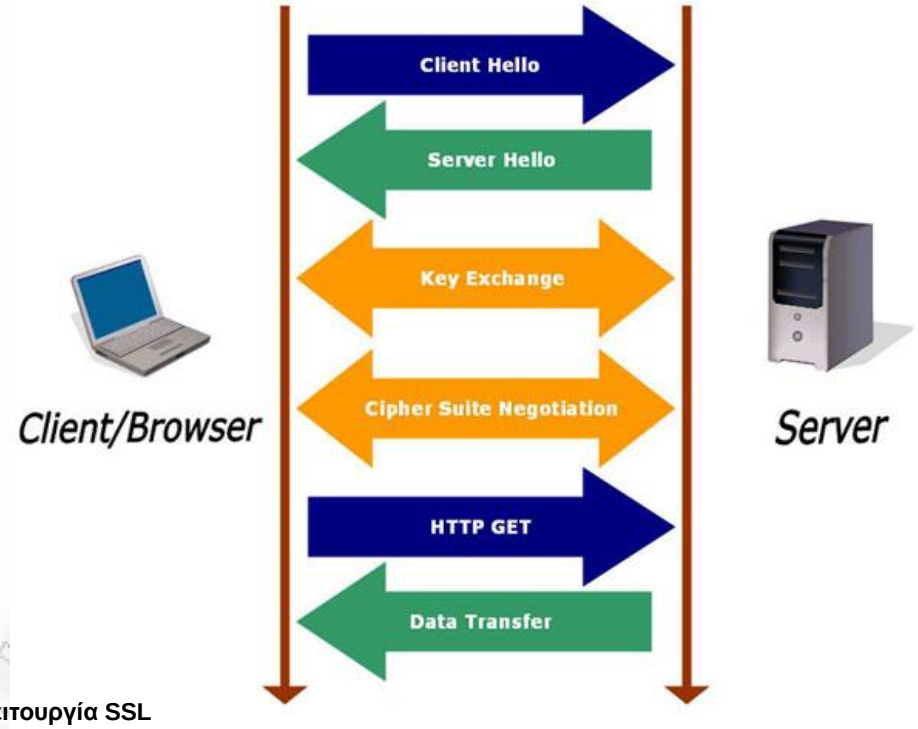
Έπειτα ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης που έχει ήδη επιλεγεί και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει.

Στην συνέχεια ο server κάνει χρήση του ιδιωτικού του κλειδιού για να αποκρυπτογραφήσει το μήνυμα που περιλαμβάνει το συμμετρικό κλειδί το οποίο θα χρησιμοποιηθεί για τη μετέπειτα σύνδεση.

Ο client στέλνει ένα μήνυμα στον server με το οποίο τον ενημερώνει ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

Ο server στέλνει ένα μήνυμα στον client με το οποίο τον ενημερώνει ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

Μετά και απ' αυτό το βήμα η χειραψία έχει πλέον ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν ο client και ο server είναι κρυπτογραφημένα.[49]




**Εικόνα 4.7.1.1 Λειτουργία SSL**
**Πηγή : https://ssl.trustwave.com/support/support-how-ssl-works.php**

### 4.7.2 Η Αρχιτεκτονική του SSL

Το SSL πρωτόκολλο τοποθετείται στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς, δεν εξαρτάται από την ύπαρξη του TCP/IP[14] και τρέχει κάτω από τα πρωτόκολλα εφαρμογών HTTP[15], FTP[16] και TELNET[17] (εικόνα 4.7.2.1)

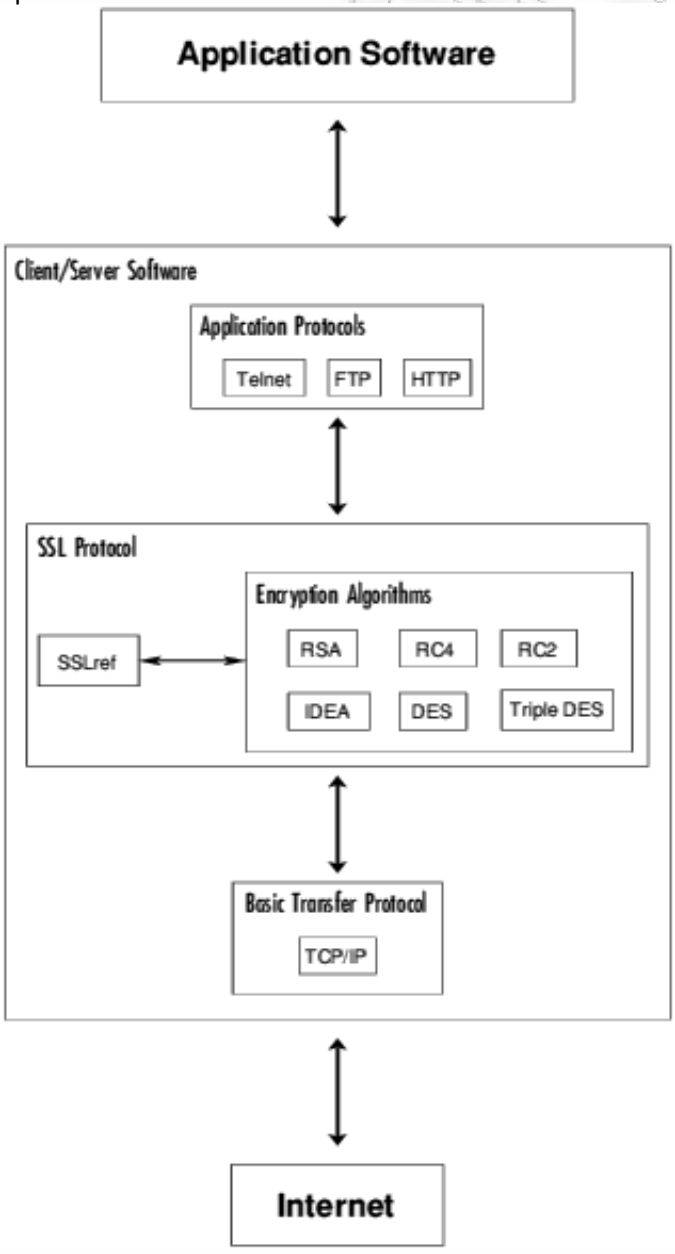
[14] Transmission Control Program / Internet Protocol είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων.

[15] HyperText Transfer Protocol είναι η κύρια μέθοδος που χρησιμοποιούν τα πρωτόκολλα του Παγκοσμίου Ιστού για να μεταφέρουν δεδομένα ανάμεσα σε έναν server και ένα client

[16] File Transfer Protocol, είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα υπολογιστών όπου ένας πελάτης μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα, κατέβασμα, μετονομασία ή διαγραφή αρχείων στον server

Το SSL λειτουργεί επί πρόσθετα στην υπάρχουσα δομή του OSI[18] χωρίς να παίρνει τη θέση κάποιου άλλου πρωτοκόλλου. Είναι σημαντικό κάθε νέο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το OSI μοντέλο, έτσι ώστε να μπορεί εύκολα να αντικαταστήσει κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο όπως είναι για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογών, πάνω από το SSL.

Το SSL πρωτόκολλο χρησιμοποιεί μία μεγάλη ποικιλία κρυπτογραφικών αλγορίθμων όπως: ο DES (Data Encryption Standard), ο DSA (Digital Signature Algorithm), ο KEA (Key Exchange Algorithm, αλγόριθμος που χρησιμοποιείται από την αμερικανική κυβέρνηση για ανταλλαγή κλειδιών), ο MD5 (Message Digest), ο RC2 και ο RC4, ο RSA, ο SHA-1 (Secure Hash Algorithm), ο SKIPJACK και ο Triple DES.




[17]TELecommunication NETwork είναι ένα πρωτόκολλο επικοινωνίας υπολογιστών δικτύου όπου ένας απομακρυσμένος χρήστης μπορεί να "ελέγχει" κάποιον υπολογιστή σαν να ήταν καθισμένος στο τερματικό του.

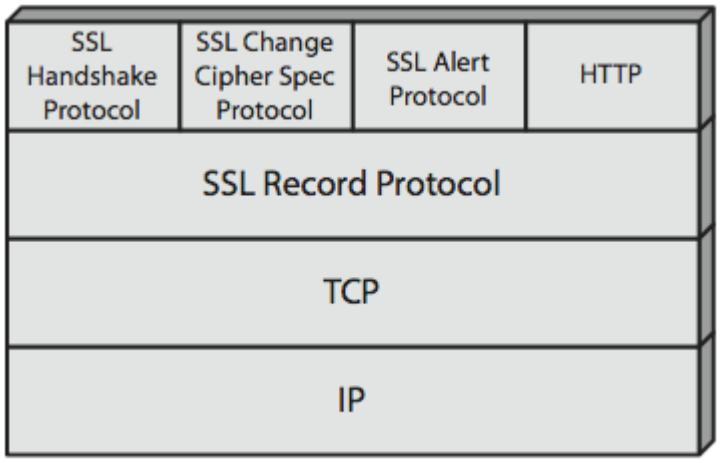
[18] Open System Interconnection γνωστό ως μοντέλο των επτά επιπέδων

**Εικόνα 4.7.2.1 Αρχιτεκτονική SSL**
**Πηγή:** http://www.islab.demokritos.gr

Το SSL δεν είναι ένα πρωτόκολλο αλλά ένας συνδυασμός δύο επιπέδων πρωτοκόλλων. Το ένα επίπεδο είναι το SSL Record Protocol και το άλλο επίπεδο περιλαμβάνει μια τριάδα πρωτοκόλλων όπως:[50]

- το Πρωτόκολλο χειραψίας (Handshake Protocol),
- το Πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας (Change Cipher Spec Protocol) και
- το Πρωτόκολλο προειδοποίησης (Alert Protocol).

Ας δούμε όμως τη λειτουργία καθ' ενός πρωτοκόλλου ξεχωριστά.




**Εικόνα 4.7.2.2 : Αρχιτεκτονική τοποθέτηση του SSL Protocol**
**Πηγή :** http://technet.microsoft.com/en-us/library/cc767139.aspx

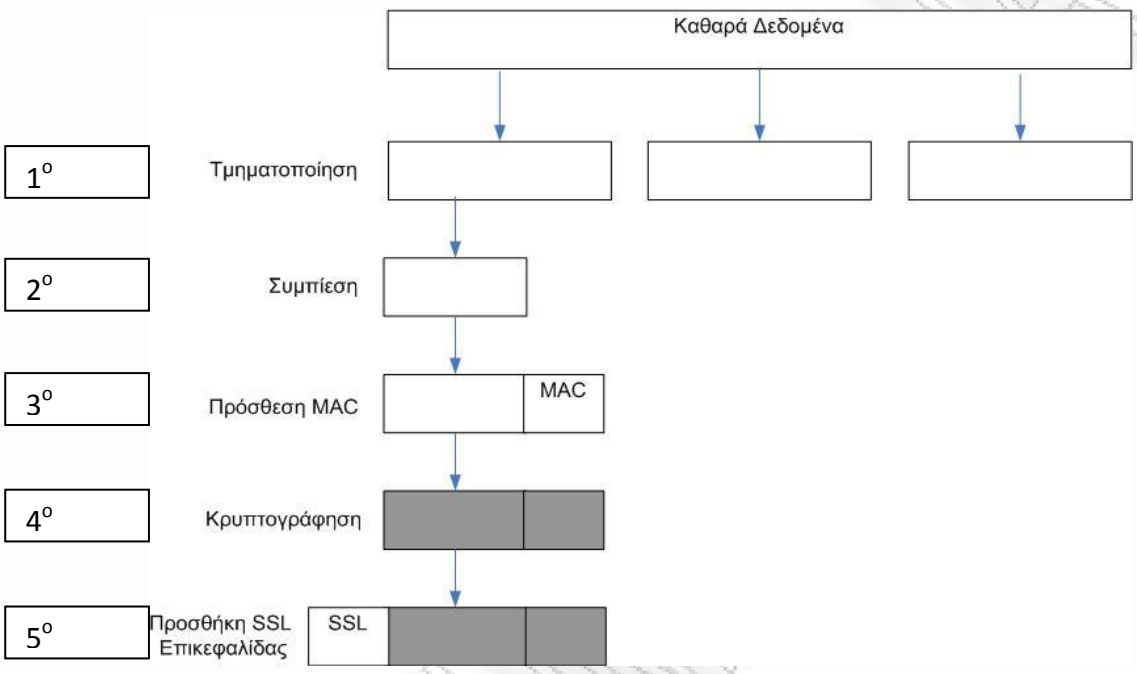
### 4.7.2.1 SSL Record Protocol

Το συγκεκριμένο πρωτόκολλο παρέχει δύο υπηρεσίες όταν πρόκειται για SSL συνδέσεις. **Εμπιστευτικότητα** και **ακεραιότητα** μηνύματος. Για τη μεν πρώτη το Handshake Protocol ορίζει ένα κοινό μυστικό κλειδί, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων του SSL και για τη δε δεύτερη, ορίζει ένα κοινό μυστικό κλειδί που χρησιμοποιείται για τη δημιουργία του message authentication code (MAC) όλων των μηνυμάτων που ανταλλάσσονται.

Στο παρακάτω σχήμα (σχήμα 4.7.2.1.1)φαίνεται η λειτουργία του SSL Record Protocol βήμα προς βήμα.

Στο πρώτο βήμα γίνεται η τμηματοποίηση κάθε μηνύματος υψηλότερου επιπέδου σε εύχρηστα blocks των 214 bytes ή λιγότερο. Έπειτα, στο δεύτερο βήμα, γίνεται προαιρετικά συμπίεση. Στο τρίτο βήμα εφαρμόζει ένα MAC πάνω από τα συμπιεσμένα δεδομένα με τη χρήση ενός διαμοιραζόμενου κλειδιού. Στη συνέχεια στο τέταρτο βήμα, το αποτέλεσμα κρυπτογραφείται με τη χρήση συμμετρικής κρυπτογράφησης, στο τελευταίο βήμα του προστίθεται μια επικεφαλίδα SSL που περιλαμβάνει τα εξής στοιχεία: τον τύπο του περιεχομένου, την κύρια έκδοση, τη δευτερεύουσα έκδοση και το συμπιεσμένο μήκος και τέλος μεταδίδει το πακέτο.

Κατά την παραλαβή των πακέτων ακολουθείται η αντίστροφη διαδικασία. Δηλαδή πρώτα αποκρυπτογραφούνται, έπειτα επιβεβαιώνονται, στη συνέχεια αποσυμπιέζονται και στο τέλος επανασυγκεντρώνονται και διανέμονται στους χρήστες των ανώτερων επιπέδων. [47]




**Εικόνα 4.7.2.1.1 : Λειτουργία SSL Record Protocol**
**Πηγή : http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/tls/tls.html**

### 4.7.2.2 SSL Handshake Protocol

Αυτό το πρωτόκολλο είναι το πιο περίπλοκο πρωτόκολλο από τα χρησιμοποιούμενα στις SSL συνδέσεις. Εκτελεί κάποιες εργασίες όπως είναι: η αρχικοποίηση και ο συγχρονισμός των παραμέτρων ασφάλειας, επιτρέπει προαιρετικά στον πελάτη και τον εξυπηρετητή να εξακριβώσουν ο ένας την ταυτότητα του άλλου, να διαπραγματευτούν τον αλγόριθμο κρυπτογράφησης, το MAC και τη μέθοδο συμπίεσης, και να δημιουργήσουν ένα κύριο μυστικό κλειδί (master secret key), από το οποίο μπορούν να προκύψουν τα διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων. Μετά την εκτέλεση του SSL Handshake Protocol αρχίζει η μεταφορά των δεδομένων από το SSL Record Protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας.

### 4.7.2.3 SSL Alert Protocol

Το SSL Alert Protocol χρησιμοποιείται για να μεταφέρει προειδοποιήσεις (alerts) μέσω του SSL Record Protocol. Οι προειδοποιήσεις περιλαμβάνουν μηνύματα προβλημάτων και λαθών που αφορούν στη σύνδεση και στη μετάδοση των μηνυμάτων μεταξύ δύο ομότιμων οντοτήτων. Με τον τρόπο αυτό ειδοποιεί το SSL να διακόψει τη σύνδεση ή να προβεί σε άλλες καθοριζόμενες ενέργειες.

### 4.7.2.4 Change Cipher Spec Protocol

Σε αντίθεση με το πρωτόκολλο χειραψίας, το πρωτόκολλο αλλαγής προδιαγραφών κρυπτογραφίας είναι το απλούστερο από τα παραπάνω πρωτόκολλα. Χρησιμοποιείται για την

αλλαγή μιας προδιαγραφής κρυπτογραφίας με μια άλλη η οποία κανονικά αλλάζει στο τέλος μιας SSL χειραψίας. Μπορεί όμως να τροποποιηθεί και σε οποιαδήποτε άλλη στιγμή.

### 4.7.3 Αντοχή του SSL σε Επιθέσεις

Ας δούμε λοιπόν πως αντιδρά το πρωτόκολλο SSL στις ήδη γνωστές μορφές επιθέσεων που είδαμε στο προηγούμενο κεφάλαιο.[49]

#### 4.7.3.1 Βίαιη Επίθεση

Είδαμε ήδη πως αυτή η μορφή επίθεσης χρησιμοποιεί έτοιμες λίστες με κωδικούς που έχουν σα στόχο την εύρεση του κλειδιού κρυπτογράφησης. Επειδή όμως το πρωτόκολλο SSL χρησιμοποιεί αλγόριθμους με κλειδιά μεγέθους 128 bits και να πέσει θύμα βίαιης επίθεσης (brute force attack) θα είναι σχεδόν ακατόρθωτο να προσβληθεί.

#### 4.7.3.2 Επίθεση Επανάληψης

Σ' αυτή τη μορφή επίθεσης είδαμε ότι κάποιος τρίτος κάνει καταγραφή και επανάληψη κάποιου μηνύματος που μεταδίδεται μεταξύ δύο μερών. Το SSL, σ' αυτή την περίπτωση προστατεύεται λόγω του ότι χρησιμοποιεί το αναγνωριστικό connection–id από μέρους του εξυπηρετητή, το οποίο είναι διαφορετικό για κάθε σύνδεση και χρησιμοποιείται με τυχαίο τρόπο.

#### 4.7.3.3 Επίθεση Παρεμβολής

Κατά την επίθεση παρεμβολής είδαμε ότι υπάρχει κάποιος τρίτος που παρεμβάλλεται μεταξύ του πελάτη και του εξυπηρετητή κατά την επικοινωνία τους και κάθε φορά προσποιείται εναλλάξ μία το ένα μέρος και μία το άλλο. Σε αυτήν την περίπτωση πάλι προστατεύεται το SSL λόγω του ότι ζητάει από τον εξυπηρετητή να αποδεικνύει την ταυτότητά του, χρησιμοποιώντας κάποιο έγκυρο πιστοποιητικό του οποίου η τροποποίηση είναι αδύνατη.

## 4.8 Ψηφιακά Πιστοποιητικά

Στον κόσμο του internet οι οικονομικές συναλλαγές που πραγματοποιούνται διαδικτυακά συναντώνται πλέον σε καθημερινή βάση ακόμα και απ' τον πιο απλό χρήστη. Αυτές θα αφορούν είτε στην αγοραπωλησία κάποιου προϊόντος είτε στην επικοινωνία κάποιου χρήστη με την τράπεζά του για τη διεκπεραίωση κάποιου λογαριασμού. Σ' αυτές τις περιπτώσεις η εμπιστοσύνη, πάνω στην οποία στηρίζεται σε μεγάλο βαθμό το internet, δεν είναι αρκετή. Στο διαδίκτυο όπως έχουμε ήδη δει, υπάρχουν πολλοί κακόβουλοι χρήστες που εποφθαλμιούν τον αριθμό της πιστωτικής μας κάρτας ή τα πάσης φύσεως μυστικά μας που διακινούνται διαδικτυακά. Οι επιχειρήσεις πάλι από τη μεριά τους, θέλουν να γνωρίζουν ότι αυτός που στέλνει έναν αριθμό πιστωτικής κάρτας είναι πράγματι αυτός που δηλώνει ότι είναι και όχι κανένας απατεώνας που προσποιείται την ταυτότητα κάποιου άλλου.

Πώς μπορούμε να ξέρουμε όμως ότι έχουμε να κάνουμε με το σωστό άτομο ή με τη σωστή ιστοσελίδα ή ότι κατά τη μεταφορά δεδομένων δεν υπάρχει κάποια παρέμβαση από κάποιον εισβολέα; Ο σημαντικότερος τρόπος αποφυγής του προαναφερθέντος προβλήματος είναι η χρήση των ψηφιακών πιστοποιητικών (digital certificates). Το ψηφιακό πιστοποιητικό που χρησιμοποιεί το πρότυπο X.509 δημιουργήθηκε για να αποτρέψει κάθε τέτοια πιθανότητα.

Μία από τις πιο σημαντικές εργασίες που έχει αναλάβει, είναι να πιστοποιεί την αυθεντικότητα κάποιου web server που χρησιμοποιεί SSL πρωτόκολλο κατά την επικοινωνία του με κάποιο φυλλομετρητή έτσι ώστε ο χρήστης όχι μόνο να αισθάνεται ασφαλής αλλά και να είναι πραγματικά ασφαλής. Αυτού του είδους η ασφάλεια είναι σημαντική κυρίως κατά τη διάρκεια εμπορικών συναλλαγών στο διαδίκτυο.

Τα ψηφιακά πιστοποιητικά μπορούμε να πούμε τουλάχιστον μέχρι σήμερα που αναφερόμαστε σε αυτά, ότι είναι ασφαλή επειδή χρησιμοποιούν πανίσχυρη τεχνολογία

απόκρυψης. Στην πραγματικότητα η ασφάλεια που παρέχουν είναι πιο ισχυρή ακόμη και από τις πραγματικές υπογραφές οι οποίες μπορούν εύκολα να πλαστογραφηθούν. Τα ψηφιακά πιστοποιητικά εκδίδονται είτε δωρεάν από διάφορους οργανισμούς όπως η cacert.org είτε έναντι αμοιβή της τάξης των 350 Ευρώ και πάνω, από ιδιωτικές εταιρίες που ονομάζονται Digital Authorities. Η VeriSign είναι μία απ' αυτές και κατέχει τη μερίδα του λέοντος στην αγορά, αλλά υπάρχουν και άλλες όπως η Thawte Digital Certificate Services, η Digital Signature Trust Co., η Euro Trust A/S, η eSign Australia, η The USERTRUST Network και άλλες, που είναι εξίσου αξιόπιστες.[19]

Μια πάρα πολύ σημαντική προϋπόθεση που θα πρέπει να πληροί ένας Πάροχος Υπηρεσιών Πιστοποίησης είναι η αρχή της «τριτότητας» («thirdness»). Ο νόμος ορίζει ότι ο πάροχος αυτός θα πρέπει να είναι ένας τρίτος, ουδέτερος οργανισμός που να μην συμμετέχει με κανέναν τρόπο στη συναλλαγή και να εμπνέει επιχειρηματική εμπιστοσύνη στις ηλεκτρονικές συναλλαγές. [51]

### 4.8.1 Ο Ρόλος των Ψηφιακών Πιστοποιητικών

Όπως περιγράφηκε παραπάνω, κατά την ασύμμετρη κρυπτογράφηση το σίγουρο είναι ότι μπορεί να επιτευχθεί η εμπιστευτικότητα του μηνύματος που μεταδίδεται, λόγω του ότι το μήνυμα κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη και αποκρυπτογραφείται μονάχα από το αποκλειστικά προσωπικό, ιδιωτικό κλειδί του τελευταίου αλλά δεν θα μπορεί να εγγυηθεί την ταυτότητα του αποστολέα αφού δεν του ζητείται με κάποιον τρόπο η διαπίστευσή του από κανέναν. Για να επιλυθεί αυτό το πρόβλημα λοιπόν θα πρέπει να βρεθεί ένας τρόπος που θα εξασφαλίζει στον παραλήπτη ότι ο αποστολέας δεν είναι πλαστός.

Η λύση σ' αυτό το πρόβλημα έρχεται με τη χρήση των ψηφιακών πιστοποιητικών που λειτουργούν ως εξής:[52]

Μία τρίτη έμπιστη οντότητα που ονομάζεται Αρχή Πιστοποίησης (Certificate Authority, CA) εκδίδει πιστοποιητικά που περιέχουν την ταυτότητα και το δημόσιο κλειδί κάποιου χρήστη και είναι υπογεγραμμένα με το ιδιωτικό κλειδί της πρώτης, έτσι, όταν κάποιος χρήστης θέλει να αποστείλει το δημόσιο κλειδί του, το στέλνει μέσω του πιστοποιητικού του, το οποίο αυτόματα πιστοποιεί την ταυτότητά του λόγω του ότι το εγγυάται η Αρχή Πιστοποίησης που το εκδίδει. Κατά τη λήψη του πιστοποιητικού αυτού από τον παραλήπτη, γίνεται αναγνώριση του δημοσίου κλειδιού της CA οπότε άμεσα συνεπάγεται ότι νόμιμος κάτοχος του δημοσίου κλειδιού που εμπεριέχεται μέσα στο πιστοποιητικό, είναι ο αποστολέας. Ως εκ τούτου το μόνο που χρειάζεται να γνωρίζει ο εκάστοτε παραλήπτης πιστοποιητικών, είναι τα δημόσια κλειδιά των διάφορων Αρχών Πιστοποίησης που υπάρχουν και όχι τα δημόσια κλειδιά όλων των χρηστών, γι 'αυτό το λόγο κάθε φυλλομετρητής έχει ενσωματωμένη μία λίστα με όλες τις κύριες αρχές πιστοποίησης που κυκλοφορούν στην αγορά μαζί με τα δημόσια κλειδιά τους.

Ένα ακόμα πρόβλημα που ανακύπτει βέβαια είναι ότι και πάλι δεν μπορούμε να γνωρίζουμε αν ο ιδιοκτήτης κάποιου ιστοχώρου (πχ καταστήματος) είναι ο πραγματικός διαχειριστής του, όπως επίσης και την ύπαρξη ή μη, νόμιμης εταιρείας πίσω από κάποιον ιστοχώρο. Η λύση σε αυτήν την περίπτωση δίνεται από τα *πιστοποιητικά εκτεταμένης πιστοποίησης/επικύρωσης* (EV Certificates). Στην περίπτωση αυτή, οι αρχές έκδοσης, αναλαμβάνουν πιο δύσκολο έργο σε σχέση με τα κοινά πιστοποιητικά διότι ερευνούν και επιβεβαιώνουν περισσότερα στοιχεία για την εταιρεία/οργανισμό/ιδιώτη που ενδιαφέρεται να αποκτήσει ένα τέτοιο πιστοποιητικό. Τα στοιχεία που ελέγχονται πέρα από την επιβεβαίωση της ιδιοκτησίας του domain name, είναι η λειτουργία και η φυσική παρουσία της εταιρείας του ιδιοκτήτη του website, όπως και η νόμιμη υπόσταση της εταιρείας αυτής, ενώ μπορεί να απαιτηθεί και η επικοινωνία του δικηγόρου ή λογιστή της εταιρείας, με την αρχή έκδοσης. Όπως είναι φυσικό οι αγοραστές τέτοιων πιστοποιητικών καλούνται να πληρώσουν πολύ παραπάνω απ' ότι στα κοινά πιστοποιητικά, εξαιτίας των επιπλέον διαδικασιών και ελέγχων που απαιτούνται για την αυξημένη διασφάλιση που προσφέρουν στους πελάτες τέτοιου ιστοχώρου.

[19] Kahate, A. (2008). *Cryptography and network security*. Second Edition. Tata McGraw-Hili Publishing Company Limited. 216-219

### 4.8.2 Απόκτηση Ψηφιακού Πιστοποιητικού

Η απόκτηση ενός πιστοποιητικού από τον κάτοχο μιας ιστοσελίδας που θέλει να θεωρείται διαπιστευμένη, γίνεται με μια αίτηση (CSR ή certification request) προς μια Αρχή Πιστοποίησης. Η CSR αίτηση που κάνει, είναι ένα ηλεκτρονικό έγγραφο που περιλαμβάνει το όνομα της ιστοσελίδας, το email επικοινωνίας της ιστοσελίδας και κάποιες πληροφορίες που αφορούν τον κάτοχο αυτής. Έπειτα ο πάροχος πιστοποιητικών ζητάει το email επικοινωνίας της ιστοσελίδας αυτής από το δημόσιο καταχωρητή domain name που έχει κάνει την καταχώρηση του ονόματος της συγκεκριμένης ιστοσελίδας και κάνει ταυτοποίηση με το email της ιστοσελίδας που κάνει την αίτηση. Αν δεν υπάρξει κάποιο πρόβλημα κατά την ταυτοποίηση τότε παράγει το ζητούμενο ψηφιακό πιστοποιητικό.[20]

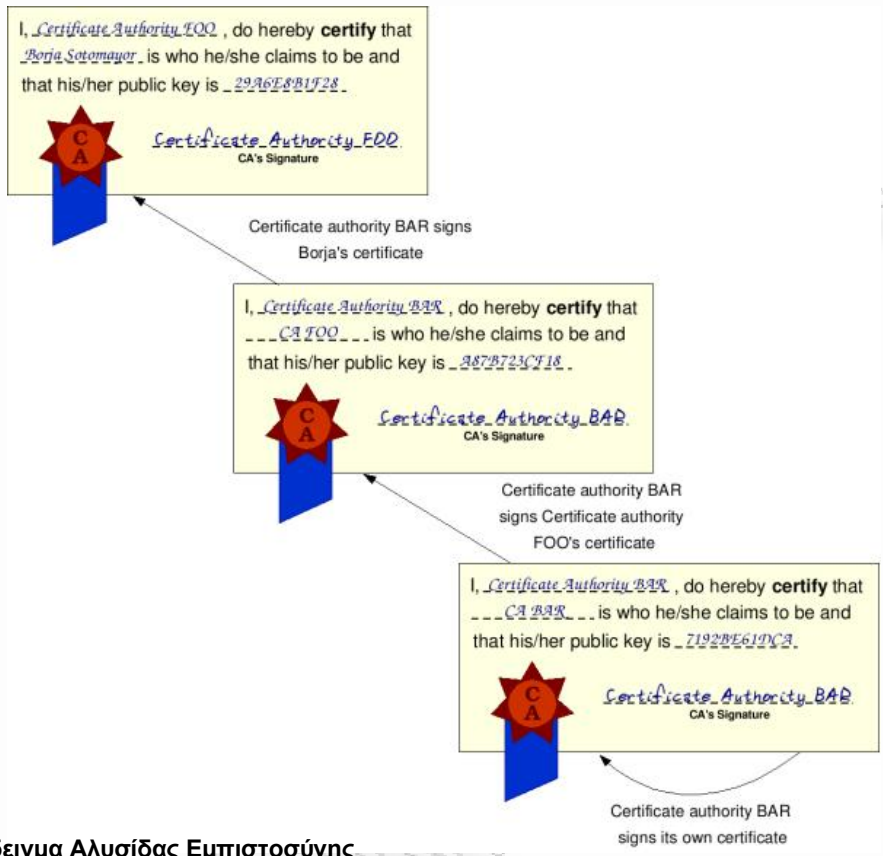
### 4.8.3 Τρόπος Επιβεβαίωσης Πιστοποιητικού από το Χρήστη

Για να εξασφαλιστεί η ασφάλεια[21] που παρέχει ένα ψηφιακό πιστοποιητικό θα πρέπει ο χρήστης κάθε φορά που θα συνδέεται σε κάποιον ασφαλή ιστοχώρο να εξετάζει το πιστοποιητικό ασφαλείας του και να βεβαιώνεται για την ύπαρξη κάποιων στοιχείων πιστοποίησης του ιστοχώρου που συνδέεται, όπως είναι το *ακριβές domain* name ή η διεύθυνση του ιστοτόπου. Στη συνέχεια θα πρέπει να κάνει έλεγχο της διαδρομής των υπογραφών του πιστοποιητικού για το ποιές αρχές πιστοποίησης εγγυώνται την αξιοπιστία του αφού ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, δημιουργώντας με τον τρόπο αυτό μια αλυσίδα εμπιστοσύνης (chain of trust). Η Αρχή Πιστοποίησης που υπέγραψε πρώτη το πιστοποιητικό ονομάζεται root Authority. Η παραπάνω διαδικασία απαιτεί σίγουρα τη σπατάλη αρκετού χρόνου, γι' αυτό και συνήθως αποφεύγεται από το χρήστη με αποτέλεσμα αρκετές φορές να πέφτει θύμα κάποιας καλοστημένης απάτης.

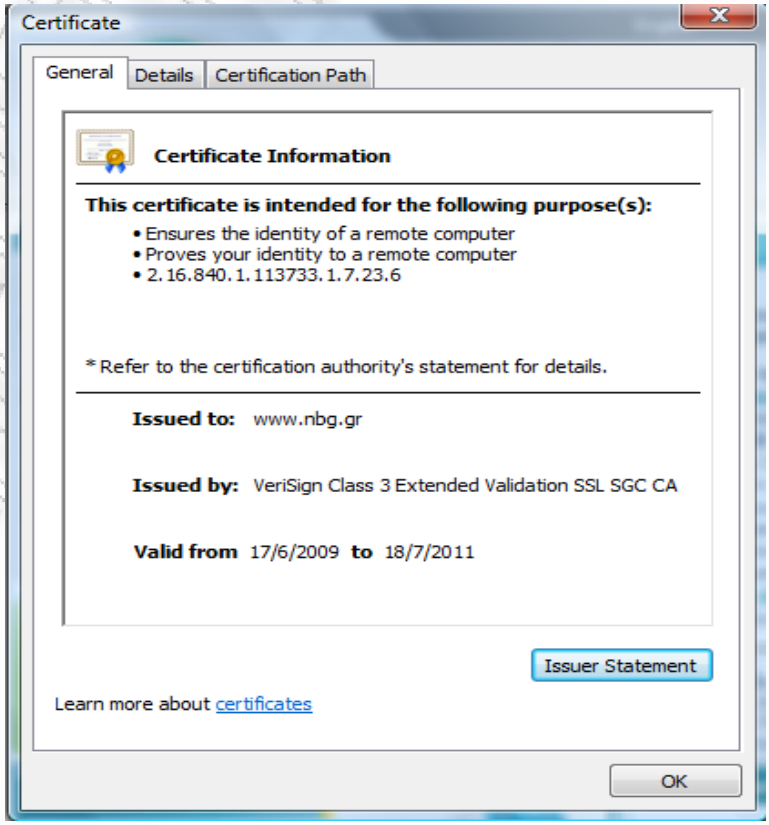
Αν για κάποιο λόγο ο χρήστης ειδοποιηθεί με κάποιο μήνυμα στον υπολογιστή του, που θα τον αποτρέπει να συνεχίσει την επικοινωνία του με την ιστοσελίδα που είναι συνδεδεμένος, αυτό αυτόματα θα σημαίνει πως κάποιο πρόβλημα θα έχει προκύψει με την αξιοπιστία του πιστοποιητικού της. Οι λόγοι που θα έχουν προκαλέσει την εμφάνιση μιας τέτοιας ειδοποίησης μπορεί να είναι διάφοροι όπως για παράδειγμα το γεγονός ότι το πιστοποιητικό θα έχει λήξει, ή ότι θα έχει εκδοθεί για διαφορετική διεύθυνση απ' αυτήν που θεωρητικά έχει συνδεθεί ο χρήστης ή ότι δεν θα είναι υπογεγραμμένο από κάποια γνωστή στον browser αρχή έκδοσης ή τέλος δεν θα είναι έγκυρο. [117]

[20] Kahate, A. (2008). *Cryptography and network security*. Second Edition. Tata McGraw-Hili Publishing Company Limited. 212-215

[21] Kahate, A. (2008). *Cryptography and network security*. Second Edition. Tata McGraw-Hili Publishing Company Limited. 220-226




**Εικόνα 4.8.3.1 Παράδειγμα Αλυσίδας Εμπιστοσύνης**
**Πηγή: http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s04.html**



**Εικόνα 4.8.3.2 Παράδειγμα έγκυρου ψηφιακού πιστοποιητικού**
**Πηγή: http://www.nbg.gr/**

### 4.8.4 Περιεχόμενα Ψηφιακών Πιστοποιητικών Τύπου X.509

Τα πιστοποιητικά τύπου X.509 περιλαμβάνουν τα διαπιστευτήρια του χρήστη τα οποία έχουν ελεγχθεί από την ουδέτερη τρίτη αρχή έκδοσης πιστοποιητικών όπως έχουμε ήδη αναφέρει και περιλαμβάνουν στη σειρά τα κάτωθι στοιχεία[22]:

| | |
|---|---|
| Έκδοση Πιστοποιητικού (Version) | Υπάρχουν 3 εκδόσεις του X.509. Η v.1, η v.2 που περιέχει επιπλέον τα πεδία issuer unique identifier και subject unique identifier και τέλος η v.3 που περιέχει επιπλέον το πεδίο extensions. |
| Serial number | Είναι μοναδικό και χρησιμοποιείται για αναγνώριση του πιστοποιητικού από την Αρχή Πιστοποίησης |
| Η ταυτότητα του αλγορίθμου | Περιλαμβάνει τα ονόματα των κρυπτογραφικών συναρτήσεων που χρησιμοποιήθηκαν με τις σχετικές τους παραμέτρους. |
| Το όνομα της Αρχής Πιστοποίησης | Διάφορα στοιχεία που αφορούν και πιστοποιούν τον εκδότη. |
| Διάρκεια Ισχύος | Περιλαμβάνει τις ημερομηνίες έναρξης και λήξης του πιστοποιητικού. |
| Το όνομα του κατόχου | Διάφορα στοιχεία που πιστοποιούν τον κάτοχο του πιστοποιητικού. |
| Ο αλγόριθμος | Το όνομα του αλγόριθμου που χρησιμοποιεί ο κάτοχος για να διαθέσει το δημόσιο κλειδί του. |
| Παράμετροι | Οι διάφοροι παράμετροι που προσδιορίζουν τη λειτουργία του παραπάνω αλγόριθμου. |
| Το δημόσιο κλειδί | Το δημόσιο κλειδί του κατόχου. |
| Issuer unique identifier | Είναι ένας μοναδικός αριθμός που ενισχύει την αναγνώριση της Αρχής Πιστοποίησης |
| Subject unique identifier | Συνδυάζεται με το όνομα της οντότητας και κάνει μοναδικό το πιστοποιητικό, σε περίπτωση που το όνομα της οντότητας χρησιμοποιείται και για άλλο πιστοποιητικό. |
| Extensions | Επιπλέον απαραίτητα στοιχεία για ειδικές απαιτήσεις. |
| Υπογραφή | Η ψηφιακή υπογραφή με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης |

### 4.8.5 Επίθεση με Χρήση Πλαστού Πιστοποιητικού

Το 2008 παρουσιάστηκε από τον Alex Sotirov στο 25C3 συνέδριο στη Γερμανία [54] ένα επιτυχημένο σενάριο επίθεσης της κρυπτογράφησης δημοσίου κλειδιού που χρησιμοποιεί

[22] Kahate, A. (2008). *Cryptography and network security*. Second Edition. Tata McGraw-Hili Publishing Company Limited. 208-210

ψηφιακά πιστοποιητικά στις ασφαλείς ιστοσελίδες του διαδικτύου. Η επίθεση υλοποιήθηκε με τη δημιουργία ενός πλαστού πιστοποιητικού (Rogue Certificate) που ήταν αποδεκτό από όλους τους φυλλομετρητές ιστοσελίδων χωρίς να γίνεται αντιληπτό κι ως εκ τούτου επέτρεπε στον επιτιθέμενο να μιμηθεί οποιαδήποτε ιστοσελίδα του διαδικτύου χρησιμοποιούσε το SSL πρωτόκολλο.

Η επίθεση αυτή εκμεταλλευόταν μια αδυναμία του MD5 αλγορίθμου που επέτρεπε τη δημιουργία διαφορετικών μηνυμάτων με την ίδια hash value, γνωστή και ως MD5 collision. Με ένα rogue certificate, ο επιτιθέμενος ήταν σε θέση να εκτελεί επιθέσεις ψαρέματος σε τέτοιου είδους ιστοσελίδες χωρίς να γίνεται αντιληπτός.

Από τότε όσες αρχές πιστοποίησης χρησιμοποιούσαν αυτόν τον αλγόριθμο για τη δημιουργία ψηφιακών πιστοποιητικών ανακοίνωσαν πως θα σταματούσαν τη χρήση του και πως θα τον αντικαθιστούσαν με πιο ισχυρούς αλγόριθμους όπως ο SHA1 ή ο SHA2.

## 4.9 Ψηφιακές Υπογραφές

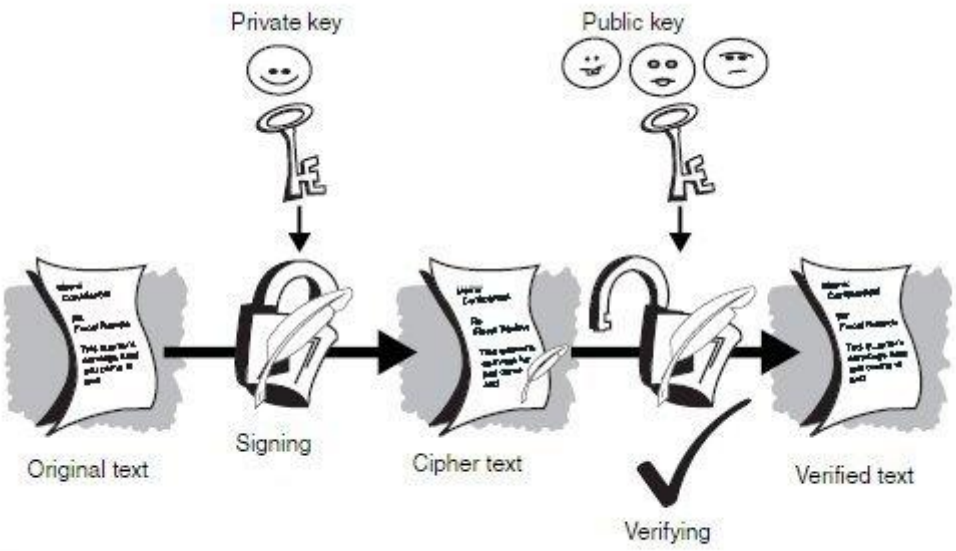
### 4.9.1 Γενικά

Μία ψηφιακή υπογραφή παίζει ακριβώς τον ίδιο ρόλο που παίζει και μία χειρόγραφη υπογραφή στην περίπτωση κανονικών εγγράφων, δηλαδή αυτόν της διασφάλισης της αυθεντικότητας του εγγράφου. Με τον όρο ψηφιακή υπογραφή δεν εννοούμε την ηλεκτρονική μεταβίβαση της ιδιόχειρης υπογραφής αλλά μια μέθοδο που περιλαμβάνει όλα εκείνα τα μέτρα που πρέπει να ληφθούν ώστε κατά τη μετάδοση ενός εγγράφου που γίνεται ηλεκτρονικά να εξασφαλίζεται η ασφάλεια της μετάδοσης του. Τα μέτρα αυτά περιλαμβάνουν τη διασφάλιση της ακεραιότητας του εγγράφου, το γεγονός δηλαδή ότι το έγγραφο παραλαμβάνεται από τον αποδέκτη χωρίς να έχει υποστεί καμία αλλοίωση, την εμπιστευτικότητα της σύνδεσης, του να αποτραπεί δηλαδή η αποκάλυψη του μηνύματος σε μη εξουσιοδοτημένα άτομα, και τη μη αποποίησης ευθύνης, το γεγονός δηλαδή ότι τα επικοινωνούντα μέρη δεν μπορούν να αρνηθούν ότι συμμετείχαν στη συναλλαγή. Στην Ελλάδα, η νομική ισοτιμία της ψηφιακής υπογραφής με την ιδιόχειρη καθιερώνεται με το Π.Δ 150/2001, στο οποίο αναφέρεται ότι κάθε γνωστό πρόσωπο, υπηρεσία ή επιχείρηση αντιπροσωπεύονται από μία μοναδική παγκοσμίως αλλά κάθε φορά διαφορετική ψηφιακή υπογραφή που επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο. Πιο συγκεκριμένα ηλεκτρονική υπογραφή θεωρεί τα “δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.” [55]

### 4.9.2 Υπογραφές Δημοσίου Κλειδιού

Η βασική μορφή των ψηφιακών υπογραφών[23] χρησιμοποιεί την κρυπτογραφία δημοσίου κλειδιού όπως ακριβώς περιγράφτηκε και στο κεφάλαιο 4.6.3.2 με μόνη διαφορά την αντίστροφη χρήση των κλειδιών κρυπτογράφησης, για να γίνει δηλαδή η κρυπτογράφηση χρησιμοποιείται το ιδιωτικό κλειδί του αποστολέα ενώ για να γίνει η αποκρυπτογράφηση από τον παραλήπτη γίνεται χρήση του δημόσιου κλειδιού του αποστολέα. Η σχέση των κλειδιών όπως και στην κρυπτογράφηση δημοσίου κλειδιού είναι τέτοια που και να γνωρίζει κάποιος το δημόσιο κλειδί, του είναι πρακτικά αδύνατον να υπολογίσει το ιδιωτικό.

[23] Kahate, A. (2008). *Cryptography and network security*. Second Edition. Tata McGraw-Hili Publishing Company Limited. 160-167




**Εικόνα 4.9.1.1 Υπογραφές Δημοσίου Κλειδιού**
**Πηγή:** http://www.ece.cmu.edu/~adrian/630-f04/PGP-intro.html

Αυτός ο τρόπος όμως εξαιτίας του τεράστιου όγκου δεδομένων που παρήγαγε είχε σαν αποτέλεσμα να κάνει την επικοινωνία πολύ αργή, γι' αυτό το λόγο χρησιμοποιήθηκε η προσθήκη μιας μονόδρομης συνάρτησης κατακερματισμού (one-way hash function) που παράλλαξε λίγο τον τρόπο λειτουργίας της. Με την εφαρμογή της, αυθαίρετα σε ένα μεγάλο κομμάτι του μηνύματος, παράγεται η σύνοψη μηνύματος (message diggest) που είναι μια σειρά από bits συγκεκριμένου μεγέθους, ανάλογα με τον τύπο του αλγόριθμου που χρησιμοποιείται. Η έννοια μονόδρομη έγκειται στο γεγονός ότι είναι αδύνατον από τη σύνοψη που παράγεται, να μπορέσει κάποιος να εξάγει το αρχικό κείμενο όπως επίσης είναι αδύνατον να παραχθούν δύο ίδιες συνόψεις από δύο διαφορετικά μηνύματα. Ας δούμε όμως αναλυτικά πως γίνεται η δημιουργία και η επαλήθευση της ψηφιακής υπογραφής.

### 4.9.3 Δημιουργία και Επαλήθευση Ψηφιακής Υπογραφής

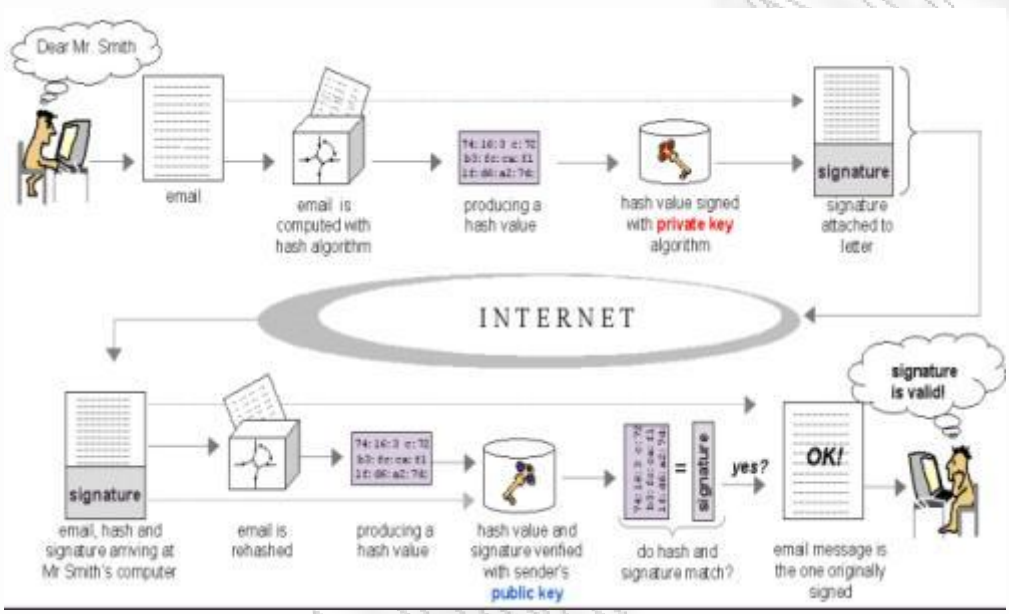
Τα βήματα που ακολουθεί ο αποστολέας για να δημιουργήσει την ψηφιακή του υπογραφή είναι τα εξής:

- Αρχικά ο αποστολέας εφαρμόζει τη συνάρτηση κατακερματισμού επάνω στο μήνυμα και μ' αυτόν τον τρόπο παράγει τη σύνοψη.
- Έπειτα χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει τη σύνοψη οπότε παράγει ένα αποτέλεσμα που καλείται ψηφιακή υπογραφή.
- Τέλος αφού γίνει η προσάρτηση της ψηφιακής υπογραφής πάνω στο αρχικό μήνυμα, μεταδίδονται και τα δύο μαζί προς τον παραλήπτη.

Αντίστοιχα τα βήματα που ακολουθεί ο παραλήπτης για την επαλήθευση της ψηφιακής υπογραφής είναι τα εξής:

- Αρχικά αποσπά την ψηφιακή υπογραφή από το μήνυμα και εφαρμόζει πάνω του την ίδια συνάρτηση κατακερματισμού ώστε να παράγει και αυτός μία σύνοψη η οποία θα πρέπει να είναι ακριβώς ίδια με τη σύνοψη του αποστολέα.

- Έπειτα αποκρυπτογραφεί την ψηφιακή υπογραφή που απέσπασε στο πρώτο βήμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα, με σκοπό να παράγει την αρχική σύνοψη.
- Τέλος συγκρίνει τις δύο συνόψεις ευελπιστώντας να βγουν ίδιες, ειδάλλως θα σημαίνει πως το μήνυμα θα έχει υποστεί αλλοίωση.




**Εικόνα 4.9.3.1 Δημιουργία και Επαλήθευση Ψηφιακής Υπογραφής**
**Πηγή:** http://www.herongyang.com/PKI/SMIME-Digital-Signature-Scheme-for-Email-Messages.html

# 5 Νομικά Μέτρα Προστασίας Προσωπικών Δεδομένων

## 5.1 Γενικά

Λίγα χρόνια μετά το δεύτερο Παγκόσμιο Πόλεμο, αφού αρχίζει να επέρχεται πλέον η ισορροπία και η ευημερία στις ήδη πληγωμένες από τον πόλεμο κοινωνίες, κάνει την εμφάνισή της, μεταξύ των αναπτυσσόμενων χωρών η πληροφορική επανάσταση. Η ανάπτυξή της τεχνολογίας της πληροφορικής γίνεται με τόσο γρήγορους ρυθμούς που οδηγεί στην ανατροπή των κλασικών μεθόδων επικοινωνίας, διαχείρισης και ελέγχου τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Η δημόσια διοίκηση αναβαθμίζεται με εξαιρετικά απίστευτους ρυθμούς και κάθε ιδιωτική επιχείρηση που κάνει ορθολογική χρήση των υπολογιστικών συστημάτων της και του διαδικτύου, βλέπει την απόδοσή της όπως και τα κέρδη της να αυξάνονται κατακόρυφα. [56]

Οι νέες όμως τεχνολογίες και το διαδίκτυο, παράλληλα με τις τεράστιες αυτές αλλαγές, που διευκόλυναν κάθε πτυχή της ανθρώπινης δραστηριότητας, δημιούργησαν και το κατάλληλο περιβάλλον για τη δημιουργία και ανάπτυξη νέων μορφών εγκληματικότητας εξ' αιτίας των αυξημένων δυνατοτήτων συλλογής και επεξεργασίας πληροφοριών που αφορούσαν στην ιδιωτική ζωή του ανθρώπου. [57]. Ήδη από τη δεκαετία του 70' η νέα μορφή εγκληματικότητας που παρουσιάστηκε, οδήγησε σταδιακά πολλές έννομες τάξεις στη θέσπιση ειδικών νομοθετικών διατάξεων καθώς έγινε φανερό ότι οι γενικές διατάξεις για την προστασία της προσωπικότητας δεν επαρκούσαν. Οι διατάξεις αυτές πέρα από χρήσιμες ήταν και αναγκαίες για να διασφαλιστεί ο φιλελεύθερος και δικαιοκρατικός χαρακτήρας της τεχνολογικής ανάπτυξης [56]. Στο νέο αυτό είδος εγκληματικότητας δόθηκαν διάφορα ονόματα[24] που όλα συνοψίζονται στον όρο Ηλεκτρονικό έγκλημα.

## 5.2 Ηλεκτρονικό έγκλημα

Ο όρος Ηλεκτρονικό έγκλημα, αποτελεί μια ευρεία έννοια η οποία εμπεριέχει όλες τις μορφές παραβατικότητας που μπορούν να εκδηλωθούν μέσω ενός ηλεκτρονικού συστήματος. Οι μορφές του είναι ποικίλες και εξαιτίας της εξέλιξης της τεχνολογίας και του διαδικτύου συνεχώς πολλαπλασιάζονται. Μια μεγάλη κατηγορία ηλεκτρονικού εγκλήματος αποτελεί το διαδικτυακό έγκλημα, το οποίο πέρα από την ύπαρξη ηλεκτρονικού υπολογιστή, προϋποθέτει επίσης και την υποχρεωτική σύνδεση του υπολογιστή με το διαδίκτυο. Το διαδικτυακό έγκλημα αποτελεί από μόνο του μεγάλη κατηγορία ηλεκτρονικού εγκλήματος πρώτον διότι μπορεί να πραγματοποιηθεί και από τον πιο απλό χρήστη, που δεν κατέχει κάποιο υψηλό υπόβαθρο πάνω σε θέματα πληροφορικής, άρα απευθύνεται σ' έναν απεριόριστο αριθμό ανθρώπων, δεύτερον εξαιτίας της διεθνούς υπόστασής του αφού μπορεί να τελεστεί σε οποιαδήποτε χώρα ανά πάσα στιγμή και τρίτον διότι μπορεί να εξαπλωθεί αστραπιαία και να προσβάλει τυχαίους αποδέκτες [58].

## 5.3 Συστάσεις του Συμβουλίου της Ευρώπης

Για να αντιμετωπιστεί η διεθνής υπόσταση του διαδικτυακού εγκλήματος, το Συμβούλιο της Ευρώπης έκρινε απαραίτητη την έκδοση τριών συστάσεων (recommendations) ως κατευθυντήριων γραμμών για την υιοθέτηση κοινής αντιμετώπισης από τα κράτη – μέλη της.

Αρχικά εξέδωσε τη σύσταση No R (1989) 9 που αφορούσε στο έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή. Έπειτα εξέδωσε τη σύσταση No R (1995) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών και τέλος εξέδωσε τη σύσταση No R (2001) 8 για την αυτορρύθμιση σε θέματα σχετικά με το περιεχόμενο του διαδικτύου. Το γεγονός όμως ότι αυτές οι συστάσεις δεν είχαν δεσμευτική ισχύ, ώθησε το Συμβούλιο να επιβάλλει νέα πιο αποτελεσματικά μέτρα, έτσι στις 23 Νοεμβρίου του 2001,

[24] Οι ξενόγλωσσοι όροι που συναντώνται στα διάφορα αγγλικά κείμενα και αφορούν στο ηλεκτρονικό έγκλημα είναι: computer crime, communication crime, digital crime, electronic crime, computer related crime.

καταλήγει στη Σύμβαση της Βουδαπέστης [59] για την καταπολέμηση του ηλεκτρονικού εγκλήματος και υποχρεώνει όλα τα κράτη – μέλη, μέσα σ' αυτά και την Ελλάδα, να προσαρμόσουν το περιεχόμενό της, τόσο σε θέματα ποινικού, όσο και Αστικού Δικαίου, στα εκάστοτε νομικά πλαίσια της κάθε χώρας.

### 5.3.1 Η Διεθνής Σύμβαση της Βουδαπέστης

Κάποιες ενδιαφέρουσες διατάξεις της Διεθνούς αυτής Σύμβασης που έχουν να κάνουν με την ασφάλεια στο διαδίκτυο, από ποινικής άποψης είναι οι εξής: [60]

α) Η Παράνομη Πρόσβαση (Illegal Access)

Σύμφωνα με το άρθρο 2 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικό αδίκημα σύμφωνα με την Εθνική του Νομοθεσία, την χωρίς δικαίωμα πρόσβαση στο ηλεκτρονικό σύστημα κάποιου, δηλαδή την παράνομη εισβολή κάποιου τρίτου με οποιοδήποτε τεχνικό τρόπο σε ξένο υπολογιστικό σύστημα. Αυτό σημαίνει ότι κάθε κάτοχος ηλεκτρονικού υπολογιστή θα πρέπει να ορίζει ο ίδιος, τα δικαιώματα χρήσης του υπολογιστή του από τρίτους. Το αντίστοιχο άρθρο του Ποινικού Κώδικα είναι αυτό που αντιστοιχεί στο άρθρο 334 που αφορά στη διατάραξη της οικιακής ειρήνης, έτσι κατ' αντιστοιχία όπως ο δικαιούχος μιας κατοικίας έχει τα δικαίωμα να ορίζει ποιος μπορεί να εισέρχεται ή όχι στην κατοικία του έτσι και ο κάτοχος ενός υπολογιστή έχει το δικαίωμα να επιτρέπει ή όχι την πρόσβαση σε τρίτους στον υπολογιστή του.

β) Η αθέμιτη παγίδευση - υποκλοπή (Illegal Interception)

Σύμφωνα με το άρθρο 3 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικό αδίκημα σύμφωνα με την Εθνική του Νομοθεσία, την εκ προθέσεως παγίδευση ή υποκλοπή με τεχνικά μέσα κάθε είδους δεδομένων που μεταφέρονται μέσω διαδικτύου ή μη όπως το e-mail ή το φαξ. Το αντίστοιχο άρθρο του Ποινικού Κώδικα είναι αυτό που αντιστοιχεί στο άρθρο 370 Α §§1 και 2 που αφορά στην παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας.

γ) Η επέμβαση σε δεδομένα (Data Interference)

Σύμφωνα με το άρθρο 4 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικό αδίκημα σύμφωνα με την Εθνική του Νομοθεσία, την εκ προθέσεως επεξεργασία δεδομένων χωρίς να έχει την απαραίτητη εξουσιοδότηση. Η επεξεργασία αυτή μπορεί να αφορά στην καταστροφή, στη διαγραφή, στη χειροτέρευση, στη μεταβολή ή στην απόκρυψη των δεδομένων. Αυτό δηλαδή που προστατεύεται μ' αυτό το άρθρο είναι η ακεραιότητα και η κανονική λειτουργία των δεδομένων. Το αντίστοιχο άρθρο του Ποινικού Κώδικα είναι αυτό που αντιστοιχεί στο άρθρο 381 που αφορά στη φθορά ξένης ιδιοκτησίας.

δ) Η επέμβαση στο σύστημα (System Interference)

Σύμφωνα με το άρθρο 5 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικό αδίκημα σύμφωνα με την Εθνική του Νομοθεσία, την εκ προθέσεως σοβαρή παρεμπόδιση, χωρίς δικαίωμα λειτουργία ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση, μεταφορά, καταστροφή, διαγραφή, χειροτέρευση, μεταβολή, ή απόκρυψη δεδομένων υπολογιστών. Αυτό δηλαδή που προστατεύεται απ' αυτό το άρθρο είναι η εσκεμμένη δολιοφθορά που μπορεί να υποστεί ένας υπολογιστής ή κάθε συσκευή που είναι συνδεδεμένη μ' αυτόν και επεξεργάζεται αυτομάτως δεδομένα, σύμφωνα με κάποιο πρόγραμμα.

ε) Κακή χρήση συσκευών (Misuse of devices)

Σύμφωνα με το άρθρο 6 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικό αδίκημα σύμφωνα με την Εθνική του Νομοθεσία, την εκ προθέσεως και χωρίς την ύπαρξη κατάλληλης εξουσιοδότησης παραγωγή, πώληση, προετοιμασία για χρήση εισαγωγή, διανομή ή διάθεση μιας συσκευής συμπεριλαμβανομένου προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως για τους σκοπούς διάπραξης οποιουδήποτε από τα αδικήματα των άρθρων 2 έως 5 της Συμβάσεως. Το αντίστοιχο άρθρο του Ποινικού Κώδικα είναι αυτό που αντιστοιχεί στο άρθρο 370 Α §7 και έχει να κάνει με τη διάθεση στο εμπόριο, τη διαφήμιση ή την προσφορά υπηρεσιών που αφορούν στην εγκατάσταση τεχνικών μέσων ειδικά και μόνο για την τέλεση των πράξεων των § 1 και 2 αυτού του άρθρου.

### 5.3.2 Συμπέρασμα

Από τα παραπάνω, μπορούμε πολύ εύκολα να διαπιστώσουμε ότι η διεθνής κοινότητα εδώ και αρκετά χρόνια έχει αναπτύξει μία έντονη ανησυχία όσον αφορά στο ηλεκτρονικό έγκλημα, αποβλέποντας στην δίωξή του είτε με την απ' ευθείας συσχέτιση του με εγκλήματα του κοινού ποινικού κώδικα είτε με την εύρεση και τον εντοπισμό νέων μορφών απειλής που περιορίζονται αποκλειστικά και μόνο στα πλαίσια του κυβερνοχώρου.

Δεδομένης της διαπίστωσης αυτής όπως επίσης και του γεγονότος ότι η ροή των πληροφοριών μέσω του διαδικτύου αποκτά διασυνοριακή διάσταση, καθίσταται επιτακτική η ανάγκη εφαρμογής κανόνων διεθνούς ποινικού δικαίου που δεν θ' αποτελούν όμως τροχοπέδη στην απρόσκοπτη λειτουργία του διαδικτύου. Κύριο χαρακτηριστικό της σύμβασης αυτής αποτελεί το γεγονός ότι καθιερώνει την υποχρέωση εναρμόνισης των εθνικών νομοθεσιών των κρατών – μελών σε θέματα εγκληματικότητας στο διαδίκτυο, αποτελώντας έτσι την πρώτη οργανωμένη απόπειρα ενάντια στο διαδικτυακό έγκλημα.

## 5.4 Ιδιωτικότητα

Η Ιδιωτικότητα (Privacy), αναγνωρίστηκε ως ένα από τα θεμελιώδη δικαιώματα του ανθρώπου σύμφωνα με το άρθρο 12 της Οικουμενικής Διακήρυξης των Ανθρωπίνων Δικαιωμάτων [61] των Ηνωμένων Εθνών στις 10 Δεκ 1948 αναφέροντας συγκεκριμένα ότι "*Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.*". Όπως γίνεται αντιληπτό το ζήτημα της προστασίας του ανθρώπου από την παράνομη επεξεργασία των προσωπικών του δεδομένων αρχίζει να απασχολεί το διεθνές δίκαιο πολύ πριν εμφανιστεί ο προσωπικός ηλεκτρονικός υπολογιστής και το διαδίκτυο μέσα στο σπίτι του καθενός, γεγονός που έκανε πλέον επιτακτική την ανάγκη για θέσπιση ενός νομικού πλαισίου με πολλές πτυχές. Η επίδραση του διαδικτύου εις βάρος της ιδιωτικότητας, χαρακτηρίστηκε ως το πιο σοβαρό θέμα που θα πρέπει να αντιμετωπίσει ο κόσμος του διαδικτύου.

Γιατί όμως να υπάρχει αυτή η διακαής ανησυχία για τις επιπτώσεις στην ιδιωτικότητα, που προκαλείται από την εξόρυξη δεδομένων και το ηλεκτρονικό φακέλωμα που γίνεται μέσω διαδικτύου; Το πρόβλημα έγκειται στο γεγονός ότι ένας κοινός χρήστης είναι πολύ πιθανό να μην είναι καν σε θέση να μπορεί να συνειδητοποιήσει τον τρόπο με τον οποίο γίνεται η υποκλοπή των προσωπικών του δεδομένων και τελικά η εκμετάλλευσή των, με σκοπό το κέρδος. Η παθητικότητα δηλαδή είναι η πιο δόλια πτυχή της διαδικτυακής κατασκοπείας, αφού κάποιος που δεν γνωρίζει αν παρακολουθείται, δεν είναι και σε θέση να αντιδράσει κατάλληλα.

Ας δούμε λοιπόν το θέμα της ιδιωτικότητας σε πιο πρακτικό επίπεδο. Αν κάποιος έμπαινε σ' ένα πραγματικό κατάστημα και ο φύλακας του καταστήματος κατέγραφε τ' όνομά του, οι κάμερες παρακολουθούσαν κάθε του βήμα, καταγράφοντας όποια αντικείμενα κοίταζε ή αγνοούσε, ο υπάλληλος υπολόγιζε πόσο χρόνο ξόδεψε σε κάθε διάδρομο και πριν από κάθε αγορά ο ταμίας του ζήταγε τα προσωπικά του στοιχεία, τότε σίγουρα η παραβίαση της ιδιωτικότητας θα γινόταν αντιληπτή από τον πελάτη και τότε η επιλογή του αν θα επισκεπτόταν ξανά αυτό το κατάστημα θα ήταν δική του. Αντιθέτως στο διαδικτυακό κατάστημα αυτή παραβίαση δε θα γινόταν αντιληπτή αφού όλες οι ενέργειες που περιγράφτηκαν παραπάνω

γίνονται αυτόματα χωρίς να χρειάζεται η συναίνεση του πελάτη. Στο διαδίκτυο όλα αυτά συμβαίνουν στην αφάνεια, χωρίς να γίνονται αντιληπτά έτσι κανείς δεν μπορεί να αποφασίσει αν θέλει να συμμετάσχει ή να εναντιωθεί σ' αυτού του είδους την κατασκοπεία.[62]

Ο αυστηρός προσδιορισμός της ιδιωτικότητας είναι μια πολύ δύσκολη υπόθεση. Υπάρχουν διάφοροι ορισμοί που έχουν δοθεί κατά καιρούς, οι οποίοι μεταξύ άλλων περιλαμβάνουν το δικαίωμα για μια ιδιωτική ζωή, το δικαίωμα να περιοριστεί η δυνατότητα πρόσβασης, το δικαίωμα να ελαχιστοποιηθεί η αδιακρισία και το δικαίωμα για μυστικότητα. Ένας από τους πρώτους ορισμούς που δόθηκαν για να περιγράψουν την ιδιωτικότητα, ήταν αυτός του Louis Brandeis, δικαστικού λειτουργού του ανώτατου δικαστηρίου των ΗΠΑ, το 1890 που έλεγε ότι "Ιδιωτικότητα είναι το δικαίωμα κάποιου να μένει μόνος" [75] και ένας άλλος ο οποίος περιλαμβάνει και την προστασία των προσωπικών δεδομένων, που είναι και το αντικείμενο αναφοράς της παρούσας εργασίας, ήταν αυτός που έδωσε ο Alan Westin το 1967 [63]. «Ιδιωτικότητα είναι η αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων».

Αυτό που πρέπει να γίνει κατανοητό σ' αυτό το σημείο ώστε να μην υπάρχει σύγχυση, είναι η διαφοροποίηση της ιδιωτικότητας (privacy) από την ασφάλεια (security). Για να επιτευχθεί η ασφάλεια σ' ένα υπολογιστικό σύστημα χρησιμοποιούνται κάποιες μέθοδοι που άλλες φορές αποτελούν ασπίδα προστασίας της ιδιωτικότητας και αλλά φορές καθαρή απειλή, όπως για παράδειγμα, η συνεχής καταγραφή των ενεργειών ενός χρήστη σ' ένα δίκτυο υπολογιστών, το οποίο κρίνεται σκόπιμο για τον εντοπισμό κάποιου επίδοξου εισβολέα στο σύστημα, γνωστό και ως το παράδοξο ασφάλειας – ιδιωτικότητας [64]. Πάνω σ' αυτό το πνεύμα κινήθηκαν και τα λόγια του Ευρωπαίου Επόπτη προστασίας δεδομένων P. Hustinx, κατά την ομιλία του στο 14 Συνέδριο προστασίας προσωπικών δεδομένων στο Wiesbaden, που είπε πως η ιδιωτικότητα και η ασφάλεια δεν αντιτάσσονται απαραιτήτως η μία απέναντι στην άλλη, γι' αυτό και θα πρέπει να εξετάζονται παράλληλα, δεδομένου ότι η πραγματική ασφάλεια δεν αποκτάται χωρίς επαρκή μέτρα προστασίας της ιδιωτικότητας, των προσωπικών δεδομένων και άλλων θεμελιωδών δικαιωμάτων. Τόνισε επίσης πόσο σημαντικό είναι, αυτά τα μέτρα προστασίας να απευθύνονται στα πρώιμα στάδια ώστε να δείξουν έγκαιρα το δρόμο, σε νόμιμες και αποδεκτές λύσεις.[92]

Το συμπέρασμα λοιπόν που προκύπτει είναι, ότι πέρα από τους μηχανισμούς ασφαλείας που πρέπει να εφαρμόζονται για την προστασία ενός υπολογιστικού συστήματος, θα πρέπει να υπάρχει και το κατάλληλο νομοθετικό πλαίσιο το οποίο θα προστατεύει τα προσωπικά δεδομένα του ατόμου και γενικότερα την ιδιωτικότητα του, από κάθε είδους απειλή.

## 5.5 Διαχρονική Προστασία της Ιδιωτικότητας σε Διεθνές Επίπεδο

Έπειτα από την Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών του 1948 που είδαμε παραπάνω και αφού έγιναν εμφανής οι δυνατότητες παρακολούθησης και αρχειοθέτησης που έφερνε μαζί της η τεχνολογία του διαδικτύου και της πληροφορίας, ήδη από τις αρχές της δεκαετίας του ΄70, άρχισαν να κάνουν την εμφάνισή τους σε πολλές περιφέρειες της Ευρωπαϊκής Ένωσης, τα πρώτα νομοθετικά κείμενα που είχαν σα θέμα, την προστασία της ιδιωτικής σφαίρας του ατόμου από τη μη εξουσιοδοτημένη επεξεργασία των προσωπικών του δεδομένων. Ο απώτερος σκοπός όλων των νομοθετικών ρυθμίσεων της ΕΕ υπό τη μορφή Οδηγιών και Κανονισμών, ήταν να επιτευχθεί ο συντονισμός μεταξύ των εθνικών νομοθετικών πράξεων όλων των χωρών της ΕΕ, έτσι ώστε η διαβίβαση των δεδομένων από την περιοχή κυριότητας του ενός κράτους στην περιοχή κυριότητας του άλλου κράτους-μέλους να μπορούσε να γίνει ανεμπόδιστα, χωρίς να διαταραχθεί η συνοχή μέσα στην ΕΕ.

Παρακάτω παρατίθενται σε χρονολογική σειρά κάποιες από τις συμβάσεις αλλά και νομοθετικές ρυθμίσεις που έλαβαν χώρα σε διεθνές επίπεδο και αποτέλεσαν το θεμέλιο λίθο των νομοθετικών διατάξεων που ισχύουν μέχρι και σήμερα παγκοσμίως.

Στις 16 Δεκ 1966 η Γενική Συνέλευση των Ηνωμένων Εθνών που πραγματοποιήθηκε στη Νέα Υόρκη υιοθέτησε το Διεθνές Σύμφωνο περί Ατομικών και Πολιτικών Δικαιωμάτων (ΔΣΑΠΔ), το οποίο προέβλεπε το απαραβίαστο της ιδιωτικής ζωής, την ελευθερία της σκέψης, της

συνείδησης, της θρησκείας, της γνώμης και της έκφρασης. Η Ελλάδα κύρωσε το παραπάνω ΔΣΑΠΔ με το νόμο 2462-1997 (ΦΕΚ Α' 25/26.2.97) [74].

Στις 19 Δεκ 1968 η Γενική Συνέλευση των Ηνωμένων Εθνών εκδίδει την απόφαση 2450 με την οποία γίνεται λόγος για τη λήψη μέτρων που θα έχουν σα στόχο την προάσπιση των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών από την παραβίαση τους, που προκαλείται εξαιτίας της τεχνολογικής προόδου των ηλεκτρονικών μέσων. [76]

Στις 12 Οκτ 1970, στο Ομοσπονδιακό κρατίδιο της Έσσης, της πρώην Δυτικής Γερμανίας ψηφίστηκε για πρώτη φορά νόμος που αντιμετώπιζε το ζήτημα της προστασίας των προσωπικών δεδομένων από την ηλεκτρονική επεξεργασία. [77] Έπειτα ακολούθησαν και άλλες χώρες όπως η Σουηδία το 1973, οι ΗΠΑ με το "Νόμο περί Ιδιωτικότητας" (Privacy Act) το 1974 [78], η Γερμανία το 1977, η Γαλλία, η Αυστρία, η Δανία, η Νορβηγία και η Ισλανδία το 1978 και τέλος η Μεγάλη Βρετανία το 1984.[79]

Στις 23 Σεπ 1980 ο Οργανισμός για Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α) (Organisation for Economic Co-operation and Development - OECD) εκδίδει τη σύσταση με τίτλο "Κατευθυντήριες οδηγίες για την προστασία της ιδιωτικής σφαίρας του ανθρώπου και τη διασυνοριακή ροή των προσωπικών δεδομένων" [80] που είχε σα σκοπό να εναρμονίσει τις εθνικές νομοθεσίες των κρατών μελών του με τις κατευθυντήριες οδηγίες που πρότεινε για την προστασία των προσωπικών δεδομένων.

Στις 28 Ιανουαρίου 1981 το Συμβούλιο της Ευρώπης εξέδωσε στο Στρασβούργο τη Σύμβαση 108, που αφορούσε την προστασία του ατόμου από την αυτόματη επεξεργασία των προσωπικών πληροφοριών αποτελώντας το πρώτο δεσμευτικό διεθνές κείμενο που έθετε τις αρχές που θα αποτελούσαν το "σκληρό πυρήνα" της προστασίας των δεδομένων προσωπικού χαρακτήρα και αναφερόταν μεταξύ άλλων, στην ποιότητα της επεξεργασίας, στα δικαιώματα των οντοτήτων που αναφέρονται τα δεδομένα, στην ίδρυση Αρχών, επιφορτισμένων με το καθήκον της εποπτείας των διατάξεων της Σύμβασης και στη θέσπιση κανόνων για τη διασυνοριακή ροή δεδομένων.[81] Η Ελλάδα υπέγραψε τη σύμβαση το 1983 αλλά την κύρωσε 12 χρόνια μετά με το νόμο 2068/1992 (ΦΕΚ Α΄118/9.7.1992) [89]. Λόγω της βαρύτητας που είχε αυτή η σύμβαση, η 28η Ιανουαρίου καθιερώθηκε από το Συμβούλιο της Ευρώπης και την Ευρωπαϊκή Επιτροπή ως Ημέρα Προστασίας Προσωπικών Δεδομένων.

Στις 14 Ιουνίου 1985 υπογράφθηκε στην πόλη Schengen του Λουξεμβούργου η "Σύμβαση Εφαρμογής της Συμφωνίας του Schengen" από το Βέλγιο, τις Κάτω Χώρες, το Λουξεμβούργο, τη Γαλλία και τη Γερμανία, η οποία στόχευε στην προοδευτική κατάργηση των ελέγχων στα εσωτερικά σύνορα[25] των συμβαλλομένων μερών[26] έτσι ώστε να μπορεί να γίνεται ελεύθερη κυκλοφορία των προσώπων και πιο συγκεκριμένα στο άρθρο 7 αναφέρει ότι *τα συμβαλλόμενα μέρη θα πρέπει να παρέχουν αμοιβαία συνδρομή και να συνεργάζονται στενά προκειμένου να εξασφαλίσουν την αποτελεσματική διεξαγωγή των ελέγχων και της επιβλέψεως. Θα μπορούν να προβούν κυρίως στην ανταλλαγή κάθε είδους κατάλληλων και σημαντικών πληροφοριών, με εξαίρεση τα ονομαστικά στοιχεία προσωπικού χαρακτήρα* [82]. Η Ελλάδα προσχώρησε στη συμφωνία στις 6 Νοε 1992 και την κύρωσε με το νόμο 2514/1997 (ΦΕΚ Α 140-26'27.6.1997) [83].

[25] τα κοινά χερσαία σύνορα των συμβαλλομένων μερών, καθώς επίσης και τα αεροδρόμια προκειμένου περί των εσωτερικών πτήσεων και τα θαλάσσια λιμάνια προκειμένου περί των κανονικών συνδέσεων πλοίων μεταφόρτωσης, που προέρχονται ή κατευθύνονται αποκλειστικώς σε άλλο λιμάνι στο έδαφος των συμβαλλομένων μερών, χωρίς να προσεγγίσουν λιμάνια εκτός των εδαφών αυτών.

[26] Μέχρι το 1996 τη σύμβαση την είχαν υπογράψει η Ιταλία, η Ισπανία, η Πορτογαλία, η Ελλάδα, η Αυστρία, η Φιλανδία, η Σουηδία και η Δανία. Η Ιρλανδία και το Ηνωμένο Βασίλειο μέχρι σήμερα διατηρούν τους ελέγχους στις στα σύνορά τους, γι' αυτό λέμε ότι συμμετέχουν μόνον εν μέρει στη Συμφωνία Σένγκεν. Από τις 21 Δεκ 2007, η Εσθονία, η Τσεχία, η Λιθουανία, η Ουγγαρία, η Λετονία, η Μάλτα, η Πολωνία, η Σλοβακία και η Σλοβενία ανήκουν στον χώρο Σένγκεν.

## 5.6 Πρόσφατες Ευρωπαϊκές Νομοθετικές Ρυθμίσεις

### 5.6.1 Οδηγία 95/46/ΕΚ

Στις 24 Οκτ 1995 το Ευρωπαϊκό Κοινοβούλιο εξέδωσε την οδηγία 95/46/ΕΚ "*για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*",[84] η οποία αποτέλεσε φάρο για το μετέπειτα Ευρωπαϊκό αλλά και Παγκόσμιο νομικό πλαίσιο πάνω σε θέματα προστασίας προσωπικών δεδομένων. Ο στόχος αυτής της οδηγίας, όπως προκύπτει από το άρθρο 1, είναι διπλός. Πρώτον στοχεύει στην προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων, και ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και δεύτερον στην εξασφάλιση της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών της ΕΕ για λόγους οικονομικής και κοινωνικής άνθισης όπως επίσης και επιστημονικής και τεχνολογικής συνεργασίας.

Απώτερος σκοπός αυτής της Ευρωπαϊκής οδηγίας ήταν να καθιερώσει ένα βασικό κοινό πρότυπο για την προστασία της ιδιωτικότητας, εξαιτίας της αδυναμίας της σύμβασης 108 να υιοθετηθεί και να εφαρμοστεί από κοινού μεταξύ όλων των κρατών μελών της, προερχόμενη πιθανώς από τη διαφορετική αντιμετώπιση της εννοίας της ιδιωτικότητας.[85] Η Οδηγία προσπαθεί με τη χρήση διαδικασιών και νομοθεσιών όλων των κρατών-μελών που την υπογράφουν, να ορίσει ένα αυστηρό πλαίσιο, πάνω στο οποίο θα στηριχθούν όλες οι νομοθεσίες των μελών της. Στα επιμέρους κεφάλαια της Οδηγίας αναλύεται το πλαίσιο αρχών, θεωρήσεων, κανόνων, λειτουργιών, διαδικασιών, ευθυνών, αλλά και ποινών που διέπει την οποιαδήποτε και με οποιοδήποτε τρόπο, επεξεργασία προσωπικών δεδομένων των φυσικών προσώπων. Τέλος καθορίζεται το πλαίσιο κάτω από το οποίο επιτρέπεται η μεταφορά προσωπικών δεδομένων σε τρίτες χώρες μέσα και έξω από την Ευρωπαϊκή Ένωση. Στη συνέχεια γίνεται μία σύντομη αναφορά στα κύρια άρθρα της οδηγίας, με την ίδια σειρά που εμφανίζονται και στο πρωτότυπο κείμενο.

Στο άρθρο 2 παρατίθενται οι ορισμοί των εννοιών που αναφέρονται και στο νόμο 2472/97, στον οποίο ενσωματώθηκε η παραπάνω οδηγία, όπως ακριβώς είδαμε και στο κεφ 2.2 της παρούσας διατριβής.

Στο άρθρο 3 ορίζεται το πεδίο εφαρμογής της οδηγίας καθώς και οι εξαιρέσεις του. Στις εξαιρέσεις αυτές εμπίπτει πρώτον η επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από το κράτος και δεν εμπίπτει στα πλαίσια των αρμοδιοτήτων της ΕΕ αλλά παραμένει προνόμιο των εθνικών κυβερνήσεων και αφορά τομείς όπως η δημόσια ασφάλεια, η εθνική άμυνα, η ασφάλεια του κράτους και δεύτερον η επεξεργασία προσωπικών δεδομένων που πραγματοποιείται στα πλαίσια προσωπικών ή οικιακών δραστηριοτήτων.

Στο άρθρο 6 αναφέρονται οι βασικοί κανόνες που πρέπει να ακολουθούνται από τα κράτη μέλη όσον αφορά τα προσωπικά δεδομένα όπως:

- Να υφίστανται θεμιτή και σύννομη επεξεργασία
- Να συλλέγονται για σαφής, νόμιμους και καθορισμένους σκοπούς.
- Να είναι κατάλληλα συναφή και όχι υπερβολικά ως προς το σκοπό για τον οποίο συλλέγονται και επεξεργάζονται.
- Να είναι ακριβή και εάν χρειάζεται να ενημερώνονται.
- Να διατηρούνται σε τέτοια μορφή που να καθίσταται δυνατός ο προσδιορισμός της ταυτότητας του προσώπου στο οποίο αναφέρονται.

Στο άρθρο 7 αναφέρονται οι βασικές αρχές της νόμιμης επεξεργασίας των δεδομένων, οι οποίες επιτρέπουν την επεξεργασία μόνο όταν:

- Υπάρχει η συναίνεση του ατόμου στο οποίο αναφέρονται.
- Είναι απαραίτητη για την εκπλήρωση συμβατικής υποχρέωσης.
- Είναι απαραίτητη για την εκπλήρωση νόμιμης υποχρέωσης.
- Είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του ατόμου στο οποίο αναφέρονται.

- Είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση δημόσιας εξουσίας.
- Είναι απαραίτητη για την επίτευξη του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας.

Στο άρθρο 8 θέτονται πολύ αυστηροί κανόνες όσον αφορά την επεξεργασία των ευαίσθητων δεδομένων, που επιτρέπουν την επεξεργασία τους μόνο υπό προϋποθέσεις και εφόσον ισχύουν συγκεκριμένοι λόγοι.

Στα άρθρα 10,11,12,13,14 και 15 ορίζονται τα παρακάτω ατομικά δικαιώματα του υποκειμένου των δεδομένων, τα οποία είναι:

- Το **Δικαίωμα της πληροφόρησης**: Το οποίο προβλέπει την ενημέρωση του προσώπου που υφίσταται τη συλλογή πληροφοριών, από τον υπεύθυνο επεξεργασίας σε θέματα που αφορούν την ταυτότητα του υπευθύνου, το σκοπό της επεξεργασίας καθώς και όποια άλλη πληροφορία θα ήταν απαραίτητη για το σύννομο της επεξεργασίας.
- Το **Δικαίωμα της πρόσβασης**: Το οποίο αφορά το δικαίωμα του υποκειμένου που υφίσταται τη συλλογή πληροφοριών, να έχει ελεύθερη και χωρίς περιορισμούς πρόσβαση και ενημέρωση σε εύλογο χρονικό διάστημα, χωρίς υπερβολική δαπάνη, για το αν έχει υποστεί επεξεργασία δεδομένων που τον αφορά, για πληροφορίες σχετικά με τους σκοπούς επεξεργασίας, για τις κατηγορίες δεδομένων που θα υποστούν επεξεργασία καθώς και για τους αποδέκτες των δεδομένων του.
- Το **Δικαίωμα της εναντίωσης:** Το οποίο αφορά το δικαίωμα του υποκειμένου που υφίσταται τη συλλογή πληροφοριών να αρνηθεί την συλλογή και επεξεργασία των προσωπικών δεδομένων που τον αφορούν για συγκεκριμένους και νόμιμους λόγους σχετικούς με την προσωπική του θέση.
- Το **Δικαίωμα μη συμμόρφωσης σε αυτοματοποιημένες ατομικές αποφάσεις** : Το οποίο αφορά το δικαίωμα του υποκειμένου που υφίσταται τη συλλογή πληροφοριών, να μη συμμορφωθεί με απόφαση που παράγει νομικά αποτελέσματα έναντι αυτού ή το θίγει σημαντικά εφόσον η εν λόγω απόφαση βασίζεται αποκλειστικώς σε αυτοματοποιημένη επεξεργασία που αξιολογεί ορισμένες πτυχές της προσωπικότητάς του, όπως η απόδοσή του στην εργασία, η φερεγγυότητά, η αξιοπιστία, η διαγωγή του κ.λπ

Στα άρθρα 16 και 17 γίνεται λόγος για την ασφάλεια της επεξεργασίας και την τήρηση του απορρήτου των πληροφοριών που υφίστανται τη συλλογή και επεξεργασία έτσι ώστε να είναι δυνατή η αποφυγή τυχόν μη εξουσιοδοτημένης πρόσβασης, καταστροφής, απώλειας, τροποποίησης ή παράνομης μετάδοσης αυτών, ιδίως κατά τη μεσολάβηση και κάποιου είδους επικοινωνίας μέσω δικτύου.

Στα άρθρα 18 έως 21 αναφέρεται η υποχρέωση του υπευθύνου της επεξεργασίας να κοινοποιεί οποιαδήποτε επεξεργασία προσωπικών δεδομένων πρόκειται να πραγματοποιήσει, σε μια Εθνική Αρχή ελέγχου, όπως προβλέπεται από το άρθρο 28 της παρούσας οδηγίας, συμπεριλαμβάνοντας σ' αυτήν διάφορες πληροφορίες που αφορούν τόσο τον ίδιο όσο και τα δεδομένα που πρόκειται να επεξεργαστεί.

Στα άρθρα 22 έως 24 αναφέρονται, το δικαίωμα του υποκειμένου της επεξεργασίας για προσφυγή ενώπιον των αρμοδίων εθνικών δικαστηρίων σε περίπτωση παραβίασης των δικαιωμάτων του καθώς και η ευθύνη και οι κυρώσεις που υφίστανται οι υπεύθυνοι της επεξεργασίας σε περίπτωση που αποδειχθεί η ευθύνη τους για το ζημιογόνο γεγονός.

Στα άρθρα 28 έως 30 τονίζεται η δημιουργία μιας Εθνικής αρχής ελέγχου, υπεύθυνη για την προστασία των φυσικών προσώπων κατά τις διαδικασίες επεξεργασίας, πρόσβασης, καταγραφής και μετάδοσης προσωπικών δεδομένων κάνοντας μία αναλυτική περιγραφή των δικαιωμάτων αλλά και των υποχρεώσεων που θα έχει.

Η Οδηγία 95/46/ΕΚ τέθηκε τελικά σε εφαρμογή απ' όλα τα κράτη – μέλη της ΕΕ στις 24 Οκτωβρίου 1998.

### 5.6.2 Οδηγία 97/66/ΕΚ

Στις 15 Δεκ 1997, η Ευρωπαϊκή Κοινότητα εξέδωσε την Οδηγία 97/66/ΕΚ «περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα» [86]. Η Οδηγία αυτή εκδόθηκε εξαιτίας των ειδικών απαιτήσεων που προέκυψαν από την επεξεργασία προσωπικών δεδομένων στα τηλεπικοινωνιακά δίκτυα και στην ουσία εξειδίκευσε και συμπλήρωσε τις διατάξεις της Οδηγίας 95/46/ΕΚ και στον τηλεπικοινωνιακό τομέα αφορώντας όχι μόνο τα φυσικά πρόσωπα αλλά και τα νομικά. Σύμφωνα με το άρθρο 1 της Οδηγίας αυτής, στόχος της είναι «*η εναρμόνιση των διατάξεων των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως δε το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, καθώς και στην ελεύθερη κυκλοφορία των δεδομένων αυτών και των τηλεπικοινωνιακών εξοπλισμών και υπηρεσιών στην Κοινότητα».* Η Ελλάδα ενσωμάτωσε την παραπάνω Οδηγία στο νόμο 2774/1999 με τίτλο «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»

### 5.6.3 Κανονισμός 45/2001/ΕΚ

Στις 18 Δεκ 2000, το ΕΚ και το Συμβούλιο, εξέδωσαν τον κανονισμό 45/2001 «*σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών*» εξαιτίας της απουσίας νομοθετικών ρυθμίσεων για την περίπτωση επεξεργασίας προσωπικών δεδομένων από τα όργανα και τους οργανισμούς της Κοινότητας που εν γένει θα μπορούσε να αποτελέσουν εμπόδιο στην κυκλοφορία των δεδομένων μεταξύ των εθνικών και κοινοτικών οργάνων [87]. Ο κανονισμός αυτός σύμφωνα με το άρθρο 1 έχει σα στόχο την τήρηση από τα όργανα και τους οργανισμούς της Κοινότητας[27] των κανόνων προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, καθώς και την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ τους ή προς αποδέκτες που υπόκεινται στην εθνική νομοθεσία των κρατών μελών που εφαρμόζουν την οδηγία 95/46/ΕΚ. Ο Κανονισμός αυτός είχε άμεση ισχύ ως εσωτερικό δίκαιο σε όλα τα κράτη μέλη της Κοινότητας.

### 5.6.4 Οδηγία 2002/58/ΕΚ

Στις 12 Ιουλίου 2002 το ΕΚ και το Συμβούλιο, εξέδωσαν την Οδηγία 2002/58, "*Σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)*" [88]. Η συγκεκριμένη Οδηγία οριοθετεί την προστασία της ιδιωτικότητας στο χώρο των ηλεκτρονικών επικοινωνιών όπως επίσης, θεσμοθετεί για πρώτη φορά την προστασία των «έννομων συμφερόντων των προσώπων νομικού δικαίου». Η συγκεκριμένη οδηγία έχει πολύ σημαντικό χαρακτήρα, αφού σχετίζεται με υπηρεσίες τηλεφωνίας, που αποτελούν πολύ διαδεδομένες υπηρεσίες και σημείο σημαντικών παραβιάσεων της ιδιωτικότητας των συνδρομητών. Η παραπάνω Οδηγία κατήργησε και αντικατέστησε[28] την Οδηγία 97/66/ΕΚ, στις 31 Οκτ 2003, εξαιτίας της ραγδαίας εξέλιξης του τομέα των τηλεπικοινωνιών προκειμένου να παράσχει το ίδιο επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής σε όλους τους χρήστες υπηρεσιών επικοινωνιών διαθέσιμων στο κοινό, ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες.

Ο στόχος της, όπως ακριβώς ήταν και της Οδηγίας 95/46/ΕΚ, είναι διπλός. Σύμφωνα λοιπόν, με το άρθρο 1 της παρούσας Οδηγίας, στοχεύει πρώτον στην εναρμόνιση των

[27] Όργανα και οργανισμοί της Κοινότητας είναι τα όργανα και οι οργανισμοί που συνιστώνται από τις συνθήκες για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή βάσει αυτών.

[28] Βλ άρθρο 19 της Οδηγίας 2002/58

διατάξεων των κρατών μελών στο χώρο των τηλεπικοινωνιών, προκειμένου να διασφαλίσει ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών κατά την επεξεργασία προσωπικών δεδομένων και δεύτερον να διασφαλίσει την ελεύθερη διακίνηση των πληροφοριών στα νέα δημόσια δίκτυα επικοινωνιών της Ευρωπαϊκής Ένωσης, γεγονός που θα ωφελούσε την ενοποιημένη ευρωπαϊκή αγορά.

Σύμφωνα με το άρθρο 4 της Οδηγίας, επιβάλλεται στο φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών καθώς και στο φορέα παροχής δημοσίου δικτύου η λήψη αναγκαίων τεχνικών και οργανωτικών μέτρων προκειμένου να προστατευτεί η ασφάλεια των παρεχομένων υπηρεσιών.

Στο άρθρο 5 γίνεται λόγος για το απόρρητο των επικοινωνιών, με το οποίο απαγορεύεται η ακρόαση, η υποκλοπή, η αποθήκευση ή οποιοδήποτε άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των, εκτός κι αν υπάρχει σχετική νόμιμη άδεια.

Στο άρθρο 6 γίνεται μνεία στα δεδομένα κίνησης, συνδρομητών και χρηστών, που υπόκεινται επεξεργασία και τελικά αποθηκεύονται από τους φορείς παροχής ηλεκτρονικών επικοινωνιών. Το άρθρο αυτό με λίγα λόγια ορίζει ότι, ο πάροχος έχει την υποχρέωση να ενημερώνει το συνδρομητή για τον τύπο των δεδομένων κίνησης που θα επεξεργαστεί καθώς και για τη διάρκεια επεξεργασίας αυτών, όπως επίσης και ότι τα δεδομένα αυτά όταν δεν θα είναι πλέον απαραίτητα για το σκοπό για τον οποίο μεταδόθηκαν, θα πρέπει να απαλείφονται (ή να καθίστανται ανώνυμα)

Στο άρθρο 13 γίνεται αναφορά στις αυτόκλητες κλήσεις. Στις κλήσεις δηλαδή που πραγματοποιούνται χωρίς την έγκριση του συνδρομητή, από συσκευές αυτόματων κλήσεων (φαξ ή ηλεκτρονικό ταχυδρομείο) που έχουν σκοπό την άμεση εμπορική προώθηση, αποκρύπτοντας την ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα. Το άρθρο αυτό λοιπόν, απαγορεύει την πραγματοποίηση τέτοιων κλήσεων, εκτός κι αν έχει δώσει ο συνδρομητής την εκ των προτέρων συγκατάθεσή του.

### 5.6.5 Οδηγία 2006/24/ΕΚ

Στις 15 Μαρ 2006 το ΕΚ και το Συμβούλιο εξέδωσαν την Οδηγία 2006/24/ΕΚ "*για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ* ", η οποία τροποποιεί την οδηγία 2002/58/ΕΚ όσον αφορά τις διατάξεις που είναι σχετικές με την υποχρέωση διατήρησης ορισμένων δεδομένων που παράγονται ή υφίστανται επεξεργασία εκ μέρους των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων, όπως ορίζονται βάσει του εθνικού δικαίου των κρατών μελών. Όπως επίσης αναφέρει το άρθρο 1, το πεδίο εφαρμογής της παρούσας οδηγίας περιορίζεται στα δεδομένα κίνησης και θέσης, στις νομικές οντότητες, στα φυσικά πρόσωπα και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του καταχωρημένου χρήστη και όχι στο περιεχόμενο των ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των πληροφοριών στις οποίες η πρόσβαση πραγματοποιείται με τη χρήση δικτύου ηλεκτρονικών επικοινωνιών. [90]

Στη συνέχεια γίνεται μία σύντομη παρουσίαση των βασικότερων άρθρων της Οδηγίας.

Στα άρθρα 3, 4 και 5 περιγράφεται ποιοι έχουν υποχρέωση για τη διατήρηση των δεδομένων, ποιοι δικαιούνται πρόσβαση σ' αυτά και τελικά ποιες είναι οι κατηγορίες των διατηρούμενων δεδομένων. Πιο αναλυτικά αναφέρεται ότι υποχρέωση για τη διατήρηση των δεδομένων αυτών έχουν οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών στο πλαίσιο της δικαιοδοσίας τους κατά την παροχή των προσδιοριζομένων υπηρεσιών επικοινωνιών και δικαίωμα πρόσβασης σ' αυτά έχουν μόνο οι αρμόδιες εθνικές αρχές, σε ειδικές περιπτώσεις και σύμφωνα με την εθνική

νομοθεσία. Οι κατηγορίες των διατηρούμενων δεδομένων όπως περιγράφονται στο άρθρο 5, είναι οι εξής:

α. δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής επικοινωνίας

β. δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας

γ. δεδομένα αναγκαία για τον προσδιορισμό της ώρας, ημερομηνίας και διάρκειας 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

στ. δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού της κινητής επικοινωνίας

Το άρθρο 6 της Οδηγίας αναφέρει ότι το χρονικό διάστημα διατήρησης των δεδομένων αυτών δεν πρέπει να είναι μικρότερο του εξαμήνου αλλά ούτε και μεγαλύτερο της διετίας από την ημερομηνία της επικοινωνίας.

Το άρθρο 7 της Οδηγίας περιγράφει τις αρχές ασφαλείας για την για προστασία και ασφάλεια των δεδομένων που πρέπει να εφαρμόζουν οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό ή δημοσίου δικτύου επικοινωνιών.

Το άρθρο 8 της Οδηγίας απαιτεί από τα κράτη μέλη να διασφαλίζει τη διατήρηση των δεδομένων με τέτοιο τρόπο ώστε αυτά όπως και κάθε άλλη πληροφορία σχετικά με αυτά να μπορεί να διαβιβαστεί κατόπιν αιτήματος στις αρμόδιες αρχές χωρίς αδικαιολόγητη καθυστέρηση.

Το άρθρο 10 αναφέρει ότι τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα στατιστικά στοιχεία για τη διατήρηση δεδομένων τα οποία παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών θα πρέπει να παρέχονται στην Επιτροπή ανά έτος.

### 5.6.6 Οδηγία 2009/136/ΕΚ

Στις 25 Νοε 2009 εκδόθηκε η Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου "*για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την*

*επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών* ". Η τροποποίηση της Οδηγίας 2002/58/ΕΚ έχει να κάνει κυρίως με θέματα που αφορούν στην ασφάλεια της πρόσβασης, μετάδοσης, αλλά και επεξεργασίας των προσωπικών δεδομένων καθώς και στα μέτρα αντιμετώπισης παραβιάσεων ασφαλείας που θα πρέπει να λαμβάνονται εκ μέρους των παρόχων τηλεπικοινωνιακών υπηρεσιών.[91]

### 5.6.7 Επίλογος

Με την Οδηγία 2009/136/ΕΚ, κλείνει ο κύκλος των Ευρωπαϊκών νομοθετικών ρυθμίσεων που θεσπίστηκαν από το 1995 έως και σήμερα, έχοντας σα στόχο τόσο την προστασία του υποκειμένου έναντι της αθέμιτης επεξεργασίας των προσωπικών του δεδομένων, όσο και την εξασφάλιση της ελεύθερης διακίνησης των πληροφοριών αυτών στα νέα δημόσια δίκτυα επικοινωνιών της Ευρωπαϊκής Ένωσης επ' ωφελεία της ενοποιημένης ευρωπαϊκής αγοράς. Μέχρι σήμερα το νομοθετικό πλαίσιο γύρω από την προστασία των προσωπικών δεδομένων έχει δεχτεί πολλά πλήγματα, κυρίως μετά τις τρομοκρατικές επιθέσεις που έλαβαν χώρα στα διάφορα σημεία του πλανήτη και ιδιαίτερα αυτή της 11$^{ης}$ Σεπ 2001 στις Η.Π.Α, όπου ήταν η αφορμή για την έκδοση αρκετών νομοθετικών ρυθμίσεων που αντιτάσσονταν στις αρχές της ιδιωτικότητας, όπως η Συμφωνία μεταξύ ΕΕ και Η.Π.Α σχετικά με την επεξεργασία και τη διαβίβαση στοιχείων μηνυμάτων χρηματοοικονομικής φύσεως από την Ευρωπαϊκή Ένωση στις

Ηνωμένες Πολιτείες της Αμερικής για σκοπούς του Προγράμματος Παρακολούθησης της Χρηματοδότησης της Τρομοκρατίας.[93]

Παρ' όλα αυτά, το σίγουρο είναι πως, η προστασία της ιδιωτικότητας όπως και η διασφάλιση των θεμελιωδών δικαιωμάτων του ανθρώπου, θα συνεχίσουν να απασχολούν, το Ευρωπαϊκό Κοινοβούλιο αλλά και την ευρωπαϊκή κοινή γνώμη για πολλά χρόνια ακόμη, εξαιτίας της καλπάζουσας εξέλιξης της τεχνολογίας που πολλές φορές θα έρχεται αντιμέτωπη με την ιδιωτική ζωή του ανθρώπου.

Η Ελλάδα όπως και όλες οι άλλες Ευρωπαϊκές χώρες, υποχρεούται να συμμορφώνεται με τις Οδηγίες της Ευρωπαϊκής Ένωσης που αναφέρθηκαν παραπάνω, γι' αυτό το λόγο, έχει θεσπίσει και η ίδια ως κράτος τις δικές της νομοθεσίες, που έχουν ως στόχο την πάταξη της αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

## 5.7 Προστασία Προσωπικών Δεδομένων στην Ελληνική Έννομη Τάξη

Στην Ελλάδα, η προστασία της προσωπικότητας του ατόμου κατοχυρώνεται από το Σύνταγμα της Ελλάδος [95], με μια σειρά άρθρων, όπως είναι για παράδειγμα τα άρθρα 2, 5 και 19, που αφορούν αντίστοιχα "το σεβασμό και την προστασία της αξίας του ανθρώπου ως πρωταρχική υποχρέωση της πολιτείας", "το δικαίωμα του προσώπου να αναπτύσσει ελεύθερα την προσωπικότητά του" καθώς επίσης και το γεγονός ότι "το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο". Δεδομένου όμως ότι, το Σύνταγμα με τη μορφή που είχε δεν προσέφερε ένα επαρκές συνταγματικό θεμέλιο αλλά ένα minimum προστασίας οδήγησε στην αναθεώρησή του, που έγινε με το Ψήφισμα της 6ης Απριλίου 2001 της Ζ΄ Αναθεωρητικής Βουλής των Ελλήνων [96], μέσα στο οποίο προστέθηκε εκτός των άλλων και το άρθρο 9Α, το οποίο ορίζει ότι "καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει". Έτσι με αυτόν τον τρόπο το ατομικό δικαίωμα προστασίας του ατόμου απέναντι στη συλλογή, αποθήκευση και επεξεργασία με συμβατικό ή ηλεκτρονικό τρόπο των προσωπικών πληροφοριών και δεδομένων, ανυψώνεται σε συνταγματικό δικαίωμα, με φορείς του δικαιώματος αυτού όχι μόνο τους έλληνες πολίτες αλλά κάθε άνθρωπο .[97] Περαιτέρω, από τη μία η αδυναμία των γενικών διατάξεων να προφυλάξουν τα προσωπικά δεδομένα του ατόμου από την αθέμιτη επεξεργασία τους και από την άλλη η ανάγκη για εναρμονισμό των νομοθετικών διατάξεων με τις οδηγίες του Κοινοτικού Δικαίου, οδήγησε στη θέσπιση πιο ειδικών νόμων, αρχής γενομένης από το νόμο 2472/97 που θεσπίστηκε τον Απρίλιο του 1997, με αντικείμενο "τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής". Στη συνέχεια ακολούθησε ο νόμος 2774/1999 με ενσωματωμένη την οδηγία 97/66/ΕΚ για την «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα», ο οποίος από τον Ιούλιο του 2006 αντικαταστάθηκε από το νόμο 3471/2006 για την «προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες» που αποτελεί προσαρμογή της νεότερης σχετικής οδηγίας 2002/58/ΕΚ. Τέλος στις 21 Φεβ 2011 εκδόθηκε ο νόμος 3917/2011 για τη «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.» Ωστόσο στην ελληνική έννομη τάξη υπάρχουν και άλλες γενικές διατάξεις που άπτονται άμεσα ή έμμεσα της προστασίας προσωπικών δεδομένων όπως το άρθρο 57 του Αστικού Κώδικα περί δικαιώματος στην προσωπικότητα ή τα άρθρα 248-250 και 370-370Α του Ποινικού Κώδικα, που τιμωρούν "την παραβίαση του απορρήτου από ταχυδρομικούς υπαλλήλους, καθώς και από υπαλλήλους τηλεπικοινωνιακών οργανισμών" και "την παραβίαση του απορρήτου των επιστολών και των τηλεφωνημάτων", αντίστοιχα. [101]

Στα αμέσως επόμενα κεφάλαια γίνεται μία αναλυτική παρουσίαση των τριών αυτών νόμων.

### 5.7.1 Νόμος 2472/1997

Ο Νόμος 2472 του 1997 [99] αποτελεί για τη χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Με τη θέσπιση του παραπάνω νόμου η Ελλάδα ανταποκρίθηκε στο "αίτημα των καιρών" [98] και συμμορφώθηκε προς τις διεθνείς και ευρωπαϊκές υποχρεώσεις της. Στη συνέχεια αυτής της ενότητας, παρουσιάζονται τα κυριότερα άρθρα του εν λόγω νόμου.

Όπως προαναφέρθηκε και παραπάνω, το αντικείμενο του, σύμφωνα και με το άρθρο 1, είναι "η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής".

Στο άρθρο 3, αναφέρεται ο τομέας εφαρμογής του, ο οποίος είναι η επεξεργασία δεδομένων με αυτοματοποιημένες[29] αλλά και με συμβατικές μεθόδους, δηλαδή παραδοσιακές χειρόγραφες μεθόδους, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, δεδομένου ότι μέχρι και στις μέρες μας ιδιαίτερα οι δημόσιες υπηρεσίες, δε χρησιμοποιούν ηλεκτρονικό υπολογιστή για την τήρηση του αρχείου τους.[30] Στη χώρα μας, σε αντίθεση με τις νομοθεσίες άλλων κρατών όπως αυτές της Νορβηγίας, της Δανίας, του Λουξεμβούργου, της Αυστρίας και της Ισλανδίας, οι ρυθμίσεις του εν λόγω νόμου περιορίζονται μόνο στα φυσικά πρόσωπα και όχι στα νομικά.[100] Στην παράγραφο 3 του συγκεκριμένου άρθρου αναφέρεται επίσης ότι ο νόμος αυτός βρίσκει εφαρμογή πρώτον, στην περίπτωση που ο υπεύθυνος επεξεργασίας βρίσκεται στην ελληνική επικράτεια ή σε τόπο, όπου εφαρμόζεται το ελληνικό δίκαιο και δεύτερον, στην περίπτωση που ο υπεύθυνος επεξεργασίας βρίσκεται σε Τρίτη χώρα εκτός ΕΕ αλλά τα μέσα που χρησιμοποιεί βρίσκονται στον ελλαδικό χώρο και η επεξεργασία αφορά κατοίκους της χώρας ή όχι.

Στο Β κεφάλαιο του νόμου, που περιλαμβάνονται τα άρθρα 4 έως 10, γίνεται αναφορά στις προϋποθέσεις θεμιτής και νόμιμης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Στο άρθρο 4, αναλύονται οι προϋποθέσεις που πρέπει να πληρούν τα δεδομένα προς επεξεργασία, οι οποίες είναι:

α) Η νομιμότητα της συλλογής και επεξεργασίας τους, που θα αποσκοπεί σε καθορισμένους, σαφείς και νόμιμους σκοπούς.

β) Η συνάφεια, και η αντιστοιχία των δεδομένων προς τους σκοπούς της συλλογής και επεξεργασίας.

γ) Η ακρίβεια και η ενημέρωση των δεδομένων.

δ) Ο χρονικός περιορισμός της διατήρησής τους ώστε να επιτρέπεται ο προσδιορισμός 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.

Στο άρθρο 5, αναφέρεται ρητά ότι για να πραγματοποιηθεί επεξεργασία δεδομένων προσωπικού χαρακτήρα, απαιτείται υποχρεωτικά η συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα, εξαιρουμένων των περιπτώσεων που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου οι οποίες είναι οι εξής:

α) Όταν η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία το συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου κατά το προσυμβατικό στάδιο όπως συμβαίνει για παράδειγμα κατά τη λήψη κάποιου τραπεζικού δανείου ή ενός ασφαλιστηρίου συμβολαίου.

β) Όταν η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο όπως για παράδειγμα η συμπλήρωση της φορολογικής δήλωσης.

γ) Όταν η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

[29] Αυτοματοποιημένες μέθοδοι θεωρούνται πέρα απ' αυτές που πραγματοποιούνται σε υπολογιστικό περιβάλλον και αυτές που τελούνται με ηλεκτρονικά μέσα αυτόματης λειτουργίας.[102]

[30] Ιγγλεζάκης, Ι. (2008). *Δίκαιο της Πληροφορικής*. Σάκκουλας Αντ. 231

δ) Όταν 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. Παράδειγμα τέτοιας περίπτωσης σύμφωνα με την απόφαση υπ' αριθμ 11/2001 της ΑΠΔΠΧ [103], αποτελεί η συλλογή και επεξεργασία προσωπικών δεδομένων από τους υποψήφιους για το βουλευτικό ή και όλα τα αιρετά αξιώματα της πολιτείας που τηρούν, αρχεία στα οποία περιλαμβάνονται τα ονόματα, οι διευθύνσεις και τα τηλέφωνα των προσώπων με τα οποία επικοινωνούν ενόψει της ανάδειξης τους στο εν λόγω αξίωμα δεδομένου ότι η συλλογή των ως άνω προσωπικών δεδομένων μπορεί να γίνεται μόνο από δημόσια προσβάσιμες πηγές και ότι απαγορεύεται η διάθεση τους σε τρίτους.

ε) Όταν 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 όπως στην περίπτωση των αρχείων που τηρούνται για την αξιολόγηση της οικονομικής φερεγγυότητας, που εφαρμόζεται στο σύστημα ΤΕΙΡΕΣΙΑΣ[31].

Με το άρθρο 6, κάθε υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιεί εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας με στόχο τη δημιουργία ενός κεντρικού μητρώου αρχείων και επεξεργασίας έτσι ώστε να είναι προσιτό σε όποιον ενδιαφέρεται να ασκήσει τα δικαιώματά του έναντι στον εκάστοτε υπεύθυνο επεξεργασίας. Οι εξαιρέσεις του παραπάνω άρθρου αναφέρονται στο άρθρο 7Α.

Σύμφωνα με το άρθρο 7, απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, εξαιρουμένων των περιπτώσεων της παραγράφου 2 του παρόντος άρθρου όπου δεν αρκεί απλώς η κοινοποίηση έναρξης αρχείου στην Αρχή, αλλά απαιτείται και η λήψη αδείας απ' αυτήν,.

Στο άρθρο 8 γίνεται λόγος για τη διασύνδεση αρχείων μεταξύ δύο υπεύθυνων επεξεργασίας. Δηλαδή τη διασταύρωση προσωπικών δεδομένων που τηρούνται σε διαφορετικά μεταξύ τους αρχεία και για διαφορετικό σκοπό. Στην περίπτωση που τα δεδομένα προσωπικού χαρακτήρα είναι απλά, για να είναι νόμιμη η διασύνδεση θα πρέπει να γνωστοποιηθεί πρώτα στην Αρχή με δήλωση από κοινού των δύο ή περισσοτέρων υπεύθυνων επεξεργασίας. Παράδειγμα τέτοιας περίπτωσης αποτελεί η απόφαση υπ' αριθμ 92/2002 της Αρχής [104] η οποία έκρινε απαραίτητη τη διασύνδεση δεδομένων μεταξύ των υπουργείων μεταφορών και επικοινωνιών, δημόσιας τάξης και οικονομικών, χωρίς τη συγκατάθεση του υποκειμένου λόγω του ότι είναι απαραίτητη για την εκτέλεση του δημόσιου έργου τους.[32] Άλλο χαρακτηριστικό παράδειγμα αποτελεί η ΤΕΙΡΕΣΙΑΣ Α.Ε, που τηρεί αρχεία πληροφοριών που αναφέρονται στην οικονομική συμπεριφορά επιχειρήσεων και ιδιωτών, πληροφοριών που αφορούν σε ταυτότητες /διαβατήρια που έχουν κλαπεί ή απολεσθεί, καθώς και πληροφοριών σχετικά με δόλια χρήση πιστωτικών καρτών προς όφελος των συναλλασσομένων και του τραπεζικού συστήματος.[105] Στην περίπτωση που τα προσωπικά δεδομένα είναι ευαίσθητα, τότε η διασύνδεση επιτρέπεται μόνο με προηγούμενη άδεια της Αρχής.

Στο άρθρο 10, διασφαλίζονται δύο στόχοι. Πρώτον, το απόρρητο της επεξεργασίας, ορίζοντας πως οι εκτελούντες την επεξεργασία θα πρέπει να είναι πρόσωπα με επαγγελματικά προσόντα που θα παρέχουν επαρκείς εγγυήσεις όσον αφορά την επαγγελματική και προσωπική τους ακεραιότητα, πως θα τελούν επίσης, υπό τον έλεγχο του υπεύθυνου επεξεργασίας και πως θα προβαίνουν σε επεξεργασία μόνο κατ' εντολή δική του και δεύτερον, θα πρέπει να διασφαλίζεται η ασφάλεια των δεδομένων και η προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας, έπειτα από τη λήψη κατάλληλων οργανωτικών και τεχνικών μέτρων από πλευράς υπευθύνων της επεξεργασίας.

[31] Το σύστημα Τειρεσίας αφορά στην πιστοληπτική ικανότητα εμπόρων και καταναλωτών και στηρίζεται σε μια βάση δεδομένων στην οποία καταχωρούνται φυσικά και νομικά πρόσωπα που κατά το παρελθόν έχουν φανεί αφερέγγυοι ως οφειλέτες .

[32] Ιγγλεζάκης, Ι. (2008). *Δίκαιο της Πληροφορικής*. Σάκκουλας Αντ. 236

Το κεφάλαιο Γ, που απαρτίζεται από τα άρθρα 11 έως 14 αναφέρεται στα δικαιώματα του υποκειμένου των δεδομένων, όπως φαίνονται παρακάτω:

α) Το δικαίωμα της ενημέρωσης. Είναι αυτό που δίνει το δικαίωμα στο υποκείμενο της επεξεργασίας να πληροφορείται και να ενημερώνεται σχετικά με πληροφορίες που αφορούν τον υπεύθυνο επεξεργασίας καθώς και το σκοπό της επικείμενης συλλογής και επεξεργασίας των προσωπικών του δεδομένων.

β) Το δικαίωμα της πρόσβασης. Είναι αυτό που δίνει το δικαίωμα στο υποκείμενο της επεξεργασίας να γνωρίζει εάν τα προσωπικά του δεδομένα αποτελούν ή αποτέλεσαν κατά το παρελθόν αντικείμενο επεξεργασίας.

γ) Το δικαίωμα της αντίρρησης. Είναι αυτό που δίνει το δικαίωμα στο υποκείμενο της επεξεργασίας να προβάλλει οποτεδήποτε, εγγράφως προς τον υπεύθυνο επεξεργασίας, αντιρρήσεις για την επεξεργασία των δεδομένων που το αφορούν. Εάν δε λάβει απάντηση μέσα σε 15 ημέρες ή η απάντηση που θα λάβει δεν είναι ικανοποιητική τότε έχει δικαίωμα να απευθυνθεί στην Αρχή και να ζητήσει την εξέταση των αντιρρήσεων του, οπότε αν οι αντιρρήσεις του είναι εύλογες τότε αυτή είναι δυνατό να επιβάλλει την άμεση αναστολή της επεξεργασίας μέχρι να εκδώσει οριστική απόφαση.

δ) Το δικαίωμα της προσωρινής δικαστικής προστασίας. Είναι αυτό που δίνει το δικαίωμα στο υποκείμενο της επεξεργασίας να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, η οποία έχει ληφθεί αυτοματοποιημένα από κάποια διοικητική αρχή, νομικό ή φυσικό πρόσωπο, και αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.

Το κεφάλαιο Δ, που απαρτίζεται από τα άρθρα 15 έως 20 αναφέρεται στη σύσταση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), που έχει σαν αποστολή την άσκηση του ελέγχου της πιστής εφαρμογής του παρόντος νόμου καθώς και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία των προσωπικών του δεδομένων. Αναλυτικότερη όμως περιγραφή της ΑΠΔΠΧ γίνεται στο κεφάλαιο 5.9.2 της παρούσας διατριβής.

Στα άρθρα 20 έως 23 αναφέρονται οι διοικητικές κυρώσεις που μπορεί να επιβάλλει η ΑΠΔΠΧ, καθώς και οι ποινικές και αστικές κυρώσεις που μπορούν να επιβάλλουν τα αρμόδια δικαστήρια, στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους, σε περίπτωση παράβασης των υποχρεώσεων τους, που απορρέουν από τον παρόντα νόμο αλλά και οποιαδήποτε άλλη νομοθετική ρύθμιση. Ενδεικτικά, στις διοικητικές κυρώσεις που μπορεί να επιβάλλει η ΑΠΔΠΧ περιλαμβάνονται οι προειδοποιήσεις, τα πρόστιμα που κυμαίνονται από 880 έως 147.000 Ευρώ, οι ανακλήσεις αδειών επεξεργασίας καθώς και η επιβολή διακοπής της επεξεργασίας ή καταστροφής του αρχείου. Οι ποινικές κυρώσεις επιβάλλονται από τα ποινικά δικαστήρια και αφορούν ποινές φυλάκισης συνοδευόμενες από χρηματικές αποζημιώσεις και οι αστικές κυρώσεις επιβάλλονται από τα αστικά δικαστήρια και αφορούν αποζημιώσεις από πρόκληση ηθικής βλάβης ή τέλεσης αδικοπραξίας.

### 5.7.2 Νόμος 2774/1999

Σκοπός του συγκεκριμένου νόμου, [106] στα πλαίσια συμπλήρωσης και εξειδίκευσης του νόμου 2472/1997, ήταν η παροχή προστασίας στην ιδιωτικότητά του ατόμου καθώς και η θέσπιση των προϋποθέσεων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Σε αντίθεση με το νόμο 2472/1997, ο παρών νόμος βρίσκει εφαρμογή και στα νομικά πρόσωπα διατηρώντας πάντα την αρχή της εξοικονόμησης των δεδομένων, κατά την οποία επιβάλλεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο απολύτως αναγκαίο για την εξυπηρέτηση των σκοπών της. Επιπρόσθετα, επιβάλλει στον τηλεπικοινωνιακό πάροχο να καθιστά δυνατή στο χρήστη, όσο βέβαια αυτό είναι εφικτό, τη χρήση των υπηρεσιών του ανωνύμως ή κάνοντας χρήση κάποιου ψευδωνύμου. Επιπλέον όσον αφορά τον πάροχο, δεν του επιτρέπει να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς πέρα απ' αυτούς για τους οποίους αρχικά είχαν οριστεί, παρά μόνο αν ο χρήστης έχει δώσει ρητά τη συγκατάθεσή του και ειδικότερα για τη

διαβίβαση σε τρίτους έχει συμφωνήσει εγγράφως. Για τη παροχή μεγαλύτερης προστασίας, ο συγκεκριμένος νόμος, επιβάλλει επίσης στον πάροχο, την απαλοιφή των αποθηκευμένων δεδομένων κίνησης μετά τη λήξη οποιασδήποτε κλήσης και αφού γίνει η προβλεπόμενη χρέωση στους συνδρομητές.

Όσον αφορά το συνδρομητή, του δίνει τη δυνατότητα να εμποδίζει τις αυτόματα προωθούμενες κλήσεις από τρίτους στην τερματική του συσκευή, καθώς και το δικαίωμα να μην συμπεριλαμβάνεται σε έντυπο ή ηλεκτρονικό κατάλογο ένα αυτός δεν το επιθυμεί. Όπως και στην περίπτωση του νόμου 2472/1997, ο παρών νόμος προβλέπει αστικές και ποινικές κυρώσεις που επιβάλλονται με χρηματική αποζημίωση για τις πρώτες και με ποινή φυλάκισης και αποζημίωσης για τις δεύτερες.

Έπειτα από την έκδοση της Οδηγίας 2002/58/ΕΚ και την ενσωμάτωσή της στο νόμο 3471/06 για την «Προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες», τροποποιήθηκαν όλες οι ρυθμίσεις του νόμου 2774/1999 με αποτέλεσμα να καταργηθεί και να αντικατασταθεί πλήρως από τον πρώτο.[33]

### 5.7.3 Νόμος 3471/2006

Η έκδοση της οδηγίας 2002/58/ΕΚ και η ενσωμάτωσή της, στο νόμο 3471/2006, [107] οδήγησε στην αναθεώρηση της οδηγίας 97/66/ΕΚ, στην τροποποίηση του νόμου 2472/1997 και στην πλήρη αντικατάσταση του νόμου 2774/1999[34]. Ο σκοπός του νόμου 3471/2006, σύμφωνα και με το άρθρο 1 του παρόντος είναι η παροχή προστασίας της ιδιωτικής ζωής του ατόμου καθώς και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

Όπως και ο νόμος 2774/99, έτσι και ο εν λόγω νόμος, επεκτείνει το πλαίσιο εφαρμογής του σε συνδρομητές που είναι όχι μόνο φυσικά πρόσωπα αλλά και νομικά[35]. Ο νόμος βρίσκει εφαρμογή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, στα πλαίσια της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικής επικοινωνίας, συμπεριλαμβανομένου δηλαδή και του διαδικτύου, ενώ στην περίπτωση υπηρεσιών επικοινωνίας μη διαθέσιμων στο κοινό τίθενται σε εφαρμογή οι διατάξεις του νόμου 2472/97[36]. Το άρθρο 3 εδ. 2, αναφέρει χαρακτηριστικά ότι ο παρών νόμος εφαρμόζεται μονάχα στην περίπτωση που απαιτούνται ειδικές ρυθμίσεις όπου δεν μπορεί να εφαρμοστεί ο νόμος 2472/1997. Ένα από τα βασικά πλεονεκτήματα της Οδηγίας 2002/58 είναι ότι συμβάλλει στην επαύξηση της προστασίας του απορρήτου των επικοινωνιών, με αποτέλεσμα ο νόμος 3471/2006 που αποτελεί την μεταφορά της παραπάνω οδηγίας, στα ελληνικά νομοθετικά πλαίσια, να εμφανίζεται ιδιαίτερα αποφασιστικός στο θέμα αυτό[37], ορίζοντας ότι, οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών[38]. Επιπλέον απαγορεύει την ακρόαση, την υποκλοπή την αποθήκευση ή οποιοδήποτε άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης[39], όπως επίσης και τη 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[40], κάνοντας μ' αυτόν τον τρόπο σαφές ότι δεν επιτρέπει τη χρήση

[33] Ιγγλεζάκης, Ι. (2008). *Δίκαιο της Πληροφορικής.* Σάκκουλας Αντ. 254

[34] Άρθρο 17 Νόμου 3471/2006

[35] Άρθρο 2 εδ .1 του ν.3471/2006

[36] Άρθρο 3 εδ. 1 του ν.3471/2006

[37] Ιγγλεζάκης, Ι. (2008). *Δίκαιο της Πληροφορικής.* Σάκκουλας Αντ. 257

[38] Άρθρο 4 εδ. 1 του ν.3471/2006

[39] Άρθρο 4 εδ. 2 του ν.3471/2006

[40] Άρθρο 4 εδ. 5 του ν.3471/2006

λογισμικών υποκλοπής δεδομένων καθώς και αρχείων "cookies"[41] χωρίς τη συγκατάθεση του χρήστη ή τη συναίνεση του νόμου όσον αφορά κάποιες ειδικές περιπτώσεις[22].

Θέτει επίσης τους κανόνες επεξεργασίας των δεδομένων προσωπικού χαρακτήρα καθώς και των δεδομένων κίνησης και θέσης, ορίζοντας ότι η επεξεργασία τους πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της, όπως επίσης και ότι ο πάροχος δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα και τα δεδομένα κίνησης και θέσης ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός αν ο συνδρομητής ή ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεσή του[42]. Επισημαίνεται δηλαδή ότι απαγορεύεται οποιαδήποτε αποθήκευση ή επεξεργασία δεδομένων από τυχαία συλλογή δεδομένων για πιθανή μελλοντική χρήση η οποία δεν θα έχει προβλεφθεί και καθοριστεί εξ' αρχής.

Επιπλέον ορίζεται ότι τα δεδομένα κίνησης που αφορούν τους συνδρομητές και χρήστες πρέπει να διατηρούνται από τον πάροχο, σε μορφή που να επιτρέπεται ο προσδιορισμός του υποκειμένου, μονάχα για το χρονικό διάστημα που υφίσταται η επικοινωνία και αντίστοιχα τα δεδομένα κίνησης που περιέχουν στοιχεία που αφορούν τη χρέωση των συνδρομητών θα πρέπει να διατηρούνται έως το τέλος της περιόδου εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή του[43]. Παρόμοια είναι και η ρύθμιση που αφορά τα δεδομένα θέσης των χρηστών και συνδρομητών, η οποία επιτρέπει την επεξεργασία των δεδομένων αυτών μονάχα αν αυτά καθίστανται ανώνυμα με την κατάλληλη κωδικοποίηση ή με τη ρητή συγκατάθεση του χρήστη ή του συνδρομητή, εξαιρουμένων των περιπτώσεων έκτακτης ανάγκης όπου απαιτείται ο εντοπισμός του καλούντος από τις διωκτικές αρχές, τις υπηρεσίες πρώτων βοηθειών και πυρόσβεσης και μόνο για το συγκεκριμένο αυτόν σκοπό[44].

Ένα επιπλέον δικαίωμα συνδρομητών και χρηστών που προβλέπεται στο νόμο 3471/2006, είναι αυτό της λήψης μη αναλυτικών λογαριασμών, όπως επίσης και το δικαίωμα του συνδρομητή να ζητήσει από τον πάροχο να διαγράψει από τον αναλυτικό λογαριασμό τα τρία τελευταία ψηφία των κληθέντων αριθμών[45]. Όσον αφορά τώρα, την ένδειξη της ταυτότητας και την αναγνώριση της καλούσας και συνδεδεμένης γραμμής, το άρθρο 8 της παρούσας διάταξης προβλέπει τη δυνατότητα του καλούντος με απλά μέσα και χωρίς χρέωση να εμποδίζει αυτή τη λειτουργία ανά κλήση. Στην περίπτωση δε, που θα παρέχεται η ένδειξη της ταυτότητας της καλούσας γραμμής, ο καλούμενος συνδρομητής θα πρέπει να έχει τη δυνατότητα, πάλι χωρίς χρέωση, να μην επιτρέπει την ένδειξη αυτή για τις εισερχόμενες κλήσεις. Επίσης, ο καλούμενος μπορεί να μην επιτρέπει την εισερχόμενη κλήση, όταν ο καλών δεν επιτρέπει την ένδειξη της ταυτότητας του, ενώ όταν παρέχεται ένδειξη της ταυτότητας της συνδεδεμένης γραμμής, ο καλούμενος θα πρέπει να έχει τη δυνατότητα να απαλείφει την ένδειξη της ταυτότητας της συνδεδεμένης γραμμής στον καλούντα χρήστη[46]. Δικαίωμα του συνδρομητή, αποτελεί επίσης το να εμποδίζει, ατελώς, τις αυτόματα προωθούμενες κλήσεις από τρίτους στην τερματική του συσκευή[47]. Επίσης ο συνδρομητής έχει το δικαίωμα έπειτα από αντίρρησή του να μην συμπεριλαμβάνεται σε έντυπο ή ηλεκτρονικό δημόσιο κατάλογο, παρά ταύτα αν αποδεχθεί να συμπεριληφθεί τότε τα προσωπικά του δεδομένα πρέπει να περιορίζονται στα απολύτως

[41] Τα αρχεία cookies, είναι μικρά αρχεία που εγκαθίστανται στο σκληρό δίσκο του υπολογιστή μας έπειτα από την επίσκεψη μας στις διάφορες ιστοσελίδες του διαδικτύου. Αυτά τα αρχεία έχουν σα στόχο την αναγνώρισή μας από τις ίδιες τις ιστοσελίδες έπειτα από μελλοντική μας επίσκεψη, γι' αυτό το λόγο είναι δυνατό να περιλαμβάνουν διάφορα στοιχεία της ταυτότητας μας, όπως το όνομα μας (εάν το έχουμε δηλώσει), τη διεύθυνση του ηλεκτρονικού ταχυδρομείου μας, το password μας καθώς και διάφορα δεδομένα προσωπικού χαρακτήρα που έχουμε ήδη αποστείλει όπως για παράδειγμα τον αριθμό της πιστωτικής μας κάρτας, τις αγοραστικές μας προτιμήσεις ή ακόμα και την επισκεψιμότητά μας στη συγκεκριμένη ιστοσελίδα. Υπάρχουν δύο κατηγορίες cookies. Τα προσωρινά και τα μόνιμα. Προσωρινά είναι αυτά που διαγράφονται αυτόματα όταν σταματήσει η σύνδεση με το διαδίκτυο, ενώ μόνιμα είναι αυτά που παραμένουν στον υπολογιστή μας, για να διευκολύνουν την αναγνώριση της «ταυτότητας» μας όταν θα θελήσουμε να επισκεφτούμε τον ίδιο διαδικτυακό τόπο ξανά.[110]

[42] Άρθρο 5 εδ. 1 και 4 του ν.3471/2006

[43] Άρθρο 6 εδ. 1 και 2 του ν.3471/2006

[44] Άρθρο 6 εδ. 3 και 4 του ν.3471/2006

[45] Άρθρο 7 εδ. 1 και 2 του ν.3471/2006

[46] Άρθρο 8 εδ. 1,2,3 και 4 του ν.3471/2006

[47] Άρθρο 9 του ν.3471/2006

απαραίτητα για την αναγνώριση της ταυτότητάς του[48]. Για ένα άλλο πολύ σημαντικό ζήτημα για το οποίο μεριμνά ο παρών νόμος είναι το θέμα της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spamming). Καθιερώνει ένα σύστημα «opt-in» που σημαίνει ότι η πραγματοποίηση μη αιτηθείσας επικοινωνίας επιτρέπεται μόνο στην περίπτωση που ο συνδρομητής, είτε είναι φυσικό είτε νομικό πρόσωπο, έχει συγκατατεθεί εκ των προτέρων ρητώς.[49] Μόνη εξαίρεση, αποτελεί η περίπτωση που τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου αποκτήθηκαν νομίμως στα πλαίσια άλλων συναλλαγών οπότε και τα στοιχεία αυτά μπορούν να χρησιμοποιούνται για την απ' ευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών[50]. Αυτό που απαγορεύει ρητά είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας[51]. Επιπρόσθετα μέτρα για την προστασία των προσωπικών δεδομένων στο διαδίκτυο προβλέπει στο άρθρο 12 του παρόντος όπου επιβάλλει στον πάροχο πρώτον, να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύσει την ασφάλεια των υπηρεσιών του και εν γένει του διαδικτύου και δεύτερον να ενημερώνει τους συνδρομητές του, στην περίπτωση ύπαρξης ιδιαίτερου κινδύνου παραβίασης ασφαλείας[52]. Τέλος όπως και οι υπόλοιποι συναφείς νόμοι, έτσι και ο νόμος 3471/2006 προβλέπει αστικές και ποινικές κυρώσεις εις βάρος των φυσικών και νομικών προσώπων που παραβαίνουν το συγκεκριμένο νόμο. Πιο συγκεκριμένα όσον αφορά τις αστικές κυρώσεις προβλέπει πλήρη αποζημίωση σε περίπτωση πρόκλησης περιουσιακής βλάβης και χρηματική ικανοποίηση κατ' ελάχιστο δέκα χιλιάδες (10.000) Ευρώ σε περίπτωση πρόκλησης ηθικής βλάβης[53]. Όσον αφορά τις ποινικές κυρώσεις προβλέπει φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον δέκα χιλιάδων (10.000) Ευρώ μέχρι και εκατό χιλιάδων (100.000) Ευρώ, εάν βέβαια η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις, σε κάθε περίπτωση που κάποιος χρησιμοποιεί συλλέγει, αποθηκεύει, λαμβάνει γνώση, αφαιρεί, αλλοιώνει, καταστρέφει, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, ή τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο[54]. Επιπλέον ορίζει ότι σε περίπτωση μη συμμόρφωσης με της πράξεις της ΑΠΔΠΧ, ο υπεύθυνος επεξεργασίας υποβάλλεται απ' αυτήν σε διοικητικές κυρώσεις προσωρινής ή οριστικής ανάκλησης αδείας και καταστροφής του αρχείου ή διακοπή της επεξεργασίας και καταστροφής των σχετικών δεδομένων και τιμωρείται με φυλάκιση τουλάχιστον δύο ετών, όπως επίσης και με χρηματική ποινή τουλάχιστον δώδεκα χιλιάδων (12.000) Ευρώ έως και εκατόν είκοσι χιλιάδων (120.000) Ευρώ[55]. Ακόμα πιο αυστηρές είναι οι ποινικές κυρώσεις που υφίσταται ο δράστης στην περίπτωση που για τις προηγούμενες πράξεις είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον, παράνομο περιουσιακό όφελος ή να βλάψει τρίτο οπότε και του επιβάλλεται κάθειρξη μέχρι δέκα έτη και χρηματική ποινή από δεκαπέντε χιλιάδες (15.000) Ευρώ έως εκατόν πενήντα χιλιάδες (150.000) Ευρώ[56]. Στην περίπτωση δε που οι παραπάνω πράξεις τελέστηκαν από αμέλεια επιβάλλεται ποινή φυλάκισης δεκαοκτώ μηνών και χρηματική ποινή μέχρι δέκα χιλιάδες (10.000) Ευρώ[57].

[48] Άρθρο 10 εδ. 2 και 3 του ν.3471/2006

[49] Ιγγλεζάκης, Ι. (2008). *Δίκαιο της Πληροφορικής.* Σάκκουλας Αντ. 263

[50] Άρθρο 11 εδ. 1,3 και 5 του ν.3471/2006

[51] Άρθρο 11 εδ. 4 του ν.3471/2006

[52] Άρθρο 12 εδ. 1 και 2 του ν.3471/2006

[53] Άρθρο 14 εδ. 1 και 2 του ν.3471/2006

[54] Άρθρο 15 εδ. 1 του ν.3471/2006

[55] Άρθρο 15 εδ. 2 του ν.3471/2006

[56] Άρθρο 15 εδ. 3 του ν.3471/2006

[57] Άρθρο 15 εδ. 4 του ν.3471/2006

### 5.7.4 Νόμος 3917/2011

Στο νόμο 3917/2011 [108] ενσωματώθηκε η Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ[58]. Σύμφωνα με το άρθρο 1 ο παρών νόμος έχει ως αντικείμενο τη διατήρηση κάποιων δεδομένων κίνησης και θέσης, φυσικών και νομικών προσώπων, που παράγονται ή υποβάλλονται σε επεξεργασία από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να καθίστανται διαθέσιμα στις αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων[59]. Τα προαναφερόμενα δεδομένα αφορούν τις εξής κατηγορίες:

- Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας.
- Δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας.
- Δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας της επικοινωνίας.
- Δεδομένα αναγκαία για τον προσδιορισμό του είδους της επικοινωνίας.
- Δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών ή του φερόμενου ως εξοπλισμού επικοινωνίας τους και
- Δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας[60].

Στο κεφάλαιο Β γίνεται λόγος για τη χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου και εικόνας σε δημόσιους χώρους και πιο συγκεκριμένα αναφέρεται ότι αυτή επιτρέπεται μόνο από τις κρατικές αρχές και για λόγους που αφορούν :

α) Τη διαφύλαξη της εθνικής άμυνας.

β) Την προστασία του πολιτεύματος και την αποτροπή εγκλημάτων προδοσίας της χώρας.

γ) Την αποτροπή και καταστολή εγκλημάτων που συνιστούν επιβουλή της δημόσιας τάξης.

δ) Την αποτροπή και καταστολή εγκλημάτων βίας, εμπορίας ναρκωτικών, κοινώς επικίνδυνων εγκλημάτων, εγκλημάτων κατά της ασφάλειας των συγκοινωνιών και εγκλημάτων κατά της ιδιοκτησίας, όταν με βάση πραγματικά στοιχεία συντρέχουν επαρκείς ενδείξεις ότι τελέσθηκαν ή πρόκειται να τελεσθούν τέτοιες πράξεις.

ε) Τη διαχείριση της κυκλοφορίας[61].

Τέλος και ο νόμος 3917/2011 προβλέπει και αυτός διοικητικές και ποινικές κυρώσεις σε περίπτωση παράβασης των παραπάνω άρθρων.

## 5.8 Διασυνοριακή Ροή Δεδομένων

Κάθε μεταβίβαση πληροφορίας που διενεργείται μέσω του διαδικτύου μπορεί να αποκτήσει διασυνοριακή διάσταση, από τι στιγμή που το διαδίκτυο δεν έχει σαφή και καθορισμένα σύνορα όπως αυτά που κατέχει ένα κράτος. Διασυνοριακή ροή δεδομένων νοείται ως η διαβίβαση ή μεταφορά δεδομένων προσωπικού χαρακτήρα με σκοπό την επεξεργασία τους, πέρα από τα εθνικά σύνορα μιας χώρας. Είναι δυνατό κάποια προσωπικά δεδομένα που συλλέγονται σε κάποια χώρα, παρανόμως ή νομίμως, να μεταφέρονται σε διαφορετικές χώρες απ' αυτήν που συλλέχθηκαν, με αποτέλεσμα να καθίσταται αδύνατος ο έλεγχος και μ' αυτόν τον τρόπο να

[58] Κεφ Α του Ν.3917/2011

[59] Άρθρο 1 και 2 του ν.3917/2011

[60] Άρθρο 5 του ν.3917/2011

[61] Άρθρο 14 εδ 1 και 2 του ν.3917/2011

καταλύεται το αναφαίρετο δικαίωμα του υποκειμένου των δεδομένων, για ενημέρωση και πρόσβαση στις πληροφορίες που το αφορούν.

Σύμφωνα με το άρθρο 24 του νόμου 3471/2006 η διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός συνόρων περιλαμβάνει δύο κατηγορίες χωρών. Στην πρώτη κατηγορία, ανήκουν οι χώρες - μέλη της Ευρωπαϊκής Ένωσης, όπου σ' αυτήν την περίπτωση, η διακίνηση δεδομένων προσωπικού χαρακτήρα γίνεται ελεύθερα και στη δεύτερη κατηγορία ανήκουν οι χώρες μη μέλη της Ευρωπαϊκής Ένωσης όπου για να γίνει η διαβίβαση δεδομένων προσωπικού χαρακτήρα θα πρέπει, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) να έχει εκδώσει σχετική άδεια αφού κρίνει πρώτα ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας[62], λαμβάνοντας υπόψη της διάφορα σχετικά κριτήρια όπως το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων. Υπάρχει βέβαια και η δυνατότητα να επιτραπεί η διακίνηση δεδομένων προσωπικού χαρακτήρα κατά περίπτωση, ακόμα και αν δεν έχει εκδοθεί προηγουμένως σχετική άδεια, εφόσον υπογραφεί μεταξύ των δύο μερών συμφωνία κατά το πρότυπο και με τους όρους που ορίζονται στο άρθρο 26 παρ 4 της οδηγίας 95/46/ΕΚ σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από τρίτες χώρες. Από αυτή την κατηγορία εξαιρείται η περίπτωση που ο αποδέκτης των πληροφοριών ενεργεί εξ' ονόματος του εξαγωγέα, υπεύθυνου της επεξεργασίας, όπου τότε θα πρέπει να υπογραφεί μια συμφωνία μεταξύ εξαγωγέα και εκτελούντα την επεξεργασία με βάση τους όρους που προβλέπονται στην απόφαση 2002/16/ΕΚ της Ευρωπαϊκής Επιτροπής.[72]

Για τις ΗΠΑ, τα πράγματα αλλάζουν λόγω του ότι η νομοθεσία τους προβλέπει ένα καθεστώς αυτορρύθμισης και αυτοπεριορισμού για τους δημόσιους ή ιδιωτικούς φορείς που επιθυμούν να επεξεργαστούν και να χρησιμοποιήσουν προσωπικά δεδομένα, γι 'αυτό το λόγο από το 2000 τέθηκε σε εφαρμογή μια συμφωνία που βασίζεται στις «αρχές του ασφαλούς λιμένα» (Safe Harbor).[73] Σύμφωνα μ' αυτήν θα πρέπει ο αποδέκτης των δεδομένων να εγγράφεται σε μια ειδική λίστα της Ομοσπονδιακής Επιτροπής Εμπορίου (Federal Trade Commission) των ΗΠΑ όπου αυτόματα θα αποδέχεται και θα υιοθετεί το πλαίσιο προστασίας των προσωπικών δεδομένων που θα ισχύει στην Ευρωπαϊκή Ένωση. Ως εκ τούτου, κάθε χώρα που θα είναι γραμμένη σ' αυτή τη λίστα θα θεωρείται ότι συμφωνεί με τις επιταγές της ΕΕ και έτσι η ροή προσωπικών δεδομένων προς αυτή θα είναι ελεύθερη.

## 5.9 Προστασία Προσωπικών Δεδομένων

Η προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί όπως προαναφέρθηκε ένα από τα βασικότερα δικαιώματα του ανθρώπου. Η νομοθεσία που αποτελεί το κυριότερο μέσο διασφάλισης του προαναφερθέντος δικαιώματος το οποίο θεωρείται και το πλέον αποτελεσματικό φρόντισε να διασφαλίσει τον έλεγχο και τη σωστή εφαρμογή του ελληνικού νομικού πλαισίου με την ίδρυση τριών ανεξάρτητων αρχών. Ο όρος αρχή συμπεριλαμβάνει, οποιαδήποτε οργανισμό ή δημόσια αρχή όπως δικαστική, αστυνομική, στρατιωτική ή πολιτική δημόσια αρχή, που έχει το δικαίωμα να αιτηθεί άρση του απορρήτου και να αποκτήσει πρόσβαση στα στοιχεία κάποιας μορφής επικοινωνίας. Για να γίνει αυτό βέβαια, θα πρέπει η μία αρχή να το αιτηθεί στην άλλη και αφού ελέγξει το αίτημά της και βεβαιωθεί ότι τα δεδομένα που ζητάει θα χρησιμοποιηθούν μόνο για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων τότε θα επιτρέψει την άρση του απορρήτου. Η πρώτη που είναι και η παλαιότερη, ονομάζεται Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ), η δεύτερη, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) και η τρίτη, Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε).

### 5.9.1 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ)

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) [70] λειτουργεί από το 1992 ως ανεξάρτητη αρχή, σύμφωνα με τις διατάξεις του νόμου 2075 αρχικά ως Εθνική Επιτροπή

[62] Έως σήμερα οι τρεις χώρες που πληρούν αυτά τα κριτήρια είναι η Ελβετία, η Ουγγαρία και ο Καναδάς, βλ αποφάσεις της Ευρωπαϊκής Επιτροπής 2000/518/ΕΚ(EEL 215/1), 2000/519/ΕΚ(EEL 215/4) και 2002/2/ΕΚ (EEL 2/13) αντίστοιχα.

Τηλεπικοινωνιών (ΕΕΤ). Σήμερα, έπειτα από το νόμο 2867/2000 ενισχύθηκε ο ρόλος της ενώ με τον ισχύοντα Ν. 3431/2006 περί ηλεκτρονικών επικοινωνιών, καθορίστηκαν οι αρμοδιότητες της αποτελώντας κατ' αυτόν τον τρόπο τον Εθνικό Ρυθμιστή που ελέγχει, ρυθμίζει και εποπτεύει:

(α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και

(β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Επιπλέον, η ΕΕΤΤ ασκεί τις αρμοδιότητες Επιτροπής Ανταγωνισμού στις εν λόγω αγορές.

Συγκροτείται από τον Πρόεδρο, τον Αντιπρόεδρο και άλλα επτά μέλη. Οι δύο πρώτοι επιλέγονται και διορίζονται από το Υπουργικό Συμβούλιο, ύστερα από πρόταση του Υπουργού Μεταφορών και Επικοινωνιών και γνώμη της Επιτροπής Θεσμών και Διαφάνειας της Βουλής. Τα υπόλοιπα μέλη διορίζονται από τον Υπουργό Μεταφορών και Επικοινωνιών. Ως μέλη της ΕΕΤΤ επιλέγονται πρόσωπα εγνωσμένου κύρους, που απολαμβάνουν ευρείας κοινωνικής αποδοχής και διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στον τεχνικό, οικονομικό ή νομικό τομέα.

#### 5.9.1.1 Αρμοδιότητες Ε.Ε.Τ.Τ

Οι αρμοδιότητες της ΕΕΤΤ όπως καθορίζονται στο νόμο 3431/2006 είναι οι εξής:

- Ρυθμίζει τα θέματα που αφορούν τον α) καθορισμό σχετικών αγορών, προϊόντων ή υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ελληνική Επικράτεια, β) τον ορισμό και τις υποχρεώσεις Παρόχων με Σημαντική Ισχύ στις ανωτέρω σχετικές αγορές σύμφωνα με την εθνική και κοινοτική νομοθεσία.
- Εποπτεύει και ελέγχει τους παρόχους δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, επιβάλλει τις σχετικές κυρώσεις, τηρεί και διαχειρίζεται το Μητρώο Παρόχων Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.
- Εκδίδει Κώδικες Δεοντολογίας για την παροχή δικτύων και υπηρεσιών των ηλεκτρονικών επικοινωνιών.
- Μεριμνά για την τήρηση της νομοθεσίας περί ηλεκτρονικών επικοινωνιών, εφαρμόζει τις διατάξεις του Ν. 703/1977, όπως ισχύει, και επιβάλει σχετικές κυρώσεις.
- Συνεργάζεται με τις Ρυθμιστικές Αρχές των λοιπών κρατών μελών της Ευρωπαϊκής Ένωσης ή τρίτων κρατών, καθώς και με κοινοτικούς ή διεθνείς φορείς σε θέματα αρμοδιότητάς της.
- Ρυθμίζει τα θέματα που αφορούν στις Γενικές Άδειες.
- Διαχειρίζεται το Εθνικό Σχέδιο Αριθμοδότησης (Ε.Σ.Α.).
- Ρυθμίζει τα θέματα φορητότητας αριθμών, της επιλογής ή/ και προεπιλογής φορέα και ελέγχει την εφαρμογή των σχετικών διατάξεων.
- Χορηγεί τα δικαιώματα χρήσης ραδιοσυχνοτήτων ή/ και αριθμών.
- Ρυθμίζει τα θέματα ονομάτων χώρου στο Διαδίκτυο με κατάληξη ".gr" και είναι αρμόδια για θέματα ονομάτων χώρου με κατάληξη ".eu".
- Ρυθμίζει τα θέματα της ηλεκτρονικής υπογραφής.
- Ρυθμίζει τα θέματα πρόσβασης και διασύνδεσης.
- Ασκεί αρμοδιότητες σχετικές με την παροχή Καθολικής Υπηρεσίας.
- Ρυθμίζει θέματα προστασίας του καταναλωτή στον τομέα των ηλεκτρονικών επικοινωνιών και στον τομέα παροχής ταχυδρομικών υπηρεσιών.
- Ρυθμίζει και εποπτεύει την αγορά παροχής ταχυδρομικών υπηρεσιών.
- Διαχειρίζεται το εμπορικό φάσμα ραδιοσυχνοτήτων με την εξαίρεση της ραδιοφωνίας και της τηλεόρασης. Στο πλαίσιο αυτό,
  - ✓ Καθορίζει τις περιπτώσεις στις οποίες απαιτούνται δικαιώματα χρήσης ραδιοσυχνοτήτων.

- ✓ Χορηγεί τα δικαιώματα χρήσης ραδιοσυχνοτήτων.
- ✓ Καθορίζει τα τέλη χρήσης ραδιοσυχνοτήτων.
- ✓ Εποπτεύει και ελέγχει την χρήση του φάσματος επιβάλλοντας σχετικές κυρώσεις.
- ✓ Τηρεί το εθνικό μητρώο ραδιοσυχνοτήτων.
- ✓ Χορηγεί τις άδειες κατασκευών κεραιών στην ξηρά.

Είναι ο αρμόδιος φορέας για τα θέματα διάθεσης και χρήσης του τερματικού τηλεπικοινωνιακού εξοπλισμού και του ραδιοεξοπλισμού.

### 5.9.2 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) [65] λειτουργεί από το 1997 σύμφωνα με τις διατάξεις του νόμου 2472/1997 και αποτελεί ένα ελεγκτικό όργανο, το οποίο είναι επιφορτισμένο να ελέγχει την εφαρμογή του νομικού πλέγματος πάνω σε αθέμιτες παραβάσεις του προσωπικού απορρήτου. Επίσης, όσον αφορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, εφαρμόζει το νόμο 3471/2006 που ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή οδηγία 58/2002.

Η αρχή αυτή, είναι ανεξάρτητη διοικητική αρχή, με δικό της προϋπολογισμό και δική της γραμματεία, συγκροτείται από τον πρόεδρο που είναι απαραίτητα δικαστικός λειτουργός βαθμού Συμβούλου της Επικρατείας ή αντίστοιχου και άνω και έξι μέλη. Τα μέλη αποτελούνται από δύο καθηγητές ή αναπληρωτές καθηγητές πανεπιστημίου, σε γνωστικό αντικείμενο του δικαίου και της πληροφορικής αντίστοιχα, έναν καθηγητή η αναπληρωτή καθηγητή πανεπιστημίου και τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα. Ο πρόεδρος επιλέγεται από το Υπουργικό Συμβούλιο ενώ τα μέλη από τη Διάσκεψη των Προέδρων της Βουλής μετά τη διατύπωση γνώμης από την Επιτροπή Διαφάνειας και Θεσμών της Βουλής, με διάρκεια θητείας τα τέσσερα έτη, με μία μόνο ανανέωση[63]

Πρωταρχικός σκοπός της Αρχής, πέρα από την παροχή προστασίας στον πολίτη οφειλόμενη στην παράνομη επεξεργασία των προσωπικών του δεδομένων, είναι και η παροχή βοήθειας σε αυτόν έπειτα από παραβίαση των σχετικών δικαιωμάτων του σε κάποιον επιχειρησιακό τομέα.

#### 5.9.2.1 Αρμοδιότητες Α.Π.Δ.Π.Χ

Οι αρμοδιότητες της Αρχής διακρίνονται σε τρεις τομείς. Στις διοικητικές – ελεγκτικές, στις κανονιστικές – συμβουλευτικές και σ' αυτές της δημοσιοποίησης – απολογισμού και συνεργασιών.[67]

Σύμφωνα με τις διοικητικές – ελεγκτικές αρμοδιότητες που έχει η Αρχή, της δίνεται η δυνατότητα να:

- ➢ Εκδίδει άδειες για τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, για τη διαβίβαση δεδομένων σε χώρες εκτός Ε.Ε. ή/και για τη διασύνδεση δεδομένων,
- ➢ Μπορεί να απευθύνει υποδείξεις και συστάσεις σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας και τέλος
- ➢ Μπορεί να ενεργήσει αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε κάθε είδους αρχείο, απόρρητο ή μη, τόσο του δημόσιου όσο και του ιδιωτικού τομέα.

[63] Αλεξανδροπούλου – Αιγυπτιάδου, Ε (2002). *Ζητήματα από το δίκαιο πληροφορικής*. Αθήνα – Κομοτηνή. Σάκκουλας Αντ. 43

Σύμφωνα με τις κανονιστικές – συμβουλευτικές αρμοδιότητες που έχει, μπορεί να:

- Εκδίδει Οδηγίες που θα αφορούν στην ενιαία εφαρμογή των ρυθμίσεων περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και Κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων,
- Απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους όπως επίσης και να βοηθάει τα επαγγελματικά σωματεία και λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία στην κατάρτιση κωδίκων δεοντολογίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και τέλος
- Γνωμοδοτεί για κάθε ρύθμιση που αφορά στην επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με τις αρμοδιότητες δημοσιοποίησης – απολογισμού και συνεργασιών που έχει, δύναται να :

- Συντάσσει ετήσια έκθεση με τον απολογισμό της αποστολής της κατά το προηγούμενο ημερολογιακό έτος,
- Ανακοινώνει στη Βουλή παραβάσεις των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Συνεργάζεται με αντίστοιχες αρχές άλλων κρατών μελών της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στο πλαίσιο άσκησης των αρμοδιοτήτων της, διενήργησε δέκα (10) διοικητικούς ελέγχους σε δημόσια και ιδιωτικά νοσοκομεία και κλινικές κατά το έτος 2011 με σκοπό την αξιολόγηση του επιπέδου ασφαλείας και προστασίας των προσωπικών δεδομένων των πληροφοριακών συστημάτων τους καθώς και τη συμβουλευτική υποστήριξή για την αντιμετώπιση των κινδύνων ασφαλείας με έμφαση στη χρήση ηλεκτρονικών δικτύων και επικοινωνιών για τη διαχείριση των δεδομένων υγείας των ασθενών, όπως επίσης και τη λειτουργία ειδικευμένων ηλεκτρονικών εφαρμογών, όπως ο ηλεκτρονικός ιατρικός φάκελος ασθενή. Ο έλεγχος δηλαδή που διεξήγαγε αφορούσε στα άρθρα 4,6,7,10,11 και 12 του νόμου 2472/97 και κατέληξε στο συμπέρασμα ότι το επίπεδο ασφάλειας ιδίως στα δημόσια νοσοκομεία είναι γενικά ανεπαρκές και οφείλεται κυρίως στην έλλειψη οργάνωσης και διαδικασιών παρά σε αμιγώς τεχνικές ελλείψεις.[66]

### 5.9.3 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε) [68], ιδρύθηκε το 2003 και λειτουργεί ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του νόμου 3115/2003. Αποσκοπεί στην προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Επιπλέον στις αρμοδιότητές της, περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου που προβλέπονται από το νόμο.

Η ΑΔΑΕ συγκροτείται από την ολομέλεια η οποία αποτελείται από τον Πρόεδρο, τον Αντιπρόεδρο και άλλα πέντε μέλη καθώς και τους αναπληρωτές τους. Η επιλογή όλων αυτών γίνεται από τη Βουλή και για να επιλεγούν θα πρέπει να διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα είτε αυτή αφορά τον τεχνικό τομέα των επικοινωνιών είτε το νομικό.

### 5.9.3.1 Αρμοδιότητες Α.Δ.Α.Ε

Οι αρμοδιότητες της ΑΔΑΕ διακρίνονται σε ελεγκτικές, γνωμοδοτικές και κανονιστικές ενώ έχει τη δυνατότητα να επιβάλλει κυρώσεις στις περιπτώσεις που θα εντοπίζει παράβαση της νομοθεσίας.

Πιο αναλυτικά οι αρμοδιότητες της όπως ακριβώς παρουσιάζονται στο νόμο 3115/2003 είναι οι εξής: [69]

- Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας τακτικούς και έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της ΕΥΠ, άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημοσίου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την *επικοινωνία*. Οι έλεγχοι διενεργούνται από τα μέλη και το προσωπικό της ΑΔΑΕ προκειμένου να διαπιστωθεί η σωστή εφαρμογή των πολιτικών ασφάλειας που επιβάλλεται να εφαρμόζουν οι πάροχοι ή για τη διαπίστωση παραβίασης του απορρήτου της επικοινωνίας.
- Λαμβάνει πληροφορίες σχετικές με την αποστολή της από τις προαναφερθείσες υπηρεσίες, οργανισμούς και επιχειρήσεις, καθώς και από τους εποπτεύοντες Υπουργούς.
- Καλεί σε ακρόαση τις ως άνω υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις και κάθε άλλο πρόσωπο, που κρίνει ότι μπορεί να συμβάλει στην εκπλήρωση της αποστολής της.
- Προβαίνει σε κατάσχεση των μέσων παραβίασης του απορρήτου που υποπίπτουν στην αντίληψή της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει επίσης στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.
- Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.
- Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών, καθώς και με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.
- Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και τη διαδικασία άρσης του.
- Εκδίδει κανονιστικές πράξεις που δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως με τις οποίες ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών.

### 5.9.3.2 Διοικητικές Κυρώσεις που Επιβάλλει η ΑΔΑΕ

Οι διοικητικές κυρώσεις που μπορεί να επιβάλλει η ΑΔΑΕ σε κάποιο νομικό ή φυσικό πρόσωπο εξαιτίας κάποιας παραβάσεως που θα αφορά το απόρρητο των επικοινωνιών ή τους όρους και τις διαδικασίες άρσης του, θα πρέπει να είναι ειδικά αιτιολογημένες αφού θα έχει προηγηθεί πρώτα κλήση για παροχή εξηγήσεων από τους υπαίτιους. Οι κυρώσεις αυτές μπορεί να είναι:

- Σύσταση για συμμόρφωση σε συγκεκριμένη διάταξη της νομοθεσίας με προειδοποίηση επιβολής κυρώσεων σε περίπτωση υποτροπής, και
- Πρόστιμο από δεκαπέντε χιλιάδες (15.000 ευρώ) έως ένα εκατομμύριο πεντακόσιες χιλιάδες ευρώ (1.500.000 ευρώ).

Οι διοικητικές κυρώσεις που μπορεί να επιβάλλει και αφορούν στο απόρρητο της τηλεφωνικής επικοινωνίας είναι:

- Σύσταση για συμμόρφωση μέσα στα χρονικά όρια της τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,
- Πρόστιμο από 20.000 ευρώ έως 5.000.000 ευρώ και
- Αναστολή από ένα μήνα έως ένα έτος ή οριστική ανάκληση του δικαιώματος παροχής υπηρεσιών τηλεφωνίας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

# 6 Σύνοψη / Συμπεράσματα

Στα πλαίσια της εργασίας αυτής έγινε μία προσπάθεια καταγραφής τόσο των τεχνικών μέτρων όσο και των νομοθετικών ρυθμίσεων που εφαρμόζονται παράλληλα σε παγκόσμιο επίπεδο αλλά και ειδικότερα στην ελληνική επικράτεια και αποβλέπουν στην καταπολέμηση κάθε αθέμιτης προσπάθειας συλλογής και επεξεργασίας προσωπικών δεδομένων.

Είναι γεγονός ότι σχεδόν όλες οι δραστηριότητες του ανθρώπου στο διαδίκτυο, όπως είναι η πραγματοποίηση αγορών, οι τραπεζικές συναλλαγές, η on-line επικοινωνία, η ανταλλαγή αρχείων, μέχρι και το απλό “σερφάρισμα” στις φαινομενικά αθώες ιστοσελίδες του, προϋποθέτουν, εκ μέρους του χρήστη, τη διαβίβαση πληροφοριών, που εμπεριέχουν στοιχεία ευαίσθητων ή μη δεδομένων προσωπικού χαρακτήρα προς αποδέκτες αμφιβόλου προελεύσεως και αξιοπιστίας. Γι’ αυτό λοιπόν το λόγο, όπως επίσης και εξαιτίας της πολυπλοκότητας του διαδικτύου, που επιτρέπει τη διείσδυση των διαφόρων κακοπροαίρετων εισβολέων, είναι δυνατόν πολλές φορές να επιτυγχάνεται η παραβίαση της ασφαλείας του απορρήτου των επικοινωνιών. Ως εκ τούτου, αναγνωρίζεται η ανάγκη για παροχή εξασφαλισμένης προστασίας των προσωπικών δεδομένων με τη συνεχή παρακολούθηση των εξελίξεων από τεχνικής απόψεως αλλά και από την πλευρά του νομοθέτη, ώστε να είναι εφικτή η καλλιέργεια ενός αισθήματος ασφάλειας από μέρους του χρήστη, το οποίο θα είναι ικανό να τον πείσει να κάνει χρήση της τεχνολογίας αυτής προς όφελός του και όχι εις βάρος της προσωπικότητας και της ιδιωτικότητάς του.

Έτσι με την εκτενή παρουσίαση και των δύο αυτών πυλώνων προστασίας των προσωπικών δεδομένων και δεδομένου ότι καθημερινά η τεχνολογία του διαδικτύου εξελίσσεται, γίνεται κατανοητό ότι το δίκαιο της πληροφορικής τεχνολογίας, καθώς και η τεχνολογία προστασίας του, πρέπει να βρίσκονται σε διαρκή εξέλιξη και να ακολουθούν από απόσταση αναπνοής τη δυναμική εξέλιξη της τεχνολογίας, ώστε να μπορούν αντιμετωπίζουν αλλά και να προλαμβάνουν εν τη γενέσει, όπου αυτό είναι εφικτό, οποιαδήποτε απειλή προκύπτει.

Καταλήγοντας μπορούμε να πούμε ότι πρακτικά, ποτέ δεν θα καταφέρουμε να αποκτήσουμε ένα σύστημα τόσο τεχνικό όσο και νομικό το οποίο θα είναι σε θέση να μας διασφαλίσει την απόλυτη ασφάλεια των προσωπικών μας δεδομένων. Αυτό που μπορεί να γίνει όμως, είναι να εξασφαλιστεί το δικαίωμα του κάθε χρήστη να γνωρίζει πότε, ποιος και για ποιο λόγο συλλέγει τα προσωπικά του δεδομένα. Η εκ των υστέρων νομική αντιμετώπιση των παραβιάσεων της σφαίρας του απορρήτου δεν αποτελεί πάντα λύση του προβλήματος, γι’ αυτό θα πρέπει να γίνει συνείδηση η ανάπτυξη και αξιοποίηση μιας προστατευτικής τεχνολογίας που θα έχει σα στόχο την ανωνυμία του χρήστη καθώς και τη δυνατότητα του χρήστη να μπορεί να φιλτράρει και να επιλέγει ο ίδιος τα δικαιώματα χρήσης των προσωπικών του δεδομένων.[109]

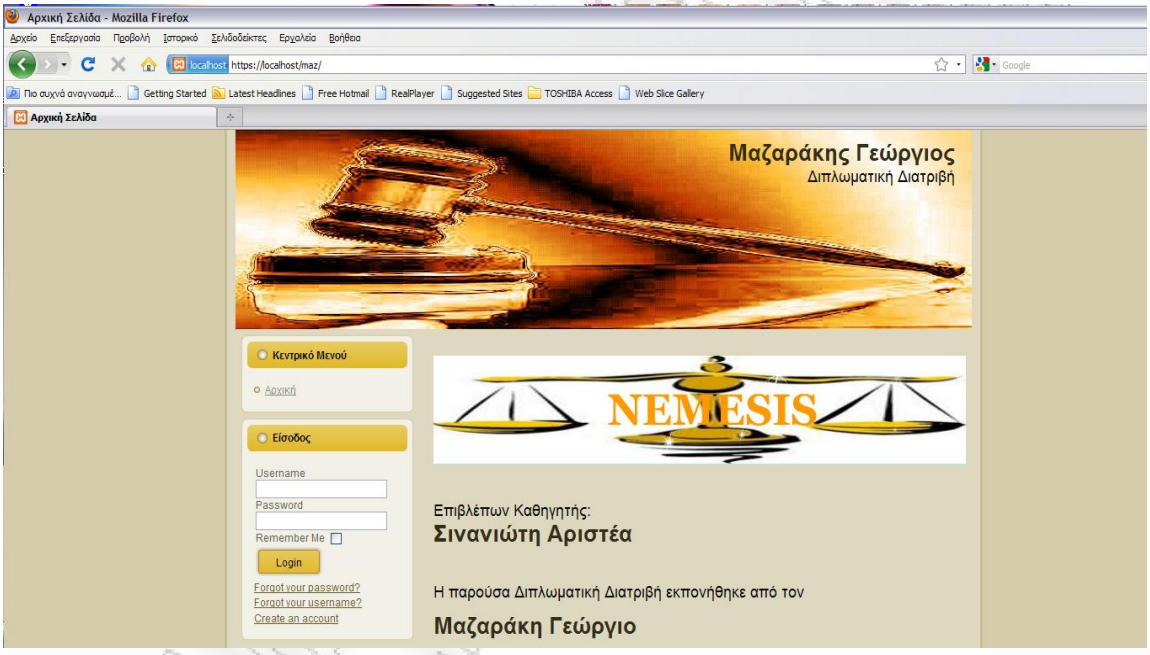
# 7 Υλοποίηση Ασφαλούς Ιστοσελίδας

## 7.1 Εισαγωγή

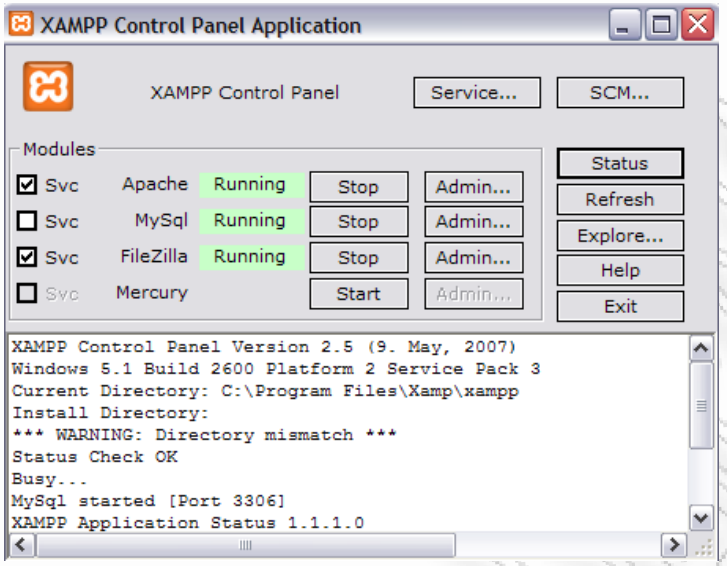
Για τη μετάβαση από τη θεωρία στην πράξη, υλοποιήθηκε η κατασκευή μιας ασφαλούς ιστοσελίδας που απευθύνεται σε δύο είδη χρηστών. Σε αυτούς που έχουν κάνει είσοδο στην ιστοσελίδα, οπότε και έχουν πρόσβαση στο περιεχόμενο της (άρθρα, εικόνες) και σ' αυτούς που είναι απλοί επισκέπτες οπότε και έχουν πρόσβαση σε γενικό περιεχόμενο αφού δεν έχουν δημιουργήσει λογαριασμό σύνδεσης.

## 7.2 Υλοποίηση Ιστοσελίδας «NEMESIS»

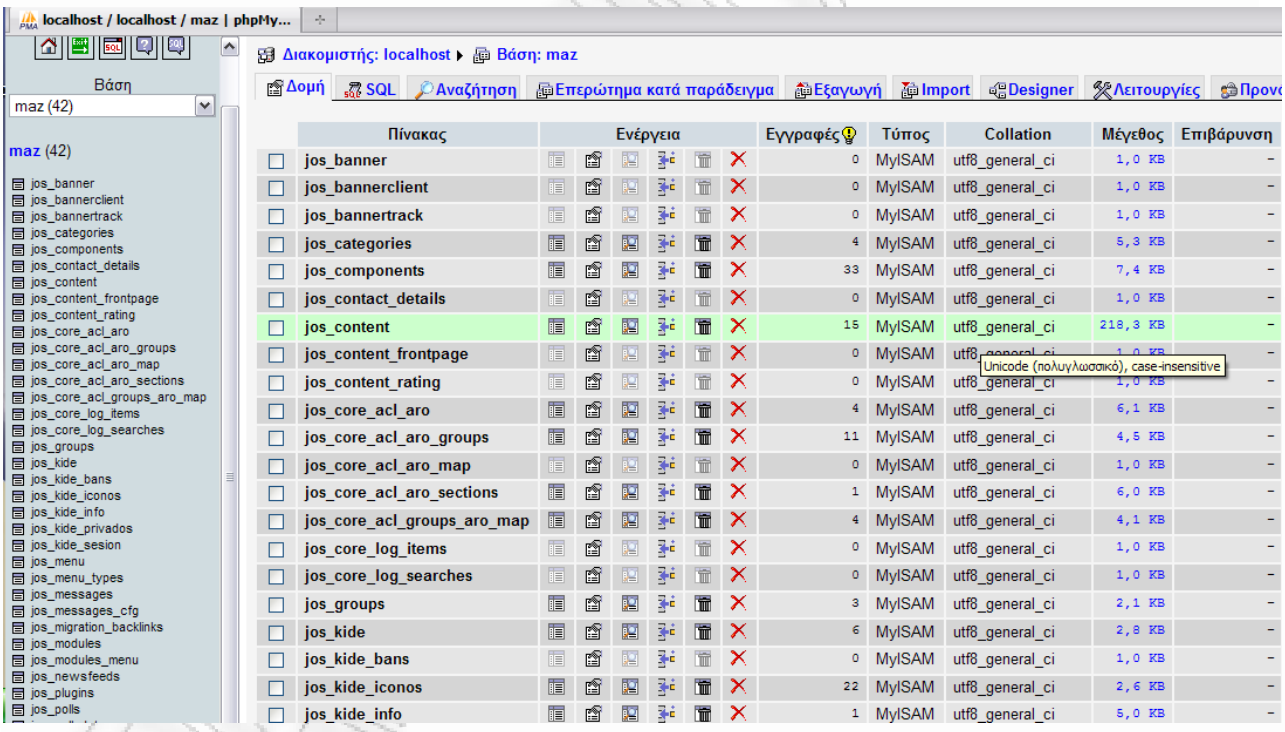
Η υλοποίηση της ασφαλούς δυναμικής ιστοσελίδας «NEMESIS» (Εικόνα 1) έχει λάβει χώρα σε υπολογιστή που τρέχει Windows XP και που χρησιμοποιεί το XAMPP 1.6.7 (Εικόνα 2) ως virtual server με Apache HTTP Server και MySQL ως βάση δεδομένων (Εικόνα 3). Ως cms (content management system) χρησιμοποιήθηκε το joomla 1.5.21 (Εικόνα 4) και για την έκδοση του πιστοποιητικού ασφαλείας χρησιμοποιήθηκε η εντολή makecert που υποστηρίζεται από το XAMPP.



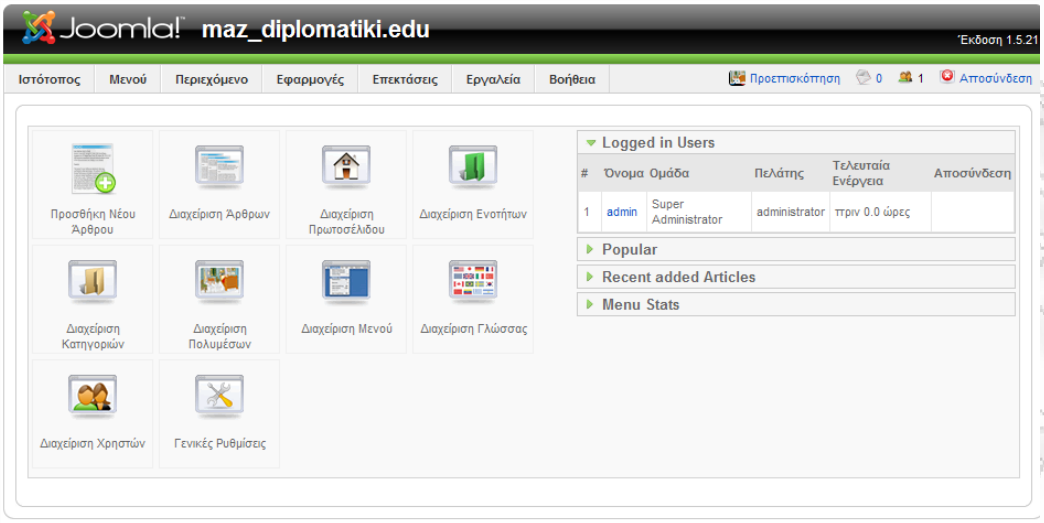

**Εικόνα 1 :Ιστοσελίδα "Nemesis"**




**Εικόνα 2 :XAMPP**




**Εικόνα 3 : Βάση Δεδομένων MySQL**

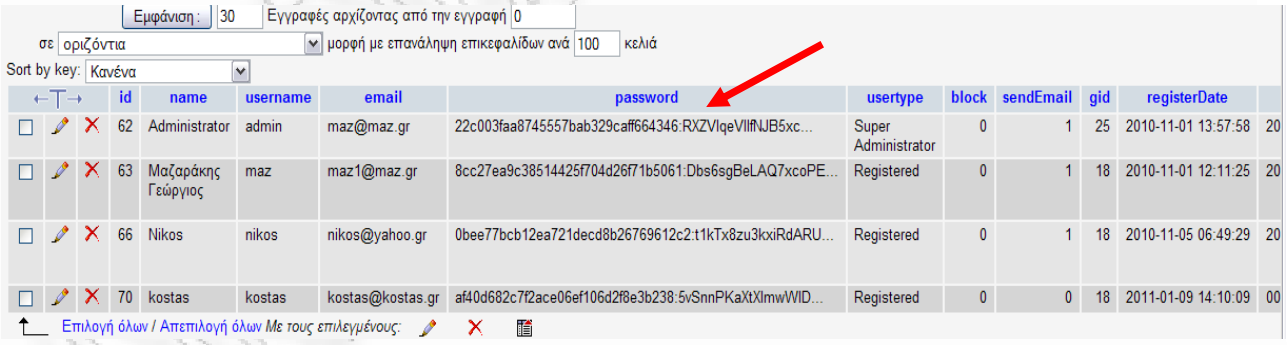



**Εικόνα 4 :Περιβάλλον Joomla**

## 7.3 Τυπικά Μέτρα Ασφαλείας

### 7.3.1 Password Hash values

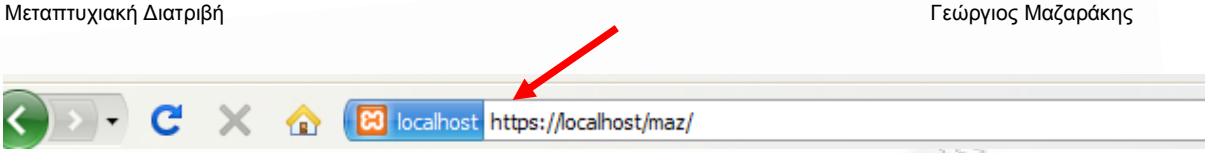
Σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι hash values των κωδικών αντί για τους ίδιους τους κωδικούς. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του. Στη συγκεκριμένη περίπτωση οι κωδικοί των χρηστών έχουν κρυπτογραφηθεί με τη βοήθεια του αλγορίθμου sha1 (Εικόνα 5).




**Εικόνα 5 :Κρυπτογραφημένος κωδικός χρήστη**

### 7.3.2 SSL Protocol

Η ιστοσελίδα στηρίζεται πάνω στο πρωτόκολλο SSL γι' αυτό το λόγο και το URL της ξεκινάει από https και όχι από το κοινό http (εικόνα 6). Τα δεδομένα που ανταλλάσσονται μεταξύ του browser και του web browser κρυπτογραφούνται σύμφωνα με τη διαδικασία που περιγράφτηκε στο 4$^{o}$ κεφάλαιο της παρούσας διατριβής.




**Εικόνα 6 : Χρήση πρωτοκόλλου SSL**

### 7.3.3 Δημιουργία Self signed Πιστοποιητικού

Για να επιτραπεί στο χρήστη η διαβίβαση των δεδομένων του να είναι κρυπτογραφημένη θα πρέπει η ιστοσελίδα μας να χρησιμοποιεί το πρωτόκολλο SSL και να είναι πιστοποιημένη από κάποια αρχή πιστοποίησης. Στη συγκεκριμένη περίπτωση επειδή η ιστοσελίδα μας είναι ανεβασμένη τοπικά, θα δημιουργήσουμε μόνοι μας το πιστοποιητικό της με τη χρησιμοποίηση της εντολής makecert που μας δίνει ο XAMPP, έτσι ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε μια γραμμή εντολής (Start->Run, γράφουμε “cmd” και πατάμε “OK)
2. Γράφουμε cd c:\xampp\apache
3. Και τέλος γράφουμε makecert

Οπότε μετά θα δούμε το εξής:

```
C:\xampp\apache>newcert
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.............................++++++
.....................................++++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
```

Πληκτρολογούμε μία μυστική φράση για το ιδιωτικό μας κλειδί και πατάμε Enter, οπότε εμφανίζεται το εξής:

```
Verifying - Enter PEM pass phrase:
```

Και ξαναγράφουμε την ίδια φράση για επιβεβαίωση και πατάμε enter οπότε προκύπτει το εξής:

```
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
```

Γράφουμε τα 2 γράμματα που αντιστοιχούν στη χώρα μας και διάφορες άλλες πληροφορίες που μας ζητάει μέχρι να φτάσουμε στο Common Name

```
State or Province Name (full name) [Some-State]:Piraeus
Locality Name (eg, city) []:Piraeus
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nemesis
Organizational Unit Name (eg, section) []:Nemesis
Common Name (eg, YOUR name) []:localhost/maz
```

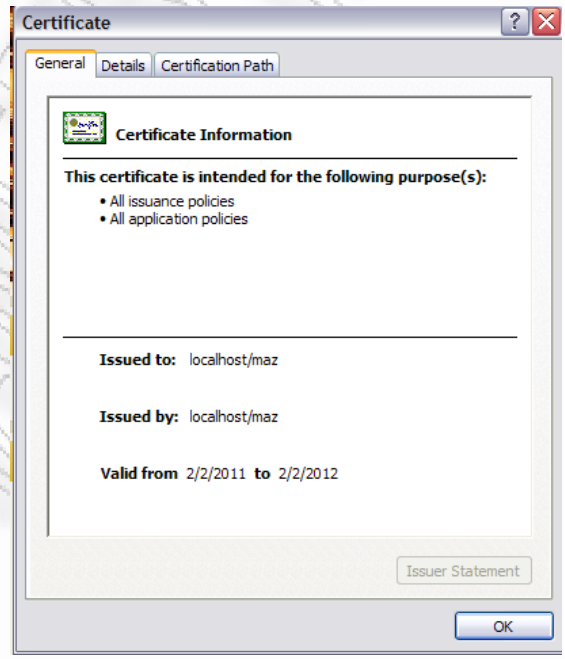
Στο Common Name (CN) θα πρέπει να βάλουμε το DNS όνομα της ιστοσελίδας μας ή το IP της. Στο challenge password θα πρέπει να βάλουμε προαιρετικά τον κωδικό που θα πιστοποιήσει τη διαδικασία ανάκλησης του πιστοποιητικού. Παρακάτω ζητάει επιπλέον πληροφορίες που μπορούμε να τις δώσουμε και τελικά μας ζητάει τη μυστική φράση που βάλαμε παραπάνω.

```
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Enter pass phrase for privkey.pem:
```

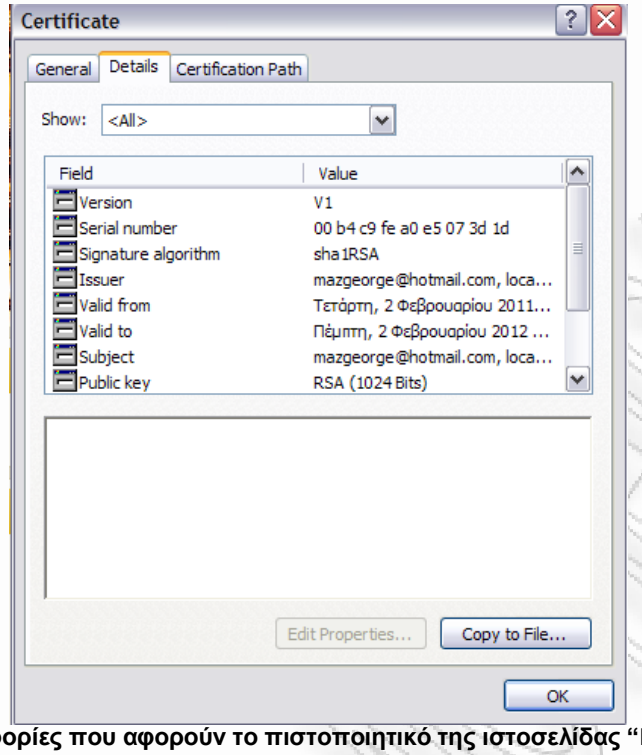
Οπότε την ξαναγράφουμε και καταλήγει στο εξής:

```
writing RSA key
Loading 'screen' into random state - done
Signature ok
subject=/C=xx/ST=xx/L=xxxx/O=xxx/CN=commonname
Getting Private key
--
Das Zertifikat wurde erstellt.
The certificate was provided.

Press any key to continue . . .

C:\xampp\apache>
```

Μ' αυτόν τον τρόπο τελειώσαμε με την κατασκευή του πιστοποιητικού και του ιδιωτικού κλειδιού της ιστοσελίδας και έτσι το makecert.bat sript θα μεταφέρει αυτόματα το πιστοποιητικό και το κλειδί στους φακέλους που πρέπει. Σαν τελευταίο βήμα αυτό που πρέπει να γίνει από εμάς λόγω του ότι το πιστοποιητικό είναι υπογεγραμμένο από εμάς και όχι από κάποια διαπιστευμένη αρχή πιστοποίησης, είναι να μεταφερθεί και να αναγνωριστεί από το φυλλομετρητή που χρησιμοποιούμε.




**Εικόνα 6 : Το πιστοποιητικό της ιστοσελίδας "Nemesis"**




**Εικόνα 7 : Πληροφορίες που αφορούν το πιστοποιητικό της ιστοσελίδας "Nemesis"**

### 7.3.4 Εισαγωγή CAPTCHA

Για την αποφυγή αυτοματοποιημένων μηνυμάτων στο Forum της ιστοσελίδας καθώς και την αποτροπή ψεύτικων εγγραφών χρησιμοποιήθηκε ένα πρόσθετο μέτρο ασφαλείας κατά την κατασκευή της ιστοσελίδας που ονομάζεται CAPTCHA («**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part»). Το πρόσθετο αυτό χρησιμοποιήθηκε για να εξασφαλίσει ότι κάθε ένας που εγγράφεται στην ιστοσελίδα είναι σίγουρα άνθρωπος. Η πιο κοινή δοκιμασία που υποβάλει το χρήστη, είναι το να του ζητήσει να πληκτρολογήσει μια σειρά από γράμματα ή αριθμούς που εμφανίζονται παραμορφωμένα.


**Εικόνα 8: Δοκιμασία CAPTCHA κατά την εγγραφή**

Χρησιμοποιήθηκε το Osol captcha το οποίο είναι διαθέσιμο στον εξής ιστότοπο: http://www.outsource-online.net/osol-captcha-download.html

### 7.3.5 Προστασία από Υποκλοπή Περιεχομένου

Η λειτουργία όλων των μηχανών αναζήτησης στηρίζεται στα λεγόμενα "robots" και "web crawlers" προγραμμάτων, που έχουν τη δυνατότητα να σαρώνουν τα περιεχόμενα καθώς και τις εικόνες των ιστοσελίδων του διαδικτύου και να τα καταχωρούν σε βάσεις δεδομένων για περαιτέρω επεξεργασία.

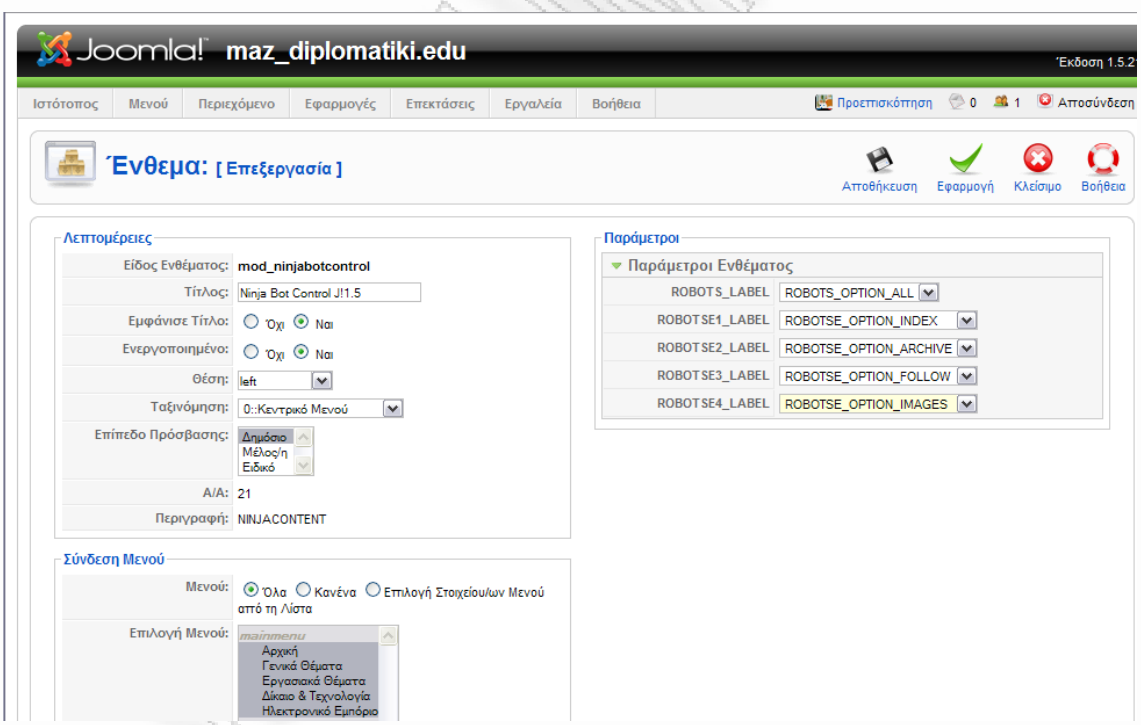
Μία λύση για την αποφυγή αυτής της ανεπιθύμητης ενέργειας είναι η δημιουργία και η τοποθέτηση του αρχείου robots.txt, στον κεντρικό φάκελο που είναι αποθηκευμένη η ιστοσελίδα μας. Στο αρχείο αυτό έχουμε τη δυνατότητα να αναγράψουμε χειροκίνητα τα αρχεία και τους φακέλους που δεν θέλουμε να είναι ορατά από τις μηχανές αναζήτησης.

Για την αποφυγή αυτής της καθόλου βολικής διαδικασίας, χρησιμοποιήθηκε το πρόσθετο NinjaBot control το οποίο έχει τις εξής δυνατότητες.

- Αποτρέπει την υποκλοπή των εικόνων καθώς και του συνδέσμου που οδηγεί στην ιστοσελίδα μας από τις διάφορες μηχανές αναζήτησης.
- Αποκρύπτει το περιεχόμενο της ιστοσελίδας μας από τις διάφορες μηχανές αναζήτησης.

Το Ninjabot control βρίσκεται στον εξής ιστότοπο και υποστηρίζει τις παρακάτω μηχανές αναζήτησης Google, Yahoo, Ask, MSN/Live.

http://extensions.joomla.org/extensions/site-management/seo-a-metadata/3927




**Εικόνα 9 : Ninjabot control**

### 7.3.6 E-mail Επιβεβαίωσης

Η χρησιμοποιηθείσα έκδοση του Joomla για την αποφυγή δημιουργίας λογαριασμού από μη ανθρώπινη υπόσταση δίνει τη δυνατότητα στο σύστημα να αποστείλει e-mail επιβεβαίωσης στο γραμματοκιβώτιο του χρήστη. Αυτό σημαίνει ότι για να ενεργοποιηθεί ο λογαριασμός του νέου χρήστη, θα πρέπει αυτός να κάνει click πρώτα, πάνω στο σύνδεσμο που του έχει αποσταλεί. Επιπλέον προστέθηκε άλλο ένα ένθεμα, το οποίο πέρα από την επιβεβαίωση του χρήστη απαιτεί και την επιβεβαίωση του administrator για να ολοκληρωθεί η διαδικασία δημιουργίας λογαριασμού.

Το πρόσθετο αυτό ονομάζεται joomlaxi-admin-approval-plugin-2.0.42 και βρίσκεται στον παρακάτω ιστότοπο:

http://extensions.joomla.org/extensions/access-a-security/authentication/10737

### 7.3.7 Αλλαγή URL εισόδου του administrator

Τέλος, επειδή οι επίδοξοι εισβολείς μπορούν εύκολα να διαπιστώσουν αν η ιστοσελίδα είναι φτιαγμένη με Joomla πληκτρολογώντας απλά /administrator στο τέλος του URL της ιστοσελίδας μας, χρησιμοποίησα ένα πρόσθετο το οποίο επιτρέπει στον administrator να εισαγάγει ένα μυστικό κωδικό στο τέλος του URL, το οποίο θα τον ανακατευθύνει κατ' ευθείαν στη σελίδα διαχείρισης της ιστοσελίδας χωρίς να χρειαστεί να περάσει από το login panel του administrator.

Για παράδειγμα αν έχουμε ορίσει σα μυστικό κωδικό τη λέξη "varadero1000", τότε για να μπούμε στην ιστοσελίδα διαχείρισης της ιστοσελίδας αρκεί να πληκτρολογήσουμε localhost/maz/administrator?varadero1000. Το πρόσθετο αυτό βρίσκεται στη ιστοσελίδα http://extensions.joomla.org/extensions/access-a-security/site-security/login-protection/15711

## 7.4 Επίλογος

Είναι γενικά παραδεκτό ότι δεν μπορεί να υπάρξει απόλυτα ασφαλές πληροφοριακό σύστημα παρά μόνο αν είναι εκτός δικτύου και βρίσκεται κλειδωμένο μόνο του σε κάποιο δωμάτιο. Ο Matthew Strebe στο βιβλίο του "Network Security Foundations" προσπάθησε να δικαιολογήσει το γεγονός της έλλειψης ασφάλειας στα πληροφοριακά συστήματα στηριζόμενος στις παρακάτω απόψεις.[111]

- Δίνεται μεγαλύτερη βαρύτητα στην ταχύτητα παραγωγής και προώθησης νέου λογισμικού παρά στην ασφάλεια, εξ' αιτίας του ανταγωνισμού
- Οι καινούργιες ιδέες λανσάρονται στην αγορά εσπευσμένα πριν μελετηθούν σωστά
- Η εξέλιξη στον τομέα της πληροφορικής είναι ραγδαία
- Οι προγραμματιστές είναι αδύνατον να μην κάνουν προγραμματιστικά σφάλματα
- Δεν υπάρχει ποικιλία στην παγκόσμια αγορά λογισμικού
- Υπάρχει καθυστέρηση στην ανεύρεση λύσεων των προγραμματιστικών κενών ασφαλείας.

Υπάρχουν κάποιες απόψεις που λένε ότι τα πιο ασφαλή συστήματα είναι τα ανοικτά, αυτά δηλαδή που έχουν την αρχιτεκτονική τους πλήρως διαθέσιμη στο κοινό και όχι αυτά που στηρίζονται στη μυστικότητα. Από μία άποψη αυτό είναι σωστό διότι τα συστήματα που στηρίζονται στη μυστικότητα είναι πολύ ευάλωτα από τη στιγμή που θα μαθευτεί η αρχιτεκτονική τους και παραβιαστεί για πρώτη φορά η ασφάλειά τους, από την άλλη δε λόγω της πολυπλοκότητας του σύγχρονου λογισμικού γίνεται αρκετά δύσκολη η διόρθωση όλων των πτυχών ασφαλείας των ανοιχτών συστημάτων. Τελικά αυτό που μπορούμε να συμπεράνουμε είναι ότι η λύση βρίσκεται στην ανάπτυξη ισχυρών μηχανισμών ασφαλείας που θα απαιτούν πολύ χρόνο και κόπο από τους επίδοξους εισβολής ώστε να καταφέρουν να παραβιάσουν τελικά την ασφάλεια τους.

## Παράρτημα Α – Ακρωνύμια

- ISP: Internet Service Provider (Πάροχος υπηρεσιών διαδικτύου)
- HTTP: HyperText Transfer Protocol
- TCP: Transmission Control Protocol (πρωτόκολλο ελέγχου μετάδοσης)
- UDP: User Datagram Protocol
- HTTPS: Hypertext Transfer Protocol Secure
- TLS: Transport Layer Security
- SSL: Secure Sockets Layer
- IP: Internet Protocol
- IPSP: IP Security Policy
- CPU: Central Processing Unit
- FTP: File Transfer Protocol
- BIOS: Basic Input/Output System
- ARPANET: Advanced Research Projects Agency Network
- DMZ: Demilitarized zone
- DLP: Data Loss Prevention software
- IDS: Intrusion Detection Systems
- NIDS: Network Detection Systems
- SMTP: Simple Mail Transfer Protocol
- POP: Post Office Protocol
- IMAP: Internet Message Access Protocol
- DES: Data Encryption Standard
- IDEA: International Data Encryption Algorithm
- CA: Certificate Authority
- MAC: Message Authentication Codes
- CSR: Certificate Request
- ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- ΑΔΑΕ: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
- ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

# Βιβλιογραφία

[1] "In.gr 19/10/2010" έρευνα Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU)
http://www.inews.gr/1/ta-dyo-disekatommyria-tha-xeperasei-fetos-o-diadiktyakos-plithysmos.htm

[2] Λάζος, Γ. (2001). *Πληροφορική και έγκλημα*, Νομική βιβλιοθήκη,16

[3] Μαρίνος, Α. (2003). *Το διαδίκτυο*, Σάκκουλας Αντ. 22

[4] http://www.technews.gr/modules/lexikon/entry.php?entryID=863

[5] www.safeline.gr/Στατιστικά-Στοιχεία

[6] Safer Internet Forum στις 21/11/10 Έρευνα του Δικτύου EU Kids Online.
(http://www.eukidsgreece.gr/)

[7] Warren, S, D and Brandeis, L, D. (1890). *The Right to Privacy*. Harvard Law Review, Vol. IV, No. 5. 193–220.

[8] Ν.2472/1997 "*Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*" άρθρο 2

[9] Επιστημονικό περιοδικό Intellectum τεύχος 4. (Μάιος 2008). 43 - 44

[10] Κιούπης, Δ. (2000). *Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα – Κενά και αδυναμίες της ποινικής νομοθεσίας.* 961

[11] Αγγέλη, Ι. ΠοινΔικ *(*2001). *Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)*. 1218

[12] Κοκολάκης, Σ. (Ιούνιος 2000). *Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτω.* Διδακτορική Διατριβή, Οικονομικό Πανεπιστήμιο Αθήνας. 34

[13] Bosworth, S and Kabay, M. (2002). *Computer Security Handbook.* fourth edition. 29-33,

[14] Steinmetz, R and Nahrstedt, K. (2004). *Multimedia applications*. x-media publishing. 55
http://books.google.gr/books?id=Zw8h5BrEEKMC&pg=PA55&dq=authenticity+non-repudiation+uniqueness&hl=el&ei=PZu-Te7NL9Dx4Qb4urn_BQ&sa=X&oi=book_result&ct=result&resnum=4&ved=0CDkQ6AEwAw#v=onepage&q&f=false

[15] Ενημερωτικός κόμβος Πανελλήνιου Σχολικού Δικτύου
http://blogs.sch.gr/internet-safety/archives/category/%CE%B3%CE%B5%CE%BD%CE%B9%CE%BA%CE%AC

[16] Σχέδιο Νόμου «*ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ ΛΟΙΠΕΣ ΔΙΑΤΑΞΕΙΣ*», Κεφ Α, Άρθρο 3, σελ 2
http://www.tovima.gr/files/1/2011/04/27/ilektrodik.pdf

[17] Καταναλωτικά Βήματα - Τεύχος Ιούνιος - Ιούλιος 2002, 18-04-08
http://kepka.org/index.php?option=com_content&task=view&id=793&Itemid=61

[18] Καράκωστας, Ι. (1998). Το *δίκαιο των ΜΜΕ*. Σάκκουλα Αντ. 326

[19] Whitman, M, E,Herbert and Mattord, J. (2009). *Management of information Security.* third edition. 117-120

[20] Πάσχου Μ. (2009). *Αποδοτικές Τεχνικές Διαχείρισης Εφαρμογών και Υπηρεσιών Διαδικτύου (Web Services) σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης (e-government).* Διπλωματική εργασία Μεταπτυχιακού διπλώματος, Πανεπιστήμιο Πατρών. 69-70

[21] Γκρίτζαλης Δ. (Ιανουάριος 2000). *Ασφάλεια και Αξιοπιστία στην Πληροφορική και τις Επικοινωνίες.* Εργαστηριακές ασκήσεις, έκδοση 1.5, Εργαστήριο Πληροφοριακών Συστημάτων και Βάσεων Δεδομένων, Οικονομικό Πανεπιστήμιο Αθήνας, βλέπε διδακτορική διατριβή Δημήτρη Λέκκα. (2002). *Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων με χρήση υπηρεσιών Έμπιστης Τρίτης Οντότητας.*σελ 26

[22] Strebe, M. (2004). *Network security foundations*. John Wiley & Sons Inc. 20-24

[23] Έθνος on-line 19/10/2010
http://www.ethnos.gr/article.asp?catid=11424&subid=2&pubid=38528948

[24] Μάχη news Live 27/12/2010 http://www.maxhnews.com/content/1951

[25] Merike, K. *Designing Network Security 2nd Edition*. Cisco Press Publications ISBN-10: 1-58705-370-5. 186-200

[26] Strebe, M. (2004). *Network security foundations.* John Wiley & Sons Inc 27-33

[27] The internet Protocol Journal, Volume 7, Number 4. *Distributed Denial of Service Attacks*

[28] Cohen, F. (1987). *Computer viruses: theory and experiments. Computers and Security*. 6(1). 22–35.

[29] Saadi, L. (2004). *Stealth Ciphers.* Victoria, B.C. 124-129

[30] Handbook of information security Volume III: Threats, Vulnerabilities,Prevention, Detection, and Management 263

[31] Weingart, S, H. (2000). *Physical security devices for computer subsystems: a survey of attacks and defenses*. 302.

[32] Schneier, B. (2000). Secrets *and Lies: Digital Security in a Networked World*. John Wiley &Sons, New York, NY, 188-193

[33] Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, τεύχος δεύτερο, αρ. φύλλου 88, 26 Ιανουαρίου 2005. Κεφ 2. Άρθρο 3
http://dide.flo.sch.gr/Plinet/Nomothesia-Internet/ADAE-KanonismosAporritou.pdf

[34] Διεύθυνση δευτεροβάθμιας εκπαίδευσης Π.Ε Φλώρινας, Περιφέρεια Δυτικής Μακεδονίας, http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Firewalls.html

[35] Firewalls FAQ
http://www.faqs.org/faqs/firewalls-faq/

[36] Evolution of the firewall industry , Cisco Documentation, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

[37] Stallings W. (2000) "Network Security Essentials: Applications and Standards".

[38] IT Security Cookbook (2002). Firewalls a technical Overview http://www.boran.com/security/it12-firewall.html

[39] IS Auditing Procedure : P6 Firewalls. (2003). http://www.isaca.org/Knowledge-Center/Standards/Pages/IS-Auditing-Procedure-P6-Firewalls1.aspx

[40] Bennett, J, Jr. (2004).*The digital umbrella: Technology's attack on personal privacy in America*. BrownWalker Press.142

[41] Scarfone, K and Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).*National Institute of Standards and Technology. Chapter 2. 4-8

[43] Διαδικτυακή πύλη του Υπουργείου Παιδείας Δ.Β.Μ.Θ. *Ασφάλεια στο διαδίκτυο*. http://www.e-yliko.gr/htmls/pc_use/smail.aspx

[44] http://www.scribd.com/doc/13055/Email-spoofing-What-is-it-and-how-does-one-deal-with-the-problem

[45] Πατσάκης, Κ, Ε και Φούντας, Ε, Χ. *Κρυπτογραφία και Εφαρμογές*. τόμος Α, Κεφ 5. Βαρβαρήγου.122

[46] Piper, F, C and Murphy, S. (2002). *Cryptography: a very short introduction.* Oxford University Press. New York.10

[47] Abhijit Das,C. E. Veni Madhavan. (2009). *Public- key cryptography: Theory and Practice.*Dorling Kindersley. India. 4-5

[48] http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/dlp_qa.pdf

[49] Rescorla, E. (November 2000). *SSL and TLS: Designing and building Secure Systems.* Addison-Wesley. Chapters 1,2,3. ISBN:9780201615982

[50] Hayoz M. (2003). *Introducing SSL*. MSc Seminar in Telecommunications. Department of Informatics. University of Freiburg. Switzerland. 9-16

[51] Κανονισμός 248/71/2002 της Ε.Ε.Τ.Τ. (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων), ΦΕΚ 603/Β'/16-5-2002, «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής».

[52] Kahate, A. (2008). *Cryptography and network security*. Second Edition. Tata McGraw-Hili Publishing Company Limited. 206-208

[53] Lehtinen, R and Russell, D and Gangemi, G, T. (2006). *Computer Security Basics.* Second edition. O'Reilly Media. 146-149

[54] Alex Sotirov. (2008). *25th Chaos Communication Congress in Berlin on December 30*,

[55] Προεδρικό Διάταγμα 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές. (ΦΕΚ Α΄125/25.6.2001)

[56] Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2002). *Ζητήματα από το Δίκαιο της Πληροφορικής*. Σάκκουλας Αντ. 21

[57] Ιγγλεζάκης, Ι. (2003). *Ευαίσθητα Προσωπικά Δεδομένα.* Σάκκουλας Αντ. *Αθήνα – Θεσσαλονίκη.* 13

[58] Αργυρόπουλος, Α. (2001). *Ηλεκτρονική εγκληματικότητα.* Σάκκουλας Αντ. Αθήνα – Κομοτηνή. 33

[59] Αγγελή, Ι. *Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.* ΠοινΔικ 12/2001.1218

[60] Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, Βουδαπέστη, της 23.11.2001, CETS αριθ.° 185. http://www.diaplous.org/library/nomothesia.php

[61] ΟΙΚΟΥΜΕΝΙΚΗ ΔΙΑΚΗΡΥΞΗ ΓΙΑ ΤΑ ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ, 10 ΔΕΚΕΜΒΡΙΟΥ 1948 http://www.inegsee.gr/equal/equal2/nomothesia/diethnis/%CE%9F%CE%99%CE%9A%CE%9F%CE%A5%CE%9C%CE%95%CE%9D%CE%99%CE%9A%CE%97%20%CE%94%CE%99%CE%91%CE%9A%CE%97%CE%A1%CE%A5%CE%9E%CE%97.pdf

[62] Lessig, L. (1999). *The Law of the Horse: What Cyberlaw Might Teach.* 113 Harv. L. Rev. 501, 504-505.

[63] A. F. Westin, Privacy and Freedom, Atheneum, 1967

[64] The Information and Privacy Commissioner/Ontario, Deloitte & Touche. (2003) ”*The Security-Privacy Paradox: Issues, Misconceptions, and Strategies*. Joint Report. 3

[65] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

[66] ΑΠΔΠΧ Δελτίο τύπου 20-04-2011 http://www.dpa.gr/portal/page?_pageid=33,15117&_dad=portal&_schema=PORTAL

[67] Αρμοδιότητες Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) http://www.dpa.gr/portal/page?_pageid=33,14983&_dad=portal&_schema=PORTAL

[68] http://www.adae.gr/portal/

[69] Νόμος 3115/2003 Ν.3115/2003, άρθρο 6 (ΦΕΚ 47/Α/27.2.2003)

[70] Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) http://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/

[71] ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3431/2006, άρθρο 12 (ΦΕΚ 13/03.02.2006)
http://www.eett.gr/opencms/export/sites/default/admin/downloads/telec/N3431.pdf

[72] Σιδηρόπουλος, Θ. (2008). *Το δίκαιο του διαδικτύου.* Β Έκδοση. Σακκούλας Αντ. 248

[73] Απόφαση 2000/520/ΕΚ της Ευρωπαϊκής Επιτροπής «*σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ*», EEL 115/14

[74] ΔΙΕΘΝΕΣ ΣΥΜΦΩΝΟ ΓΙΑ ΤΑ ΑΤΟΜΙΚΑ ΚΑΙ ΠΟΛΙΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ (ΟΗΕ), 1997,
http://www.nis.gr/npimages/docs/2462-97.pdf

[75] Warren, S and Brandeis, L .(1890) *The Right to Privacy*. 4 Harvard Law Review. 193-220.

[76] Αλεξανδροπούλου – Αιγυπτιάδου, Ε (2002). *Ζητήματα από το δίκαιο πληροφορικής.* Αθήνα – Κομοτηνή. Σάκκουλας Αντ. 48

[77] Gesetz- und Verordnungsblatt für das Land Hessen - Teil I - Nr. 4, Wiesbaden 12.Oktober 1970, 625ff

[78] Public Law No 93-579,88 Stat. 1897 (Dec. 31,1974), 5 U.S.C 552a.

[79] Γέροντας, Α. (1989). *Η ηλεκτρονική επεξεργασία των προσωπικών πληροφοριών (ο γερμανικός ομοσπονδιακός νόμος για την προστασία του πολίτη από την αυτόματη επεξεργασία των προσωπικών πληροφοριών*), σελ 58

[80] Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[81] Convention for the Protection of Individuals with regard to Automatic processing of Personal Data Strasbourg, 28.I.1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[82] ΣΥΜΒΑΣΗ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΣΥΜΦΩΝΙΑΣ ΤΟΥ ΣΕΝΓΚΕΝ της 14ης Ιουνίου 1985
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EL:HTML

[83] Νόμος 2514/1997 (ΦΕΚ Α 140-26'27.6.1997), http://www.opengov.gr/yptp/?p=63

[84] Οδηγία 95/46/ΕΚ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 24ης Οκτωβρίου 1995
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

[85] Σύσταση της Επιτροπής της 29ης Ιουλίου 1981, επίσημη εφημερίδα των Ευρωπαϊκών Κοινοτήτων , 29/08/1981

[86] Οδηγία 97/66 για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.
http://www.go-online.gr/files/legislation/prosopika_dedomena/Odhgies/Odhgia_97_66.pdf

[87] Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EL:HTML

[88] Οδηγία 2002/58/ΕΚ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 12ης Ιουλίου 2002
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EL:PDF

[89] Νόμος 2068/1992 (ΦΕΚ Α 118-9.7.1992),
http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=Nh-i7eUlbMc%3d&tabid=132

[90] Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EL:HTML

[91] Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/LEXURISERV.PDF

[92] Hustinx ,P, J. (2005) .*Data Protection and Security in the European Union.* Wiesbaden. 2
http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2005/05-06-23_Wiesbaden_EN.pdf

[93] ΣΥΜΦΩΝΙΑ, μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών, 30/09/2009
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/d1813d5911e138bdc2256cbd00313d1c/c5ffdf5b790ad656c2256cbe0036f9d8/$FILE/%CE%A3%CE%A5%CE%9C%CE%A6%CE%A9%CE%9D%CE%99%CE%91.pdf

[94]Ασφάλεια στο διαδίκτυο Windows Microsoft
http://windows.microsoft.com/el-GR/windows7/Making-your-network-more-secure

[95] ΣΥΝΤΑΓΜΑ ΤΗΣ ΕΛΛΑΔΑΣ, ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ, ISBN: 978-960-560-097-6,
http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/syntagmaHanatheoritikiVouli_1.pdf

[96] ΦΕΚ Α΄85/18.4.2001

[97] Ιγγλεζάκης, Ι. (2008). *Δίκαιο της Πληροφορικής.* Σάκκουλας Αντ. 224

[98] Αλεξανδροπούλου – Αιγυπτιάδου, Ε (2002). *Ζητήματα από το δίκαιο πληροφορικής.* Αθήνα – Κομοτηνή. Σάκκουλας Αντ. 22

[99] Νόμος 2472/1997
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/2472_97_APR_10_FINAL.PDF

[100] Ιγγλεζάκης Ι. "Ευαίσθητα Προσωπικά Δεδομένα", εκδόσεις Σάκκουλας, 2003, ISBN: 9789603017363

[101] Μήτρου Λ., (2006-2007) *Σημειώσεις στο μάθημα Αρχές Δικαίου και Προστασίας προσωπικών Δεδομένων*, Πανεπιστημίο Αιγαίου.

[102] Παπακωνσταντίνου Ε. (2006). *Νομικά θέματα Πληροφορικής*. Σάκκουλας Αντ. 44

[103] ΑΠΔΠΧ 15.1.2001 Απόφαση υπ' αριθμ. 11 / 2001
http://www.dpa.gr/portal/page?_pageid=33,6948&_dad=portal&_schema=PORTAL

[104] ΑΠΔΠΧ 12.02.2008 Απόφαση υπ' αριθμ 92/2002
http://www.dpa.gr/portal/page?_pageid=33,6948&_dad=portal&_schema=PORTAL

[105] ΤΕΙΡΕΣΙΑΣ Α.Ε http://www.tiresias.gr/

[106] Νόμος 2774/1999 http://www.elinyae.gr/el/lib_file_upload/287A_99.pdf

[107] Νόμος 3471/2006 http://www.nis.gr/npimages/docs/3471-2006.pdf

[108]Νόμος 3917/2011,
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/N%203917_2011.PDF

[109] Ι. Καράκωστας «Δίκαιο και internet. Νομικά ζητήματα του διδικτύου», 2003, ISBN:9604201999

[110] Γεώργιος Νούσκαλης, Ψηφιακή Τεχνολογία και Δίκαιο, εκδόσεις Αντ.Ν. Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2004

[111] Strebe, M .(2004) *Network Security Foundations.* Sybex.