ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΠΛΗΡΟΦΟΡΙΚΗ»

ΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΘΕΜΑ: «ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

ΦΟΙΤΗΤΡΙΑ: ΕΜΜΑΝΟΥΕΛΑ ΓΕΩΡΓΙΟΥ ΠΑΝΑΓΙΩΤΑΚΗ

Τριμελής Εξεταστική Επιτροπή:

1. Αριστέα Σινανιώτη, Επιβλέπουσα Καθηγήτρια
2. Νικήτας Ασημακόπουλος, Καθηγητής
3. Δημήτριος Βέργαδος, Λέκτορας

ΠΕΙΡΑΙΑΣ, 2010

Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Τίτλος:ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
Ονοματεπώνυμο Φοιτητή	Όνομα και επώνυμο: ΕΜΜΑΝΟΥΕΛΑ ΠΑΝΑΓΙΩΤΑΚΗ
Πατρώνυμο	Όνομα πατέρα: ΓΕΩΡΓΙΟΣ
Αριθμός Μητρώου	ΜΠΠΛ/ 07059 ……..
Επιβλέπων	Όνομα Επώνυμο, Βαθμίδα: Δρ. ΑΡΙΣΤΕΑ ΣΙΝΑΝΙΩΤΗ ΚΑΘΗΓΗΤΡΙΑ

ΠΡΑΚΤΙΚΟ ΕΞΕΤΑΣΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ

Στον Πειραιά σήμερα……..ημέρα……και ώρα…….. συνήλθε η παρακάτω Τριμελής Εξεταστική Επιτροπή που έχει οριστεί από το Πρόγραμμα Μεταπτυχιακών Σπουδών «Πληροφορική», για να αξιολογήσει τη μεταπτυχιακή διατριβή της φοιτήτριας Εμμανουέλας Γ. Παναγιωτάκη.

Μετά το τέλος της εξέτασης συντάχτηκε το παρών πρακτικό και δόθηκε ο βαθμός:……..

Τριμελής Εξεταστική Επιτροπή:

1. Αριστέα Σινανιώτη, Επιβλέπουσα Καθηγήτρια
2. Νικήτας Ασημακόπουλος, Καθηγητής
3. Δημήτριος Βέργαδος, Λέκτορας

Τριμελής Εξεταστική Επιτροπή

Ημερομηνία Παράδοσης **Ιούνιος 2010**

Αριστέα Σινανιώτη Καθηγήτρια	Νικήτας Ασημακόπουλος Καθηγητής	Δημήτριος Βέργαδος Λέκτορας

- Το κείμενο να είναι γραμμένο σε font size 10pt με μονό διάστιχο (single spacing) και απόσταση παραγράφων 3pt (after).
- Η πρώτη παράγραφος κάθε ενότητας να μην έχει εσοχή πρώτης γραμμής ενώ οι επόμενες να έχουν εσοχή πρώτης γραμμής.
- Τα περιθώρια σελίδας να είναι 3cm και στις τέσσερεις πλευρές (πάνω, κάτω, αριστερά, δεξιά).
- Τα Headings να είναι όλα με font **Arial Black** και όχι Bold. Το **Heading 1 να είναι 12pt**, το **Heading 2 να είναι 11pt**, το **Heading 3 να είναι 10pt**. Να μην χρησιμοποιείτε Heading 4 και πέρα.
- Να μην αφήνετε κενές γραμμές πριν ή μετά από τα headings και κάθε επίπεδο heading να απέχει 18pt before και 6pt after.
- Οι λεζάντες (captions) στα σχήματα και τους πίνακες να είναι αριστερά στοιχισμένες και να είναι **Arial bold 9pt**.
- Σε κάθε σελίδα να υπάρχει footer (Arial 8pt) με τον τίτλο της διατριβής στα αριστερά. Στο footer επίσης να υπάρχει αρίθμηση σελίδας στα δεξιά και πάλι με font Arial 8pt.
- Σε κάθε σελίδα να υπάρχει header (Arial 8pt) με το όνομα του φοιτητή στα δεξιά και το λεκτικό «Μεταπτυχιακή Διατριβή» στα αριστερά.
- Τα header και footer να απέχουν από τα άκρα του χαρτιού 2.5cm (στο Page Setup).
- Η διατριβή να περιέχει απαραίτητα:
    - Περίληψη (Abstract) σε χωριστή σελίδα (μισή σελίδα Ελληνικά και μισή στα Αγγλικά).
    - Εισαγωγή – Σύντομη Περιγραφή Προβλήματος/Αντικειμένου (μέχρι 3 σελίδες).
    - ....
    - Συμπεράσματα – Περίληψη
    - Βιβλιογραφία

Ευχαριστίες

Από τη θέση αυτή επιθυμώ να ευχαριστήσω από καρδιάς:

- Την καθηγήτρια μου κυρία Αριστέα Σινανιώτη και εισηγήτρια του θέματος της παρούσας εργασίας, για την πολύτιμη πηγή πληροφοριών και την υποστήριξη που μου παρείχε, στα πλαίσια της εκπόνησης της Μεταπτυχιακής Διπλωματικής Διατριβής μου.

- Τον καθηγητή μου και επιβλέποντα κύριο Νικήτα Ασημακόπουλο, που συνέβαλε επικουρικά στη συγγραφή και αξιολόγηση της Μεταπτυχιακής Διπλωματικής Εργασίας μου.

- Το Πανεπιστήμιο Πειραιώς, που μου έδωσε τη δυνατότητα να πραγματοποιήσω το Πρόγραμμα Μεταπτυχιακών Σπουδών στην Πληροφορική. Το «ΜΠΣ Πληροφορική» μου παρέχει την ευκαιρία να ανταποκριθώ με επιτυχία σε σύγχρονα ζητήματα τεχνολογίας και εφαρμογών της επιστήμης, που απαιτεί η ταχύτητα εξέλιξης της πληροφορικής στην ευρύτερη αγορά εργασίας.

- Τους γονείς μου που με στηρίζουν σε όλη την πορεία της ζωής μου και των σπουδών μου και ειδικά τη μητέρα μου που με παρότρυνε να συνεχίσω και να αποκτήσω άρτια υψηλού επιπέδου εκπαίδευση, επιστημονική κατάρτιση και εξειδικευμένες γνώσεις Πληροφορικής.

- Τέλος είμαι ιδιαιτέρως ευγνώμων στο Νίκο μου, για τη σπουδαία και σημαντική βοήθεια, αλλά και την υποστήριξή του.

Απρίλιος 2010

Εμμανουέλα Γ. Παναγιωτάκη

ΠΡΟΛΟΓΟΣ

Στην εργασία αυτή θα προσπαθήσω να αναπτύξω το θέμα της επίδρασης του διαδικτύου στον καταναλωτή. Η μελέτη αυτή θα προσπαθήσει να ερμηνεύσει έννοιες όπως το ηλεκτρονικό έγκλημα, το ηλεκτρονικό εμπόριο, το Spamming και τα Firewalls. Ακόμα έχω εργαστεί πάνω στο μείζον θέμα της προστασίας των ανηλίκων στο διαδίκτυο, αναπτύσσοντας έναν κώδικα γονικής προστασίας που δίνει τη δυνατότητα στους γονείς να απαγορεύουν την πρόσβαση στα ανήλικα παιδιά τους στους κατά την κρίση τους επικίνδυνους ιστοχώρους. Τέλος, δεν θα μπορούσα εφόσον μιλάμε για τη σχέση καταναλωτή διαδικτύου να μην επεκταθώ στην προστασία δεδομένων του καταναλωτή αναφέροντας τους νόμους και τους θεσμούς που τον προστατεύουν.

PREFACE

In this work I will try to develop the subject of effect of internet in the consumer. This study will try it interprets significances as the electronic crime the electronic trade, Spamming and Firewalls. Still I have worked on to more major subject of protection of minors in the internet, developing code of parental protection that gives the possibility in the parents of prohibiting the access in their underage children in at the crisis the dangerous websites. Finally, I have reported the laws and the institutions that protect the consumer in the internet.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Η "*κοινωνία της πληροφορίας*" είναι ο όρος αυτός που χαρακτηρίζει απόλυτα τη νέα εποχή που βαδίζει η ανθρωπότητα σήμερα. Το στοιχείο που χαρακτηρίζει την "*κοινωνία της πληροφορίας*" κατά κύριο λόγο είναι η τεχνολογική ανάπτυξη με ιδιαίτερη σημασία να δίνεται στη ραγδαία ανάπτυξη της τεχνολογίας των υπολογιστών. Με την εργασία αυτή θα προσπαθήσουμε να συμβάλουμε στην παρουσίαση των νέων δεδομένων που διαμορφώνονται για τους καταναλωτές στη νέα εποχή.

Αυτό το νέο είδος κοινωνίας στο οποίο έχουμε εισέλθει, επηρεάζει καταλυτικά πολλές πλευρές της πολιτικής, οικονομικής και κοινωνικής ζωής του ανθρώπου. Αυτό γίνεται άμεσα αντιληπτό εάν συλλογιστούμε την ανάπτυξη του διαδικτύου και τις υπηρεσίες που προσφέρει αυτό στις μέρες μας, την τεράστια επιχειρηματική εκμετάλλευση του διαδικτύου (παροχή ηλεκτρονικών υπηρεσιών, ηλεκτρονικό εμπόριο κ.α.) και γενικότερα την εισχώρηση του ηλεκτρονικού τρόπου ζωής σε όλες τις πτυχές της καθημερινότητας μας (εργασία, οικογένεια, διασκέδαση, εκπαίδευση κ.α.).

Το Internet είναι ένα παγκόσμιο δίκτυο υπολογιστών. Ένα δίκτυο χωρίς κεντρική εξουσία ή κεντρική διαχείριση. Κανένας δεν είναι υπεύθυνος για την λειτουργία του. Υπάρχει επειδή πολλοί οργανισμοί και μεμονωμένα άτομα συμφώνησαν να ανταλλάσσουν πληροφορίες με έναν συγκεκριμένο τρόπο, χρησιμοποιώντας μια συγκεκριμένη τεχνολογία. Αυτή η αποκέντρωση και ατομική προσέγγιση είναι που προσδιορίζει το άρωμα και το στυλ του Internet σήμερα.[1]

Για τους περισσότερους ανθρώπους, το έργο που επιτελείται στο παρασκήνιο προκειμένου να υφίσταται και να λειτουργεί το Internet είναι αόρατο. Για τους εκατομμύρια χρήστες, το Internet είναι απλά κάτι που τους επιτρέπει να μεταφέρουν πληροφορίες κάθε είδους, από το ένα μέρος στο άλλο. Και αυτή η ευελιξία είναι εκείνη που προσδίδει στο Internet την τόσο μεγάλη δύναμή του.

[1] *Καταναλωτικά Βήματα - Τεύχος Οκτωβρίου 2000*

Η παγκόσμια κοινωνία των πληροφοριών αποτελεί σήμερα μια απτή πραγματικότητα, η οποία μας ανήκει και στην οποία ανήκουμε κατά τρόπο αδιαμφισβήτητο, μας περιβάλλει από παντού, γεμίζοντάς μας με την αφθονία της, σαγηνεύοντάς μας με τις υποσχέσεις της και τρομάζοντάς μας με τις εκπλήξεις της. Ο εικονικός κόσμος καταργεί το χώρο και το χρόνο, είναι πάντα εδώ και τώρα δημιουργώντας ένα σύμπαν διαφορετικό και φευγαλέο. Οι αναφορές αλλάζουν. Το Δίκτυο ανοίγει μια ουσιαστική συζήτηση με ολόκληρη την κοινωνία.

Οι συνέπειες της επιταχυνόμενης εφαρμογής του γίνονται αισθητές σε όλα της τα πεδία: στις οικογενειακές σχέσεις, στην ψυχολογική συμπεριφορά των ανθρώπων, στην πολιτική οργάνωση, στον κόσμο των επιχειρήσεων και του εμπορίου, στην εκπαίδευση, στον τρόπο που δουλεύουμε και διασκεδάζουμε. Μας προσφέρει αφθονία πληροφοριών, γκρεμίζει τα γεωγραφικά σύνορα της γνώσης, συνενώνοντας τις εμπειρίες των ανθρώπων και παγκοσμιοποιώντας τους μύθους τους. [2]

Κατά πόσο όμως αυτό το νέο είδος παγκοσμίου και πολύμορφου διαλόγου έχει επηρεάσει την προσωπική μας ζωή; Το διαδίκτυο κρύβει μέσα του κάποιες δυνατότητες που μπορούν να γίνουν καταστροφικές για τα προσωπικά δεδομένα του χρήστη. Αυτό πηγάζει κυρίως από την ανωνυμία του κάθε χρήστη και την εύκολη δυνατότητα πρόσβασης που έχει σε θέματα με ευαίσθητο περιεχόμενο. Κάθε χρήστης κρυμμένος πίσω από την ανωνυμία του, μπορεί να περιπλανάται σε ομαδικές συζητήσεις, αρχεία, αναζήτηση συνομιλητών τις περισσότερες φορές χωρίς τις καλύτερες προθέσεις.

Τα απεριόριστα οφέλη που απολαμβάνουμε από το internet τη σημερινή εποχή είναι αναμφισβήτητα, όπως επίσης αναμφισβήτητο είναι και το γεγονός ότι το διαδίκτυο έχει συντελέσει στη βελτίωση της ποιότητας της ζωής μας. Από την άλλη πλευρά όμως, η μη δημιουργική και ασφαλής χρήση του διαδικτύου μπορεί να μας φέρει αντιμέτωπους με πολύ σοβαρούς κινδύνους. Έτσι το διαδίκτυο από ένα χρήσιμο εργαλείο για τον καθέναν μας, μπορεί να μετατραπεί ανάλογα με τη χρήση που του κάνουμε σ' ένα μέσο που θα μας βλάψει.

Κατά τη χρήση του διαδικτύου πολλοί είναι οι τρόποι με τους οποίους μπορούν να προκληθούν κίνδυνοι. Τέτοια παραδείγματα είναι τα συνημμένα επικίνδυνα αρχεία, τα οποία διακινούνται με τη χρήση του ηλεκτρονικού

[2] *Καταναλωτικά Βήματα - Τεύχος Οκτωβρίου 2000*

ταχυδρομείου, διάφορα προγράμματα πειρατικού λογισμικού και προγραμμάτων άγνωστης και ύποπτης λειτουργικότητας που πρέπει να γίνονται αντικείμενα μεγάλης προσοχής από το χρήστη, διότι έχουν σκοπό να τον βλάψουν.

Κανείς, παρόλο αυτά, δεν είναι απροστάτευτος στο διαδίκτυο. Υπάρχουν δικαιώματα, τρόποι πρόληψης, φορείς και αρχές για την προστασία των χρηστών. Η εργασία αυτή έχει δημιουργηθεί για να σας δώσει οδηγίες και συμβουλές για μια ασφαλή, σωστή και ηθική χρήση του διαδικτύου, έτσι ώστε να προστατευτείτε όσο είναι δυνατόν από τους κινδύνους που ελλοχεύουν στο χώρο του διαδικτύου.[3]

Εισαγωγικά, αναφέρονται κάποια βασικά σημεία που πρέπει να δίνουμε ιδιαίτερη σημασία κατά την πλοήγηση μας στο διαδίκτυο, έτσι ώστε η χρήση του να γίνει περισσότερο ασφαλείς. Έτσι κατά τη χρήση του διαδικτύου πρέπει να γνωρίζουμε τα παρακάτω: [4] [5]

- Για καμία πληροφορία που περιέχεται στον κυβερνοχώρο δεν έχει ελεγχθεί η εγκυρότητα της. Έτσι πολλές από τις πληροφορίες που βομβαρδιζόμαστε καθημερινά από το διαδίκτυο δεν είναι έγκυρες.

- Όσο είναι δυνατόν να αποφεύγεται η κοινοποίηση των προσωπικών στοιχείων (όνομα, τηλέφωνο, email, διεύθυνση, αριθμοί πιστωτικών καρτών).

- Όσον αφορά τη χρήση του διαδικτύου από ανηλίκους, οι γονείς πρέπει να φροντίζουν έτσι ώστε η τοποθέτηση του υπολογιστή να γίνεται σε σημείο που τους επιτρέπει να επιβλέπουν τις ιστοσελίδες που επισκέπτονται τα παιδιά τους.

- Να αποφεύγεται η χρήση του υπολογιστή από ενήλικες χωρίς την παρουσία κάποιου ενήλικα.

- Οι γονείς θα πρέπει να διαμορφώνουν την κατάλληλη επικοινωνία με τα παιδιά τους, έτσι ώστε αυτά να ενθαρρύνονται να δίνουν πληροφορίες

[3] *www.dart.gov.gr/news.aspx*

[4] *http://www.infosoc.gr/infosoc/el-GR/*

[5] www.chania.gr/.../oi_kakotopies_toy_diadiktyoy_kai_mesa_prostasias

σχετικά με αυτούς που μιλάνε στο διαδίκτυο εάν έχουν πέσει θύματα απειλής κα.

- Το διαδίκτυο κάνει την επικοινωνία με άλλα άτομα πολύ εύκολη. Έτσι το διαδίκτυο είναι και αυτό μια κοινωνία και κατ' επέκταση κρύβει τους κινδύνους μιας κοινωνίας.

2. ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

2.1 Ορισμός

Στις μέρες μας, παρατηρείται μια αξιοσημείωτη αλλαγή της καθημερινότητας του ανθρώπου, καθώς και των σχέσεων που αναπτύσσουν μεταξύ τους (οικογένεια, εργασία κ.α.). Σε αυτό έχει συντελέσει η ραγδαία πρόοδος της τεχνολογίας, η ανάπτυξη της πληροφορικής και του διαδικτύου. Πλέον, η πληροφορική έχει εισχωρήσει σε κάθε κλάδο της κοινωνίας μας, βοηθώντας στην πρόοδο και τη βελτίωση της ποιότητας ζωής του ανθρώπου. Σήμερα, ο τρόπος που εξυπηρετούνται οι ανάγκες του ανθρώπου (παραγωγή, εκπαίδευση, συναλλαγές), δε θυμίζει σε τίποτα το παρελθόν και αυτό βασίζεται στην πληροφορική και το διαδίκτυο. Μέσα σ' αυτή τη σύγχρονη κοινωνία, κάποιοι ωφελούμενοι από τις ανατριχιαστικές δυνατότητες που δίνουν οι νέες τεχνολογίες και το διαδίκτυο, βρήκαν να αναπτύξουν μια νέα μορφή εγκλήματος που καλείται με τον όρο **ηλεκτρονικό έγκλημα.**

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα, αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η στενή έννοια "ηλεκτρονική εγκληματικότητα" αναφέρεται στις αξιόποινες πράξεις, όπως είναι η ηλεκτρονική απάτη, η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά, δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα, η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.[6]

2.2 Μορφές Ηλεκτρονικού Εγκλήματος

Τροχοπέδη για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελούν οι μορφές με τις οποίες το συναντάμε. Υπάρχουν ποικίλες μορφές ηλεκτρονικής εγκληματικότητας και με την ακατάπαυστη πρόοδο της τεχνολογίας,

[6] www.e-crime.gr

των υπολογιστικών συστημάτων και του διαδικτύου, εμφανίζονται ακόμα κι άλλες.[7]

Έτσι, δημιουργήθηκε η ανάγκη για την ανάλυση του προβλήματος και τη χάραξη μιας αποτελεσματικής στρατηγικής για την αντιμετώπιση της ηλεκτρονικής εγκληματικότητας. Σήμερα, υπάρχουν νομοθετήματα που προφυλάσσουν τον πολίτη του σύγχρονου ψηφιακού κόσμου από τα ηλεκτρονικά εγκλήματα. Τα νομοθετήματα αυτά προβλέπουν αδικήματα όπως:

- Αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.

- Αδικήματα που σχετίζονται με τους υπολογιστές, όπως η απάτη με Η/Υ και πλαστογραφία.

- Αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.

- Αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Η συνθήκη της Βουδαπέστης (23/11/2001) στην οποία αποτυπώνονται τα συμπεράσματα του Συνεδρίου για το ηλεκτρονικό έγκλημα (convention on Cybercrime), είναι το βασικότερο κείμενο σχετικά με το ηλεκτρονικό έγκλημα στην Ευρώπη. Υπάρχουν όμως και άλλα νομοθετήματα που δρουν για την καταπολέμηση αυτής της νέου είδους εγκληματικότητας.

- Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί εικοσιτέσσερις ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.

- Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.

[7] www.itlawyers.gr/e-crime.htm

- Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.

- Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

- Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων .

- Το έγγραφο με αριθμό 2000/C 124/01, σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.

- Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.[8]

Παρακάτω παρουσιάζονται και να αναλύονται οι μορφές με τις οποίες εμφανίζονται τα ηλεκτρονικά εγκλήματα και πως αυτά καλύπτονται νομοθετικά:

Κυβερνοσφετερισμός – Προστασία των Domain names

Κυβερνοσφετερισμός (cybersquatting) είναι το ηλεκτρονικό αδίκημα κατά το οποίο κάποιος χρήστης του Διαδικτύου για εμπορικούς σκοπούς κατοχυρώνει και χρησιμοποιεί ηλεκτρονική διεύθυνση (domain name) που περιέχει είτε την επωνυμία γνωστών επιχειρήσεων, είτε σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νόμιμων δικαιούχων αλλά και αποκλεισμός τους από τη χρήση του Διαδικτύου με την επωνυμία τους.

[8] *Ευρωπαϊκή νομοθεσία κατά του ηλεκτρονικού εγκλήματος*

Η προστασία γύρω από τα domain names έχει να κάνει με το θέμα της ονομασίας (name) και πιο συγκεκριμένα τα άρθρα 57 και 58 του Αστικού Κώδικα, παρέχουν προστασία στην περίπτωση που τη διαδικτυακή διεύθυνση αποτελεί ένα όνομα. Το άρθρο 13 του νόμου 146/1914, εξασφαλίζει την περίπτωση που υπάρχει εμπορική επωνυμία, δηλαδή όταν ένας έμπορος πραγματοποιεί τις συναλλαγές του μ' ένα συγκεκριμένο όνομα. Ακόμα το άρθρο 13 του νόμου 146/1914, εφαρμόζεται όταν ένα domain name χαρακτηρίζει ένα εικονικό κατάστημα, πράγμα ευρέως διαδεδομένο στις σύγχρονες συναλλαγές. Τέλος τα άρθρα 4, 18 και 26 του νόμου 2239/1994 περί σημάτων, εφαρμόζεται για την αποφυγή συγχύσεων στις συναλλαγές σχετικά με την περίπτωση που η ηλεκτρονική διεύθυνση ταυτίζεται με το θέμα.

Παράνομη διείσδυση σε δεδομένα (hacking, cracking)- Προστασία του απορρήτου στο Διαδίκτυο

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ. [9]

Cracking είναι η αλλαγή των κωδικών πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους. [10]

Το άρθρο 370Γ τιμωρεί την άνευ εξουσιοδότησης διείσδυση-πρόσβαση σε συστήματα. Στην Ευρώπη κατά καιρούς διατυπώνονται εργασίες οι οποίες προπαρασκευάζουν νομοθετήματα για την πάταξη του hacking. Τέτοιες προσπάθειες είναι: [11]

- Η ανακοίνωση της επιτροπής με αριθμό com/2001/0298 για την ασφάλεια δικτύων και πληροφοριών. Σε αυτή την ανακοίνωση γίνεται εκτενής ανάλυση γύρω από την παράνομη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, ακόμα εκτιμούνται οι ζημιές που προκαλεί το hacking και παρατίθενται συμπεράσματα και πιθανές λύσεις.

[9] *www.kybernografoi.gr*

[10] *www.lawnet.gr/case_study.asp*

[11] *www.apodimos.com*

- Η πρόταση κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού οργανισμού για την ασφάλεια δικτύων και πληροφοριών. Αυτή η πρόταση περιλαμβάνει ένα σύνολο κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και έχει ως στόχο την διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και συστήματα πληροφοριών.
- Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό com/2002/0173-CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών. Σε αυτή τη πρόταση αναλύεται το αδίκημα της μη εξουσιοδοτημένης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική περιγραφή στο τι σημαίνει παράνομη παρεμβολή σε συστήματα πληροφοριών.

Προστασία των δεδομένων από ιούς

Οι ιοί των υπολογιστών είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται μόνα τους, έχοντας ως κύριο στόχο την αλλοίωση ή την διαγραφή των δεδομένων. Υπάρχουν δυο κατηγορίες ιών: οι ιοί των προγραμμάτων και οι ιοί των συστημάτων. Αυτή η μορφή ηλεκτρονικού εγκλήματος αποτελεί σήμερα μια συνήθης και επικίνδυνη τεχνική στα χέρια κάθε επίδοξου ηλεκτρονικού εγκληματία. Στην Ευρωπαϊκή Ένωση υπάρχουν νομοθετήματα για την ασφάλεια δικτύων και πληροφοριών, όπου γίνεται αναλυτική και λεπτομερής παρουσίαση της έννοιας του ιού, των τρόπων με τους οποίους αυτοί βλάπτουν ένα υπολογιστικό σύστημα και τις μεθόδους αντιμετώπισης τους. Πιο συγκεκριμένα στην Ελλάδα υπάρχουν: [12]

- Τα άρθρα 577 και 578 του Αστικού Κώδικα. Προβλέπουν την αστική και συμβατική ευθύνη του προμηθευτή και κάθε υπαιτίου, εφόσον υπάρχει πώληση προγραμμάτων που δημιουργούν ιούς σε υπολογιστικά συστήματα.
- Τα άρθρα 914 και 919 του Αστικού Κώδικα που θεσπίζουν την αδικοπρακτική ευθύνη του δράστη.
- Το άρθρο 381 του Ποινικού Κώδικα που θεσπίζει την ποινική ευθύνη κάθε υπαιτίου.

[12] *www.geology.upatras.gr*

Εγκλήματα κατά της ηθικής και της αξιοπρέπειας-Προστασία ανηλίκων από παράνομο και βλαβερό περιεχόμενο

Η δυσφήμηση του διαδικτύου και η διάδοση πορνογραφικού υλικού, αποτελείται από παράνομο και βλαβερό περιεχόμενο που θίγει την προσωπικότητα και την ηθική των ατόμων. Οι διατάξεις 361, 362, 366 και 367 του ΠΚ, προστατεύουν το άτομο που έχει διαφημιστεί. Ακόμα πιο σοβαρό ζήτημα είναι η διακίνηση πορνογραφικού υλικού στο διαδίκτυο, που πολλές φορές γίνεται αντικείμενο παρακολούθησης από ανηλίκους. Μερικά από τα μέτρα που έχουν ληφθεί στην Ευρωπαϊκή Ένωση με σκοπό την αντιμετώπιση αυτού του είδους ηλεκτρονικής εγκληματικότητας και ιδικά όσον αφορά την προστασία των ανηλίκων από την έκθεση σε παράνομο και βλαβερό περιεχόμενο, είναι τα εξής:

- Η Απόφαση του Συμβουλίου με αριθμό 2000/c 8/06, που περιλαμβάνει εισηγήσεις του Συμβουλίου προς τα κράτη μέλη και την Κεντρική Επιτροπή, ώστε να ληφθούν τα απαραίτητα μέτρα για την προστασία των ανηλίκων στο διαδίκτυο και στα οπτικοακουστικά μέσα.
- Η σύσταση με αριθμό 98/560/ΕΚ η οποία καταγράφει συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και τις ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης.
- Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΗ, στην οποία τα κράτη μέλη της Ευρωπαϊκής Ένωσης παρουσιάζουν και αναλύουν τα μέτρα που έχουν λάβει προκειμένου ο κάθε χρήστης-θύμα να βοηθά στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα τα παιδιά.
- Η Απόφαση του Συμβουλίου με αριθμό 2001/0301 στην οποία βρίσκουμε προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων στο διαδίκτυο και τα media με την συμμετοχή των γονέων.
- Η Απόφαση του Συμβουλίου με αριθμό 1999/c 362/06, η οποία καταλήγει ότι η διερεύνηση και δίωξη ποινικών αδικημάτων που σχετίζονται με την παιδική πορνογραφία στο διαδίκτυο, θα πρέπει να γίνεται υπό την αποτελεσματική συνεργασία των κρατών μελών της Ευρωπαϊκής Ένωσης.

- Το Ψήφισμα του Συμβουλίου με αριθμό 2002/c 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών.
- Η Απόφαση 276/1999/ΕΚ για την έγκριση, τη διάρκεια, τη χρηματοδότηση και τους στόχους προγραμμάτων που προωθούν την ασφαλέστερη χρήση του διαδικτύου.
- Η Ανακοίνωση της Επιτροπής com/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του διαδικτύου μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα.

Ένα ακόμα μεγάλο αγκάθι που δημιουργείται στη σχέση ανήλικα και διαδικτύου, είναι η πραγματοποίηση ηλεκτρονικών συναλλαγών μέσω του διαδικτύου. Κάθε προμηθευτής θα πρέπει να γνωρίζει εξ' αρχής ότι κάθε συναλλαγή με ανήλικα θεωρείται άκυρη και ότι φέρει την ποινική ευθύνη εφόσον το περιεχόμενο αυτής της συναλλαγής δεν απευθύνεται σε παιδιά και εφήβους. Ακόμα, για το λόγο ότι η εξακρίβωση των στοιχείων του καταναλωτή στις ηλεκτρονικές συναλλαγές είναι δύσκολη. Κάθε προμηθευτής που χρησιμοποιεί το διαδίκτυο για τις συναλλαγές του, θα πρέπει εκ των προτέρων να έχει προβλέψει στους όρους χρήσης του ιστοχώρου του, ότι δεν επιτρέπονται οι συναλλαγές με ανηλίκους και ότι η ιστοσελίδα δεν φέρει καμία ευθύνη.

Προστασία δεδομένων προσωπικού χαρακτήρα

Η προστασία των προσωπικών δεδομένων των χρηστών του διαδικτύου αποτέλεσε έναν από τους βασικότερους πυλώνες για την πάταξη του ηλεκτρονικού εγκλήματος. Η συγκέντρωση, η μη εξουσιοδοτημένη πρόσβαση και επεξεργασία των προσωπικών δεδομένων των χρηστών, αποτελεί το σημαντικότερο κίνδυνο της ιδιωτικής ζωής τους. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση έχουν χαραχθεί νομοθετικοί άξονες στους οποίους στηρίζεται η σημερινή νομοθεσία για την προστασία δεδομένων προσωπικού χαρακτήρα. Τέτοιες οδηγίες είναι:

- Η οδηγία 2002/58 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.
- Η οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Απάτη μέσω του Διαδικτύου

Σύμφωνα με τον Ποινικό Κώδικα, οι απάτες που πραγματοποιούνται με τη χρήση του διαδικτύου χωρίζονται σε δυο κατηγορίες. Την πρώτη κατηγορία την προβλέπει το άρθρο 386 του Ποινικού Κώδικα, όπου σύμφωνα με αυτό το μέσο τέλεσης μιας απάτης είναι ο υπολογιστής και το άρθρο 386 Α του Ποινικού Κώδικα προβλέπει την δεύτερη κατηγορία, όπου το οικονομικό όφελος ή η ζημία προκύπτει με απευθείας παρέμβαση στον υπολογιστή, στο πρόγραμμα και τα δεδομένα του. Στην Ευρωπαϊκή Ένωση ισχύει η απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών.

Spamming

Πολλές επιχειρήσεις προκειμένου να καλύψουν τις προωθητικές τους ανάγκες χρησιμοποιώντας έναν δημοφιλή τρόπο διαφήμισης στο διαδίκτυο, το λεγόμενο spamming. Με τον όρο spamming, εννοούμε την αποστολή πολυάριθμων email με διαφημιστικό περιεχόμενο σε πολυάριθμους καταναλωτές-χρήστες του διαδικτύου ταυτόχρονα. Η οδηγία 2002.58 απαγορεύει ρητά αυτή την τακτική διαφήμισης, αναφέροντας στο άρθρο 15 ότι «η χρησιμοποίηση αυτομάτων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτομάτων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνο στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεση τους». Παρόμοια νομοθετήματα υπάρχουν και στην Ελλάδα.

Προστασία της Πνευματικής Ιδιοκτησίας

Μια άλλη ευρέως διαδεδομένη μορφή ηλεκτρονικού εγκλήματος έχει να κάνει με την καταπάτηση της πνευματικής ιδιοκτησίας στο διαδίκτυο. Η ευρεία χρήση του διαδικτύου και οι δυνατότητες που προσφέρει αυτό, έχει κάνει την αντιγραφή και διάδοση των πνευματικών δημιουργημάτων εξαιρετικά απλή διαδικασία. Αυτό βέβαια έχει ως αποτέλεσμα να καταπατείται κάθε δικαίωμα πνευματικής ιδιοκτησίας που έχουν οι δημιουργοί πάνω στα δημιουργήματα τους. Η εργασία αυτή αναλύει παρακάτω αυτό το θέμα σε περισσότερο βάθος.

2.3 Δικαιοδοσία στο διαδίκτυο

Φυσικό επακόλουθο αυτών των τεράστιων δυνατοτήτων που δίνει ο υπολογιστής και το διαδίκτυο στην ηλεκτρονική επεξεργασία δεδομένων είναι ότι η ηλεκτρονική εγκληματικότητα εμπλουτίζεται συνεχώς με νέες μορφές και μεθόδους πραγματοποίησης. Αυτό καθιστά πολύ δύσκολη τη δουλειά του νομοθέτη, ο οποίος καλείται να δώσει λύση σ' ένα εξαιρετικά πολυδιάστατο πρόβλημα. Αυτό που πραγματικά χρειάζεται για την αντιμετώπιση της εγκληματικότητας είναι μια εποικοδομητική συνεργασία μεταξύ όλων των κρατών μελών και η χάραξη μιας ενιαίας πολιτικής που στόχο θα έχει την αντιμετώπιση της ηλεκτρονικής εγκληματικότητας. Πολλά θεσμικά κείμενα έχουν ήδη προβλέψει την πραγματοποίηση τέτοιων συνεργασιών.

Για τα εγκλήματα που τελούνται στο διαδίκτυο, ισχύει ένα διαφορετικό καθεστώς δικαιοδοσίας για το λόγο ότι το διαδίκτυο είναι ένα παγκόσμιο δίκτυο δίνοντας έτσι τη δυνατότητα σε οποιονδήποτε να εισάγει και να καταστήσει προσβάσιμη οποιαδήποτε πληροφορία θέλει από τη μια άκρη του κόσμου στην άλλη. Έτσι, έχει επικρατήσει ως κύριο κριτήριο για την ανεύρεση της αρμοδιότητας του δικαστηρίου ο τόπος τέλεσης του αδικήματος. Στην νομική επιστήμη, υπάρχουν τέσσερις θεωρίες για τον καθορισμό του τόπου τέλεσης του αδικήματος.

- Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθει η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.

- Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

- Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

- Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Τόσο στην Ελλάδα όσο και στην Ευρώπη, η θεωρία που έχει υιοθετηθεί είναι η θεωρία του **βαρύνοντος τόπου**.

2.4 Ποιες οι συνέπειες του ηλεκτρονικού εγκλήματος για τον καταναλωτή;

Αναμφισβήτητα το διαδίκτυο έχει προσφέρει τρομερές δυνατότητες στο χρήστη για την κάλυψη των καταναλωτικών του αναγκών. Το ηλεκτρονικό εμπόριο έχει ριζώσει βαθειά στις καταναλωτικές μας συνήθειες και είναι ένα σημαντικό εργαλείο στα χέρια του καταναλωτή για την πραγματοποίηση των συναλλαγών του. Όπως ήταν αναμενόμενο, το ηλεκτρονικό έγκλημα έχει εισχωρήσει σε αυτόν τον ευαίσθητο κλάδο των υπηρεσιών της πληροφορικής, κάνοντας τις ηλεκτρονικές συναλλαγές μη ασφαλής για τα προσωπικά δεδομένα και τα χρήματα των καταναλωτών. [13]

Ο ηλεκτρονικός εγκληματίας επηρεάζει τις ηλεκτρονικές συναλλαγές με τη μέθοδο της υποκλοπής στοιχείων πιστωτικών καρτών των καταναλωτών που επιχειρούν να πραγματοποιήσουν μια συναλλαγή μέσω του διαδικτύου. Έτσι ο χρήστης-θύμα ανακαλύπτει μετά από καιρό από τον αναλυτικό λογαριασμό της κάρτας του ότι έχει πέσει θύμα απάτης. Η νομοθεσία όμως προβλέπει ότι ο κάτοχος της κάρτας μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσία του φυσικού σώματος της κάρτας.

Κάθε κάτοχος πιστωτικής κάρτας, ο οποίος πραγματοποιεί ηλεκτρονικές συναλλαγές, θα πρέπει να γνωρίζει ότι σε περίπτωση που πραγματοποιηθεί συναλλαγή με κλεμμένα στοιχεία καρτών, ο νόμιμος κάτοχος της πιστωτικής κάρτας μπορεί να αρνηθεί την καταβολή του συγκεκριμένου ποσού στην τράπεζα, η οποία με τη σειρά της όχι μόνο δε θα πληρώσει το ποσό στον προμηθευτή αλλά θα απαιτήσει και τα έξοδα ακύρωση της συναλλαγής.

Η νομοθεσία απαγορεύει ρητά τη συλλογή στοιχείων επικοινωνίας και προσωπικών δεδομένων των χρηστών, τη χρησιμοποίηση τους χωρίς την εξουσιοδότηση των υποκειμένων από τους προμηθευτές ή από τρίτους για διαφημιστικές ενέργειες μέσω του spamming για έρευνες αγοράς και για direct marketing, διότι προσβάλλεται η ιδιωτική ζωή του ατόμου.

[13] *www.synigoroskatanaloti.gr*

2.5 Τι προβλέπει η νομοθεσία για την πάταξη της ηλεκτρονικής εγκληματικότητας;

Όπως έχουμε ήδη αναφέρει η πάταξη της ηλεκτρονικής εγκληματικότητας είναι μια δύσκολη διαδικασία εξ' αιτίας της πολυμορφικότητας, με την οποία αυτό παρουσιάζεται στη σημερινή σύγχρονη ψηφιακή κοινωνία. Πολλές είναι οι νομοθετικές προσπάθειες που έχουν πραγματοποιηθεί κατά καιρούς, όμως δεν καλύπτουν πλήρως νομικά τις ποικίλες μορφές του ηλεκτρονικού εγκλήματος.

Στο ελληνικό δίκαιο υπάρχουν τέτοιες διατάξεις όπως οι διατάξεις του ποινικού κώδικα περί απάτης, με τη χρήση υπολογιστή περί θεμιτής πρόσβασης σε συστήματα πληροφοριών, υποκλοπής και παραβίασης απορρήτων, η ειδική νομοθεσία περί προστασίας προσωπικών δεδομένων (Ν. 2472/1997) με τις τροποποιήσεις (Ν. 3625/2007, Ν. 3471/2006), η νομοθεσία περί διασφάλισης του απορρήτου των επικοινωνιών (Ν.3674/2008), η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και άλλες τέτοιες διατάξεις. Πιο συγκεκριμένα, το άρθρο 5 του Ν. 1805/1988, προσέθεσε στο άρθρο 386 του Ποινικού Κώδικα περί απάτης, το συμπληρωματικό άρθρο 386Α που αναφέρεται στην απάτη με υπολογιστή. Σύμφωνα με το άρθρο 386Α του Ποινικού Κώδικα λοιπόν, όποιος έχει σκοπό να αποκτήσει για τον εαυτό του ή για άλλους παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα αρχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος, είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με ποινές φυλάκισης που προβλέπονται για την απάτη.

Τα παραπάνω νομοθετήματα που αναφέραμε προβλέπουν και τις ανάλογες ποινές ανάλογα με τη βαρύτητα κάθε αδικήματος. Οι ποινές αυτές κυμαίνονται από φυλάκιση τριών μηνών έως και φυλάκιση τριών ετών σε περιπτώσεις που προκληθεί μεγαλύτερη ζημιά. Πιο συγκεκριμένα:

- Τα άρθρα 370Α και 370Β του Ποινικού Κώδικα προβλέπουν ποινές φυλάκισης για τον διαδικτυακό δράστη που προβαίνει σε παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας, παραβίαση επαγγελματικών απορρήτων ή παράνομη αντιγραφή προγραμμάτων ηλεκτρονικού υπολογιστή.
- Η ψήφιση του νόμου 3674/2008, ενισχύει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας,

θεσπίζοντας ειδικές υποχρεώσεις του παρόχου υπηρεσιών για την ασφάλεια δικτύου και συγκεκριμένες διαδικασίες άρσης του απορρήτου υπό την εποπτεία της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ).

- Το άρθρο 292Α του Ποινικού Κώδικα, τιμωρεί τα εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών με φυλάκιση τουλάχιστον ενός έτους και χρηματικές ποινές που αρχίζουν από είκοσι χιλιάδες ευρώ και αυξάνονται ανάλογα με τη βαρύτητα του αδικήματος και την ιδιότητα του δράστη.
- Ακόμα, ο νόμος 3674/2008 τροποποίησε το άρθρο 370Α του Ποινικού Κώδικα θεσπίζοντας αυστηρές κυρώσεις που μπορούν να φτάσουν ως κάθειρξη μέχρι δέκα ετών για όσους παραβιάσουν το απόρρητο της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας. Με την τροποποίηση του ίδιου άρθρου, θεσπίζονται διοικητικές κυρώσεις (χρηματικά πρόστιμα, ανάκληση αδειών κλπ) κατά των εκπροσώπων, εταιριών, παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών.
- Το άρθρο 348Α του Ποινικού Κώδικα, τιμωρεί με φυλάκιση και χρηματικές ποινές την πορνογραφία ανηλίκων οποιοσδήποτε κι αν είναι ο υλικός φορέας αποτύπωσης του πορνογραφικού υλικού.
- Ο νόμος 3587/2007 προβλέπει ειδικές κυρώσεις περί της προστασία του καταναλωτή. Συγκεκριμένα, ο νόμος αυτός εξειδικεύεται στις εξ' αποστάσεως συμβάσεις πρόσβασης σε υπηρεσίες ηλεκτρονικού εμπορίου. Ακόμα η νομοθεσία αυτή απαγορεύει τις παραπλανητικές εμπορικές πρακτικές, ενώ προβλέπει διοικητικές κυρώσεις κατά των παραβατών.
- Ο νόμος 3471/2006 προβλέπει επίσης διοικητικές αστικές και ποινικές ευθύνες κατά των παραβατών που διεκπεραιώνουν πράξεις ηλεκτρονικής εγκληματικότητας όπως, πλαστογραφία, εξύβριση, δυσφήμηση, προσβολή του νόμου περί απορρήτου, του νόμου 2121/1993 περί πραγματικής ιδιοκτησίας ή του νόμου 3431/2006 περί ηλεκτρονικών επικοινωνιών.
- Το άρθρο 11 του νόμου 3471/2006, ο οποίος υιοθέτησε στο Ελληνικό δίκαιο την οδηγία 2002/58/ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ρυθμίζει το spamming στην Ελλάδα. Σύμφωνα με το άρθρο αυτό, η χρησιμοποίηση αυτόματων συστημάτων κλήσης ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή

χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.

- Το άρθρο 914 του Αστικού Κώδικα περί αδικοπραξίας, δίνει τη δυνατότητα στο χρήστη που έπεσε θύμα ηλεκτρονικής απάτης, να κινηθεί δικαστικά εναντίον του προσβολέα ζητώντας αποζημίωση.

Όπως ήδη έχουμε αναφέρει, η παγκοσμιότητα του διαδικτύου και η ανωνυμία του χρήστη δυσχεραίνουν κατά πολύ τη διερεύνηση του ηλεκτρονικού εγκλήματος. Έτσι, ο ηλεκτρονικός εγκληματίας καταφέρνει να κρατάει άγνωστη την ταυτότητα αλλά και τον τόπο από τον οποίο διαπράττει το έγκλημα του. Ακόμα, η τεχνική τέλεσης ενός ηλεκτρονικού εγκλήματος είναι δύσκολο να ανακαλυφθεί, επειδή εάν ο τόπος που έχει γίνει το έγκλημα είναι το εξωτερικό, δεν είναι δυνατόν να πραγματοποιηθούν οι προκαθορισμένες ενέργειες από το Ελληνικό δίκαιο. Όλο αυτό έχει σαν αποτέλεσμα ο δράστης να έχει απεριόριστο χρόνο, ώστε να καταφέρει να καλύψει τα νότα του.

Τα διαδικτυακά εγκλήματα δεν περιορίζονται γεωγραφικά στα πλαίσια μιας χώρας, έτσι η δίωξη ενός ηλεκτρονικού εγκλήματος απαιτεί τη συνεργασία πολλών κρατών. Στην Ευρωπαϊκή Ένωση έχουν παρθεί πολλές αποφάσεις προς την κατεύθυνση αυτή. Όμως, πολλές ήταν οι διαφωνίες που δημιουργήθηκαν μεταξύ των κρατών γύρω από κάποιες περιπτώσεις ασάφειας των περιγραφών των εγκλημάτων και προβλημάτων εφαρμογής. Το Ελληνικό κράτος υπήρξε από τους κυριότερους υποστηρικτές αυτής της κίνησης.

Από την πλευρά της Ευρωπαϊκής Ένωσης έχουν παρθεί πολλές πρωτοβουλίες για την καταπολέμηση διακίνησης επιβλαβούς και παράνομου περιεχομένου μέσω διαδικτύου, που στοχεύουν στη δημιουργία συνήθως ασφαλούς χρήσης του διαδικτύου μέσω αυτορρύθμισης και κωδικών δεοντολογίας. Όσον αφορά τα προληπτικά μέτρα που έχουν εφαρμοσθεί από την Ευρωπαϊκή Ένωση, είναι η λειτουργία ειδικών τηλεφωνικών γραμμών (hotlines) με τις οποίες ο χρήστης-θύμα μπορεί να επικοινωνήσει για να καταγγείλει το ηλεκτρονικό έγκλημα που διαπράχθηκε εις βάρος του και να δώσει τα απαιτούμενα στοιχεία για την εξιχνίαση του εγκλήματος ώστε να παρθούν τα απαιτούμενα μέτρα από τις αρχές του αρμοδίου κράτους. Τέλος, ο Ευρωπαϊκός οργανισμός για την ασφάλεια ENISA, έχει εκδώσει δυο εκθέσεις περί ασφάλειας και μέτρων αντιμετώπισης της ανεπιθύμητης εμπορικής επικοινωνίας που εφαρμόζουν οι πάροχοι διαδικτυακών υπηρεσιών στην Ευρώπη.

2.6 Ποια τα μέσα προστασίας του καταναλωτή από το ηλεκτρονικό έγκλημα

Σαφώς κάποιες κινήσεις διεθνούς κινητοποίησης και συνεργασίες έχουν πραγματοποιηθεί κατά καιρούς, όμως εμπόδια όπως η παγκοσμιότητα του διαδικτύου, η ανωνυμία των ηλεκτρονικών εγκλημάτων, η εύκολη απόκρυψη ή διαγραφή των αποδεικτικών στοιχείων, καθιστούν αυτές τις δράσεις αναποτελεσματικές. Ακόμα έχει αποδειχθεί ότι η ταχύτητα ενεργοποίησης των μηχανισμών προστασίας του χρήστη του διαδικτύου είναι πολύ χαμηλή, όπως και η απονομή δικαιοσύνης θεωρείται ανύπαρκτη. Αυτό έχει οδηγήσει στο φαινόμενο οι καταναλωτές των υπηρεσιών του διαδικτύου να λαμβάνουν μέτρα πρόληψης και προστασίας από μόνοι τους. Κάθε χρήστης του διαδικτύου μπορεί από μόνος του να λάβει κάθε στοιχειώδη μέτρα τεχνικής προστασίας του και να ακολουθεί κάποιους στοιχειώδης κανόνες αυτοπροστασίας του κατά τη διάρκεια που βρίσκεται συνδεμένος ή ακόμα πιο δραστικά πρέπει να είναι τα μέτρα σε περίπτωση που πραγματοποιείται ηλεκτρονική συναλλαγή μέσω του διαδικτύου. Τέτοια μέτρα για παράδειγμα είναι οι υπηρεσίες ανώνυμης πρόσβασης, οι οποίες σβήνουν τα ηλεκτρονικά ίχνη της δικτυακής παρουσίας του χρήστη, αποτρέποντας να χρησιμοποιηθούν τα στοιχεία του σε διαδικασίες που δεν έχει επιλέξει ο ίδιος.

Σήμερα, έχει επικρατήσει κάθε ιστοχώρος να παρέχει ενημέρωση σχετικά με τα προσωπικά δεδομένα που συλλέγει και επεξεργάζεται. Αυτή η ενημέρωση ανήκει στα δικαιώματα κάθε χρήστη αλλά και στις υποχρεώσεις των υπευθύνων για τη λειτουργία της διαδικτυακής σελίδας.

Πιο συγκεκριμένα, για τους καταναλωτές που χρησιμοποιούν το διαδίκτυο ως μέσο για τις συναλλαγές τους, θα πρέπει να γίνει γνωστό ότι για την ασφάλεια των συναλλαγών τους θα πρέπει να προτιμούν αναγνωρισμένα και δημοφιλή ηλεκτρονικά καταστήματα από ύποπτης προέλευσης, διαδικτυακές εμπορικές ιστοσελίδες που χρησιμοποιούν ελκυστικές τιμές ως παγίδα για τα θύματα του. Για κανένα λόγο να μην παρέχει προσωπικά στοιχεία και τραπεζικούς λογαριασμούς. Θα πρέπει να λαμβάνει γνώση όλων των όρων χρήσης κάθε υπηρεσίες και των λεπτομερειών όσον αφορά τη διεκπεραίωση της συναλλαγής (τελικής χρέωσης, χρόνοι παράδοσης, όροι υπαναχώρησης, πολιτική επιστροφή, πολιτική ασφάλεια κ.τ.λ.). Καλό θα είναι κάθε καταναλωτής να χρησιμοποιεί στον υπολογιστή προγράμματα προστασίας από τους ιούς (antivirus, firewalls) και όταν πρόκειται για ηλεκτρονικές συναλλαγές να προτιμά συνδέσεις πιστοποιημένων και γνωστών προμηθευτών. Πιο ασφαλής γίνονται οι

συναλλαγές του καταναλωτή εάν χρησιμοποιεί μέθοδο κρυπτογραφίας, διατάξεις ηλεκτρονικής και ψηφιακά πιστοποιητικά. Ο ψηφιακός καταναλωτής θα πρέπει να χρησιμοποιεί ως μέσο για τις πληρωμές των διαδικτυακών του αγορών τη χρεωστική κάρτα. Η χρεωστική κάρτα ή αλλιώς ηλεκτρονικό πορτοφόλι, είναι στην ουσία ένας λογαριασμός που μπορεί κάθε κάτοχος να καταθέσει ένα χρηματικό ποσό για τις ηλεκτρονικές του αγορές. Με αυτόν τον τρόπο, αποφεύγεται η αθέμιτη απεριόριστη χρέωση των πιστωτικών καρτών σε περίπτωση υποκλοπής των στοιχείων.

Οι χρήστες του ηλεκτρονικού ταχυδρομείου θα πρέπει να μην δίνουν τους κωδικούς προσωπικών στοιχείων και κωδικούς σε τρίτους μέσω του email τους, εφόσον το ηλεκτρονικό ταχυδρομείο δεν αποτελεί ασφαλή τρόπο επικοινωνίας. Ακόμα ο χρήστης θα πρέπει να αγνοεί τα μηνύματα που ανακοινώνουν κάποιο κέρδος ή κάποια δώρα, αφού τέτοιου είδους μηνύματα χρησιμοποιούνται ως μέσα απάτης για το χρήστη. Ομοίως, θα πρέπει να αγνοεί διάφορα συνημμένα αρχεία που εισέρχονται στο λογαριασμό του, διότι το πιθανότερο είναι να περιέχουν ιούς.

Στο ευαίσθητο θέμα της σχέσης διαδικτύου και ανηλίκων, ειδική μέριμνα πρέπει να παρέχουν οι γονείς, οι οποίοι θα πρέπει συνεχώς να βρίσκονται σε εγρήγορση προκειμένου να προφυλάξουν τα παιδιά τους από τους κινδύνους του διαδικτύου. Πιο συγκεκριμένα, οι γονείς δεν πρέπει να επιτρέπουν την ανεξέλεγκτη χρήση του υπολογιστή από τα παιδιά τους, καλό είναι να τοποθετούν τον υπολογιστή σε σημείο από το οποίο θα μπορούν να έχουν τη συνεχή εποπτεία της δράσης των παιδιών τους. Πολύ χρήσιμη θα είναι και η εγκατάσταση των ειδικών λογισμικών που λειτουργούν σαν φίλτρα και απαγορεύουν την πρόσβαση των παιδιών σε ιστοσελίδες που ενδεχομένως ελλοχεύουν κίνδυνοι, όπως για παράδειγμα ιστοσελίδες που περιέχουν χυδαίες λέξεις, βλαβερό και παράνομο περιεχόμενο (πορνογραφία, ρατσισμός, τρομοκρατία) και ιστοσελίδες ομαδικών συζητήσεων (chat room) με άγνωστα άτομα.

Στην περίπτωση που αντιληφθούμε ότι σε κάποια ιστοσελίδα παροχής υπηρεσιών δεν τηρούνται οι προκαθορισμένες αρχές λειτουργίας ως προς το περιεχόμενο, τη διαφήμιση, τη χρέωση, την πρόσβαση στην υπηρεσία, την προστασία των προσωπικών δεδομένων, τότε θα πρέπει αμέσως να λάβουμε κάποιο από τα παρακάτω μέτρα:

- Να επικοινωνήσουμε με τον υπεύθυνο παροχής της υπηρεσίας και να καταγγείλουμε το γεγονός.

- Να διακόψουμε αμέσως τη σύνδεση μας με τη συγκεκριμένη ιστοσελίδα και να ενημερώσουμε άμεσα τις αρμόδιες ιδιωτικές αρχές.
- Να ενημερώσουμε αμέσως την Ομάδα Ψηφιακής Ασφάλειας (D.A.R.T) στην ηλεκτρονική διεύθυνση www.dart.gov.gr. Η ομάδα D.A.R.T. (Digital Awareness & Response to Threats) είναι μια κοινή προσπάθεια της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και του Σώματος Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας, με στόχο την αντιμετώπιση κινδύνων από τη χρήση τεχνολογίας ηλεκτρονικών επικοινωνιών.
- Να απευθυνθούμε στο Συνήγορο του καταναλωτή, ο οποίος με τη σειρά του θα εξετάσει εάν εμπίπτει στην αρμοδιότητα του να ενεργήσει για την απονομή της δικαιοσύνης βοηθώντας τις αρμόδιες ιδιωτικές αρχές.

2.7 ΔΙΕΘΝΕΣ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ – ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΤΗΣ ΕΥΡΩΠΗΣ

Συστάσεις του Συμβουλίου της Ευρώπης:

Η νομική αντιμετώπιση του φαινομένου της εγκληματικότητας αποτελεί μια από τις προτεραιότητες του Συμβουλίου της Ευρώπης. Μάλιστα αυτή η νέα μορφή εγκληματικότητας και η ραγδαία εξέλιξη έφεραν την Ευρωπαϊκή Ένωση προ τετελεσμένων γεγονότων και η ανάγκη για δημιουργία μιας αποτελεσματικής στρατηγικής αντιμετώπισης του προβλήματος ήταν επιτακτική.

Πιο συγκεκριμένα, το Συμβούλιο Ασφάλειας της Ευρωπαϊκής Ένωσης προχώρησε στην έκδοση τριών συστάσεων (recommendation), οι οποίες θα αποτελούσαν για τα κράτη μέλη μια κατεύθυνση στην οποία έπρεπε να βαδίζουν ώστε να αναπτύξουν τα δικά τους σχέδια αντιμετώπισης. Βέβαια, η συμπεριφορά που θα αναπτύσσει κάθε κράτος μέλος χωριστά θα πρέπει να συμβαδίζει με τις κατευθυντήριες γραμμές και τις υποδείξεις της Ευρωπαϊκής Ένωσης.

Οι προαναφερθείσες συστάσεις είναι οι εξής: Η σύσταση R 9/1989 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R 9/1989 on Computer-related crime). Η σύσταση R 13/1995 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R 13/1995 Problems of criminal procedural Law connected with information technology), στην οποία

καθιερώνονται για πρώτη φορά σε διεθνές επίπεδο γενικές δικονομικές αρχές που θα πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων. Τέλος, η σύσταση R 8/2001 για την αυτορρύθμιση σε θέματα σχετικά με το περιεχόμενο του διαδικτύου (Recommendation No R 8/2001 on self-regulation concerning cyber content).

Οι παραπάνω συστάσεις ναι μεν αποτελούν ένα σημαντικό βήμα, αλλά δεν ήταν τίποτε άλλο από κάποιες οδηγίες χωρίς σημαντική ισχύ προς τα κράτη-μέλη. Έτσι, ήταν επιτακτική ανάγκη να γίνει κάτι πιο δραστικό και αυτό επιτεύχθηκε στις 23 Νοεμβρίου του 2001, όταν το Συμβούλιο της Ευρώπης προέβη σε μια διεθνή σύμβαση για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, η οποία υποχρεώνει τα κράτη μέλη να συμμορφώνουν τις εσωτερικές νομικές ρυθμίσεις τους με τις διατάξεις της σύμβασης.

Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)

Ο ΣΚΟΠΟΣ ΤΗΣ ΣΥΜΒΑΣΗΣ

Η ολοένα αυξανόμενη εγκληματικότητα στο διαδίκτυο έφερε την Ευρωπαϊκή Ένωση μπροστά σ' ένα μείζον πρόβλημα και η πρόκληση αλλά και η ανάγκη για αντιμετώπιση του προβλήματος ήταν μεγάλες. Αυτό οδήγησε το Συμβούλιο της Ευρώπης να προβεί στην υπογραφή σύμβασης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο στις 23 Νοεμβρίου 2001 στη Βουδαπέστη. Αυτή η σύμβαση είναι μείζονος σημασίας θεσμικό κείμενο και αποτελεί τη βάση στην οποία στηρίζονται όλες οι εσωτερικές νομοθεσίες των κρατών μελών. [14]

Κύριο χαρακτηριστικό της σύμβασης της Βουδαπέστης είναι η προσπάθεια για τη χάραξη μιας διεθνούς αναγνώρισης κοινής πολιτικής για την αντιμετώπιση των εγκλημάτων στο διαδίκτυο. Για να επιτευχθεί αυτή η διεθνής συνεργασία όμως, θα πρέπει η εσωτερική νομοθεσία κάθε κράτους μέλους να εναρμονίζεται με το περιεχόμενο της σύμβασης στον τομέα της ηλεκτρονικής εγκληματικότητας και πιο συγκεκριμένα στη θέσπιση εσωτερικών δικονομικών διατάξεων για την έρευνα, τη δίωξη και την εκδίκαση των εγκλημάτων του διαδικτύου, ακόμα και τη θέσπιση κανόνων αναφορικά με τη διεθνή συνεργασία.

[14] *Σύμβαση της Βουδαπέστης* για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)

Επομένως, σκοπός της σύμβασης είναι η προστασία της διεθνούς κοινότητας αναφορικά με την εγκληματικότητα που εκδηλώνεται στο διαδίκτυο μέσω της θεμελίωσης κοινών ουσιαστικών και δικονομικών ποινικών αρχών, της θέσπισης της κατάλληλης νομοθεσίας από τα κράτη μέλη, καθώς και μέσω της επίτευξης της ανάλογης δικαστικής συνεργασίας μεταξύ των κρατών μελών.

ΤΟ ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΣΥΜΒΑΣΗΣ

Στην εισαγωγή της σύμβασης της Βουδαπέστης αναφέρεται η επιτακτική ανάγκη θεσπίσεως νομοθεσίας, σχετική με την ηλεκτρονική εγκληματικότητα στο διαδίκτυο. Ακόμα, το Συμβούλιο της Ευρώπης τονίζει τις σημαντικότατες αλλαγές που επήλθαν στο χώρο των υπολογιστών και στο τέλος της εισαγωγής εκφράζει νέων μορφών ηλεκτρονικής εγκληματικότητας και για την ολοένα αυξανόμενη διαδικτυακή εγκληματικότητα.

Το συμβούλιο της Ευρώπης χρησιμοποιεί το πρώτο κεφάλαιο της σύμβασης για να εισάγει ορισμούς κάποιων εννοιών, προκειμένου η πλούσια τεχνική και πολλές φορές δυσνόητη ορολογία να γίνει κοινώς αποδεκτή και κατανοητή. Έτσι θα περιοριστούν πολλές συγχύσεις και διαφωνίες όσον αφορά την έννοια των τεχνικών όρων και θα επικρατήσει μια ομοιογενής εννοιολογική προσέγγιση απ' όλα τα κράτη μέλη, πράγμα που θα βοηθήσει στην ανάπτυξη των εσωτερικών θεσμικών κειμένων. Έννοιες που αναλύονται για παράδειγμα είναι το ηλεκτρονικό σύστημα (computer system), ηλεκτρονικό δεδομένο (computer data), διαδίκτυο (internet), παροχέας πρόσβασης (service provider) κ.α.

Το Συμβούλιο της Ευρωπαϊκής Ένωσης, λαμβάνοντας υπόψη του ότι μέσω του διαδικτύου διακινείται μεγάλο πλήθος δεδομένων που αποτελούν προσωπικά στοιχεία του χρήστη που αφορούν την ιδιωτική του ζωή (π.χ. αριθμοί πιστωτικών καρτών, θρήσκευμα, ηλικία), αντιλήφτηκε τη σημασία αλλά και την ανάγκη της θέσπισης μέτρων για την αντιμετώπιση εγκλημάτων κατά της εμπιστευτικότητας των δεδομένων και των συστημάτων, της ακεραιότητας των δεδομένων και των συστημάτων και της διαθεσιμότητας των δεδομένων και συστημάτων. Σκόπιμο είναι να αναφερθούμε στην εννοιολογική ανάλυση των παραπάνω όρων.

- Με τον όρο εμπιστευτικότητα (confidentiality) των δεδομένων και των συστημάτων, εννοούμε την ιδιότητα που έχουν τα δεδομένα να

καθίστανται προσπελάσιμα μόνο στους εξουσιοδοτημένους χρήστες του συστήματος.

- Με τον όρο ακεραιότητα (integrity) των δεδομένων και των συστημάτων, εννοούμε την ιδιότητα που έχουν τα δεδομένα να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, ενώ κάθε αλλαγή σε αυτά να γίνεται κατόπιν εξουσιοδότησης.
- Με τον όρο διαθεσιμότητα (availability) των δεδομένων και συστημάτων, εννοούμε την ιδιότητα των πόρων ενός πληροφοριακού συστήματος να καθίστανται άμεσα προσπελάσιμοι στον εκάστοτε εξουσιοδοτημένο χρήστη του συστήματος.

Έτσι το Συμβούλιο της Ευρώπης στο δεύτερο κεφάλαιο αναφέρει τα νομοθετικά μέτρα που πρέπει να ληφθούν από κάθε κράτος μέλος για την αντιμετώπιση των παραπάνω εγκλημάτων. Συμπερασματικά, το δεύτερο κεφάλαιο της σύμβασης προστατεύει το δικαίωμα κάθε χρήστη για να αποφευχθεί η διαρροή προσωπικών στοιχείων που αφορούν την ιδιωτική του ζωή, αλλά και το δικαίωμα της ασφαλούς διακίνησης αυτών των δεδομένων.

Μια υποχρέωση που απορρέει από κάθε κράτος μέλος που αποδέχεται τους όρους της σύμβασης, είναι να ποινικοποιήσει ορισμένες συμπεριφορές που σχετίζονται με τις δραστηριότητες στο διαδίκτυο. Έτσι, κατά το άρθρο 2 της Σύμβασης κάθε μέλος υποχρεούται να λάβει νομοθετικά μέτρα για τη θεμελίωση της ειδικής υπόστασης του εγκλήματος της παράνομης πρόσβασης (illegal access) στις περιπτώσεις της εκ προθέσεως και χωρίς δικαίωμα πρόσβασης σε σύστημα ηλεκτρονικών υπολογιστών. [15]

Στην ουσία το άρθρο 2 της Σύμβασης της Βουδαπέστης αποσκοπεί στην ποινικοποίηση του hacking, δηλαδή της μη εξουσιοδοτημένης πρόσβασης σε ξένα συστήματα με διάφορους τεχνικούς τρόπους, είτε για λόγους δολιοφθοράς, είτε για λόγους ικανοποίησης από την παράκαμψη συστημάτων ασφαλείας. Η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης στο σύστημα από μη εξουσιοδοτημένα άτομα, αποτελεί έννομο αγαθό για κάθε χρήστη και πρέπει να προστατεύεται νομικά, όμως θα πρέπει να ξεκαθαριστεί και να θεμελιωθεί ποινικά η περίπτωση του άμεσου και του έμμεσου δόλου.

Σύμφωνα με το άρθρο 3 της Σύμβασης, τα κράτη μέλη καλούνται να ποινικοποιήσουν την αθέμιτη υποκλοπή δεδομένων ηλεκτρονικών υπολογιστών

[15] *Σύμβαση της Βουδαπέστης* για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)

(illegal interception) από, προς ή εντός ενός συστήματος υπολογιστών. Η διάταξη αυτή βρίσκει εφαρμογή σε κάθε μορφής υποκλοπή ηλεκτρονικών δεδομένων που διακινούνται στο διαδίκτυο με το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol), το ηλεκτρονικό ταχυδρομείο (e-mail) και με άλλες παρόμοιες υπηρεσίες του διαδικτύου. Κάθε χρήστης του διαδικτύου έχει το έννομο δικαίωμα στην ιδιωτική ζωή και στην ασφάλεια των τηλεπικοινωνιών. Σε περιπτώσεις παραβίασης και καταπάτησης αυτού του δικαιώματος, θα πρέπει να εξετάζεται και το στοιχείο του άμεσου δόλου, όπως δηλαδή συμβαίνει και για το έγκλημα της παράνομης πρόσβασης.

Με βάση το άρθρο 4 της Σύμβασης, κάθε κράτος μέλος δεσμεύεται να λάβει τα απαραίτητα νομοθετικά μέτρα, προκειμένου να καθιερώσει ως ποινικό αδίκημα την επέμβαση σε ηλεκτρονικά δεδομένα (data interference), η οποία αναλύεται στην άνευ δικαιώματος καταστροφή (damaging), διαγραφή (deletion), φθορά (deterioration), μεταβολή (alteration) ή απόκρυψη (suppression) δεδομένων. Σε αυτήν την περίπτωση, το προστατευόμενο έννομο αγαθό είναι η υλική ακεραιότητα και η λειτουργία των δεδομένων και των ηλεκτρονικών προγραμμάτων και για την προστασία λοιπόν των δεδομένων και των προγραμμάτων των ηλεκτρονικών υπολογιστών από κάθε εξωτερική παρέμβαση στον υλικό φορέα τους, ψηφίστηκε το άρθρο 4 της Συνθήκης της Βουδαπέστης. Όπως και στις άλλες περιπτώσεις, έτσι και σε αυτή εξετάζεται το ενδεχόμενο της πρόθεσης. [16]

Στη συνέχεια της Σύμβασης και συγκεκριμένα στο άρθρο 5 υπαγορεύεται η ποινικοποίηση της επέμβασης σε σύστημα (system interference), η οποία τελείται με την εκ προθέσεως και άνευ δικαιώματος παρακώλυση της λειτουργίας ενός συστήματος υπολογιστών μέσω της εισαγωγής (inputting), μεταφοράς (transmitting), καταστροφής (damaging), διαγραφής (deleting), φθοράς (deterioration), μεταβολής (alteration) ή απόκρυψης (suppression) ηλεκτρονικών δεδομένων. Με το άρθρο 5, επιτυγχάνεται η ποινικοποίηση της δολιοφθοράς σε υπολογιστικά συστήματα (computer sabotage).

Στο άρθρο 6 της Σύμβασης, κάθε κράτος μέλος αναλαμβάνει την υποχρέωση να ποινικοποιήσει την κατάχρηση των υπηρεσιών του διαδικτύου (misuse of devices), νοώντας την εκ προθέσεως και χωρίς δικαίωμα παραγωγή, πώληση, προετοιμασία για χρήση, εισαγωγή, διανομή ή με οποιοδήποτε τρόπο διάθεση μιας συσκευής, συμπεριλαμβανομένου και προγράμματος υπολογιστή

[16] *Σύμβαση της Βουδαπέστης* για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)

που έχει σχεδιαστεί ή προσαρμοστεί με σκοπό τη διάπραξη οποιουδήποτε αδικήματος των άρθρων 2 έως 5 της Σύμβασης.

Επίσης στο δεύτερο κεφάλαιο της Σύμβασης, συμπεριλαμβάνονται οι διατάξεις του ποινικού δικονομικού δικαίου. Αναλυτικότερα, αυτές οι διατάξεις αναφέρονται σε θέματα ταχείας διαφύλαξης αποθηκευμένων δεδομένων σε ηλεκτρονικό υπολογιστή (expedited preservation of stored computer data), ταχείας διαφύλαξης και γνωστοποίησης διακινούμενων αρχείων (expedited preservation and disclosure of traffic data), εντολής παροχής πληροφοριών (production order) έρευνας και κατάσχεσης αποθηκευμένων σε ηλεκτρονικό υπολογιστή στοιχείων (search and seizure of stored computer data), πραγματικού χρόνου συλλογής διακινούμενων δεδομένων (real-time collection of traffic data), καθώς και παγίδευσης – υποκλοπής περιεχομένου δεδομένων (intercention of content data). Τέλος, το δεύτερο κεφάλαιο αναφέρεται και σε θέματα δικαιοδοσίας όσον αφορά τα εγκλήματα που διαπράττονται στον κυβερνοχώρο.

Το τρίτο κεφάλαιο περιλαμβάνει τις διατάξεις που αφορούν τη διεθνή δικαστική διαδικασία που πρέπει να αναπτύσσουν σύμφωνα με τη σύμβαση της Βουδαπέστης τα κράτη μέλη, προκειμένου να ποινικοποιούν τα εγκλήματα στον κυβερνοχώρο. Οι διατάξεις αυτές αναφέρονται στην έκδοση, στον καθορισμό ενεργειών σχετικά με την αμοιβαία συνδρομή σε παροχή αυτοματοποιημένων πληροφοριών, στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε υπολογιστή και στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων πληροφοριών.

Επιπλέον, η Σύμβαση προβλέπει για τα κράτη μέλη τη θέσπιση ειδικών ποινικών διατάξεων για τα εγκλήματα σχετιζόμενα με υπολογιστές (computer related offences). Πολύ συχνά σοβαρά εγκλήματα που σχετίζονται με υπολογιστές είναι η πλαστογραφία και η απάτη. Ακόμα, με ιδιαίτερη προσοχή μελετώνται τα εγκλήματα που σχετίζονται με το περιεχόμενο που διακινείται στο διαδίκτυο, με όλο το βάρος να πέφτει στην παιδική πορνογραφία. Ωστόσο, δεν παραλείπεται και η αναφορά για τα εγκλήματα που είναι σχετικά με τις παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων (offences related to infringement of Copyright and related rights). Στο τέλος, συμπεριλαμβάνονται και διατάξεις δογματικού ποινικού χαρακτήρα για την απόπειρα, τη συμμετοχή και την ευθύνη των νομικών προσώπων.

Τη Συνθήκη της Βουδαπέστης για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο ήρθε να συμπληρώσει το Πρόσθετο Πρωτόκολλο της Σύμβασης που υπογράφηκε στο Στρασβούργο στις 28 Ιανουαρίου 2003. Στο Πρωτόκολλο

του Στρασβούργου ποινικοποιούνται πράξεις ρατσισμού και ξενοφοβίας που διαπράττονται μέσω του κυβερνοχώρου. [17]

Κοινή διαπίστωση είναι ότι η εγκληματικότητα στον κυβερνοχώρο, είναι ένα μεγάλο αγκάθι της σημερινής σύγχρονης ψηφιακής κοινωνίας και η πορεία της στο χρόνο επιβεβαιώνει τους φόβους των αρμόδιων για ανεξέλεγκτη αύξηση των ηλεκτρονικών εγκλημάτων. Έτσι, εφόσον βρισκόμαστε σε μια δεδομένη κατάσταση, όπου το διαδίκτυο αποτελεί ένα αναπόσπαστο και αναπόφευκτο κομμάτι της καθημερινότητας του ανθρώπου, ο νομοθέτης καλείται να ρυθμίσει νομοθετικά το φαινόμενο κατάχρησης του διαδικτύου. Αυτή η νομοθετική ρύθμιση θα πρέπει να αποσκοπεί στην καθιέρωση κάποιων αντικειμενικών υποστάσεων που θα θέτουν όρια στις δραστηριότητες των χρηστών στο διαδίκτυο.

Η ανάγκη για επιβολή κοινών κανόνων διεθνούς ποινικού δικαίου είναι επιτακτική για την αντιμετώπιση των εγκλημάτων που εκτυλίσσονται στο διαδίκτυο, λόγω της παγκοσμιότητας του αλλά και των διαφορετικών νομοθετικών δεδομένων περί αυτού που υπάρχουν σε κάθε κράτος. Έτσι, καταστάσεις όπως η επιλογή του εφαρμοστέου κάθε φορά δικαίου, δυσχεραίνουν σε μεγάλο βαθμό την ποινική λύση του εγκλήματος, καθώς και την απονομή δικαιοσύνης, κάνοντας έτσι την ομοιογενοποίηση του δικαίου όλο και πιο επιβεβλημένη λύση για το θέμα της δικαιοδοσίας.

Συμπερασματικά, η Σύμβαση της Βουδαπέστης αποτελεί την πρώτη διεθνή απόπειρα συνεργασίας για την πάταξη του ηλεκτρονικού εγκλήματος, υποχρεώνοντας τα κράτη μέλη που έκαναν δεκτούς τους όρους της Σύμβασης, να προσαρμόσουν τις επιμέρους εθνικές ποινικές νομοθεσίες πάνω στις διατάξεις της Σύμβασης, ποινικοποιώντας ορισμένες συμπεριφορές που λαμβάνουν χώρα στο διαδίκτυο.

Ας δούμε τώρα η Ελλάδα ως χώρα που υπέγραψε τη Συνθήκη της Βουδαπέστης, ποια νομοθετικά μέτρα έχει λάβει:

Η Ελληνική Αστυνομία προχώρησε στη σύνταξη εξειδικευμένης υπηρεσίας για την εξιχνίαση εγκλημάτων που τελούνται μέσω του διαδικτύου. Το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος, με μονάδες σε Αθήνα και Θεσσαλονίκη, αναλαμβάνουν υποθέσεις ηλεκτρονικού εγκλήματος σε όλη την

[17] *Σύμβαση της Βουδαπέστης* για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)

Ελλάδα, ενώ παράλληλα συνεργάζονται με τις αντίστοιχες υπηρεσίες του εξωτερικού. Τα στελέχη του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος είναι εξειδικευμένοι αστυνομικοί, οι οποίοι με στόχο την πρόληψη του διαδικτυακού εγκλήματος, περιηγούνται στο διαδίκτυο για την αναζήτηση επικίνδυνων περιπτώσεων. Παράλληλα τα στελέχη του Τ.Δ.Η.Ε. διερευνούν καταγγελίες που έχουν λάβει από πολίτες και διενεργούν σχετικές προανακρίσεις.

Το Τ.Δ.Η.Ε. επικεντρώνεται κυρίως σε διαδικτυακούς τόπους που έχουν πρόσβαση όλοι οι χρήστες του διαδικτύου και το περιεχόμενο τους είναι σε κοινή θέα (chat rooms, blogs, sites). Ακόμα, στην ευαίσθητη περίπτωση διακίνησης υλικού παιδικής πορνογραφίας ή της απάτης εναντίον του ανηλίκου, εφαρμόζονται άμεσα οι προβλεπόμενες διαδικασίες εντοπισμού του δράστη σύμφωνα με τις ισχύουσες διατάξεις. Κατόπιν, εφόσον προκύπτει η διαδικασία του αυτόφωρου, η Ελληνική Αστυνομία αναλαμβάνει τη σύλληψη των δραστών και την προσαγωγή τους ενώπιον της δικαιοσύνης.

Επίσης, η Υπηρεσία Προστασίας Ανηλίκων που ανήκει στο Υπουργείο Δημόσιας Τάξης παρέχει συμβουλές-οδηγίες που απευθύνονται στους γονείς και έχουν να κάνουν με την προστασία των παιδιών τους από την αρνητική επίδραση του διαδικτύου. Ακόμα, η συγκεκριμένη Υπηρεσία προχώρησε στην παρουσίαση μέσω Μ.Μ.Ε οδηγιών προς τους γονείς για κάποια μέτρα που πρέπει να λαμβάνουν για την πρόληψη της αρνητικής επίδρασης του διαδικτύου προς τα παιδιά τους, καθώς και στην παρουσίαση μηχανισμών φιλτραρίσματος που παρεμποδίζουν την είσοδο των ανηλίκων σε ύποπτες ιστοσελίδες.[18]

2.8 ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Παρακάτω γίνεται μια προσπάθεια ώστε να αναφερθεί η υπάρχουσα νομοθεσία για το ηλεκτρονικό έγκλημα. Η μονοθεσία για το ηλεκτρονικό έγκλημα περιλαμβάνει άρθρα ποινικού κώδικα, νόμους, προεδρικά διατάγματα, οδηγίες της Ευρωπαϊκής Ένωσης, Διεθνής Συμβάσεις και Αποφάσεις.

2.8.1 Άρθρα Ποινικού Κώδικα

[18] http://www.ydt.gr

Άρθρο 348Α - Πορνογραφία ανηλίκων.

Άρθρο 370Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας.

Άρθρο 370Β - Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.

Άρθρο 370Γ - Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.

Άρθρο 386Α - Απάτη με υπολογιστή.

2.8.2 Νόμοι

Ν. 2225/94 – «Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας».

Ν. 2472/97 και 2774/99 – «Περί προσωπικών δεδομένων».

Ν. 2472/1997 – «Για την προστασία των προσωπικών δεδομένων στο Διαδίκτυο».

Ν. 2774/1999 – «Για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα».

Ν. 2867/2000 - «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών».

Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων».

Ν. 2225/1994 όπως τροπ. Με Ν. 3115/2003 – «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις».

Ν. 3411/2006 – «Περί ηλεκτρονικών επικοινωνιών».

2.8.3 Προεδρικά Διατάγματα

Π.Δ. 131/2003 – «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας» .

Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές».

Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».

2.8.4 Οδηγίες Ευρωπαϊκής Ένωσης

Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision - ONP).

Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών.

Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.

Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).

Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση).

Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).

Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).

Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

2.8.5 Διεθνείς Συμβάσεις

Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας.

Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001.

Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948.

Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ).

2.8.6 Αποφάσεις

Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».

Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr».

Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής».

3. Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΚΑΤΑΝΑΛΩΤΩΝ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

3.1 Εισαγωγή

Όπως ήταν φυσικό, η επίδραση του διαδικτύου στην Κοινωνία της Πληροφορίας, όπως χαρακτηριστικά έχει ονομαστεί η σημερινή κοινωνία μας, δε θα μπορούσε να αφήσει ανεπηρέαστες τις καταναλωτικές μας συνήθειες. Ανέκαθεν ο άνθρωπος είχε καταναλωτικές ανάγκες και για να τις ικανοποιήσει πραγματοποιούσε συναλλαγές (ανταλλαγή προϊόντων έναντι χρημάτων κ.α.), όπως και σήμερα, βέβαια μόνο που στη σημερινή ψηφιακή κοινωνία που ζούμε, το διαδίκτυο ήρθε για να αλλάξει θεαματικά τον τρόπο με τον όποιον πραγματοποιούνται οι συναλλαγές.

Ο όρος παγκόσμια ηλεκτρονική αγορά, περιγράφει απόλυτα αυτό το εργαλείο που έχει στα χέρια του ο καταναλωτής, προκειμένου να εξυπηρετεί τις καταναλωτικές του ανάγκες. Όμως, μαζί με τον καταναλωτή και οι επιχειρήσεις είδαν το ηλεκτρονικό εμπόριο ως μια πάρα πολύ καλή προοπτική για νέες και πιο κερδοφόρες δραστηριότητες. Οι ηλεκτρονικές συναλλαγές παρέχουν άνεση στον καταναλωτή, δίνουν αξία στα χρήματα του και την ευκαιρία για την καλύτερη επιλογή. Η παγκόσμια ηλεκτρονική αγορά είναι μια πρόκληση για όλους μας, όμως κρύβει μέσα της και πολλούς κινδύνους. [19]

Το ηλεκτρονικό εμπόριο ή αλλιώς e-commerce, είναι η παροχή αγαθών και υπηρεσιών, μέσω internet, συνήθως, έναντι αμοιβής. Συνδεόμαστε με μια ιστοσελίδα, η οποία προσφέρει κάποια συγκεκριμένη υπηρεσία, συμβουλευόμαστε τον κατάλογο, επιλέγουμε το προϊόν, που θέλουμε και συμπληρώνουμε την εντολή αγοράς, διευκρινίζοντας τον τρόπο πληρωμής (π.χ. πιστωτική κάρτα, επιταγή ή εξόφληση τοις μετρητοίς, κατά την παραλαβή του προϊόντος).

Ηλεκτρονικό εμπόριο είναι επίσης, η παροχή μη υλικών αγαθών, όπως μουσική ή προγράμματα λογισμικού. Είναι πλέον γνωστό σε όλους μας ότι αρκεί μια απλή πληκτρολόγηση του αριθμού της πιστωτικής μας κάρτας, ώστε να "κατεβάσουμε" το τραγούδι ή το λογισμικό της επιλογής μας. Μπορούμε να παρακολουθούμε τις μετοχές στη Σοφοκλέους και να διενεργούμε

[19] *http://kepka.org/index.php*

αγοραπωλησίες, αν θέλουμε, μέσω των on - line υπηρεσιών, που πολλές χρηματιστηριακές εταιρίες προσφέρουν. Ακόμη και πλειστηριασμοί μπορούν να γίνουν, μέσω internet, ή αγοραπωλησίες σε χοντρική τιμή, στο λεγόμενο e-marketplace, μια εικονική αγορά, όπου πωλητές και πιθανοί αγοραστές συναλλάσσονται εκ του μακρόθεν.

Το ηλεκτρονικό εμπόριο αποτελεί μόδα για την εποχή μας και αυτό έχει ως επακόλουθο πολλές επιχειρήσεις να θέλουν να ενταχθούν σε αυτό. Χαρακτηριστικό παράδειγμα αποτελεί η ψηφιακή τηλεόραση, ένας καινούριος όρος που αναμένεται να μπει στην καθημερινότητα μας.

Ποιο είναι όμως το μεγάλο μειονέκτημα του ηλεκτρονικού εμπορίου; Έχει αποδειχθεί ότι η ασφάλεια των συναλλαγών αποτελεί την πληγή των ηλεκτρονικών συναλλαγών, αναγκάζοντας έτσι μεγάλο ποσοστό καταναλωτών να αποφεύγουν το ηλεκτρονικό εμπόριο, με το φόβο ότι πρόκειται να πέσουν θύματα απάτης. Πολλές είναι οι περιπτώσεις όπου αγνοήθηκαν παντελώς, παραγγελίες που έχουν κατατεθεί, καταναλωτές που δεν πήραν πίσω τα χρήματα τους, ενώ επέστρεψαν πίσω εγκαίρως το προϊόν που αγόρασαν, χρέωναν την πιστωτική κάρτα του καταναλωτή τη στιγμή της παραγγελίας, παραβιάστηκε η οδηγία σύμφωνα μα την οποία ο καταναλωτής μπορεί να γυρίσει το προϊόν που αγόρασε πίσω σε συγκεκριμένο χρονικό διάστημα χωρίς αιτιολόγηση της απόφασης του. Τα ηλεκτρονικά καταστήματα δεν είναι αληθείς πληροφορίες για το τελικό κόστος των προϊόντων και την περίπτωση που οι ιστοσελίδες ηλεκτρονικού εμπορίου δεν παρείχαν επαρκής πληροφορίες για την προστασία των δεδομένων των καταναλωτών.

3.2. ΜΟΡΦΕΣ ΑΠΑΤΗΣ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Βάση συστατικών, πολλές είναι οι απάτες που τελούνται στο ηλεκτρονικό εμπόριο σε όλο τον κόσμο καθημερινώς. Ας δούμε τώρα τις μορφές με τις οποίες εμφανίζεται η απάτη στο χώρο του ηλεκτρονικού εμπορίου. [20]

- **Δημοπρασίες στο διαδίκτυο:** πρόκειται για δημοπρασίες που λαμβάνουν χώρα στο διαδίκτυο και έχουν ως στόχο την εξαπάτηση του πλειοδότη, είτε με την παρουσίαση παραποιημένων προϊόντων, είτε με την παράδοση των προϊόντων στο νικητή της δημοπρασίας.

[20] *www.enepam.gr*

- **Παρουσίαση παραποιημένων προϊόντων:** συνηθισμένη τακτική είναι και η παραποιημένη παρουσίαση των προϊόντων, με σκοπό την προσέλκυση καταναλωτών. Πολλές είναι οι περιπτώσεις όπου οι έμποροι παρουσιάζουν ένα προϊόν που όμως δεν ανταποκρίνεται στην πραγματικότητα.
- **Μη παράδοση των προϊόντων στον πελάτη:** Μια συνηθισμένη απάτη που πραγματοποιείται στο ηλεκτρονικό εμπόριο, είναι η μη παράδοση των προϊόντων στους καταναλωτές ενώ έχει γίνει η παραγγελία και στις περισσότερες εκ των περιπτώσεων ακόμα και η πληρωμή.
- **Έκκληση για χρηματικές προσφορές:** Πολλοί επιτήδειοι επικαλούνται εράνους για τη βοήθεια συνανθρώπων μας με σκοπό να αποκομίζουν μεγάλα χρηματικά ποσά.
- **Ψεύτικο hardware και software υπολογιστών:** Πρόκειται για εξοπλισμό (hardware) υπολογιστών ή προγράμματα (software) που τα χαρακτηριστικά που παρουσιάζει ο προμηθευτής δεν ανταποκρίνονται στην πραγματικότητα.
- **Χρεώσεις υπηρεσιών στο διαδίκτυο:** Εταιρείες που παρέχουν υπηρεσίες στο διαδίκτυο, υπερχρεώνουν τον καταναλωτή ακόμα και για υπηρεσίες που δε ζήτησε ή ζήτησε και δεν πήρε ποτέ.
- **Πρόσβαση σε πορνογραφικές ιστοσελίδες:** Χρήστες που συνδέονται σε πορνογραφικές ιστοσελίδες. Βλέπουν να φουσκώνουν οι λογαριασμοί των πιστωτικών καρτών και των τηλεφωνικών λογαριασμών τους από υπηρεσίες που ποτέ δεν τους παραδόθηκαν.
- **Δάνεια και πιστωτικές κάρτες μέσω διαδικτύου:** Πολλοί είναι οι τοκογλύφοι που δρουν μέσω του διαδικτύου και προσελκύουν καταναλωτές μέσω ψεύτικων όρων και υποσχέσεων, ώστε να δανειστούν χρηματικά ποσά και να εκδώσουν πιστωτικές κάρτες.
- **Επιχειρήσεις φαντάσματα:** Ηλεκτρονικοί εγκληματίες ανοίγουν ιστοσελίδες ηλεκτρονικού εμπορίου χωρίς να έχουν τίποτα να πουλήσουν από όλα αυτά που παρουσιάζουν, με σκοπό να εξαπατήσουν τους καταναλωτές.
- **Παροχή ψευδών πληροφοριών στον καταναλωτή:** Πληροφορίες που δίνονται για το προϊόν όπως η τιμή, πρόσθετες επιβαρύνεις αλλά και τα χαρακτηριστικά του, είναι ανακριβής.
- **Ανύπαρκτες εγγυήσεις των προϊόντων:** Πολιτικές επιστροφής, παροχής εγγυήσεων καλής λειτουργίας των παραπόνων των καταναλωτών ή αποζημίωσης των καταναλωτών, είναι ανύπαρκτες.

Αφού έγινε η ανάλυση των μορφών με τις οποίες εμφανίζεται η εγκληματικότητα στο ηλεκτρονικό εμπόριο, το συμπέρασμα που βγήκε είναι ότι η ασφάλεια των συναλλαγών, η εμπιστευτικότητα των προσωπικών δεδομένων και η ασφάλεια των δεδομένων δε βρίσκονται πάντα στο καλύτερο επίπεδο, φέρνοντας έτσι τον καταναλωτή και τα προσωπικά του δεδομένα εκτεθειμένα σε κίνδυνο.

Τι πρέπει όμως να προσέχουμε σε μια ηλεκτρονική συναλλαγή;

Κάθε καταναλωτής πριν πραγματοποιήσει μια ηλεκτρονική συναλλαγή θα πρέπει να δώσει ιδιαίτερη προσοχή στα στοιχεία της ιστοσελίδας του ηλεκτρονικού καταστήματος, στην ταυτότητα καθώς και στα συστήματα ασφαλείας που χρησιμοποιεί. Συγκεκριμένα, κάθε καταναλωτής που χρησιμοποιεί το διαδίκτυο για την πραγματοποίηση των συναλλαγών του, θα πρέπει να αναζητεί πληροφορίες σχετικά με την:

- Πραγματική ταυτότητα του προμηθευτή
- Τρόπους επικοινωνίας με τον προμηθευτή (τηλέφωνο, email, fax)
- Τελική τιμή του προϊόντος που θέλει να αγοράσει
- Τις εγγυήσεις που του δίνονται
- Τον τρόπο αποστολής, το χρόνο παράδοσης, τη δυνατότητα υπαναχώρησης, τον τρόπο πληρωμής και παράδοσης.
- Την πολιτική προστασίας των προσωπικών δεδομένων που χρησιμοποιούν οι καταναλωτές για την πραγματοποίηση της συναλλαγής
- Επιβεβαίωση παραλαβής της παραγγελίας[21]

3.3 Ασφάλεια Ηλεκτρονικών Πληρωμών

Η ανασφάλεια και η αβεβαιότητα των χρηστών σχετικά με την εκτέλεση ηλεκτρονικών αγορών, αποτελούν ίσως τους σημαντικότερους περιοριστικούς λόγους εξάπλωσης του ηλεκτρονικού εμπορίου. Οι χρήστες προκειμένου να

[21] *Καταναλωτικά Βήματα – Τεύχος Οκτώβριος 2000*

πραγματοποιήσουν τις αγορές τους στο διαδίκτυο, πρέπει να είναι σίγουροι ότι τα προσωπικά τους δεδομένα προστατεύονται κατάλληλα και ότι δεν πρόκειται να πέσουν θύματα απάτης. Είναι γνωστό ότι οι ηλεκτρονικές πληρωμές στο διαδίκτυο εισάγουν πρόσθετους κινδύνους σε σχέση με τις παραδοσιακές πληρωμές και άρα πρέπει να λαμβάνονται πρόσθετα μέτρα ασφάλειας. Τα ηλεκτρονικά συστήματα πληρωμών αντιμετωπίζουν τα εξής επιπλέον προβλήματα: [22]

- Τα ψηφιακά έγγραφα μπορούν αυθαίρετα να αντιγραφούν.
- Οι ψηφιακές υπογραφές μπορούν να παραχθούν από οποιονδήποτε γνωρίζει το ιδιωτικό κλειδί.
- Η ταυτότητα του πληρωτή μπορεί να συνδεθεί με κάθε συναλλαγή πληρωμής, με αποτέλεσμα να γίνονται γνωστές οι καταναλωτικές και όχι μόνο συνήθειες του πληρωτή.

Προφανώς χωρίς πρόσθετα μέτρα ασφάλειας, το διαδεδομένο ηλεκτρονικό εμπόριο δεν θα ήταν βιώσιμο. Γενικά, τα ηλεκτρονικά συστήματα πληρωμών αντιμετωπίζουν τους εξής επιτιθέμενους:

- Αυτούς που κρυφακούν στη γραμμή επικοινωνίας και συλλέγουν πληροφορίες (π.χ. αριθμούς πιστωτικών καρτών) τις οποίες χρησιμοποιούν για απάτες με σκοπό το δικό τους οικονομικό όφελος.
- Αυτούς που επεμβαίνουν και τροποποιούν τα μηνύματα που ανταλλάσσονται σε μια συναλλαγή πληρωμής, προκειμένου να κλέψουν αγαθά ή χρήματα.
- Τους ανέντιμους συμμετέχοντες στη συναλλαγή πληρωμής (π.χ. έμπορας), οι οποίοι χρησιμοποιούν για απάτες τις πληροφορίες πληρωμής (π.χ. αριθμούς πιστωτικών καρτών) που τους δίνει ο πελάτης.

Τα γενικά χαρακτηριστικά που αναφέρονται παρακάτω αποτελούν τα συστατικά στοιχεία ασφαλείας που θα πρέπει να έχει ένα σύστημα ηλεκτρονικών πληρωμών: [23]

[22] *www.*mis.uoa.gr

[23] www.cyber-point.gr

Αυθεντικοποίηση Πληρωμής: Τόσο ο πληρωτής, όσο και ο δικαιούχος πληρωμής, θα πρέπει να αποδεικνύουν τις ταυτότητες τους, οι οποίες δεν είναι απαραίτητα ίδιες με τις αληθινές τους ταυτότητες. Η αυθεντικοποίηση δεν υπονοεί ότι απαραίτητα η ταυτότητα του πληρωτή αποκαλύπτεται.

Ακεραιότητα Πληρωμής: Το σύστημα θα πρέπει να διασφαλίζει ότι τα δεδομένα της συναλλαγής, πληρωμής δεν μπορούν να τροποποιηθούν από αναρμόδιους συμβαλλόμενους.

Έγκριση Πληρωμής: Το σύστημα θα πρέπει να εξασφαλίζει ότι δεν θα αποσυρθούν χρήματα από τον λογαριασμό του πελάτη, χωρίς τη ρητή άδεια του και ότι το καθορισμένο ποσό μπορεί να αποσυρθεί μόνο από εξουσιοδοτημένο συμβαλλόμενο.

Εμπιστευτικότητα Πληρωμής: Το σύστημα θα πρέπει να διασφαλίζει την προστασία των δεδομένων της συναλλαγής από τρίτους.

3.4 Υπηρεσίες Ασφάλειας Πληρωμών

Ένα ηλεκτρονικό σύστημα πληρωμών που χρησιμοποιείται στις συναλλαγές ηλεκτρονικού εμπορίου, θα πρέπει να περιλαμβάνει τις εξής υπηρεσίες ασφάλειας:

Ανωνυμία Χρήστη: Προστατεύει από την κοινοποίηση της ταυτότητας του χρήστη σε μια συναλλαγή πληρωμής. Συνήθως ο χρήστης επιθυμεί να πραγματοποιεί τις συναλλαγές του ανώνυμα.

Μη Ανίχνευση Θέσης: Προστατεύει από την κοινοποίηση της θέσης όπου γίνεται η συναλλαγή. Χρησιμοποιώντας μόνο ανωνυμία του χρήστη, η IP διεύθυνση και το host name του υπολογιστή, από τον οποίο στάλθηκε κάποιο μήνυμα ή έγινε κάποια συναλλαγή, είναι γνωστά. Και στην περίπτωση που ο υπολογιστής είναι προσωπικός, είναι δεδομένη η IP διεύθυνση του και άρα μπορεί να προσδιοριστεί ο χρήστης. Με την υπηρεσία μη ανίχνευσης θέσης εξασφαλίζεται ότι η IP διεύθυνση και το host name του υπολογιστή δεν θα αποκαλυφθούν.

Μη Ανίχνευση Συναλλαγής Πληρωμής: Προστατεύει από τη σύνδεση δύο διαφορετικών συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πελάτη. Ένας πληρωτής θέλοντας να διατηρήσει την ανωνυμία του, μπορεί να κρύβεται πίσω από ένα ψευδώνυμο, π.χ. μια αριθμητική ταυτότητα. Εάν χρησιμοποιεί την

ίδια ταυτότητα σε όλες τις συναλλαγές του, τότε η συμπεριφορά του μπορεί να παρατηρηθεί και σε συνδυασμό με άλλες πληροφορίες και η ταυτότητα του μπορεί να αποκαλυφθεί. Η υπηρεσία μη ανίχνευσης συναλλαγής πληρωμής, κρύβει τη σύνδεση μεταξύ συναλλαγών πληρωμών που περιλαμβάνουν τον ίδιο πληρωτή.

Εμπιστευτικότητα των Δεδομένων της Συναλλαγής Πληρωμής: Προστατεύει από την κοινοποίηση των δεδομένων της συναλλαγής πληρωμής σε τρίτους. Επιπλέον, η υπηρεσία αυτή προστατεύει και κάποια δεδομένα της συναλλαγής πληρωμής από επιλεγμένους εμπλεκόμενους. Για παράδειγμα αποκρύπτει από τον έμπορα τις πληροφορίες για την πιστωτική κάρτα του πελάτη.

Μη αποκήρυξη των Μηνυμάτων της Συναλλαγής Πληρωμής: Προστατεύει από ενδεχόμενη άρνηση της προέλευσης των μηνυμάτων που ανταλλάσσονται σε μια συναλλαγή πληρωμής. Μπορεί ένας πελάτης να υποστηρίξει ότι ποτέ δεν έδωσε εντολή πληρωμής, ή ένας έμπορας να υποστηρίξει ότι δεν έλαβε πληρωμή από τον πελάτη. Η υπηρεσία μη αποκήρυξης μηνυμάτων λύνει τέτοιες διαφωνίες χρησιμοποιώντας μηχανισμούς ψηφιακής υπογραφής.

Μη Επανάληψη Μηνυμάτων Συναλλαγής Πληρωμής: Προστατεύει από επαναλαμβανόμενα μηνύματα σε συναλλαγή πληρωμής. Σε περίπτωση που ένας πελάτης στείλει ένα μήνυμα με τις πληροφορίες της πιστωτικής του κάρτας ως πληρωμή, το μήνυμα αυτό, ακόμη και σε κρυπτογραφημένη μορφή, μπορεί να παρθεί από έναν επιτιθέμενο ο οποίος να το επαναχρησιμοποιήσει. Η υπηρεσία μη επανάληψης μηνυμάτων προστατεύει από τέτοιου είδους επιθέσεις.

3.5 Ασφάλεια Συναλλαγών Πληρωμής

Ανωνυμία Χρήστη και Μη ανίχνευση Θέσης: Η ανωνυμία χρήστη θα μπορούσε να πραγματοποιηθεί με τη χρήση ενός ψευδωνύμου αντί της πραγματικής ταυτότητας του χρήστη. Σε περίπτωση όμως που το δίκτυο συναλλαγής παγιδευόταν, τέτοιος τύπος ανωνυμίας δεν είναι ικανοποιητικός. Η υπηρεσία μη ανίχνευσης θέσης μπορεί να προστατεύσει από την κοινοποίηση της θέσης όπου γίνεται η συναλλαγή, χρησιμοποιώντας ανώνυμα hosts μέσω των οποίων στέλλονται τα μηνύματα κατά τη διάρκεια της συναλλαγής πληρωμής.

Κατηγορίες Ψηφιακού Χρήματος: Γενικά υπάρχουν δύο ξεχωριστοί τύποι ηλεκτρονικού χρήματος (e-money): το ηλεκτρονικό χρήμα που προσδιορίζει την

ταυτότητα του ιδιοκτήτη του (identified e-money) και το ανώνυμο ηλεκτρονικό χρήμα (anonymous e-money), γνωστό επίσης και ως ψηφιακά μετρητά (digital cash). Ο πρώτος τύπος περιλαμβάνει πληροφορίες που γνωστοποιούν την ταυτότητα του προσώπου που έκανε την ανάληψη χρημάτων από την τράπεζα (οργανισμό έκδοσης των χρημάτων αυτών) και βοηθάει την τράπεζα να ανιχνεύσει την διακίνηση του μέσα στην οικονομία, λειτουργεί δηλαδή με τον ίδιο τρόπο με τον οποίο λειτουργούν και οι πιστωτικές κάρτες. Τα ψηφιακά νομίσματα, όπως και τα παραδοσιακά χαρτονομίσματα έχουν ένα serial number. Είναι εύκολο να δημιουργηθεί ένα μεγάλο αρχείο στο οποίο θα καταχωρείται ποιος πελάτης έλαβε ποιους serial number ψηφιακών νομισμάτων, αμέσως μόλις ο πελάτης αγοράσει ψηφιακά νομίσματα από την τράπεζα. Ο δεύτερος τύπος ηλεκτρονικού χρήματος μοιάζει με τα χάρτινα μετρητά που κυκλοφορούν. Το ανώνυμο ηλεκτρονικό χρήμα μπορεί να ξοδευτεί ή και να χαθεί ακόμα, χωρίς όμως η τράπεζα να γνωρίζει κάτι για τη διακίνηση του από την ανάληψη του και μετά.

Οι πιο πάνω τύποι ηλεκτρονικού χρήματος συναντιόνται σε δύο κατηγορίες: on-line και offline. Η πρώτη κατηγορία προϋποθέτει αλληλεπίδραση του πελάτη με την τράπεζα (διαμέσου δικτύου) για να διεξαχθεί η εμπορική πράξη μέσω του έμπορα. Με τη δεύτερη κατηγορία ηλεκτρονικού χρήματος δεν απαιτείται η απευθείας εμπλοκή της τράπεζας για να διεκπεραιωθεί η οικονομική συναλλαγή. Η συναλλαγή με offline ανώνυμο ηλεκτρονικό χρήμα είναι και η περισσότερο περίπλοκη συναλλαγή ηλεκτρονικού χρήματος, αφού η μυστικότητα η οποία προσφέρει δημιουργεί και την ευκαιρία διπλού ξοδέματος του από τον κάτοχο του.

3.6 Ψηφιακές Υπογραφές:

Για την απόδειξη της γνησιότητας ενός εγγράφου, χρησιμοποιούνται οι συμβατικές υπογραφές. Ειδικότερα, η υπογραφή αποτελεί μαρτυρία της εγκυρότητας του υπογεγραμμένου εγγράφου έτσι ώστε ο υπογράφων να μη μπορεί να το απαρνηθεί. Στις συναλλαγές ηλεκτρονικού εμπορίου καθίσταται αναγκαία η χρησιμοποίηση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής υπογραφής. Ο μηχανισμός της ηλεκτρονικής υπογραφής θα πρέπει να παρέχει απόδειξη της προέλευσης, της γνησιότητας και της ακεραιότητας των εναλλασσομένων μηνυμάτων. Απαιτείται δηλαδή ένα σύστημα, μέσω του οποίου κάποιος θα μπορεί να στείλει ένα υπογεγραμμένο μήνυμα σε κάποιον άλλο με τέτοιο τρόπο ώστε:

- Ο παραλήπτης να μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο αποστολέας.
- Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος.
- Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.

Οι ηλεκτρονικές υπογραφές που βασίζονται στην κρυπτογραφία ονομάζονται ψηφιακές υπογραφές. Η ψηφιακή υπογραφή εξαρτάται άμεσα από το μήνυμα το οποίο στέλνεται, είναι γνωστή μόνο στον αποστολέα αλλά μπορεί να επιβεβαιωθεί από τον καθένα. Η ψηφιακή υπογραφή θα πρέπει να είναι εύκολο να υπολογιστεί και να επιβεβαιωθεί από οποιονδήποτε ενδιαφερόμενο. Παράλληλα όμως θα πρέπει να είναι αδύνατο να αντιγραφεί. [24]

3.7 Έξυπνες κάρτες

Τα τελευταία χρόνια η τεχνολογία έξυπνων καρτών (smart cards) εφαρμόζεται στο ηλεκτρονικό εμπόριο και παρέχει ένα ασφαλές περιβάλλον εκτέλεσης των ηλεκτρονικών συναλλαγών.

Η τεχνολογία των έξυπνων καρτών χρησιμοποιείται για την προσέγγιση και επίλυση προβλημάτων πρόσβασης, διαχείρισης και διακίνησης πληροφορίας σχεδόν σε όλους τους τομείς της οικονομίας και της κοινωνίας. Ένας από τους σημαντικότερους τομείς της οικονομίας, όπου η τεχνολογία των έξυπνων καρτών χρησιμοποιείται, είναι το ηλεκτρονικό εμπόριο. Ο ρόλος των έξυπνων καρτών εστιάζεται κυρίως στη διασφάλιση περιβάλλοντος εμπιστοσύνης στις συναλλαγές μεταξύ πολιτών και παροχέων υπηρεσιών στο ηλεκτρονικό εμπόριο.

Μια έξυπνη κάρτα είναι μια πλαστική ίση σε μέγεθος με μια πιστωτική κάρτα, στην οποία έχει ενσωματωθεί ένα ολοκληρωμένο κύκλωμα (chip), στην εμπρόσθια αριστερή πλευρά. Το ολοκληρωμένο κύκλωμα μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Ουσιαστικά οι έξυπνες κάρτες είναι μικροσκοπικοί υπολογιστές. Ανάμεσα στα βασικότερα πλεονεκτήματα που διαφοροποιούν την έξυπνη από την απλή κάρτα είναι ότι το ολοκληρωμένο κύκλωμα μπορεί να παρέχει μια ασφαλή δομή αποθήκευσης δεδομένων καθιστώντας δύσκολη την πρόσβαση στα στοιχεία και την παραποίηση αυτών,

[24] www.eett.gr

να υπολογίζει κρυπτογραφικές συναρτήσεις και να αντιλαμβάνεται άμεσα προσπάθειες παράνομης (ή λανθασμένης) πρόσβασης. Οι έξυπνες κάρτες αναπόφευκτα αλλάζουν το ηλεκτρονικό εμπόριο λόγω της επαναστατικής ευκολίας και αξιοπιστίας που προσφέρουν, όσον αφορά το πώς τα δεδομένα αποθηκεύονται, προσπελάζονται, επεξεργάζονται και μεταβάλλονται. Λόγω του υψηλού επιπέδου ασφάλειας που παρέχουν οι εν λόγω κάρτες μειώνεται σημαντικά η πιθανότητα απάτης.

Οι έξυπνες κάρτες παρέχουν δύο βασικές λειτουργίες: αυθεντικοποίηση, και αποθήκευση δεδομένων. Η αυθεντικοποίηση διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να αποκτήσουν πρόσβαση σε συστήματα και κτιριακές εγκαταστάσεις. Μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί και σαν φορητή συσκευή αποθήκευσης έχοντας τη δυνατότητα να αποθηκεύει ένα ευρύ σύνολο από δεδομένα διαφορετικού τύπου και για διαφορετικούς σκοπούς. Επιπλέον μπορεί να χρησιμοποιηθεί και ως ηλεκτρονικό πορτοφόλι και να αποθηκεύει χρήματα σε ποικίλα συναλλάγματα καθώς επίσης και πιστωτικά υπόλοιπα και άλλες μορφές αξιών.

Οι έξυπνες κάρτες λόγω της ενσωματωμένης τεχνολογίας τους, έχουν ποικίλες εφαρμογές στο ηλεκτρονικό εμπόριο. Μια έξυπνη κάρτα μπορεί να είναι μια πιστωτική ή χρεωστική κάρτα με υψηλότερο επίπεδο ασφάλειας από ότι οι μαγνητικές κάρτες. Ένας από τους πιο ασφαλείς τρόπους για τη διασφάλιση της προστασίας του ιδιωτικού κλειδιού είναι η αποθήκευση του σε μια έξυπνη κάρτα. Οι κάρτες αυτές, μπορούν να συνδεθούν σε ένα υπολογιστή και να στείλουν το ιδιωτικό κλειδί για κρυπτογράφηση ή για δημιουργία ψηφιακής υπογραφής. Αυτό σημαίνει ότι το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να αποθηκευτεί στον υπολογιστή και ότι κάποιος για να έχει πρόσβαση στο ιδιωτικό κλειδί πρέπει να κλέψει την έξυπνη κάρτα. Αλλά ακόμα και σε αυτή την περίπτωση δεν θα μπορέσει να έχει πρόσβαση στο ιδιωτικό κλειδί διότι η έξυπνη κάρτα ζητά έναν κωδικό πρόσβασης (PIN) πριν δώσει το ιδιωτικό κλειδί. Επιπλέον, η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί ως ηλεκτρονικό πορτοφόλι όπου αποθηκεύονται μονάδες χρήματος και στη συνέχεια ο κάτοχος της τη χρησιμοποιεί για τις ηλεκτρονικές αγορές του στο διαδίκτυο. Επίσης, οι έξυπνες κάρτες μπορούν να παρέχουν υψηλό επίπεδο αυθεντικοποίησης. Συγκεκριμένα, μπορούν να αποθηκεύουν ψηφιακά πιστοποιητικά και συνεπώς να παρέχουν αυθεντικοποίηση στον κάτοχο τους κατά την πρόσβαση του σε κάποιο δίκτυο ή σύστημα. Λόγω της επεξεργαστικής δυνατότητας που έχουν, οι έξυπνες κάρτες μπορούν να δημιουργούν ζεύγος κλειδιών, να αποθηκεύουν το ιδιωτικό κλειδί και να δημιουργούν ψηφιακές υπογραφές με υψηλό επίπεδο ασφάλειας και αξιοπιστίας. Γενικά, τα οφέλη που προσφέρουν οι έξυπνες κάρτες στο

ηλεκτρονικό εμπόριο είναι πολλά και αναμφισβήτητα θα αλλάξουν ριζικά τις σχέσεις ανάμεσα σε καταναλωτές και οργανισμούς ηλεκτρονικού εμπορίου (εμπόρους).

3.7.1 Ιστορία Έξυπνων Καρτών

Η ιστορία της έξυπνης κάρτας είναι παράλληλη με την ανάπτυξη της τεχνολογίας των chip κατά τη διάρκεια των τελευταίων 40 ετών. Το 1969 παρουσιάστηκε στη Γαλλία, από τον δημοσιογράφο Roland Moreno, μία ιδέα για μία κάρτα με ενσωματωμένο κύκλωμα. Έτσι γεννήθηκε η έξυπνη κάρτα. Οι έξυπνες κάρτες αναπτύχθηκαν ανεξάρτητα στη Γερμανία (1967), στην Ιαπωνία (1970) και στις Η.Π.Α. (1972). Οι έξυπνες κάρτες άνθισαν τη δεκαετία του 1980.

Στο διάστημα 1982-84 η Cartes Bancaire (Ένωση Τραπεζικών Καρτών της Γαλλίας) έτρεξε το πρώτο πιλοτικό πρόγραμμα για έξυπνες κάρτες. Μετά την πολύ πετυχημένη δοκιμή, οι Γαλλικές τράπεζες εισήγαγαν τη χρήση των έξυπνων καρτών για τραπεζικές λειτουργίες στο ευρύ κοινό. Η χρήση αυτή είναι το πρώτο παράδειγμα δημόσιας λειτουργίας των έξυπνων καρτών για τραπεζικές λειτουργίες.

3.7.2 Τεχνικά Χαρακτηριστικά

Ο διεθνής οργανισμός τυποποίησης ISO (International Organization for Standardization) χρησιμοποιεί τον όρο κάρτα ολοκληρωμένων κυκλωμάτων για να καλύψει όλες εκείνες τις συσκευές όπου ένα ολοκληρωμένο κύκλωμα περιλαμβάνεται μέσα σε ένα κομμάτι πλαστικό. Η κάρτα είναι διαστάσεων 85.6mm X 53.98mm X 0.76mm και είναι η ίδια με την τραπεζική κάρτα με τη μαγνητική λωρίδα, που χρησιμοποιείται ως όργανο πληρωμής για τις πολυάριθμες οικονομικές συναλλαγές.

Η κύρια περιοχή αποθήκευσης σε τέτοιες κάρτες είναι συνήθως Ηλεκτρονικά Διαγραφόμενη Προγραμματιζόμενη Μόνο-Ανάγνωσης Μνήμη (Electrically Erasable Programmable Read Only Memory, EEPROM), η οποία έχει τη δυνατότητα να ενημερώνει και να διατηρεί τα περιεχόμενα της. Τα νεότερα chip έξυπνων καρτών ενσωματώνουν μερικές φορές μαθηματικούς συνεπεξεργαστές στο chip του μικροεπεξεργαστή, και έτσι είναι σε θέση να εκτελέσουν αρκετά σύνθετες ρουτίνες κρυπτογράφησης σχετικά γρήγορα. Για το

λόγω αυτό χρησιμοποιούνται στο ηλεκτρονικό εμπόριο και εκτελούν λειτουργίες κρυπτογράφησης και δημιουργίας ψηφιακών υπογραφών.

Το chip μιας έξυπνης κάρτας έχει τη δυνατότητα να αποθηκεύσει πολύ περισσότερα στοιχεία από εκείνα που μπορεί να συγκρατήσει μια αντίστοιχη μαγνητική κάρτα, και όλα αυτά μέσα σε ένα εξαιρετικά ασφαλές περιβάλλον. Τα στοιχεία που καταχωρούνται στο chip μπορούν να προστατευθούν αποτελεσματικά από εξωτερική αλλαγή. Στη συνέχεια περιγράφονται τα είδη έξυπνων καρτών:

Κάρτες μικροεπεξεργαστών (Integrated Circuit (IC) Microprocessor Cards): Οι κάρτες με μικροεπεξεργαστή είναι οι κλασσικές έξυπνες κάρτες οι οποίες μπορούν να διαχειριστούν και να επεξεργαστούν τα δεδομένα που βρίσκονται αποθηκευμένα σε αυτές. Οι κάρτες αυτές, εκτός από CPU, διαθέτουν μνήμη μόνο ανάγνωσης (Read Only Memory, ROM) για την αποθήκευση του λειτουργικού συστήματος της κάρτας, μνήμη RAM (Random Access Memory) για γρήγορη εκτέλεση υπολογισμών και μνήμη EEPROM για την αποθήκευση εφαρμογών και δεδομένων. Οι μικροεπεξεργαστές των καρτών αυτών έχουν τη δυνατότητα να εκτελούν υπολογισμούς τοπικά μέσα στα κυκλώματα της κάρτας, καθώς επίσης και να τρέχουν μικρά προγράμματα υπολογισμών. Αυτές οι κάρτες χρησιμοποιούνται για ποικίλες μικρές εφαρμογές, ειδικά για εκείνες που ενσωματώνουν αλγόριθμους κρυπτογράφησης, πράγμα το οποίο απαιτεί το χειρισμό μεγάλων αριθμών.

Υπάρχουν κάποιες έξυπνες κάρτες οι οποίες εκτελούν περισσότερες από μια εφαρμογές και έχουν ανοικτά λειτουργικά συστήματα (Java, MULTOS). Οι κάρτες αυτές ονομάζονται έξυπνες κάρτες πολλαπλών εφαρμογών (multi-application smart cards).

Κάρτες Μνήμης (Integrated Circuit (IC) Memory Cards): Η κάρτα μικροεπεξεργαστών μπορεί να προσθέσει, να διαγράψει και γενικά να χειριστεί τις αποθηκευμένες σε αυτήν πληροφορίες, ενώ μια κάρτα μνήμης (π.χ. προπληρωμένη τηλεφωνική κάρτα) μπορεί να αναλάβει μόνο μια προκαθορισμένη λειτουργία: την αποθήκευση πληροφορίας. Οι κάρτες μνήμης δεν έχουν απολύτως καμιά δυνατότητα επεξεργασίας και χειρισμού πληροφοριών, ενώ η μνήμη τους δε μπορεί να ξεπεράσει (τουλάχιστον για τις υπάρχουσες τυποποιήσεις ISO) τα 4KB. Ακριβώς επειδή δεν έχουν

μικροεπεξεργαστική ικανότητα, οι κάρτες μνήμης συγκαταλέγονται καταχρηστικά στις έξυπνες κάρτες.

Οι κάρτες αυτές στοιχίζουν οπωσδήποτε λιγότερο από τις κάρτες με μικροεπεξεργαστή, ωστόσο όμως υστερούν αρκετά στην ασφάλεια της πληροφορίας που συγκρατούν στο εσωτερικό τους. Εξαρτώνται άμεσα από την ασφάλεια του αναγνώστη καρτών (smart card reader) για την επεξεργασία και είναι ιδανικές όταν οι απαιτήσεις ασφάλειας δεν προϋποθέτουν υψηλό επίπεδο ασφάλειας.

Οπτικές Κάρτες Μνήμης (Optical Memory Cards): Οι οπτικές κάρτες μνήμης μπορούν να αποθηκεύουν μέχρι 4MB πληροφορίας. Βέβαια μόλις γραφτούν, τα στοιχεία δεν μπορούν να αλλάξουν ή να αφαιρεθούν. Κατά συνέπεια, αυτός ο τύπος κάρτας είναι ιδανικός για την φύλαξη αρχείων (π.χ. ιατρικά αρχεία ή e-books).

Οι έξυπνες κάρτες, ανάλογα με τον τρόπο επικοινωνίας τους με το εξωτερικό περιβάλλον, διακρίνονται στις εξής κατηγορίες:

- Έξυπνες κάρτες με επαφή (contact cards). Μια έξυπνη κάρτα με επαφή χρειάζεται να τοποθετηθεί σε ένα αναγνώστη καρτών (card reader) προκειμένου να διαβαστούν ήδη υπάρχουσες πληροφορίες ή να εισαχθούν νέες.
- Ασύρματες έξυπνες κάρτες (contactless cards). Οι κάρτες αυτές έχουν ενσωματωμένη κεραία και έτσι μπορούν να επικοινωνούν με μια κεραία λήψης ασύρματα, χωρίς δηλαδή φυσική επαφή.
- Υβριδικές και συνδυασμένες κάρτες (hybrid & combination cards). Οι κάρτες αυτές ενσωματώνουν και τους δύο τρόπους μετάδοσης και συνεπώς, μπορούν να επικοινωνήσουν κατά περίπτωση, είτε με ασύρματο είτε με ενσύρματο τρόπο.

3.8 ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Το ηλεκτρονικό εμπόριο είναι μια μορφή εμπορίου και συνεπώς, βρίσκουν εφαρμογή σε αυτό όλες οι κοινοτικές οδηγίες (το κοινοτικό δίκαιο) και οι

εθνικές διατάξεις, για την προστασία του Καταναλωτή, που αφορούν το εμπόριο γενικότερα. [25]

- Ο Ν. 2251/94, για την "Προστασία Καταναλωτών", στο άρθρο 4, ρυθμίζει τις συμβάσεις από απόσταση. Εδώ εμπίπτει και το ηλεκτρονικό εμπόριο.
- Ο Ν. 2472/97 αναφέρεται στην προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και ο Ν. 2174/99 στην προστασία δεδομένων προσωπικού χαρακτήρα, στον τηλεπικοινωνιακό τομέα. Την Αρχή Προστασίας Προσωπικών Δεδομένων τη βρίσκουμε στη διεύθυνση www.dpa.gr.
- Το πρόσφατο Προεδρικό Διάταγμα 150/2001, Φ.Ε.Κ. Α' 125, για τις ηλεκτρονικές υπογραφές, κάνει εμφανή την προσπάθεια της πολιτείας να προσφέρει μια σωστή βάση νομοθετικών πλαισίων.
- Το Προεδρικό Διάταγμα 131/2003, για το ηλεκτρονικό εμπόριο δίνει έμφαση στην εξώδικη επίλυση διαφορών, στη συνεργασία των κρατών - μελών της Ευρωπαϊκής Ένωσης, για την επίλυση των προβλημάτων των Καταναλωτών, στη θέσπιση κανόνων δεοντολογίας, με υποχρεωτική ισχύ, για τους αποδέκτες τους, στην ευθύνη των ενδιάμεσων, στη σύναψη των ηλεκτρονικών συμβάσεων, στις πληροφορίες, που πρέπει να παρέχονται στις εμπορικές επικοινωνίες (διαφημιστικά, χορηγίες, προσφορές κ.λπ.), στον τόπο εγκατάστασης των φορέων παροχής υπηρεσιών.
- Οι Καταναλωτές, όταν αγοράζουμε από χώρες εκτός της Ευρωπαϊκής Ένωσης πριν προβούμε σε οποιαδήποτε αγορά, πρέπει να αναζητήσουμε τις πληροφορίες, που διαθέτει ο έμπορος στο ηλεκτρονικό του κατάστημα και αφορούν το νομοθετικό κανονιστικό πλαίσιο, που θα διέπει τις αγορές μας.
- Η Σύμβαση των Βρυξελλών προβλέπει ότι, σε περίπτωση διαφοράς, που θα προκύψει με αλλοδαπό έμπορο ή εταιρία, ο Καταναλωτής, για τις χώρες μέλη της Ευρωπαϊκής Ένωσης, μπορεί να απευθυνθεί στο δικαστήριο του τόπου κατοικίας του. Το δε Δίκαιο, που θα εφαρμοστεί από το δικαστήριο, καθορίζεται από τη Σύμβαση της Ρώμης και, στις περισσότερες περιπτώσεις, είναι το Δίκαιο της χώρας του Καταναλωτή, καθώς, επίσης και οι Οδηγίες, για την προστασία του Καταναλωτή.

[25] *www.emporiko-oplostasio.com*

- Σύμφωνα με την οδηγία για το ηλεκτρονικό εμπόριο, εφαρμοστέο δίκαιο, όσον αφορά την παροχή προϊόντων και υπηρεσιών στο internet (εξαιρούνται οι συμβάσεις με Καταναλωτές), είναι η νομοθεσία του τόπου, όπου είναι εγκατεστημένος ο φορέας παροχής υπηρεσιών της κοινωνίας της πληροφορίας.

4. Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΩΝ ΚΑΤΑΝΑΛΩΤΩΝ

Παν πρόσωπο δικαιούται το σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. [26]

4.1 Εισαγωγή

Προσωπικά δεδομένα είναι στοιχεία που προσδιορίζουν ένα άτομο, όπως είναι το όνομα, η ηλικία ή η φωτογραφία του. Στην καθημερινή μας ζωή πολλές είναι οι φορές που καλούμαστε να δώσουμε προσωπικά στοιχεία, όπως για παράδειγμα για την εγγραφή μας σ' ένα video club, για τη συμπλήρωση ενός βιογραφικού σημειώματος για αναζήτηση εργασίας, για τη συμπλήρωση μιας φόρμας στο διαδίκτυο για την πραγματοποίηση μιας συναλλαγής ή τη συμπλήρωση ενός εντύπου για την έκδοση ενός τραπεζικού λογαριασμού. Όπως καταλαβαίνουμε, τα προσωπικά μας δεδομένα μπορεί να είναι καταχωρημένα στο video club της γειτονιάς μας μέχρι στον πιο μεγάλο τραπεζικό όμιλο του κόσμου. Πολλές φορές τα προσωπικά μας δεδομένα μπορεί να χρησιμοποιηθούν και για άλλους σκοπούς ή να μεταφέρονται από δω και από κει χωρίς να το γνωρίζουμε. [27]

Σίγουρα η ραγδαία εξάπλωση της τεχνολογίας και των υπολογιστών καθώς και η ανάπτυξη νέων και πιο σύγχρονων τηλεπικοινωνιακών δικτύων, έκανε την μεταβίβαση των προσωπικών δεδομένων πολύ απλή και γρήγορη διαδικασία. Έτσι, τα προσωπικά μας δεδομένα μπορούν να γίνουν αντικείμενο επεξεργασίας από τη μια άκρη του κόσμου στην άλλη. Κοινή διαπίστωση είναι ότι οι διαδικτυακοί τύποι ελλοχεύουν πολλούς κινδύνους για τα δεδομένα προσωπικού χαρακτήρα των χρηστών, αφού πολλές είναι οι περιπτώσεις που έχουμε παράνομη πρόσβαση και επεξεργασία σε προσωπικά δεδομένα. Έτσι λοιπόν, οδηγούμαστε στην ανάγκη για τη νομοθετική ρύθμιση της διαβίβασης των δεδομένων έτσι ώστε, τα προσωπικά στοιχεία κάθε χρήστη να είναι ασφαλή.

---

[26] somatikitimoria.gr/nomothesia.htm

[27] *ΔΟΝΟΥ/ΜΗΤΡΟΥ/ΜΙΤΤΛΕΤΟΥ/ΠΑΠΑΚΩΝΣΤΑΝΤΙΝΟΥ, « Η αρχή προστασίας δεδομένων και η επάυξηση των δικαιωμάτων»*

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής των χρηστών, αποτελεί τον οδηγό για τη θέσπιση της κατάλληλης νομοθεσίας από κάθε κράτος. Κάθε φορέας που επεξεργάζεται προσωπικά δεδομένα θα πρέπει να ακολουθεί πρακτικές ορθής μεταχείρισης των προσωπικών στοιχείων με ασφάλεια και εντιμότητα, καθώς και η χρησιμοποίηση των προσωπικών στοιχείων να γίνεται για διαφανής και θεμιτούς σκοπούς. Κάθε χρήστης που εισάγει προσωπικά δεδομένα στο διαδίκτυο, πρέπει να είναι πλήρως προστατευμένος από τους εγχώριους νόμους και η προστασία της προσωπικής ζωής να αποτελεί έννομο αγαθό για κάθε χρήστη.

4.2 ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τα προσωπικά δεδομένα και η ιδιωτική ζωή των πολιτών προστατεύονται από την Ευρωπαϊκή Ένωση. Τα στοιχεία των καταναλωτών που αποθηκεύονται από τους φορείς παροχής υπηρεσιών στα πλαίσια των συναλλαγών του ηλεκτρονικού εμπορίου, είναι προσωπικά δεδομένα και άρα προστατεύονται από την Ευρωπαϊκή Ένωση μέσω της κοινοτικής Οδηγίας 95/46/ΕΚ καθώς και της Οδηγίας 2002/58/ΕΚ, η οποία έχει τεθεί σε εφαρμογή για την αντικατάσταση της προηγούμενης Οδηγίας 97/96/ΕΚ.

Κοινοτική Οδηγία 95/46/ΕΕ

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, έχει διπλό στόχο: την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής του ατόμου και την εξασφάλιση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, για την επίτευξη οικονομικής και κοινωνικής προόδου και συνεργασίας, καθώς και τεχνικής και επιστημονικής συνεργασίας στην ολοένα αναπτυσσόμενη κοινωνία της πληροφορικής και των τηλεπικοινωνιών.

Η Οδηγία 95/46/ΕΚ αποτελεί το κείμενο αναφοράς σε ευρωπαϊκό επίπεδο στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα. Θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση. Η εν λόγω Οδηγία ορίζει ως «δεδομένα προσωπικού χαρακτήρα», κάθε πληροφορία που αναφέρεται σε φυσικό

πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί το πρόσωπο στο οποίο αναφέρονται τα δεδομένα.

Οι διατάξεις της παρούσας οδηγίας εφαρμόζονται στην αυτοματοποιημένη, εν όλων ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. πληροφοριακή βάση δεδομένων πελατών), καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο (παραδοσιακά αρχεία σε χαρτί).

Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει δυνάμει της παρούσας οδηγίας σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον η επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Συνεπώς, η Ελλάδα είναι υπεύθυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται οι οργανισμοί ηλεκτρονικού εμπορίου που είναι εγκατεστημένοι στα γεωγραφικά όρια της Ελλάδας. [28]

Στη συνέχεια ακολουθούν κάποιες γενικές προϋποθέσεις που ορίζει η Οδηγία 95/46/ΕΚ, σχετικά με τη θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα:

Αρχές που Πρέπει να Τηρούνται ως Προς την Ποιότητα των Δεδομένων

Τα κράτη μέλη καθορίζουν τις προϋποθέσεις υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη. Προβλέπεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται σύννομη και θεμιτή επεξεργασία και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Θα πρέπει εξάλλου τα δεδομένα αυτά να είναι ακριβή και αν χρειάζεται να ενημερώνονται.

Βασικές Αρχές της Νόμιμης Επεξεργασίας Δεδομένων

Τα κράτη μέλη προβλέπουν ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται μόνον εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή αν η επεξεργασία είναι απαραίτητη:

[28] *ΜΟΥΛΙΝΟΣ Κ., ΚΑΜΠΟΥΡΑΚΗ Κ., «E-Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή», Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*

- Για την εκτέλεση σύμβασης της οποίας το υπόψη πρόσωπο αποτελεί συμβαλλόμενο μέρος.
- Για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας.
- Για τη διαφύλαξη ζωτικού συμφέροντος του υπόψη προσώπου.
- Για την εκτέλεση αποστολής δημόσιου συμφέροντος.
- Για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.

Ειδικές Κατηγορίες Επεξεργασίας

Τα κράτη μέλη απαγορεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Η διάταξη αυτή συνοδεύεται από επιφυλάξεις που αφορούν π.χ. την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του υπόψη προσώπου ή για σκοπούς προληπτικής ιατρικής και ιατρικής διάγνωσης.

Ενημέρωση του Ενδιαφερόμενου Προσώπου

Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας ή ο εκπρόσωπός του πρέπει να παρέχει στο πρόσωπο από το οποίο συλλέγονται δεδομένα που το αφορούν, πληροφορίες για την ταυτότητα του υπευθύνου της επεξεργασίας, για τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα, καθώς και άλλες πληροφορίες, όπως για παράδειγμα τους αποδέκτες των δεδομένων κλπ.

Εξαιρέσεις και Περιορισμοί

Τα κράτη μέλη μπορούν να περιορίζουν με νομοθετικά μέτρα την εμβέλεια των υποχρεώσεων και δικαιωμάτων που προβλέπονται στην παρούσα οδηγία, όταν ο περιορισμός αυτός απαιτείται για τη διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημόσιας ασφάλειας και της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης παραβάσεων του ποινικού νόμου ή της δεοντολογίας των νομοθετικά κατοχυρωμένων επαγγελμάτων.

Απόρρητο και Ασφάλεια της Επεξεργασίας

Κάθε πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου της επεξεργασίας δεν δύναται να επεξεργαστεί τα προσωπικά δεδομένα παρά κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο υπεύθυνος της επεξεργασίας θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα έναντι τυχαίας ή παράνομης καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια.

Τα κράτη μέλη προβλέπουν ότι κάθε πρόσωπο θα πρέπει να έχει τη δυνατότητα νομικής προσφυγής στην περίπτωση παραβίασης των δικαιωμάτων που εγγυώνται οι εθνικές διατάξεις, οι οποίες ισχύουν για τη σχετική επεξεργασία δεδομένων. Εξάλλου, τα άτομα που έχουν υποστεί βλάβη λόγω μιας παράνομης επεξεργασίας των προσωπικών τους δεδομένων, έχουν το δικαίωμα να επιτύχουν αποκατάσταση της ζημίας που υπέστησαν.

Επιτρέπονται οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι η εν λόγω τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Αντίθετα, οι εν λόγω μεταβιβάσεις δεν μπορούν να πραγματοποιηθούν προς τρίτες χώρες οι οποίες δε διαθέτουν το κατάλληλο επίπεδο προστασίας, εκτός από συγκεκριμένες περιπτώσεις παρέκκλισης οι οποίες απαριθμούνται περιοριστικά.

Κάθε κράτος μέλος προβλέπει τη δημιουργίας μίας ή περισσότερων ανεξάρτητων κρατικών αρχών, οι οποίες επιφορτίζονται με την εποπτεία της εφαρμογής στο εθνικό έδαφος των εθνικών διατάξεων που έχουν θεσπιστεί από τα κράτη μέλη κατ' εφαρμογή της παρούσας οδηγίας.

Κοινοτική Οδηγία 2002/58/ΕΕ

Η Οδηγία 2002/58/ΕΚ αποτελεί βασικό στοιχείο του κανονιστικού πλαισίου που επιδιώκει να εξασφαλίσει τη συνέχιση της ανάπτυξης του τομέα ηλεκτρονικών επικοινωνιών, με οφέλη για το σύνολο των εταιρειών και των ιδιωτών που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικών επικοινωνιών.

Η Οδηγία 2002/58/ΕΚ αναθεωρεί και αναπροσαρμόζει την προηγούμενη Οδηγία 97/96/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, προκειμένου να ληφθούν υπόψη οι νέες υπηρεσίες και τεχνολογικές εξελίξεις.

Η εν λόγω Οδηγία επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η

δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου.

Με την Οδηγία 2002/58/ΕΚ εναρμονίζονται οι διατάξεις των κρατών μελών, οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση.

Ασφάλεια

Ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οφείλει να λαμβάνει από κοινού με τους φορείς παροχής δημόσιων δικτύων επικοινωνιών, καθόσον αφορά την ασφάλεια του δικτύου, τα ενδεδειγμένα τεχνικά και οργανωτικά μέσα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Οι εν λόγω φορείς υποχρεώνονται να ενημερώνουν τους συνδρομητές σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος για την ασφάλεια του δικτύου.

Απόρρητο των Επικοινωνιών

Το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, αποτελεί βασικό δικαίωμα του πολίτη και ως τέτοιο κατοχυρώνεται από την εκάστοτε ισχύουσα εθνική νομοθεσία.

Γενικά, στο πλαίσιο της διασφάλισης του απορρήτου απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερόμενων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια (π.χ. για περιπτώσεις της δημόσιας ασφάλειας).

Η πιο πάνω απαγόρευση δεν επηρεάζει οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής, με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής.

Δεδομένα Κίνησης

Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τους φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να απαλείφονται όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας.

Ο φορέας παροχής υπηρεσιών πρέπει να ενημερώνει το χρήστη σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασίας αυτής, προτού ο χρήστης δώσει τη συγκατάθεση του γι' αυτήν την επεξεργασία.

Δεδομένα Θέσης εκτός των Δεδομένων Κίνησης

Διασφαλίζεται η προστασία της ιδιωτικής ζωής για τους χρήστες, όσον αφορά τις υπηρεσίες πληροφοριών θέσης κινητών συσκευών. Η επεξεργασία των συναφών δεδομένων επιτρέπεται μόνο με τη ρητή συγκατάθεση του χρήστη, ο οποίος πρέπει να ενημερώνεται για το είδος, τους σκοπούς και τη διάρκεια της επεξεργασίας.

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

Στη χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 2774/99 (Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα).

Ο Νόμος 2472/97 ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ και αναφέρεται στην "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Με λίγα λόγια, καθορίζει τις υποχρεώσεις των φορέων και των υπηρεσιών που "εκτελούν την επεξεργασία" και θέτει τα δικαιώματα προστασίας των ατόμων, όσον αφορά την προστασία και διαφύλαξη των προσωπικών τους δεδομένων. [29]

[29] http://el.wikipedia.org

Με βάση το νόμο 2472/97:

- Η επεξεργασία προσωπικών πληροφοριών είναι επιτρεπτή μόνο στις περιπτώσεις που ο νόμος προσδιορίζει περιοριστικά και δεσμευτικά.
- Η επεξεργασία επιτρέπεται μόνο για νόμιμους, θεμιτούς και εξειδικευμένους σκοπούς που είναι γνωστοί στον πολίτη.
- Αναγνωρίζονται και κατοχυρώνονται νέα δικαιώματα των πολιτών για να αμύνονται έναντι των προσβολών της ιδιωτικής ζωής και της προσωπικότητας τους (δικαίωμα προηγούμενης πληροφόρησης, διόρθωσης, αποζημίωσης).

Οι ρυθμίσεις του νόμου 2472/97 συμπληρώθηκαν από το νόμο 2774/99 (Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα). Ο νόμος αυτός κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών.

4.3 ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΡΗΤΟΥ ΕΠΙΚΟΙΝΩΝΙΩΝ

Κανονισμοί Α.Δ.Α.Ε.

Η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) είναι ένας νέος φορέας που λειτουργεί με βάσει το Ν. 3115/2003 με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών. [30]

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

[30] *Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), (2006),« Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις Συναφείς Υπηρεσίες και Εφαρμογές»*

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

Το ηλεκτρονικό εμπόριο βασίζεται στην επικοινωνία των πελατών με τους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου. Για να γίνει μια ηλεκτρονική συναλλαγή, πρέπει πρώτα να επικοινωνήσει ο πελάτης με τον έμπορα, να δώσει τα προσωπικά του στοιχεία, τον αριθμό της πιστωτικής του κάρτας και να λάβει πληροφορίες σχετικές με τη συναλλαγή. Είναι προφανές ότι η επικοινωνία αυτή πρέπει να είναι απόρρητη, αφού σε καμιά περίπτωση τα προσωπικά στοιχεία του πελάτη και ιδιαίτερα οι αριθμοί των πιστωτικών του καρτών δεν πρέπει να γνωστοποιούνται σε τρίτους. Όπως αναφέρθηκε πιο πάνω, σκοπός της ΑΔΑΕ είναι η προστασία του απορρήτου των επικοινωνιών. Συνεπώς κάθε οργανισμός ηλεκτρονικού εμπορίου υπόκειται σε έλεγχο από την ΑΔΑΕ. Η ΑΔΑΕ έχει εκδώσει κάποιους κανονισμούς για τη διασφάλιση του απορρήτου των επικοινωνιών και κάθε οργανισμός ηλεκτρονικού εμπορίου, σύμφωνα με τα παραπάνω, πρέπει να τους ακολουθεί. Η ΑΔΑΕ ελέγχει τους οργανισμούς ηλεκτρονικού εμπορίου για την τήρηση των κανόνων, και η ίδια ελέγχεται από το κράτος.

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

Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις Συναφείς Υπηρεσίες και Εφαρμογές

Σκοπός του συγκεκριμένου Κανονισμού είναι:

- Η διασφάλιση του απορρήτου των διαδικτυακών επικοινωνιών.
- Η ασφάλεια των διαδικτυακών τηλεπικοινωνιακών φορέων και Δημοσίων οργανισμών.
- Η θέσπιση των υποχρεώσεων των εν λόγω φορέων αναφορικά με την ασφάλεια και το απόρρητο των επικοινωνιών.
- Ο έλεγχος στους εν λόγω φορείς σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους. [31]

Στις διατάξεις του Κανονισμού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα οι:

- Παροχή πρόσβασης στο Διαδίκτυο (σταθεροί και κινητοί τηλεπικοινωνιακοί παροχή, Internet Service Providers κλπ.).
- Παροχή διαδικτυακών υπηρεσιών.
- Παροχή διαδικτυακών υπηρεσιών προστιθέμενης αξίας.

[31] *Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), (2006), «Κανονισμός για τη Διασφάλιση του Απορρήτου Διδικτυακών Υποδομών»*

Οι οργανισμοί ηλεκτρονικού εμπορίου είναι παροχή διαδικτυακών υπηρεσιών, αφού οι ηλεκτρονικές συναλλαγές πραγματοποιούνται μέσω του διαδικτύου. Συνεπώς οι οργανισμοί αυτοί πρέπει να εφαρμόζουν τον συγκεκριμένο Κανονισμό. Η ΑΔΑΕ ελέγχει του οργανισμούς αυτούς για την τήρηση του εν λόγω και όχι μόνο, κανονισμού.

Περιεχόμενο Πολιτικής Ασφάλειας

Πρωταρχικό στοιχείο για τη διασφάλιση του απορρήτου των επικοινωνιών στο Διαδίκτυο αποτελεί η ύπαρξη των παρόχων πολιτικής ασφάλειας. Η πολιτική ασφάλειας ορίζεται ως το «σύνολο των τεχνικών, οργανωτικών και κανονιστικών μέτρων», τα οποία εφαρμόζονται από πάροχο διαδικτυακών επικοινωνιών και αποβλέπουν στη διασφάλιση του απορρήτου και γενικά στην ασφαλή λειτουργία των δικτύων διαδικτυακών επικοινωνιών».

Η πολιτική ασφάλειας παρόχου πρέπει να καθορίζει την πολιτική πρόσβασης σε συστήματα και πληροφορίες, την πολιτική αποδεκτής χρήσης, τις ενέργειες που ακολουθούνται για τη διατήρηση της ασφάλειας και τα μέτρα που εφαρμόζονται σε περιπτώσεις παραβίασης της ασφάλειας. Η πολιτική ασφάλειας διασφαλίζει το απόρρητο των επικοινωνιών, την προστασία των υπολογιστικών συστημάτων και των δικτυακών υποδομών και την προστασία των διαδικτυακών υπηρεσιών.

Για να ικανοποιήσει τις απαιτήσεις της πολιτικής ασφάλειας, ο πάροχος θα πρέπει αρχικά να εξακριβώσει τα στοιχεία που πρέπει να προστατευτούν και να προσδιορίσει τους κινδύνους και τις απειλές γι' αυτά. Στη συνέχεια θα πρέπει να προσδιορίσει την πιθανότητα να πραγματοποιηθούν οι απειλές και τέλος να υλοποιήσει μέτρα προστασίας των στοιχείων αυτών με κριτήριο το κόστος υλοποίησης και εφαρμογής. Μια πολιτική ασφάλειας θα πρέπει τουλάχιστον:

- Να είναι πλήρης και αποτελεσματική.
- Να μπορεί να υλοποιηθεί μέσω διαδικασιών, οι οποίες τουλάχιστον περιλαμβάνουν τη διαπίστωση ταυτότητας, την εξουσιοδότηση, τον έλεγχο πρόσβασης, την εμπιστευτικότητα, την ακεραιότητα, την τήρηση του απορρήτου και τον έλεγχο παραβίασης της ασφάλειας.
- Να ορίζει ξεκάθαρα τις περιοχές ευθύνης των χρηστών, των χρηστών παρόχου και της διοίκησης του παρόχου. Λέγοντας χρήστης παρόχου

εννοείται «κάθε φυσικό πρόσωπο που εργάζεται στην επιχείρηση ή το νομικό πρόσωπο που παρέχει στο προσωπικό του την απαραίτητη δικτυακή υποδομή για χρήση διαδικτυακών επικοινωνιών στα πλαίσια της εργασίας του».

- Να είναι ανεξάρτητη, από τεχνικής απόψεως, από το συγκεκριμένο χρησιμοποιούμενο υλικό και λογισμικό.

Η πολιτική ασφάλειας υπόκειται σε έλεγχο από την ΑΔΑΕ, τόσο ως προς την πληρότητα και αποτελεσματικότητα της, όσο και ως προς τον βαθμό εφαρμογής της.

Περιεχόμενο Πολιτικής Πρόσβασης

Η πολιτική πρόσβασης, η οποία αποτελεί αναπόσπαστο τμήμα της πολιτικής ασφάλειας, καθορίζει το επίπεδο πρόσβασης χρηστών και χρηστών παρόχου σε καθένα από τα συστήματα υλικού και λογισμικού από τα οποία αποτελείται ο εξοπλισμός του παρόχου. Η πολιτική πρόσβασης περιγράφει για κάθε σύστημα διαδικασίες προσθήκης και ταυτοποίησης χρηστών και χρηστών παρόχου στο σύστημα, διαδικασίες εξουσιοδότησης για προσθήκη, τροποποίηση και διαγραφή σε αρχεία του συστήματος και διαδικασίες πρόσβασης χρηστών και χρηστών παρόχου σε συστήματα που διατηρούν τα δεδομένα επικοινωνίας των χρηστών.

Ο πάροχος οφείλει να ορίζει έναν Υπεύθυνο Πρόσβασης, ο οποίος καθορίζει το είδος της πρόσβασης των χρηστών και των χρηστών παρόχου στο σύστημα και έναν Υπεύθυνο Συστήματος, ο οποίος υλοποιεί τις αποφάσεις του Υπευθύνου Πρόσβασης.

Απόρρητο-Προστασία Επεξεργασίας Δεδομένων Επικοινωνίας

Το απόρρητο των επικοινωνιών οι οποίες διενεργούνται μέσω δημόσιων δικτύων επικοινωνιών κατοχυρώνεται μέσω της εθνικής και ευρωπαϊκής νομοθεσίας. Συγκεκριμένα, απαγορεύεται η ακρόαση, η υποκλοπή, η αποθήκευση ή άλλο είδος παρακολούθησης των επικοινωνιών και των πληροφοριών και δεδομένων από πρόσωπα, πλην των χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια. Παράλληλα επιτρέπεται από το νόμο η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης όταν πραγματοποιούνται

κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής. Για παράδειγμα, ένας οργανισμός ηλεκτρονικού εμπορίου καταγράφει τις επικοινωνίες με τους πελάτες του, ώστε να έχει αποδεικτικά στοιχεία για τις συναλλαγές που πραγματοποιούνται.

Οι πάροχοι θα πρέπει να ενημερώνουν τους χρήστες σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για τη διασφάλιση του απορρήτου των επικοινωνιών, για παράδειγμα τη χρήση συγκεκριμένου τύπου λογισμικού ή τεχνολογιών κρυπτογράφησης.

Ο πάροχος οφείλει να ενημερώνει τους χρήστες για το σκοπό συλλογής των πληροφοριών που τους αφορούν, καθώς και για τους πιθανούς τρόπους επεξεργασίας ή χρήσης τους. Επιπλέον, οφείλει να τους ενημερώνει για τα δεδομένα επικοινωνίας τα οποία πιθανόν αποθηκεύονται σε αντίγραφα ασφάλειας και τα οποία είναι ανακτήσιμα ακόμη και μετά τη διαγραφή τους από το χρήστη.

Οι πάροχοι οφείλουν να λαμβάνουν υπόψη και να εφαρμόζουν στο τμήμα της πολιτικής τους τις διατάξεις της κείμενης νομοθεσίας για την προστασία της επεξεργασίας των δεδομένων επικοινωνίας.

Διαδικασία Ελέγχου από την ΑΔΑΕ

Η ΑΔΑΕ σε τακτά χρονικά διαστήματα διενεργεί έλεγχο σε κάθε πάροχο που εμπίπτει στις διατάξεις του Κανονισμού αυτού. Η διαδικασία ελέγχου διενεργείται από τις αρμόδιες υπηρεσίες της ΑΔΑΕ ή από ειδικούς που τελούν υπό την άμεση επίβλεψη της ΑΔΑΕ. [32]

Κατά την διάρκεια του ελέγχου, η ομάδα ελέγχου της ΑΔΑΕ καταγράφει τις ενέργειες τις οποίες προβαίνει σε ειδικό έντυπο και κοινοποιεί το πόρισμα της στην ολομέλεια της ΑΔΑΕ. Η ολομέλεια της ΑΔΑΕ αξιολογεί τα ευρήματα του ελέγχου και σε περίπτωση μη λήψης των κατάλληλων μέτρων, επιβάλλονται κυρώσεις.

[32] *Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), (2006), «Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου»*

Άσκηση Εποπτείας

Κάθε πάροχος στο τέλος του ημερολογιακού έτους υποβάλλει στην ΑΔΑΕ ετήσια έκθεση με στοιχεία που αφορούν την ασφάλεια των διαδικτυακών επικοινωνιών και τη διασφάλιση του απορρήτου. Το περιεχόμενο της ετήσιας έκθεσης πρέπει να περιλαμβάνει τουλάχιστον περιστατικά που απείλησαν την ασφάλεια του παρόχου και τη διασφάλιση του απορρήτου καθώς και τυχόν βλάβες που υπέστη ο πάροχος, οι χρήστες του και οι χρήστες παρόχου εξαιτίας αυτών.

Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών

Σκοπός του συγκεκριμένου Κανονισμού είναι:

- Η ασφάλεια των διαδικτυακών υποδομών των παρόχων και η διασφάλιση του απορρήτου αυτών.
- Η θέσπιση των υποχρεώσεων των εν λόγω παρόχων αναφορικά με την ασφάλεια και το απόρρητο των διαδικτυακών τους υποδομών.
- Ο έλεγχος στους εν λόγω παρόχους σχετικά με τις ανωτέρω αναφερόμενες υποχρεώσεις τους.

Στις διατάξεις του Κανονισμού αυτού εμπίπτουν όλοι οι Τηλεπικοινωνιακοί Πάροχοι Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα:

- Πάροχοι σταθερής και κινητής πρόσβασης στο Διαδίκτυο.
- Πάροχοι διαδικτυακών υπηρεσιών, υπηρεσιών προστιθέμενης αξίας και υπηρεσιών εφαρμογών.

4.4 ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Όπως διαπιστώνουμε, οι πιθανότητες να γίνει κακή χρήση των προσωπικών μας δεδομένων στο διαδίκτυο είναι πάρα πολλές. Ας δούμε κάποιες συμβουλές προστασίας που θα πρέπει να ακολουθούμε για την

καλύτερη δυνατή προστασία των προσωπικών μας στοιχείων σε μια ηλεκτρονική συναλλαγή. [33]

- **Περιορισμός της αποκάλυψης των προσωπικών στοιχείων**
  Η αποκάλυψη των προσωπικών πληροφοριών πρέπει να περιοριστεί όσο το δυνατόν περισσότερο και να γίνεται η παροχή μόνο των απαραίτητων πληροφοριών. Αποφυγή της αποκάλυψης βιογραφικών στοιχείων και στις περιπτώσεις που πρόκειται να χρησιμοποιηθούν ψευδώνυμα. Πολλές ιστοσελίδες ζητούν παραπάνω στοιχεία από τα απαραίτητα, πράγμα το οποίο πρέπει να αποφεύγεται. Μεγάλη προσοχή πρέπει να δίνεται σε κάποιες εφαρμογές του λογισμικού μας, οι οποίες διακινούν αυτομάτως προσωπικά δεδομένα. Αυξημένης επικινδυνότητας για τα προσωπικά μας δεδομένα, είναι διαδικτυακές ιστοσελίδες όπως «δωμάτια» διαλόγου ή ομάδες αλληλογραφίας (chat). Σε αυτούς τους χώρους πολλά από τα προσωπικά μας στοιχεία συχνά αποθηκεύονται και δημοσιοποιούνται χωρίς τη συγκατάθεση μας.

- **Δημιουργία ξεχωριστού λογαριασμού ηλεκτρονικής αλληλογραφίας**
  Μια πολύ σημαντική κίνηση για την προστασία των προσωπικών μας δεδομένων είναι η δημιουργία ξεχωριστών λογαριασμών ηλεκτρονικής αλληλογραφίας, που θα χρησιμοποιούνται μόνο για ηλεκτρονικές συναλλαγές, δωμάτιο διαλόγου κ.τ.λ. Η δημιουργία λογαριασμών ηλεκτρονικής αλληλογραφίας είναι μια απλή και χωρίς κόστος διαδικασία, γεγονός που μας παρέχει τη δυνατότητα να είμαστε κάτοχοι περισσότερων από ένα λογαριασμών (προσωπικοί, επαγγελματικοί). Έτσι, σε περιπτώσεις που αντιληφτούμε ανεπιθύμητη αλληλογραφία, αμέσως θα πρέπει να ξεκινήσουμε την απλή διαδικασία της απενεργοποίησης του λογαριασμού.

[33] *http://europa.eu/legislation_summaries/information_society/l14012_el.htm*

- **Απόρριψη των cookies**
  Ρύθμιση των κατάλληλων επιλογών στο λογισμικό μας, ώστε κατά την περιήγηση μας στο διαδίκτυο να διαγραφούν τα cookies.

- **Χρήση εργαλείων για την προστασία των προσωπικών δεδομένων**
  Η χρήση κατάλληλου λογισμικού για την προστασία των προσωπικών δεδομένων έχει αποδειχθεί ένα αποτελεσματικό μέσο. Μπορούμε να προστατεύσουμε τα προσωπικά μας δεδομένα, χρησιμοποιώντας υπηρεσίες που επιτρέπουν την ανώνυμη πλοήγηση στο διαδίκτυο και εμποδίζουν τις ιστοσελίδες να συλλέξουν πληροφορίες για εμάς, όπως κωδικοποίηση για ασφαλείς επικοινωνίες, προστατευτικοί τοίχοι (firewalls), που αποτρέπουν στον υπολογιστή μας να αποκαλύπτει πληροφορίες μας σε άλλους και ειδικές ρυθμίσεις, που επιτρέπουν την μόνιμη διαγραφή από τον υπολογιστή μας αρχείων, που περιλαμβάνουν προσωπικές μας πληροφορίες.

- **Γνώση των νόμιμων προστασιών μας**
  Κάθε χρήστης του διαδικτύου που πραγματοποιεί ηλεκτρονικές συναλλαγές, θα πρέπει να είναι ενήμερος για τις νομοθεσίες που τον προστατεύουν. Ακόμα, θα πρέπει να γνωρίζει τις ενέργειες που πρέπει να κάνει σε περίπτωση που παραβιαστεί η ιδιωτική του ζωή στο διαδίκτυο.

4.5 ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΑΚΟΛΟΥΘΕΙ Ο ΙΣΤΟΧΩΡΟΣ UNITEDSTUDENTS

Συλλογή και χρήση προσωπικών δεδομένων

Για τη χρήση των υπηρεσιών του unitedstudents.gr θα πρέπει ο χρήστης να συμπληρώσει μία φόρμα εγγραφής στην οποία του ζητούνται και προσωπικά στοιχεία. Τα στοιχεία που συλλέγει το unitedstudents.gr κατά την εγγραφή του χρήστη είναι τα εξής: όνομα χρήστη, διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail), κωδικό (Password), πόλη, διεύθυνση, ενδιαφέροντα (hobby), σχολή στην οποία σπουδάζει και τηλέφωνο. Το όνομα χρήστη (username), είναι ένα εικονικό όνομα (ψευδώνυμο) που επιλέγει ο επισκέπτης/χρήστης και αποτελεί την

ονομασία του κατά την επίσκεψη των σελίδων και των υπηρεσιών του unitedstudents.gr. [34]

Οι λόγοι συλλογής των στοιχείων αυτών είναι κυρίως στατιστικοί λόγοι καθώς και η ενημέρωση των μελών για νέες υπηρεσίες, προσφορές, τεχνική υποστήριξη τους στις διάφορες υπηρεσίες του unitedstudents.gr, δικαίωμα συμμετοχής σε διαγωνισμούς ή άλλα ερωτηματολόγια. Επίσης, κάθε μέλος του unitedstudents.gr λαμβάνει ενημερωτικό δελτίο με τα τελευταία νέα του unitedstudents.gr. Ιδίως οι πληροφορίες για τα ενδιαφέροντα (hobby) του χρήστη, τη σχολή στην οποία σπουδάζει, τη διεύθυνσή του και το τηλέφωνό του ζητούνται προαιρετικά για την περίπτωση που επιθυμεί να λαμβάνει εξειδικευμένη ενημέρωση των υπηρεσιών και των προσφορών του unitedstudents.gr καθώς και για την πληρέστερη εξυπηρέτησή του.

Διοχέτευση-αποκάλυψη προσωπικών δεδομένων σε τρίτους

Το unitedstudents.gr δεσμεύεται ρητά να μη διοχετεύσει, διαθέσει, πουλήσει, νοικιάσει με κανένα τρόπο τα προσωπικά στοιχεία των μελών του σε τρίτους. Παροχή προσωπικών δεδομένων μπορεί να γίνει μόνο όταν: 1) δοθεί η συγκατάθεση του επισκέπτη/χρήστη γι' αυτό 2) επιβάλλεται από το νόμο με σκοπό τη συμμόρφωση με τις διατάξεις του, 3) μετά από αίτηση του επισκέπτη/χρήστη χρειαστεί τα στοιχεία του να διοχετευτούν σε συνεργάτες του unitedstudents.gr με σκοπό την ικανοποίηση επιθυμιών των μελών και 4) όταν ανακαλύψουμε ότι η συμπεριφορά του επισκέπτη/χρήστη στο website δεν συμφωνεί με τους «όρους χρήσης» του unitedstudents.gr ή με οποιαδήποτε από τις οδηγίες μας για συγκεκριμένα προϊόντα ή υπηρεσίες.

Το unitedstudents.gr απαγορεύει στους επισκέπτες/χρήστες του να δημοσιεύουν/ αποκαλύπτουν προσωπικά δεδομένα τους και συνιστά σε αυτούς να περιορίζονται στην καταγραφή και ανταλλαγή μόνο τόσων στοιχείων όσων είναι απολύτως απαραίτητα για την μεταξύ τους επικοινωνία. Σε καμία περίπτωση δεν ευθύνεται το unitedstudents.gr και ο επισκέπτης/χρήστης δεν προστατεύεται από τις διατάξεις περί προστασίας προσωπικών δεδομένων, αν ο τελευταίος αποκαλύψει/δημοσιεύσει στοιχεία των προσωπικών δεδομένων του μέσω των υπηρεσιών του unitedstudents.gr, όπως ιδίως μέσω των: Chat,

[34] *www.unitedstudents.gr*

SHOUTBOX, Υπηρεσίας Μηνυμάτων, Υπηρεσίας Gallery, Υπηρεσίας Αγγελιών, E-Writing και FORUM.

Cookies

Το unitedstudents.gr μπορεί να χρησιμοποιεί cookies για την αναγνώριση του επισκέπτη/χρήστη ορισμένων υπηρεσιών και σελίδων του. Τα δίσκο κάθε επισκέπτη-χρήστη και δεν λαμβάνουν γνώση οποιουδήποτε εγγράφου ή αρχείου από τον υπολογιστή του. Χρησιμοποιούνται μόνο για τη διευκόλυνση πρόσβασης του επισκέπτη-χρήστη σε συγκεκριμένες υπηρεσίες του unitedstudents.gr και για στατιστικούς λόγους προκειμένου να καθορίζονται οι περιοχές στις οποίες οι υπηρεσίες του unitedstudents.gr είναι χρήσιμες ή δημοφιλείς ή για λόγους marketing. Ο επισκέπτης-χρήστης του unitedstudents.gr μπορεί να ρυθμίσει τον διακομιστή (browser) του κατά τέτοιο τρόπο ώστε είτε να τον προειδοποιεί για τη χρήση των cookies σε συγκεκριμένες υπηρεσίες του unitedstudents.gr, είτε να μην επιτρέπει την αποδοχή της χρήσης cookies σε καμία περίπτωση. Σε περίπτωση που ο επισκέπτης-χρήστης των συγκεκριμένων υπηρεσιών και σελίδων του unitedstudents.gr δεν επιθυμεί τη χρήση cookies για την αναγνώριση του δεν μπορεί να έχει περαιτέρω πρόσβαση στις υπηρεσίες αυτές.

Internet Protocol (IP) Addresses

Η διεύθυνση IP καθορίζεται από τον παροχέα (Internet Provider) της σύνδεσης μέσω της οποίας ο Η/Υ του επισκέπτη/χρήστη έχει πρόσβαση στο Διαδίκτυο και στη συνέχεια στο unitedstudents.gr κρατείται για τεχνικούς λόγους και αξιοποιείται αποκλειστικά και μόνο για την συγκέντρωση στατιστικών στοιχείων. Οι πληροφορίες αυτές είναι ανώνυμες και περιέχουν τα domain names και/ή τις I.P δύναται όμως να παραδοθούν στις αρμόδιες αστυνομικές ή δικαστικές αρχές, εφόσον ζητηθεί, στην περίπτωση που ο χρήστης προβαίνει σε πράξεις ή δημοσιεύσεις περιεχομένου που παραβιάζουν τους νόμους του κράτους.

Ενημερωτικά δελτία

Το unitedstudents.gr διατηρεί μία λίστα e-mail για όλα τα εγγεγραμμένα μέλη του με σκοπό την αποστολή ενημερωτικών δελτίων (newsletter) μέσω ηλεκτρονικού ταχυδρομείου (e-mail), σχετικά με υπηρεσίες, προϊόντα ή άλλες δραστηριότητές. Το unitedstudents.gr έχει το δικαίωμα τήρησης αυτής της λίστας για την αποστολή και άλλων μηνυμάτων ενημερωτικού ή οικονομικού χαρακτήρα

πέρα από τα newsletters εκτός αν ο παραλήπτης δηλώσει ρητά ότι δεν επιθυμεί κάτι τέτοιο οπότε και μπορεί να διαγραφεί από αυτήν.

Σύνδεσμοι (links)

Το unitedstudents.gr περιλαμβάνει συνδέσμους (links) προς άλλες ιστοσελίδες (websites) τα οποία δεν ελέγχονται από το ίδιο αλλά από τους τρίτους φορείς (φυσικά ή νομικά πρόσωπα). Σε καμία περίπτωση δεν ευθύνεται το unitedstudents.gr για τους Όρους Προστασίας των Προσωπικών Δεδομένων των επισκεπτών-χρηστών τους οποίους οι φορείς αυτοί ακολουθούν.

Προστασία ανηλίκων

Επισκέπτες/χρήστες του unitedstudents.gr που είναι ανήλικοι δεν επιτρέπεται να έχουν πρόσβαση στις υπηρεσίες του unitedstudents.gr που μπορεί να θεωρούνται ακατάλληλες για ανηλίκους και οι οποίες δεν είναι δυνατό να ελεγχθούν από το unitedstudents.gr. Εάν παρόλα αυτά ανήλικοι χρήστες αυτοβούλως επισκεφτούν σελίδες με υλικό ακατάλληλο/προσβλητικό/ανήθικο και το οποίο δεν είναι δυνατό να ελέγχεται συνεχώς, το unitedstudents.gr δε φέρει καμία ευθύνη.

Προσωπική σελίδα μέλους

Το unitedstudents.gr δεν έχει καμία απολύτως ευθύνη για το περιεχόμενο το οποίο αναρτούν ή/και δημοσιεύουν οι επισκέπτες/χρήστες στην προσωπική τους σελίδα. Ο προαπαιτούμενος έλεγχος του unitedstudents.gr έχει μόνο σκοπό να εξακριβώσει αν όλα τα απαιτούμενα στοιχεία έχουν συμπληρωθεί και όχι αν αυτά είναι αληθινά πράγμα δύσκολο και αδύνατο. Οι άλλοι επισκέπτες/χρήστες επισκέπτονται με δική τους ευθύνη τις προσωπικές αυτές σελίδες. Σε περίπτωση που εξακριβωθεί από το unitedstudents.gr οποιοδήποτε ψεύδος ή ανακρίβεια, ή λάβει ειδοποίηση ότι το περιεχόμενο σε κάποια/ες προσωπική/ες σελίδα/ες που φιλοξενεί θίγει τρίτα πρόσωπα ή/και παραβιάζει τα προσωπικά δεδομένα τρίτων προσώπων διατηρεί το δικαίωμα να προβεί άμεσα και χωρίς προειδοποίηση σε διαγραφή των σχετικών σελίδων ή/και του επισκέπτη/χρήστη που προέβη στη σχετική ανάρτηση ή/και δημοσίευση. Σε κάθε όμως περίπτωση το unitedstudents.gr δύναται να μη δημοσιεύσει μία προσωπική σελίδα εάν υπάρχει η οποιαδήποτε αμφιβολία για την ορθότητα του περιεχομένου της. Η παρούσα ρήτρα ισχύει για υλικό κάθε μορφής (κείμενα, φωτογραφίες, εικόνες, ηχητικά αρχεία, αρχεία video κλπ) που μπορούν οι επισκέπτες/χρήστες να αναρτούν/δημοσιεύουν στις προσωπικές τους σελίδες. Σε καμία περίπτωση δεν ευθύνεται το unitedstudents.gr και ο επισκέπτης/χρήστης δεν προστατεύεται από

τις διατάξεις περί προστασίας προσωπικών δεδομένων, αν ο τελευταίος αποκαλύψει/δημοσιεύσει στοιχεία των προσωπικών δεδομένων του μέσω της υπηρεσίας αυτής.

Gallery

Το unitedstudents.gr παρέχει στους επισκέπτες/χρήστες του την απαραίτητη τεχνολογική υποδομή και τα μέσα για ανάρτηση/δημοσίευση εικόνων και φωτογραφιών, ωστόσο το περιεχόμενο αυτό, είτε αναρτάται δημόσια είτε μεταφέρεται ιδιωτικά, παραμένει στην αποκλειστική ευθύνη του φυσικού ή νομικού προσώπου από το οποίο το περιεχόμενο πηγάζει. Το unitedstudents.gr δεν έχει καμία απολύτως ευθύνη για το περιεχόμενο το οποίο αναρτούν ή/και δημοσιεύουν οι επισκέπτες/χρήστες στην υπηρεσία Gallery. Ο επισκέπτης/χρήστης είναι αποκλειστικά υπεύθυνος για όλες και οποιεσδήποτε φωτογραφίες και εικόνες αναρτά, δημοσιεύει, αποστέλλει, μεταφέρει ή άλλως καθιστά διαθέσιμες μέσω της υπηρεσίας Gallery του unitedstudents.gr. Σε κάθε περίπτωση ο επισκέπτης/χρήστης οφείλει να σέβεται τους δεοντολογικούς κανόνες και του νόμους. Σε καμία περίπτωση δεν ευθύνεται το unitedstudents.gr και ο επισκέπτης/χρήστης δεν προστατεύεται από τις διατάξεις περί προστασίας προσωπικών δεδομένων, αν ο τελευταίος αποκαλύψει/δημοσιεύσει στοιχεία των προσωπικών δεδομένων του μέσω της υπηρεσίας αυτής.

Αγγελίες

Το unitedstudents.gr διαθέτει υπηρεσία παροχής υπηρεσιών αγγελιών μέσω του Διαδικτύου σύμφωνα με τους ειδικότερους όρους που αυτό τάσσει. Η ισχύς της αγγελίας είναι αδύνατο να διαπιστωθεί από το unitedstudents.gr, η εξακρίβωση των όσων λέγονται στην αγγελία θα πρέπει να γίνεται από τον επισκέπτη/χρήστη που ενδιαφέρεται γι' αυτήν. Το unitedstudents.gr σε καμία περίπτωση δε φέρει ευθύνη για οποιαδήποτε συναλλαγή προκύψει από μία αγγελία και δεν διευκολύνει την επαφή των ενδιαφερομένων παρά μόνο μέσω της φόρμας επικοινωνίας που συνοδεύει κάθε αγγελία. Εάν το unitedstudents.gr λάβει ειδοποίηση ότι οποιαδήποτε πληροφορία που αναρτάται/δημοσιεύεται στις σελίδες/υπηρεσίες αυτές, παραβιάζει τα προσωπικά δεδομένα τρίτων προσώπων, διατηρεί το δικαίωμα να προβεί στην άμεση διαγραφή της και του μέλους. Σε καμία περίπτωση δεν ευθύνεται το unitedstudents.gr και ο επισκέπτης/χρήστης δεν προστατεύεται από τις διατάξεις περί προστασίας προσωπικών δεδομένων, για όσα στοιχεία προσωπικών δεδομένων του

δημοσιεύσει/αποκαλύψει ο τελευταίος στο περιεχόμενο της αγγελίας του που θα αναρτήσει σε αυτήν την υπηρεσία.

Εφαρμοστέο Δίκαιο

Η διαχείριση και προστασία των προσωπικών δεδομένων του επισκέπτη/χρήστη των υπηρεσιών του unitedstudents.gr υπόκειται στους όρους του παρόντος τμήματος καθώς και στις σχετικές διατάξεις της ελληνικής νομοθεσίας και ελέγχεται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Οι παρόντες όροι διατυπώνονται λαμβανομένων υπόψη τόσο της ραγδαίας ανάπτυξης της τεχνολογίας και ειδικότερα του Διαδικτύου όσο και του υπάρχοντος - αν και μη πλήρως ανεπτυγμένου - πλέγματος νομικών ρυθμίσεων σχετικά με τα ζητήματα αυτά. Σε αυτό το πλαίσιο, οποιαδήποτε ενδεχόμενη σχετική ρύθμιση θα αποτελέσει αντικείμενο του παρόντος τμήματος. Σε κάθε περίπτωση το unitedstudents.gr διατηρεί το δικαίωμα αλλαγής των όρων προστασίας των προσωπικών δεδομένων κατόπιν ενημέρωσης των επισκεπτών/χρηστών και μέσα στο υπάρχον ή και ενδεχόμενο νομικό πλαίσιο.

Εάν κάποιος επισκέπτης/χρήστης δε συμφωνεί με τους όρους προστασίας των προσωπικών δεδομένων που προβλέπονται στο παρόν οφείλει να μη χρησιμοποιεί τις υπηρεσίες του unitedstudents.gr. Αρμόδια δικαστήρια για επίλυση τυχόν διαφορών είναι τα Δικαστήρια Θεσσαλονίκης.

5. ΠΡΟΣΤΑΣΙΑ ΑΝΗΛΙΚΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η εξέλιξη της τεχνολογίας των υπολογιστών και του διαδικτύου τα τελευταία χρόνια έχει πάρει ανεξέλεγκτη τροπή, σε βαθμό που έχει εισχωρήσει σε κάθε πτυχή της καθημερινής ζωής του ανθρώπου και αποτελεί κύριο γνώρισμα της σύγχρονης ψηφιακής κοινωνίας στην οποία ζούμε. Αυτό το νέο μέσο που έχουμε στα χέρια μας, δίνει στο σύγχρονο άνθρωπο τεράστιες δυνατότητες και διευκολύνσεις στην καθημερινότητα του, όμως έβαλε και πολλούς κινδύνους στη ζωή του χρήστη. [35]

Πλέον το διαδίκτυο έχει εισχωρήσει σε κάθε σπίτι κι έτσι κάθε παιδί έχει άμεση πρόσβαση στον κυβερνοχώρο. Η χρήση του διαδικτύου από τους ανηλίκους, αποτελεί σήμερα ένα τεράστιο θέμα προς συζήτηση των διαφόρων κοινωνικών φορέων της κοινωνίας μας. Το κύριο χαρακτηριστικό του διαδικτύου, ότι δεν υπόκεινται σε έλεγχο οι πληροφορίες που διανέμονται μέσω αυτού, πολλές φορές έχει αρνητικό αντίκτυπο για τους ανηλίκους, οι οποίοι οποιαδήποτε στιγμή λόγω της ευελιξίας του διαδικτύου μπορούν να βρεθούν μπροστά σε διαδικτυακό περιεχόμενο που μπορεί να τους βλάψει.

Αυτό που πρέπει να γίνει πρώτα απ' όλα, είναι να κατανοήσουμε σε βάθος τη χρησιμότητα του διαδικτύου και να μάθουμε να ξεχωρίζουμε τους κινδύνους που κρύβονται μέσα σε αυτό. Έτσι, αυτή η γνώμη και εμπειρία θα μπορέσει να μεταλαμπαδευτεί και στις επόμενες γενιές με επακόλουθο η χρήση του διαδικτύου να γίνεται ασφαλέστερη, απολαμβάνοντας μόνο τα θετικά οφέλη, τα οποία μας προσφέρει. Με αυτόν τον τρόπο, κάθε χρήστης του διαδικτύου ακόμα και ανήλικος θα έχει αποκτήσει την κρητική σκέψη, η οποία θα τον διευκολύνει να ξεχωρίζει την ασφαλή από την επικίνδυνη χρήση.

Η συμβολή των γονέων για την προστασία των παιδιών τους από την κακή επίδραση του διαδικτύου είναι καθοριστική. Κάθε γονέας είναι υπεύθυνος για την προστασία των παιδιών τους από κάθε είδους απειλή, έτσι λοιπόν θα πρέπει να ενεργήσει με απόλυτη προσοχή και αποτελεσματικότητα στην αποτροπή της επαφής των παιδιών με παράνομο και βλαβερό περιεχόμενο στο διαδίκτυο. [36]

[35] www.safechild.gr

[36] www.synigoroskatanaloti.gr

Ο ανήλικος χρήστης του διαδικτύου μπορεί να βρεθεί μπροστά σε κινδύνους που μπορεί να τον βλάψουν ανά πάσα στιγμή, γι' αυτό και οι γονείς θα πρέπει να επικεντρώνουν την προσοχή τους στην περιήγηση των παιδιών τους στο διαδίκτυο συνεχώς με την εφαρμογή δραστικών μέτρων προστασίας.

Έτσι, λοιπόν κάθε γονέας οφείλει να είναι ενήμερος για τη χρήση του διαδικτύου, καθώς και για τα σημαντικά οφέλη που προσφέρει αυτό στη σύγχρονη ψηφιακή κοινωνία. Ακόμα, όμως θα πρέπει να γνωρίζει και τους κινδύνους που ελλοχεύουν κατά τη χρήση του διαδικτύου, έτσι ώστε να εξασφαλίσει στα παιδιά του μια ασφαλή περιήγηση στο διαδίκτυο. Πολύ σημαντικό επίσης, είναι να ενημερωθούν τα παιδιά εξίσου για τους κινδύνους της χρήσης του διαδικτύου, κατόπιν συζήτησης με τους γονείς, οι οποίοι θα πρέπει να δείξουν το δρόμο για την ασφαλέστερη χρήση.

Έχει αποδειχθεί ότι η τοποθέτηση του υπολογιστή σε κοινό μέρος του σπιτιού και όχι στο παιδικό δωμάτιο, βοηθάει το γονικό έλεγχο. Πρέπει ακόμα οι γονείς να μάθουν στα παιδιά τους να μη δίνουν ποτέ προσωπικά τους στοιχεία στο διαδίκτυο και για κανένα λόγο χωρίς την έγκριση του γονέα τους. Σκόπιμο είναι οι γονείς να ελέγχουν συνεχώς τις ιστοσελίδες που επισκέπτονται τα παιδιά τους μέσω των κατάλληλων εφαρμογών που προσφέρει το λογισμικό του υπολογιστή.

Η χρήση ειδικού λογισμικού που λειτουργεί ως φίλτρο και αποτρέπει τη σύνδεση των παιδιών με ιστοσελίδες βλαβερού περιεχομένου, αποτελεί ένα δραστικό μέτρο για την προστασία του ανηλίκου χρήστη. Με αυτό το λογισμικό μπορεί ο γονέας να αποτρέψει την πρόσβαση του παιδιού σε ιστοσελίδες επικίνδυνου περιεχομένου.

Το ζήτημα της ασφαλούς πρόσβασης των ανηλίκων στο Διαδίκτυο είναι ιδιαίτερα σημαντικό, αφού έχει κοινωνικές, πολιτισμικές, παιδαγωγικές, επιστημονικές και άλλες πτυχές. Το Υπουργείο Εθνικής Παιδείας και Θρησκευμάτων (Υπ.Ε.Π.Θ. - www.ypepth.gr) αναγνωρίζει την κρισιμότητα του ζητήματος και εφαρμόζει μέσω του **Πανελλήνιου Σχολικού Δικτύου** (www.sch.gr) μία συγκεκριμένη πολιτική προστασίας των μαθητών από την έκθεσή τους σε ακατάλληλο περιεχόμενο του Διαδικτύου μέσα από το σχολείο. Η πολιτική είναι εναρμονισμένη με τη διεθνή πρακτική και τις νομικές απαιτήσεις και διαρθρώνεται σε πέντε άξονες: [37]

1. Στον ορισμό των **Πολιτικών Αποδεκτής Χρήσης** του Διαδικτύου και των Σχολικών Εργαστηρίων Πληροφορικής από τα σχολεία και τους

[37] www.ypepth.gr

μαθητές. Για το σκοπό αυτό το Υπ.Ε.Π.Θ. έχει θεσμοθετήσει τα αρμόδια συλλογικά όργανα, αποτελούμενα από ειδικούς επιστήμονες, τα οποία έχουν την ευθύνη της χάραξης πολιτικής και διαχείρισης του περιεχομένου που διακινείται μέσω του Πανελλήνιου Σχολικού Δικτύου και των υπηρεσιών του, όπως η υπηρεσία ελέγχου περιεχομένου (web filtering), οι χώροι συζητήσεων (forum), οι λίστες ηλεκτρονικής επικοινωνίας (mailing lists), η δημοσίευση ιστοσελίδων (web hosting), κλπ.

2. Στην **ανάπτυξη και εφαρμογή τεχνικών (φίλτρα)** που υλοποιούν τις πολιτικές αυτές. Αντίστοιχες τεχνικές εφαρμόζονται διεθνώς στα εκπαιδευτικά δίκτυα πολλών προηγμένων χωρών και αποτρέπουν με σημαντικό δείκτη επιτυχίας την πρόσβαση σε ιστοσελίδες που ανήκουν σε κατηγορίες όπως:

    - «porn» (ιστοσελίδες με πορνογραφικό περιεχόμενο)
    - «gambling» (ιστοσελίδες με τυχερά παιχνίδια)
    - «drugs» (ιστοσελίδες που προωθούν τα ναρκωτικά)
    - «aggressive» (ιστοσελίδες που προπαγανδίζουν την επιθετική συμπεριφορά και το ρατσισμό) και
    - «violence» (ιστοσελίδες που προωθούν την βία)

Επειδή η ταξινόμηση των ιστοσελίδων στις παραπάνω κατηγορίες γίνεται με τη χρήση αυτοματοποιημένης διαδικασίας (λόγω του τεράστιου πλήθους των ιστοσελίδων στο Διαδίκτυο), είναι πιθανό κάποια ιστοσελίδα να ταξινομηθεί λανθασμένα. Για το λόγο αυτό το Πανελλήνιο Σχολικό Δίκτυο ακολουθεί τη διεθνή πρακτική και παρέχει τη δυνατότητα στους χρήστες του να ενημερώνουν τους αρμόδιους τεχνικούς όταν διαπιστώσουν οποιαδήποτε δυσλειτουργία της υπηρεσίας, οι οποίοι πλέον χειρωνακτικά διορθώνουν τη βάση δεδομένων.

3. Στη διαρκή **ενημέρωση και ευαισθητοποίηση** της σχολικής κοινότητας, καθώς οποιαδήποτε τεχνική λύση είναι αδύνατο να αποδώσει αν δεν είναι σωστά ενημερωμένη και ευαισθητοποιημένη η σχολική κοινότητα. Για το σκοπό αυτό το Πανελλήνιο Σχολικό Δίκτυο ενημερώνει τους εκπαιδευτικούς, τους γονείς και τους μαθητές μέσω του δικτυακού του τόπου (**www.sch.gr/safe**), μέσω του ηλεκτρονικού περιοδικού (**www.sch.gr/magazine**) και μέσω της συμμετοχής του σε διάφορες εκδηλώσεις (ημερίδες, συνέδρια, κλπ, www.sch.gr/docs).

4. Στη **συνεργασία με ειδικές δράσεις για την ασφάλεια στο Διαδίκτυο** όπως το Ελληνικό όργανο για την αυτορρύθμιση στο Διαδίκτυο (Safeline, www.safeline.gr) και την κοινοτική δράση για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου (Safer-Internet, www.saferinternet.gr).

5. Στη δημιουργία **θετικής αντιπρότασης**, δηλαδή στην ανάπτυξη αξιόλογου ή/και πιστοποιημένου εκπαιδευτικού υλικού στο οποίο αξίζει να έχουν πρόσβαση οι μαθητές και στη διανομή στην εκπαιδευτική κοινότητα μέσω των εκπαιδευτικών και δικτυακών πυλών όπως: www.e-yliko.gr, www.sch.gr, www.neagenia.gr, www.kee.gr, www.greeklanguage.gr, www.pi-schools.gr, κλπ, οι οποίες λειτουργούν είτε υπό την άμεση ευθύνη του Υπ.Ε.Π.Θ. είτε υπό την ευθύνη εποπτευόμενων φορέων του.

Το πλαίσιο συμπληρώνεται από την εφαρμογή μεθόδων για την **προστασία της υπηρεσίας ηλεκτρονικής αλληλογραφίας** (e-mail) των σχολείων, των εκπαιδευτικών και των μαθητών από απρόκλητη / διαφημιστική αλληλογραφία (spam) και από κακόβουλο λογισμικό (ιοί - viruses), όπως αναλυτικά παρουσιάζεται στις δικτυακές τοποθεσίες **www.sch.gr/spam** και **www.sch.gr/virus**.

5.1 Δυνητικοί κίνδυνοι που ενέχει το διαδίκτυο για τους ανήλικους

Κατά την περιήγηση του ένας ανήλικος στο διαδίκτυο μπορεί να βρεθεί μπροστά σε επιβλαβές περιεχόμενο, που μπορεί να επηρεάσει τη σωματική και τη νοητική του διάπλαση. Καλό είναι οι ανήλικοι να γνωρίζουν τους κινδύνους που ενδέχεται να συναντήσουν στο διαδίκτυο.

- Σε πολλές ιστοσελίδες εκφράζονται ιδέες που βοηθούν τη διάδοση του ρατσισμού, του φανατισμού και της βίας. Σε αυτές τις ιστοσελίδες βρίσκουν χώρο φράσεις, κάποιες ακραίες απόψεις γύρω από τις φυλετικές διακρίσεις, δημιουργώντας έτσι στον ανήλικα «κακές» επιρροές γι αυτό το ευαίσθητο θέμα.
- Πολλοί προσπαθούν να προωθήσουν τη χρήση του αλκοόλ και των ναρκωτικών μέσω του διαδικτύου. Αυτές οι προσπάθειες στοχεύουν στους ανήλικες οι οποίοι είναι και οι πιο ευάλωτοι.
- Η διαφήμιση και η παρακίνηση συμμετοχής σε τυχερά παιχνίδια, πιάνει αρκετό χώρο σε κάθε ιστοσελίδα, βάζοντας πολλούς από τους ανήλικους

χρήστες στον πειρασμό να δοκιμάσουν την τύχη τους, με αποτέλεσμα πολλοί από αυτούς να εθίζονται στον τζόγο από μικρή ηλικία.

- Μια πολύ αρνητική επίδραση για τον ανήλικα χρήστη του διαδικτύου είναι οι ιστοσελίδες που περιέχουν πορνογραφικό περιεχόμενο.
- Πολλά κυκλώματα παιδεραστίας αναλαμβάνουν δράση μέσω του διαδικτύου.
- Πολλοί επιτήδειοι ηλεκτρονικοί εγκληματίες προσελκύουν τους ανήλικους χρήστες για να αποσπάσουν προσωπικά δεδομένα (αριθμοί πιστωτικών καρτών).

5.2 Συμβουλές ασφαλούς χρήσης του Διαδικτύου για τους ανηλίκους

Για μια ασφαλέστερη περιήγηση στο διαδίκτυο οι ανήλικες χρήστες θα πρέπει να ακολουθούν τις ακόλουθες συμβουλές ασφαλούς χρήσης.

- Να αποφεύγετε να δίνετε προσωπικά στοιχεία που αφορούν την ιδιωτική σας ζωή στο διαδίκτυο.
- Μη δίνεται στο διαδίκτυο τα στοιχεία επικοινωνίας σας (τηλέφωνο, e-mail, fax), καθώς και κωδικούς πρόσβασης που χρησιμοποιείτε.
- Μην πραγματοποιείτε ηλεκτρονικές συναλλαγές και μη δίνετε αριθμούς πιστωτικών καρτών.
- Μη συμπληρώνετε με προσωπικά σας στοιχεία ηλεκτρονικές φόρμες που σας ζητούν πολλές ιστοσελίδες.
- Μην εμπιστεύεστε άτομα που γνωρίζετε μέσω του διαδικτύου.
- Διαγράψτε email από αγνώστους αποστολείς, πολύ πιθανόν είναι να περιέχουν ιούς.
- Μη στέλνετε μέσω του διαδικτύου προσωπικό σας υλικό (φωτογραφίες, video).

5.3 ΑΠΟΦΑΣΗ 1351/2008/ΕΚ

- Η απόφαση 1351/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου για τη θέσπιση πολυετούς κοινοτικού προγράμματος σχετικά με την προστασία των παιδιών που χρησιμοποιούν το διαδίκτυο και άλλες τεχνολογίες της επικοινωνίας, αποτελεί το σημαντικότερο θεσμικό κείμενο για την προστασία των ανηλίκων από τους κινδύνους του διαδικτύου. Η

απόφαση υπογράφτηκε στις 16 Δεκεμβρίου στο Στρασβούργο, αφού το Ευρωπαϊκό Κοινοβούλιο έλαβε υπόψη του τα παρακάτω: [38]

- Η χρήση του Διαδικτύου και άλλων τεχνολογιών της επικοινωνίας, όπως τα κινητά τηλέφωνα, συνεχίζει να αυξάνεται σημαντικά στην Ευρωπαϊκή Ένωση και παρέχει σε όλους τους πολίτες μεγάλες ευκαιρίες, μεταξύ άλλων, συμμετοχής, διαδραστικότητας και δημιουργικότητας. Ωστόσο, συνεχίζουν να υφίστανται κίνδυνοι για τα παιδιά, καθώς και κατάχρηση των τεχνολογιών ενώ, εξαιτίας των μεταβαλλόμενων τεχνολογιών και κοινωνικών συμπεριφορών, συνεχίζουν να προκύπτουν νέοι κίνδυνοι και καταχρήσεις. Θα πρέπει να ληφθούν μέτρα σε επίπεδο ΕΕ για την προστασία της σωματικής, ψυχικής και ηθικής ακεραιότητας των παιδιών, που ενδέχεται να υποστεί ζημία από την πρόσβασή τους σε ακατάλληλο περιεχόμενο. Επιπλέον, προκειμένου να ενθαρρυνθούν οι πολίτες να αξιοποιούν τις ευκαιρίες και να απολαμβάνουν τα θετικά οφέλη που παρέχει το Διαδίκτυο και οι λοιπές τεχνολογίες της επικοινωνίας, απαιτείται η λήψη μέτρων για την προώθηση της ασφαλέστερης χρήσης τους.

- Θα υπάρχει διαρκώς η ανάγκη για ανάληψη δράσης τόσο στο πεδίο του δυνητικά επιβλαβούς περιεχομένου για παιδιά, ιδίως του πορνογραφικού υλικού, όσο και στο πεδίο του παράνομου περιεχόμενου, ιδίως υλικό που αφορά τη σεξουαλική κακοποίηση των παιδιών. Ομοίως, εξακολουθεί να υφίσταται ανάγκη για την ανάληψη δράσης ώστε τα παιδιά να μην καθίστανται θύματα επιβλαβούς και παράνομης συμπεριφοράς με αποτέλεσμα την πρόκληση σωματικών και ψυχολογικών βλαβών ούτε να δελεάζονται να μιμηθούν ανάλογες συμπεριφορές προξενώντας βλάβη στους εαυτούς τους και σε άλλους. Θα πρέπει να καταβληθούν ιδιαίτερες προσπάθειες για την αναζήτηση λύσεων με στόχο να αποτρέπονται οι ενήλικες από τη διατύπωση προτάσεων με δόλια πρόθεση, μέσω των τεχνολογιών της πληροφορίας και της επικοινωνίας, προκειμένου να συναντηθούν με ένα παιδί με σκοπό τη διάπραξη σεξουαλικής κακοποίησης ή άλλων σεξουαλικών εγκλημάτων. Παράλληλα θα πρέπει να δίδεται ιδιαίτερη προσοχή στο σύστημα ισότιμης υποστήριξης.
- Οι δράσεις θα πρέπει επίσης να στοχεύουν στην πρόληψη του ψυχολογικού εκβιασμού των παιδιών με απειλές, παρενόχληση και

[38] Η απόφαση 1351/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου για τη θέσπιση πολυετούς κοινοτικού προγράμματος σχετικά με την προστασία των παιδιών που χρησιμοποιούν το διαδίκτυο και άλλες τεχνολογίες της επικοινωνίας

εξευτελισμό μέσω του Διαδικτύου ή/και των διαδραστικών ψηφιακών τεχνολογιών, συμπεριλαμβανομένων των κινητών τηλεφώνων..

- Η απόφαση αριθ. 276/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Ιανουαρίου 1999, για ένα πολυετές κοινοτικό πρόγραμμα δράσης για την προώθηση ασφαλέστερης χρήσης του Διαδικτύου και νέων επιγραμμικών τεχνολογιών μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχόμενου κυρίως στον τομέα της προστασίας των παιδιών και των ανηλίκων (σχέδιο δράσης για ασφαλέστερη χρήση του Διαδικτύου, 1998-2004) και η απόφαση αριθ. 854/2005/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαΐου 2005, σχετικά με την καθιέρωση πολυετούς κοινοτικού προγράμματος για προαγωγή ασφαλέστερης χρήσης του διαδικτύου και νέων επιγραμμικών τεχνολογιών (πρόγραμμα Safer Internet plus,2005 έως 2008), παρέχουν κοινοτική χρηματοδότηση η οποία έχει ενθαρρύνει επιτυχώς ποικίλες πρωτοβουλίες και έχει προσδώσει «ευρωπαϊκή προστιθέμενη αξία», όπως προκύπτει από τις αξιολογήσεις των προγραμμάτων που έχουν υποβληθεί στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή των Περιφερειών [COM(2001)0690 COM(2003)0653 και COM(2006)0663].
- Το πρόγραμμα που θεσπίζεται με την παρούσα απόφαση θα πρέπει να στοχεύει μεταξύ άλλων στη δημιουργία εκπαιδευτικών «πακέτων» για γονείς, κηδεμόνες, δασκάλους και παιδαγωγούς.
- Η εξέλιξη των τεχνολογιών, οι αλλαγές στους τρόπους με τους οποίους ενήλικες και παιδιά χρησιμοποιούν το Διαδίκτυο και τις άλλες τεχνολογίες της επικοινωνίας, καθώς και οι μεταβολές στην κοινωνική συμπεριφορά οδηγούν σε νέους κινδύνους για τα παιδιά. Η βάση γνώσεων που μπορεί να χρησιμοποιηθεί για το σχεδιασμό αποτελεσματικών δράσεων θα πρέπει να ενισχυθεί ώστε να βελτιωθεί η αντίληψη σχετικά με τις εν λόγω αλλαγές. Διάφορα μέτρα και δράσεις θα πρέπει να συνδυαστούν πολύπλευρα και συμπληρωματικά. Θα πρέπει για παράδειγμα να περιλαμβάνουν τη λήψη μέτρων για την προώθηση της ασφαλούς και υπεύθυνης χρήσης του Διαδικτύου, την περαιτέρω ανάπτυξη τεχνολογιών υποστήριξης και την προώθηση βέλτιστων πρακτικών για δεοντολογικούς κώδικες που θα περιλαμβάνουν γενικά συμφωνημένους κανόνες συμπεριφοράς ή συνεργασίας με τον κλάδο για τους συμφωνημένους στόχους αυτών των κωδίκων.
- Το πρόγραμμα θα πρέπει επίσης να στηρίζει τη λήψη μέτρων για την ενθάρρυνση της προσφοράς θετικού περιεχομένου για παιδιά.
- Το μεταβαλλόμενο περιβάλλον των μέσων επικοινωνίας, λόγω της εμφάνισης νέων τεχνολογιών και καινοτομιών στα μέσα, καθιστά

αναγκαία την εκπαίδευση των παιδιών, αλλά και των γονέων, των κηδεμόνων, των δασκάλων και των παιδαγωγών σχετικά με την ασφαλή και αποτελεσματική χρήση των επιγραμμικών υπηρεσιών πληροφορίας.

- Θα πρέπει να καταβληθούν προσπάθειες για την προστασία των παιδιών μέσω της ανάπτυξης για παράδειγμα, αποτελεσματικών συστημάτων εξακρίβωσης της ηλικίας και εθελοντικού σήματος πιστοποίησης.

- Η διεθνής συνεργασία είναι ουσιαστικής σημασίας δεδομένου του παγκόσμιου χαρακτήρα του προβλήματος. Το παράνομο περιεχόμενο μπορεί να παράγεται σε μια χώρα, να φιλοξενείται σε δεύτερη, αλλά η πρόσβαση και τηλεφόρτωσή του να γίνεται σε ολόκληρο τον κόσμο. Η διεθνής συνεργασία που έχει ενθαρρυνθεί μέσω των δικτυακών δομών της Κοινότητας θα πρέπει να ενισχυθεί ώστε να προστατευτούν καλύτερα τα παιδιά από κινδύνους διασυνοριακής κλίμακας, όπου περιλαμβάνονται και τρίτες χώρες. Η ανταλλαγή βέλτιστων πρακτικών μεταξύ ευρωπαϊκών οργανισμών και οργανισμών σε άλλα μέρη του κόσμου μπορεί να αποβεί αμοιβαία επωφελής.

Έτσι, το Ευρωπαϊκό Κοινοβούλιο αποφάνθηκε τα εξής: Στο άρθρο 1 έθεσε το στόχο του προγράμματος διατυπώνοντας τα παρακάτω:

1. Με την παρούσα απόφαση θεσπίζεται κοινοτικό πρόγραμμα για την προώθηση ασφαλέστερης χρήσης του Διαδικτύου και άλλων τεχνολογιών της επικοινωνίας, ιδιαίτερα για παιδιά, καθώς και για την καταπολέμηση παράνομου περιεχόμενου και επιβλαβούς επιγραμμικής συμπεριφοράς. Το πρόγραμμα καλείται πρόγραμμα για «Ασφαλέστερη χρήση του διαδικτύου» ή «Ασφαλέστερο Διαδίκτυο»(εφεξής «το πρόγραμμα»).

2. Καθορίζονται οι ακόλουθες γραμμές δράσης:

α) ευαισθητοποίηση του κοινού·

β) καταπολέμηση του παράνομου περιεχόμενου και της επιβλαβούς επιγραμμικής συμπεριφοράς·

γ) προώθηση ασφαλέστερου επιγραμμικού περιβάλλοντος

Το άρθρο 2 κάνει αναφορά για τις νομικές οντότητες που μπορούν να συμμετέχουν στο πρόγραμμα. Αξιοσημείωτο γεγονός αποτελεί ότι το Ευρωπαϊκό Κοινοβούλιο δίνει τη δυνατότητα συμμετοχής και σε άλλες νομικές οντότητες που δεν ανήκουν στην Ευρωπαϊκή Ένωση, αναζητώντας έτσι τη διεθνή συνεργασία για την αντιμετώπιση του προβλήματος.

Το άρθρο 3 της Απόφασης θέτει τις αρμοδιότητες της υπεύθυνης επιτροπής για την εκτέλεση του προγράμματος. Πιο συγκεκριμένα, το άρθρο 3 αναφέρει ότι η Επιτροπή έχει την ευθύνη για την εφαρμογή του προγράμματος, αλλά και για την κατάρτιση ετησίων προγραμμάτων εργασιών. Ακόμα η Επιτροπή σύμφωνα με το άρθρο αυτό θέτει προτεραιότητες και διασφαλίζει την προσαρμοστικότητα όλων των κρατών-μελών.

Το άρθρο 5 καθορίζει τις ενέργειες για την παρακολούθηση και αξιολόγηση του προγράμματος.

Η Απόφαση 1351/2008/ΕΚ παρακάτω αναλύει το πρόγραμμα της δράσης που θα ακολουθήσει για την προστασία των ανηλίκων από τους κινδύνους του διαδικτύου.

Στόχος του προγράμματος είναι η προώθηση ασφαλέστερης χρήσης του Διαδικτύου και άλλων τεχνολογιών της επικοινωνίας («επιγραμμικών τεχνολογιών»), η εκπαίδευση των χρηστών και ιδιαίτερα των παιδιών, των γονέων, των κηδεμόνων, των δασκάλων και των παιδαγωγών και η καταπολέμηση παράνομου περιεχομένου και επιβλαβούς επιγραμμικής συμπεριφοράς.

Για την επίτευξη του εν λόγω στόχου το πρόγραμμα θα εστιαστεί σε πρακτική βοήθεια προς τους τελικούς χρήστες, ιδιαίτερα τα παιδιά, τους γονείς, τους κηδεμόνες, τους δασκάλους και τους παιδαγωγούς, ενθαρρύνοντας συμπράξεις μεταξύ ενδιαφερομένων διαφόρων συμφερόντων. Γενικός σκοπός του προγράμματος είναι η προώθηση ασφαλέστερης χρήσης του Διαδικτύου και άλλων τεχνολογιών της επικοινωνίας (εφεξής «επιγραμμικές τεχνολογίες»), ιδίως από παιδιά, η προώθηση της ανάπτυξης ασφαλούς επιγραμμικού περιβάλλοντος, ο περιορισμός του όγκου του παράνομου περιεχόμενου που διανέμεται επιγραμμικά, η αντιμετώπιση δυνητικά επιβλαβούς επιγραμμικής συμπεριφοράς (περιλαμβανομένης της ψυχολογικής χειραγώγησης των παιδιών με σκοπό την σεξουαλική κακοποίηση και της προσέγγισης και συναναστροφής με παιδιά με σκοπό την σεξουαλική κακοποίηση (grooming), της ηλεκτρονικής παρενόχλησης και των ηλεκτρονικών αρχείων που δείχνουν σωματική και/ή ψυχολογική βία) και η εξασφάλιση της ευαισθητοποίησης του κοινού σχετικά με

τους κινδύνους στο Διαδίκτυο και τις προφυλάξεις, καθώς επίσης και η ανάπτυξη παιδαγωγικών εργαλείων βάσει υγιών πρακτικών.

Για την εξασφάλιση συνεκτικής προσέγγισης των κινδύνων, εφόσον είναι δυνατή η πρόσβαση σε περιεχόμενο και υπηρεσίες και η χρήση τους τόσο στο Διαδίκτυο όσο και εκτός αυτού, όπως στην περίπτωση των βιντεοπαιχνιδιών, το πρόγραμμα μπορεί να αντιμετωπίσει και τους δύο τύπους πρόσβασης και χρήσης. Το πρόγραμμα θα υλοποιηθεί μέσω τεσσάρων γενικών γραμμών δράσης:

(1) Ευαισθητοποίηση του κοινού

Οι δραστηριότητες θα στοχεύουν σε μεγαλύτερη ευαισθητοποίηση του κοινού, ιδιαίτερα των παιδιών, των γονέων, των κηδεμόνων, των δασκάλων και των παιδαγωγών, σχετικά με τις ευκαιρίες και τους κινδύνους που σχετίζονται με τη χρήση επιγραμμικών τεχνολογιών και μέσου ασφαλούς επιγραμμικής επικοινωνίας. Θα εστιάζουν επίσης στις δυνατότητες και τους κινδύνους των υπηρεσιών που χρησιμοποιούν νέες πλατφόρμες διανομής, όπως οι οπτικοακουστικές υπηρεσίες μέσω δικτύων κινητής τηλεφωνίας. Όπου χρειάζεται, οι πληροφορίες θα διατίθενται σε πολύγλωσσες εκδοχές. Οι κύριες προγραμματιζόμενες δράσεις είναι:

- *Ευαισθητοποίηση του κοινού και διάδοση πληροφοριών σχετικά με ασφαλέστερη χρήση επιγραμμικών τεχνολογιών.*

Οι δραστηριότητες θα προαγάγουν την ευαισθητοποίηση του κοινού με συντονισμένο τρόπο σε ολόκληρη την Ευρωπαϊκή Ένωση, στέλνοντας ένα θετικό μήνυμα σχετικά με τις δυνατότητες για ευρύτερη και εντατικότερη χρήση της τεχνολογίας της πληροφορίας και των επικοινωνιών, παρέχοντας παράλληλα κατάλληλες πληροφορίες σχετικά με τους κινδύνους και τους τρόπους αντιμετώπισής τους. Οι δραστηριότητες αυτές θα ενθαρρύνονται ώστε να επιτραπεί στα παιδιά να χρησιμοποιούν υπεύθυνα τις επιγραμμικές τεχνολογίες, ιδίως μέσω προγραμμάτων για την απόκτηση γνώσεων και την εκπαίδευση γύρω από τα μέσα επικοινωνίας. Οι δραστηριότητες θα ενθαρρύνουν οικονομικά αποδοτικά μέσα διανομής πληροφοριών ευαισθητοποίησης και ενημέρωσης σε μεγάλο αριθμό χρηστών, για παράδειγμα σε συνεργασία με τα μέσα ενημέρωσης, με την επιγραμμική διανομή υλικού παραγόμενου από τους χρήστες, και μέσω του εκπαιδευτικού συστήματος. Οι μέθοδοι διάδοσης και παρουσίασης των μηνυμάτων θα προσαρμόζονται στις διάφορες ομάδες στόχου (σε διαφορετικές ηλικιακές ομάδες παιδιών και στους γονείς τους, τους κηδεμόνες, τους δασκάλους και τους παιδαγωγούς).

- *Δημιουργία σημείων επαφής όπου γονείς και παιδιά μπορούν να λαμβάνουν απαντήσεις σε ερωτήματα σχετικά με την ασφαλή επιγραμμική επικοινωνία, συμπεριλαμβανομένων συμβουλών για την αντιμετώπιση της προσέγγισης με βλέψεις σεξουαλικής κακοποίησης και της παρενόχλησης μέσω κυβερνοχώρου.*

Οι δραστηριότητες θα στοχεύουν στη διευκόλυνση των χρηστών να κάνουν ενημερωμένες και υπεύθυνες επιλογές, παρέχοντάς τους συμβουλές σχετικά με συναφείς πληροφορίες και προφυλάξεις για ασφαλή επιγραμμική επικοινωνία.

- *Ενθάρρυνση της βελτίωσης αποτελεσματικών και οικονομικά αποδοτικών μεθόδων και μέσων ευαισθητοποίησης.*

Οι δράσεις θα στοχεύουν στη βελτίωση συναφών μεθόδων και μέσων ευαισθητοποίησης, με σκοπό να καταστούν αποτελεσματικότερες και οικονομικά αποδοτικότερες μακροπρόθεσμα.

- *Εξασφάλιση της ανταλλαγής βέλτιστων πρακτικών και διασυνοριακής συνεργασίας σε επίπεδο ΕΕ.*

Θα αναληφθούν δράσεις για την εξασφάλιση αποτελεσματικής διασυνοριακής συνεργασίας και αποτελεσματικής ανταλλαγής βέλτιστων πρακτικών, εργαλείων, μεθόδων, εμπειρίας και πληροφοριών σε επίπεδο ΕΕ.

- *Εξασφάλιση ανταλλαγής βέλτιστων πρακτικών και συνεργασίας σε διεθνή κλίμακα.*

Οι δράσεις θα στοχεύουν στην προώθηση της συνεργασίας και της ανταλλαγής βέλτιστων πρακτικών, εργαλείων, μεθόδων, εμπειρίας και πληροφοριών σε διεθνή κλίμακα, ώστε να ενθαρρυνθούν κοινές προσεγγίσεις και μέθοδοι εργασίας και να βελτιωθεί και να ενισχυθεί η αποτελεσματικότητα ή η οικονομική απόδοση και η εμβέλεια παγκόσμιων πρωτοβουλιών.

(2) Καταπολέμηση του παράνομου περιεχομένου και της επιβλαβούς επιγραμμικής συμπεριφοράς

Οι δραστηριότητες στοχεύουν στον περιορισμό του όγκου του παράνομου περιεχόμενου που κυκλοφορεί επιγραμμικά, καθώς και στην κατάλληλη αντιμετώπιση επιβλαβούς επιγραμμικής συμπεριφοράς, με ιδιαίτερη εστίαση στην επιγραμμική διανομή υλικού σεξουαλικής κακοποίησης παιδιών, συναναστροφών με βλέψεις σεξουαλικής κακοποίησης και

παρενόχλησης/εκφοβισμού μέσω κυβερνοχώρου. Οι κύριες γενικές δράσεις που σχεδιάζεται να αναληφθούν είναι:

- *Παροχή στο κοινό και προώθηση της ύπαρξης σημείων επαφής και ανοικτών γραμμών επικοινωνίας για την καταγγελία επιγραμμικού παράνομου περιεχόμενου και επιβλαβούς συμπεριφοράς.*

Οι δραστηριότητες θα διασφαλίζουν ότι τα εν λόγω σημεία επαφής είναι αποτελεσματικά και ορατά στο κοινό, ότι συνδέονται στενά με άλλους φορείς που αναλαμβάνουν δράσεις σε εθνικό επίπεδο (ιδίως με αστυνομικές μονάδες ειδικευμένες στο έγκλημα στον κυβερνοχώρο) και συνεργάζονται σε επίπεδο ΕΕ για την αντιμετώπιση διασυνοριακών θεμάτων και για την ανταλλαγή βέλτιστων πρακτικών. Αυτά τα σημεία επαφής προσφέρουν επίσης στο κοινό τις αναγκαίες πληροφορίες για τους τρόπους καταγγελίας παράνομου περιεχομένου και αξιολόγησης του περιεχομένου των επιγραμμικών υπηρεσιών πληροφορίας που ενδέχεται να βλάπτουν τη σωματική, ψυχική ή ηθική ακεραιότητα των παιδιών.

- *Αντιμετώπιση επιβλαβούς επιγραμμικής συμπεριφοράς, ιδίως των συναναστροφών με βλέψεις σεξουαλικής κακοποίησης και της παρενόχλησης/εκφοβισμού μέσω κυβερνοχώρου. Οι δραστηριότητες θα στοχεύουν στην αντιμετώπιση των επιγραμμικών επαφών με βλέψεις σεξουαλικής κακοποίησης, καθώς και περιπτώσεις παρενόχλησης/εκφοβισμού μέσω κυβερνοχώρου.*

Οι δράσεις θα πραγματεύονται θέματα τεχνικού, ψυχολογικού και κοινωνιολογικού χαρακτήρα σχετικά με τα αιτήματα αυτά και θα αποβλέπουν στην προώθηση της συνεργασίας και του συντονισμού μεταξύ των ενδιαφερόμενων.

- *Ενθάρρυνση εφαρμογής τεχνικών λύσεων για ενδεδειγμένη αντιμετώπιση του παράνομου περιεχόμενου και της επιβλαβούς επιγραμμικής συμπεριφοράς και πληροφόρηση των τελικών χρηστών για τον τρόπο εφαρμογής αυτής της τεχνολογίας.*

Οι δραστηριότητες θα ενθαρρύνουν τον σχεδιασμό, την ανάπτυξη ή προσαρμογή και/ή την προώθηση αποτελεσματικών τεχνολογικών εργαλείων για ενδεδειγμένη αντιμετώπιση παράνομου περιεχόμενου και την καταπολέμηση της επιβλαβούς επιγραμμικής συμπεριφοράς, ιδιαίτερα δε εκείνων που διατίθενται δωρεάν, προς εύκολη γενική χρήση εκ μέρους των ενδιαφερόμενων και την προώθηση από τους φορείς παροχής υπηρεσιών, της ασφαλούς και υπεύθυνης χρήσεως των διαδικτυακών συνδέσεων για την προστασία των

παιδιών από παράνομες και επιβλαβείς δραστηριότητες. Οι ενδιαφερόμενοι θα πληροφορούνται για τη διαθεσιμότητα της τεχνολογίας αυτής και την ορθή χρήση της. Θα μπορούσαν να εξετασθούν, μεταξύ άλλων, τα εξής μέτρα:

α) έγκριση ενός σήματος ποιότητας για φορείς παροχής υπηρεσιών, ώστε οι χρήστες να μπορούν εύκολα να διαπιστώνουν εάν κάποιος συγκεκριμένος πάροχος εφαρμόζει ή όχι έναν κώδικα δεοντολογίας.

β) υποστήριξη της χρήσης από τους τελικούς χρήστες φίλτρων τα οποία να εμποδίζουν τη δίοδο πληροφοριών, οι οποίες θα μπορούσαν να βλάψουν τη σωματική, ψυχική ή ηθική ακεραιότητα των παιδιών.

γ) στήριξη και προώθηση μέτρων για την ενθάρρυνση της προσφοράς θετικού περιεχομένου για παιδιά.

δ) μέτρα που στοχεύουν στη διερεύνηση της αποτελεσματικότητας των εργαλείων που έχουν αναπτυχθεί σε συνεργασία με τον κλάδο του Διαδικτύου και τα οποία επιτρέπουν στις υπηρεσίες επιβολής του νόμου να εντοπίζουν εγκληματίες στο Διαδίκτυο.

Προώθηση συνεργασίας και ανταλλαγής πληροφοριών, εμπειρίας και βέλτιστων πρακτικών μεταξύ των ενδιαφερόμενων σε εθνικό επίπεδο και σε επίπεδο ΕΕ.

Οι δραστηριότητες θα αποβλέπουν στη βελτίωση του συντονισμού των ενδιαφερομένων που συμμετέχουν στην καταπολέμηση της διανομής παράνομου περιεχομένου και επιζήμιας επιγραμμικής συμπεριφοράς, και θα ενθαρρύνουν τη συμμετοχή και την εμπλοκήτων εν λόγω ενδιαφερομένων. Ειδικότερα, οι δραστηριότητες θα ενθαρρύνουν τη διεθνή ανταλλαγή εμπειρογνωμοσύνης και ιδεών μεταξύ κυβερνήσεων, υπηρεσιών επιβολής του νόμου, γραμμών βοήθειας, τραπεζικών/χρηματοοικονομικών/πιστωτικών ιδρυμάτων, συμβουλευτικών κέντρων για την κακοποίηση παιδιών, οργανώσεων για την ευημερία των παιδιών, καθώς και της βιομηχανίας του Διαδικτύου.

Βελτίωση της συνεργασίας, της ανταλλαγής πληροφοριών και εμπειριών στην καταπολέμηση του επιγραμμικού παράνομου περιεχόμενου και της επιβλαβούς συμπεριφοράς σε διεθνή κλίμακα.

Οι δραστηριότητες θα στοχεύουν στη βελτίωση της συνεργασίας με τρίτες χώρες, την εναρμόνιση προσεγγίσεων όσον αφορά την αντιμετώπιση παράνομου περιεχόμενου και επιβλαβούς επιγραμμικής συμπεριφοράς διεθνώς και στην ενθάρρυνση της ανάπτυξης συνδέσμων για τον συντονισμό των

βάσεων δεδομένων των κρατών μελών σε ό,τι αφορά τη σεξουαλική κακοποίηση των παιδιών, καθώς και κοινών προσεγγίσεων και μεθόδων εργασίας. Ειδικότερα, οι δραστηριότητες θα στοχεύουν στη δημιουργία στενής συνεργασίας μεταξύ των εθνικών αρχών, της αστυνομίας και των σημείων επαφής. Θα αναληφθούν δράσεις για τη δημιουργία κοινής βάσης δεδομένων της ΕΕ, όπου θα συλλέγονται πληροφορίες σχετικά με σεξουαλική κακοποίηση παιδιών και για την εξασφάλιση της σύνδεσής της με την Europol.

Χρησιμοποίηση μητρώων ονομάτων τομέα, όπου δεν υπάρχει και ενίσχυση της υφιστάμενης συνεργασίας.

Στο πλαίσιο της εθνικής νομοθεσίας, οι δραστηριότητες έχουν ως στόχο τη συμπλήρωση των υφισταμένων δράσεων με τη βελτίωση της χρησιμοποίησης μητρώων ονομάτων τομέα (domain name registries) στα κράτη μέλη και με την ενθάρρυνση θετικών σχέσεων με μητρώα εκτός ΕΕ προκειμένου να καταστεί δυνατή η ταχύτερη ανίχνευση δυνητικά παράνομου περιεχομένου και η ελαχιστοποίηση της μακροβιότητας ιστοσελίδων που είναι γνωστό ότι προσφέρουν περιεχόμενο σεξουαλικής κακοποίησης παιδιών.

(3) Προώθηση ασφαλέστερου επιγραμμικού περιβάλλοντος

Οι δραστηριότητες θα αποβλέπουν να φέρουν σε επαφή τα ενδιαφερόμενα μέρη στην εξεύρεση τρόπων προώθησης ασφαλέστερου επιγραμμικού περιβάλλοντος και την προστασία των παιδιών από περιεχόμενο που μπορεί να είναι επιβλαβές γι' αυτά. Οι κύριες γενικές δράσεις που προγραμματίζονται είναι:

Βελτίωση της συνεργασίας, ανταλλαγή πληροφοριών, εμπειρίας και βέλτιστων πρακτικών μεταξύ ενδιαφερόμενων.

Οι δραστηριότητες θα στοχεύουν στη βελτίωση της εργασίας, την εναρμόνιση προσεγγίσεων για τη δημιουργία ασφαλέστερου επιγραμμικού περιβάλλοντος για παιδιά και την ανταλλαγή βέλτιστων πρακτικών και μεθόδων εργασίας.

Οι δράσεις θα στοχεύουν να εφοδιάσουν τους ενδιαφερόμενους με μια ανοικτή πλατφόρμα συζήτησης των θεμάτων που συνδέονται με την προώθηση ασφαλέστερου επιγραμμικού περιβάλλοντος και τρόπων προστασίας των παιδιών από δυνητικά επιβλαβές περιεχόμενο, σε διάφορες πλατφόρμες.

Ενθάρρυνση των ενδιαφερόμενων για την ανάπτυξη και υλοποίηση και ανάπτυξη νέων τεχνολογιών και υπηρεσιών.

Ενθάρρυνση και παροχή βοήθειας στους παρόχους για την ανάπτυξη σήμανσης.

Οι δράσεις θα στοχεύουν στην ενθάρρυνση και την παροχή βοήθειας στους παρόχους διαδικτυακών υπηρεσιών για την ανάπτυξη, ως εργαλείου αυτορρύθμισης, ενός «ασφαλούς για τα παιδιά» κοινού σήματος για ιστοσελίδες. Στις δράσεις αυτές μπορούν να περιλαμβάνονται, μεταξύ άλλων, η διερεύνηση της δυνατότητας διαμόρφωσης συστήματος κοινών περιγραφικών συμβόλων ή μηνυμάτων προειδοποίησης που να υποδηλώνουν την ηλικιακή ομάδα και/ή τις πτυχές του περιεχομένου που επέβαλαν την αναγραφή μιας σύστασης για ορισμένη ελάχιστη ηλικία, πράγμα που θα βοηθούσε τους χρήστες να αντιλαμβάνονται καλύτερα το ενδεχομένως επιβλαβές επιγραμμικό περιεχόμενο

Ενθάρρυνση της συμμετοχής των παιδιών στη δημιουργία ασφαλέστερου επιγραμμικού περιβάλλοντος.

Οι δράσεις θα στοχεύουν στη συμμετοχή των παιδιών, διασφαλίζοντας ίση συμμετοχή κοριτσιών και αγοριών, με σκοπό να γίνουν καλύτερα κατανοητές οι απόψεις και οι εμπειρίες τους όσον αφορά τη χρήση επιγραμμικών τεχνολογιών, καθώς και με την υποστήριξη ειδικών, να γίνει καλύτερα κατανοητός ο τρόπος προώθησης ασφαλέστερου επιγραμμικού περιβάλλοντος για τα παιδιά. Η συμμετοχή αυτή θα ασκείται σε τακτά χρονικά διαστήματα στο πλαίσιο δραστηριοτήτων όπως το Ευρωπαϊκού Φόρουμ για τα δικαιώματα των ανηλίκων, το Φόρουμ για ένα ασφαλέστερο Διαδίκτυο και άλλων.

Βελτιωμένη πληροφόρηση σχετικά με τα ενδεδειγμένα μέσα αντιμετώπισης επιβλαβούς επιγραμμικού περιεχόμενου.

Οι δραστηριότητες θα αποβλέπουν στη βελτίωση της πληροφόρησης, ιδίως των γονέων, κηδεμόνων, δασκάλων και παιδαγωγών, σχετικά με την απόδοση και την αποτελεσματικότητα των εργαλείων, όπως των φίλτρων, για την αντιμετώπιση δυνητικά επιβλαβούς επιγραμμικού περιεχόμενου, καθώς και στον τακτικό εφοδιασμό όλων των χρηστών με απλές παιδαγωγικές πληροφορίες, μέσα και εφαρμογές που θα τους υποστηρίζουν καταλλήλως στην αντιμετώπιση επιβλαβούς περιεχόμενου σε διαφορετικές πλατφόρμες.

Εξασφάλιση της συμβατότητας των προσεγγίσεων στην Ευρωπαϊκή Ένωση και διεθνώς.

Οι δραστηριότητες θα προωθήσουν τη συνεργασία και την ανταλλαγή πληροφοριών εμπειριών και βέλτιστων πρακτικών μεταξύ των ενδιαφερόμενων σε επίπεδο ΕΕ και διεθνώς.

(4) Δημιουργία βάσης γνώσεων

Οι δραστηριότητες θα στοχεύουν στη δημιουργία βάσης γνώσεων για την ενδεδειγμένη αντιμετώπιση υφιστάμενων και νέων χρήσεων στο επιγραμμικό περιβάλλον, καθώς και συναφών κινδύνων και συνεπειών, αποβλέποντας στο σχεδιασμό κατάλληλων δράσεων που θα στοχεύουν στην εξασφάλιση επιγραμμικής ασφάλειας για όλους τους χρήστες. Το περιεχόμενο αυτής της βάσης γνώσεων θα κοινοποιείται στους ενδιαφερομένους και θα διαδίδεται στα κράτη μέλη. Οι κύριες γενικές δράσεις που προγραμματίζονται είναι:

Ενθάρρυνση της συντονισμένης προσέγγισης όσον αφορά τη διερεύνηση συναφών πεδίων.

Οι δράσεις θα διασφαλίσουν τον συντονισμό των προσπαθειών ώστε να έλθουν σε επαφή επιστήμονες και εμπειρογνώμονες που ασχολούνται με την επιγραμμική ασφάλεια για τα παιδιά σε επίπεδο ΕΕ, την τόνωση της διεθνούς συνεργασίας και συντονισμού, καθώς και την επικαιροποίηση των επισκοπήσεων ως προς την υφιστάμενη και μελλοντική έρευνα.

Παροχή επικαιροποιημένων πληροφοριών όσον αφορά τη χρήση επιγραμμικών τεχνολογιών από παιδιά.

Θα αναληφθούν δράσεις για την επικαιροποίηση των πληροφοριακών στοιχείων σχετικά με τη χρήση επιγραμμικών τεχνολογιών από παιδιά, καθώς και τον τρόπο με τον οποίο παιδιά, γονείς, κηδεμόνες, δάσκαλοι και παιδαγωγοί αντιμετωπίζουν τόσο τις ευκαιρίες όσο και τους κινδύνους. Οι δράσεις θα περιλαμβάνουν ποιοτικές και ποσοτικές πτυχές. Επίσης, θα στοχεύουν στη βελτίωση των γνώσεων σχετικά με τις στρατηγικές των παιδιών στην αντιμετώπιση κινδύνων σε επιγραμμικό περιβάλλον και θα αξιολογούν την αποτελεσματικότητά τους.

Ανάλυση στατιστικών και τάσεων στα διάφορα κράτη μέλη.

Θα αναληφθούν δράσεις για την ανάλυση στατιστικών και τάσεων από τα διάφορα κράτη μέλη, ούτως ώστε οι υπηρεσίες επιβολής του νόμου και οι αρμόδιες αρχές των κρατών μελών να μπορούν να μειώνουν την αλληλο – κάλυψη των πραγματοποιούμενων προσπαθειών και να μεγιστοποιούν τη χρήση των σημερινών και μελλοντικών πόρων.

Προώθηση της διερεύνησης περιπτώσεων στις οποίες τα παιδιά καθίστανται θύματα επιγραμμικών δραστηριοτήτων:

Οι δράσεις, που θα περιλαμβάνουν μια ευαίσθητη από άποψη φύλου προσέγγιση, θα στοχεύουν στη διερεύνηση τεχνικών, ψυχολογικών και κοινωνιολογικών θυμάτων, που συνδέονται με μηχανισμούς δημιουργίας θυμάτων παιδιών σε επιγραμμικό περιβάλλον, συμπεριλαμβανομένων της παρενόχλησης/εκφοβισμού μέσω κυβερνοχώρου, της συναναστροφής με βλέψεις σεξουαλικής εκμετάλλευσης, θεμάτων που συνδέονται με επιγραμμικό υλικό σεξουαλικής κακοποίησης παιδιών και με νέες μορφές συμπεριφοράς που μπορούν να είναι επικίνδυνες για τα παιδιά.

Προώθηση ερευνών σχετικά με αποτελεσματικούς τρόπους βελτίωσης της ασφαλούς χρήσης επιγραμμικών τεχνολογιών.

Οι δράσεις μπορούν να αφορούν έρευνες και δοκιμές μεθόδων και μέσων ευαισθητοποίησης, επιτυχείς μηχανισμούς αυτορύθμισης και συρρύθμισης, την αποτελεσματικότητα διαφόρων λύσεων τεχνικού και μη χαρακτήρα, καθώς και άλλα συναφή θέματα.

Αύξηση των γνώσεων σχετικά με τα αποτελέσματα της χρήσης σημερινών και αναδυόμενων τεχνολογιών στα παιδιά.

Οι δράσεις, που θα περιλαμβάνουν μια ευαίσθητη από άποψη φύλου προσέγγιση, θα στοχεύουν στη βελτιωμένη κατανόηση των ψυχολογικών, συμπεριφορικών και κοινωνιολογικών επιπτώσεων στα παιδιά από τη χρήση επιγραμμικών τεχνολογιών, από τα αποτελέσματα της έκθεσής τους σε επιβλαβές περιεχόμενο και συμπεριφορές έως και σε συναναστροφές με βλέψεις σεξουαλικής κακοποίησης, την παρενόχληση/εκφοβισμό μέσω κυβερνοχώρου σε διάφορες πλατφόρμες, από τους υπολογιστές και τα κινητά τηλέφωνα έως τις κονσόλες παιχνιδιών και άλλες αναδυόμενες τεχνολογίες.

5.4 ΕΦΑΡΜΟΓΗ ΓΟΝΙΚΟΥ ΕΛΕΓΧΟΥ

Το πρόβλημα

Με τη δημοτικότητα του Διαδικτύου και την εξάπλωση του σε ένα νεώτερο, ηλικιακά ακροατήριο, εμφανίστηκε ο κίνδυνος της υποβολής των παιδιών/ανηλίκων και σε ενδεχομένως επιβλαβές υλικό. Έτσι, αναζητήθηκαν λύσεις που θα μπορούσαν να βοηθήσουν τους γονείς, τους εκπαιδευτικούς και γενικότερα όσους έχουν την ευθύνη για ό, τι έρχεται σε επαφή με τα αισθητήρια

των ανηλίκων όταν πλοηγούνται στο διαδίκτυο. Σε αυτήν την εργασία, σκοπός μας είναι να αναπτύξουμε μια λύση που θα λύνει αυτό το πρόβλημα.

Άλλες λύσεις.

Λόγω της φύσης του προβλήματος, έχουν δημιουργηθεί αρκετά προϊόντα λογισμικού που σκοπό έχουν να προστατέψουν τους ανήλικους δια του περιορισμού της πρόσβασης σε διάφορα websites.

Ένα από τα πολλά γονικά λογισμικά ελέγχου που προσφέρονται στην αγορά είναι ***WebWatcher.*** Μαζί με τις ικανότητές του ως όργανο ελέγχου Ιστού χρησιμεύει επίσης ως ένα όργανο καταγραφής συνομιλίας. Αυτό είναι ευεργετικό για πολλούς γονείς που μπορούν έτσι να εμποδίσουν τα παιδιά τους από το να πέσουν θύματα παρενόχλησης στο διαδίκτυο. Επίσης, δίνει τη δυνατότητα να ελεγχθούν καθώς επίσης και να εμποδιστούν οι ανεπιθύμητοι ιστοχώροι από την πρόσβαση. Τέλος, πρόκειται για ένα λογισμικό που ρυθμίζεται και χρησιμοποιείται εύκολα ακόμα και από μη εξιδικευμένους χρήστες, πράγμα που το κάνει κατάλληλο για οικιακή/οικογενειακή χρήση.

Το ***SpyAgent*** έχει όλα τα χαρακτηριστικά γνωρίσματα ενός προγράμματος ελέγχου πρόσβασης. Επιπλέον, το SpyAgent καταγράφει και το σταλμένο και λαμβανόμενο ηλεκτρονικό ταχυδρομείο. Το κυριότερο γνώρισμα του προγράμματος είναι η δυνατότητά του να εμποδίσει την πρόσβαση ενός χρήστη στα προγράμματα όπως τη συνομιλία (chat) και Instant Messengers που μπορούν να αποτελέσουν πιθανούς κινδύνους.

Λογισμικό – Πλατφόρμες.

Αναπτύξαμε την λύση μας χρησιμοποιώντας την γλώσσα προγραμματισμού C++. Για την ανάπτυξη χρησιμοποιήσαμε το ολοκληρωμένο περιβάλλον προγραμματισμού Visual Studio 2008, της Microsoft. Το τελικό πρόγραμμα εκτελείται σε περιβάλλον Microsoft Windows (δοκιμάστηκε σε εκδόσεις XP 32bit SP3 και Vista 32bit).

Αρχιτεκτονική.

Το πρόγραμμα ουσιαστικά αποτελείται από δύο τμήματα. Το πρώτο είναι το γραφικό περιβάλλον του προγράμματος, δηλαδή ο πίνακας ελέγχου που επιτρέπει στους διαχειριστές (τους γονείς) να κάνουν τις απαραίτητες λειτουργίες, που θα περιγραφούν παρακάτω. Το άλλο είναι ένα windows service που όταν εγκατασταθεί, παρατηρεί (monitor) το σύστημα και ψάχνει για web

requests. Αν εντοπιστούν και αφορούν μια από τις «απαγορευμένες» ιστοσελίδες, μπλοκάρονται.

Ο πηγαίος κώδικας του γραφικού περιβάλλοντος βρίσκεται στον φάκελο «myparentalcontrol». Αποτελείται από την υπο-εφαρμογή Form1 (Form1.h & Form1.cpp) που αποτελεί την αρχική οθόνη της εφαρμογής (εικόνα 1).

Η υπο-εφαρμογή installservice (installservice.h & installservice.cpp) αναλαμβάνει να εγκαταστήσει την υπηρεσία (βλ. παρακάτω) και να ειδοποιήσει τον χρήστη για την κατάσταση της (εικόνα 2).

Η υπο-εφαρμογή Mainprogramm υλοποιεί τον πίνακα ελέγχου της εφαρμογής (εικόνα 3 και εξής).

Η υπο-εφαρμογή changecredentials υλοποιεί την αλλαγή των στοιχείων πρόσβασης (εικόνα 7).

Τέλος, η About είναι το παράθυρο «βοήθειας του χρήστη» (εικόνα 6) . Ο πηγαίος κώδικας της υπηρεσίας βρίσκεται στον φάκελο «parentalcontrolcpp». Τα κυριότερα αρχεία, αυτά που υλοποιούν την υπηρεσία είναι τα «parentalcontrolcppWinService.h» και «parentalcontrolcppWinService.cpp». Η λειτουργία τους είναι η εξής: με την εκκίνηση/εγκατάσταση της υπηρεσίας, ελέγχουν το σύστημα πρώτον για το ποιος χρήστης είναι συνδεδεμένος και δεύτερον για το ποια web requests κάνει. Αν δεν είναι ο σωστός χρήστης, δηλαδή είναι κάποιος ανήλικος (που προφανώς πρέπει να μπαίνει στο μηχάνημα με λογαριασμό διαφορετικό από του γονέα) τότε κοιτάμε το URI το οποίο ζητάει, με την βοήθεια της κλάσης System::Net::HttpWebRequest. Ελέγχουμε αν το ζητούμενο URI βρίσκεται μέσα στην λίστα (accesslist.txt) και αν βρίσκεται το request γίνεται σιωπηλά (για ευνόητους λόγους) abort. Αλλιώς, μένει untouched.

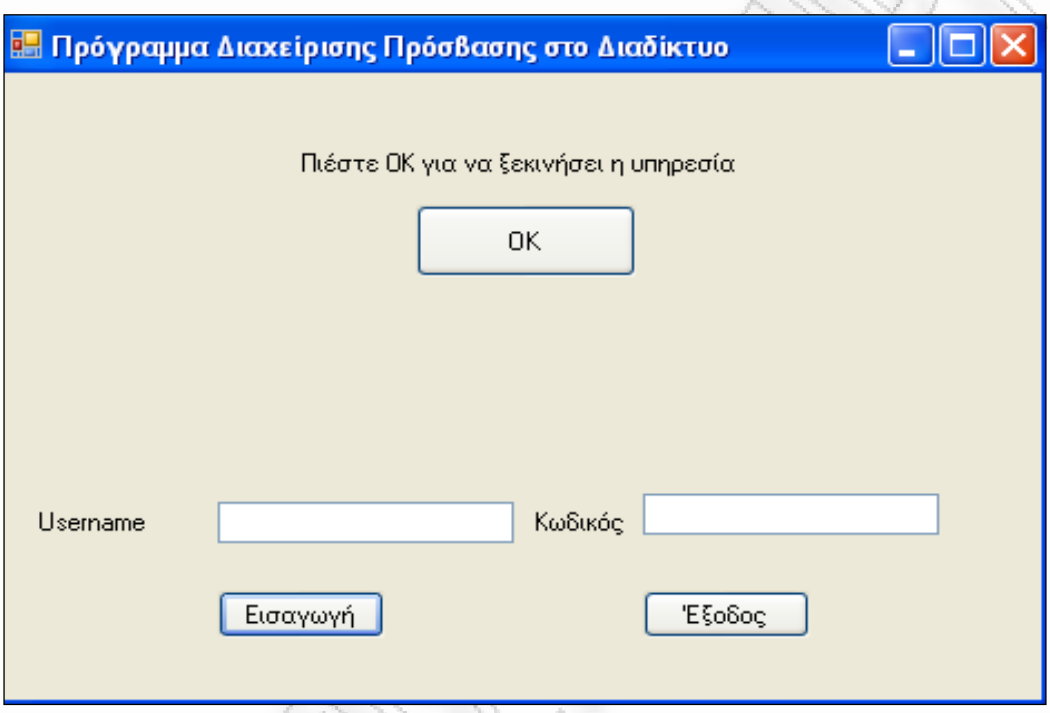
Εκτέλεση - Χρήση.

Για να εκτελέσει ο χρήστης το πρόγραμμα, το μόνο που χρειάζεται είναι να πλοηγηθεί στον φάκελο «release» και να εκτελέσει το «myparentalcontrol.exe». Το Interface του προγράμματος είναι απλό και εξηγείται παρακάτω.

Υπάρχει η δυνατότητα να γίνουν και τροποποιήσεις στο πρόγραμμα, μιας που δίνεται και ο πηγαίος κώδικας του. Για να γίνει αυτό, όμως πρέπει να

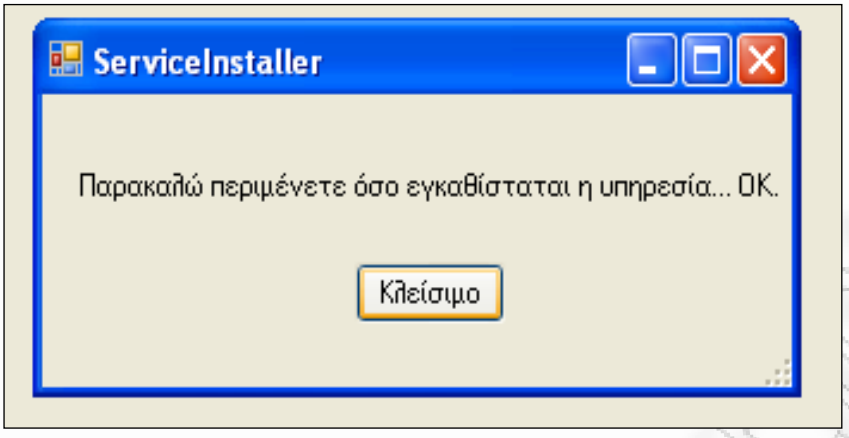
υπάρχει εγκατεστημένο το Visual Studio και να φορτωθεί σε αυτό το αντίστοιχο solution, που ονομάζεται «myparentalcontrol.sln». Η δομή του πηγαίου κώδικα περιγράφεται στην προηγούμενη ενότητα.

Στην επόμενη εικόνα φαίνεται η αρχική οθόνη του προγράμματος. Όπως βλέπουμε, έχουμε δυο επιλογές. Η μία είναι να ζητήσουμε την εγκατάσταση της υπηρεσίας ελέγχου πρόσβασης και η άλλη είναι να εισάγουμε τα κατάλληλα στοιχεία για να αποκτήσουμε πρόσβαση στον πίνακα διαχείρισης.



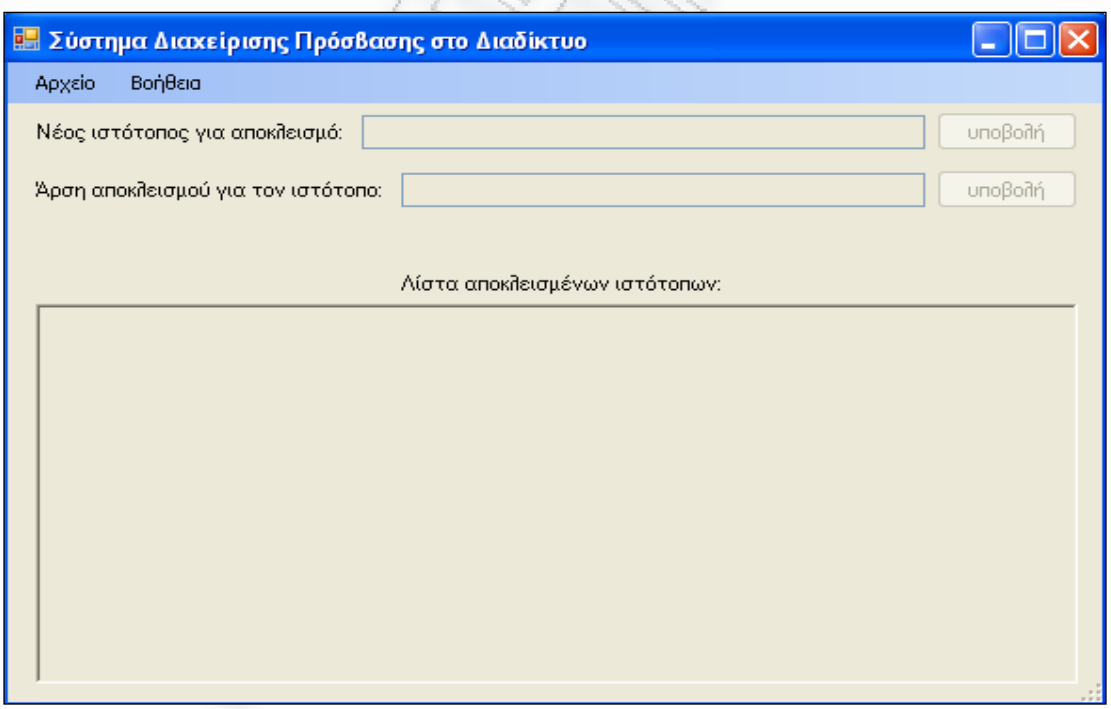
Εικόνα 1

Αν ζητήσουμε να ξεκινήσει η υπηρεσία, τότε θα εμφανιστεί στιγμιαία μια γραμμή εντολών (command prompt) που μας περιγράφει την εξέλιξη της εγκατάστασης. Όταν αυτή ολοκληρωθεί, θα εμφανιστεί ένα pop-up window που θα μας πληροφορεί για την επιτυχία της διαδικασίας. Πατώντας OK η εφαρμογή κλείνει, αλλά η υπηρεσία λειτουργεί και θα λειτουργεί συνέχεια.



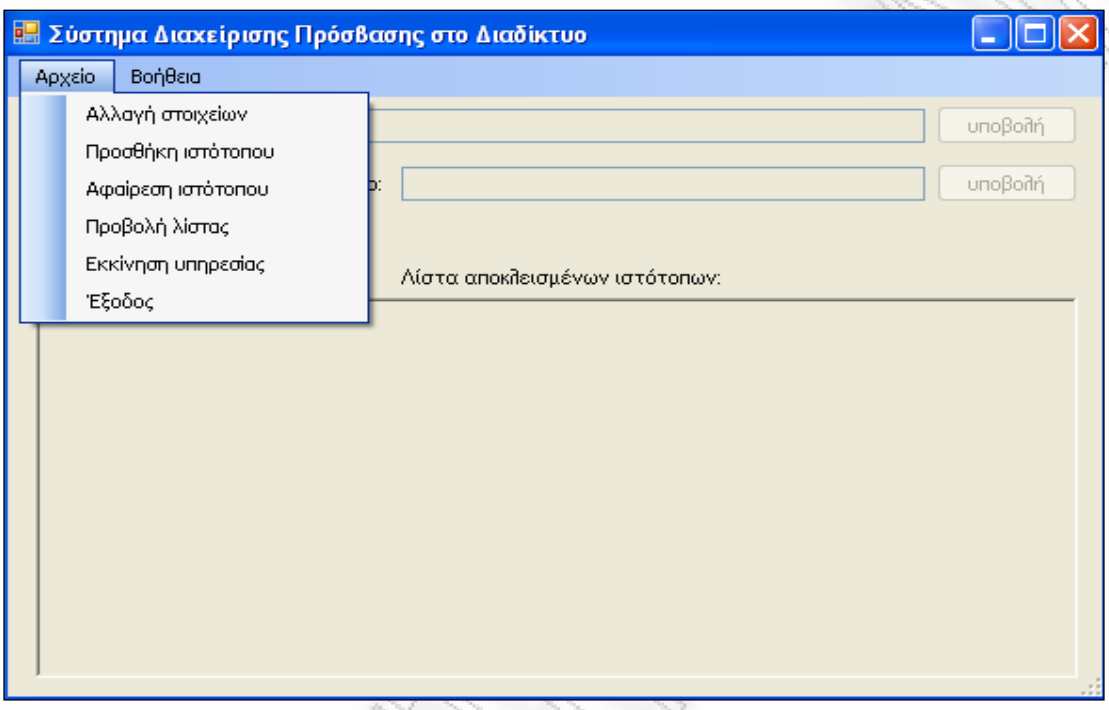
Εικόνα 2

Αν θέλουμε να κάνουμε κάποια διαχειριστική ενέργεια, πρέπει να εισάγουμε το όνομα και τον κωδικό χρήστη και να πατήσουμε «εισαγωγή». Αν τα στοιχεία είναι λανθασμένα, θα εμφανιστεί αντίστοιχο μήνυμα σφάλματος. Αλλιώς θα εμφανιστεί ο πίνακας ελέγχου.

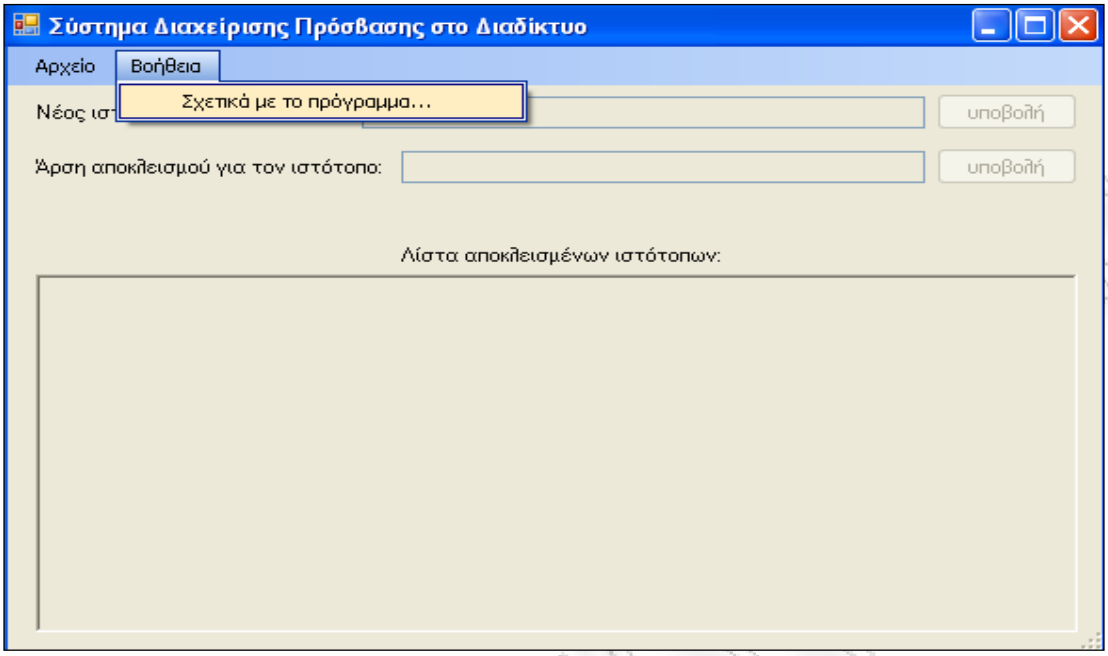


Εικόνα 3

Όπως παρατηρούμε, στην αρχή είναι όλο το panel απενεργοποιημένο. Το σκεπτικό είναι ότι κάθε επιλογή ενεργοποιείται μόνο αν επιλεγεί από τον χρήστη. Όλες οι επιλογές δίνονται στο μενού στο πάνω μέρος του παραθύρου.

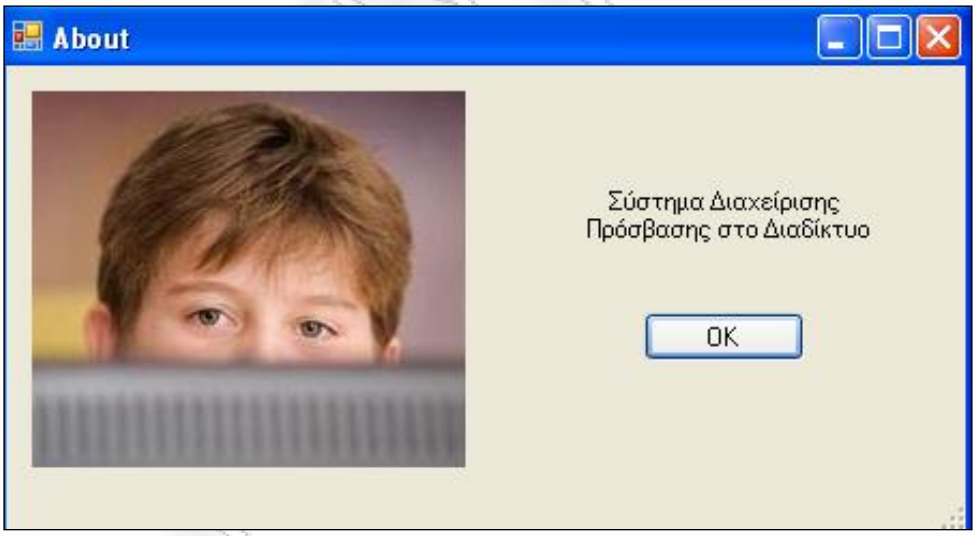


Εικόνα 4



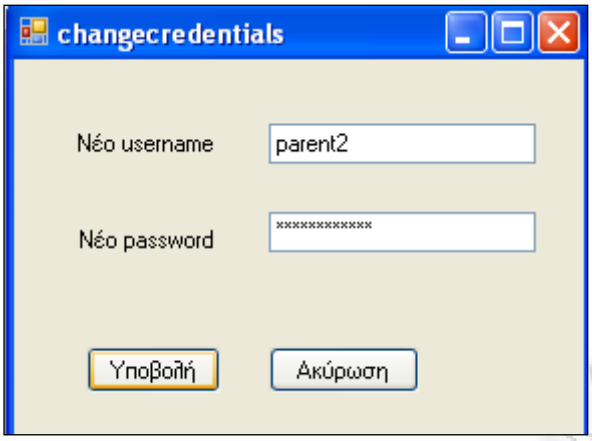
Εικόνα 5

Αν επιλέξουμε Βοήθεια → Σχετικά με το πρόγραμμα... τότε θα εμφανιστεί το κλασσικό «About…» που φαίνεται στην επόμενη εικόνα.



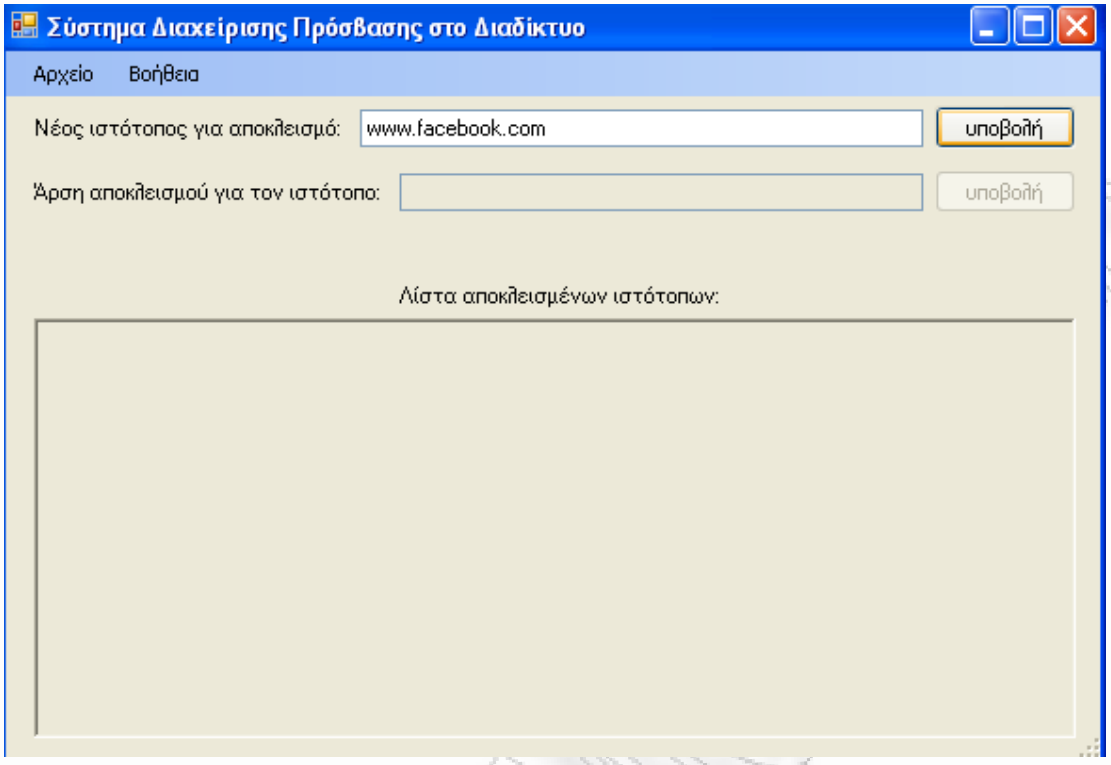
Εικόνα 6

Αν επιλέξουμε Αρχείο→ Αλλαγή στοιχείων, θα εμφανιστεί μια φόρμα όπου ο χρήστης μπορεί να εισάγει ένα νέο όνομα χρήστη και κωδικό. Η διαδικασία φαίνεται στην παρακάτω εικόνα.

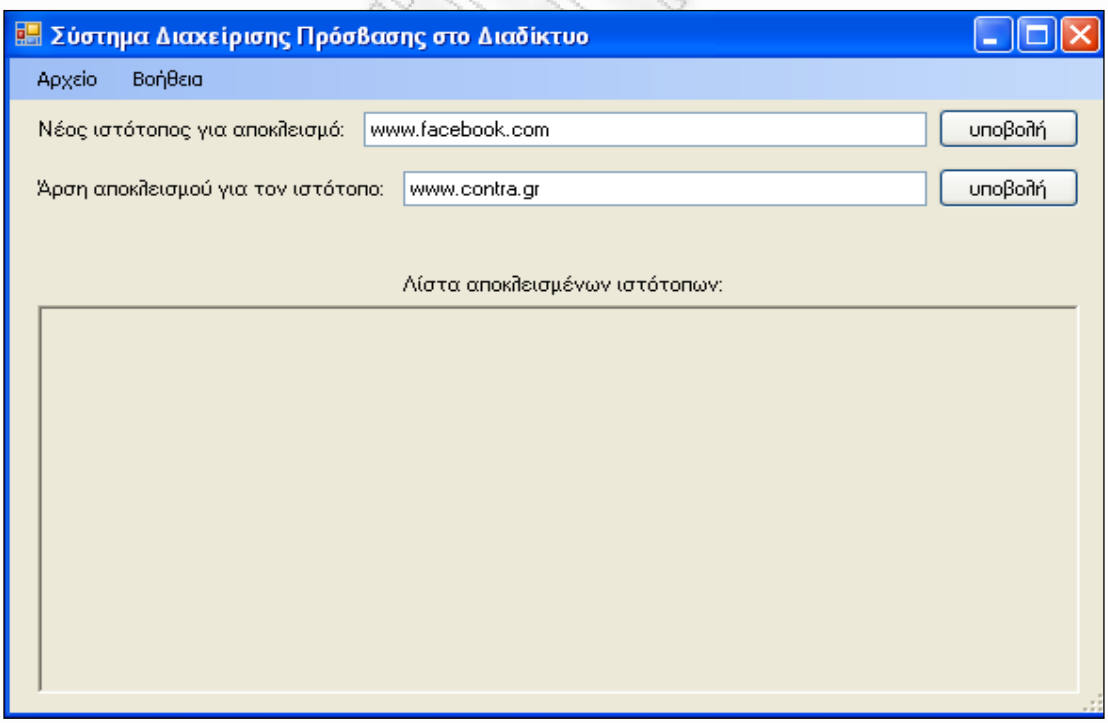


Εικόνα 7

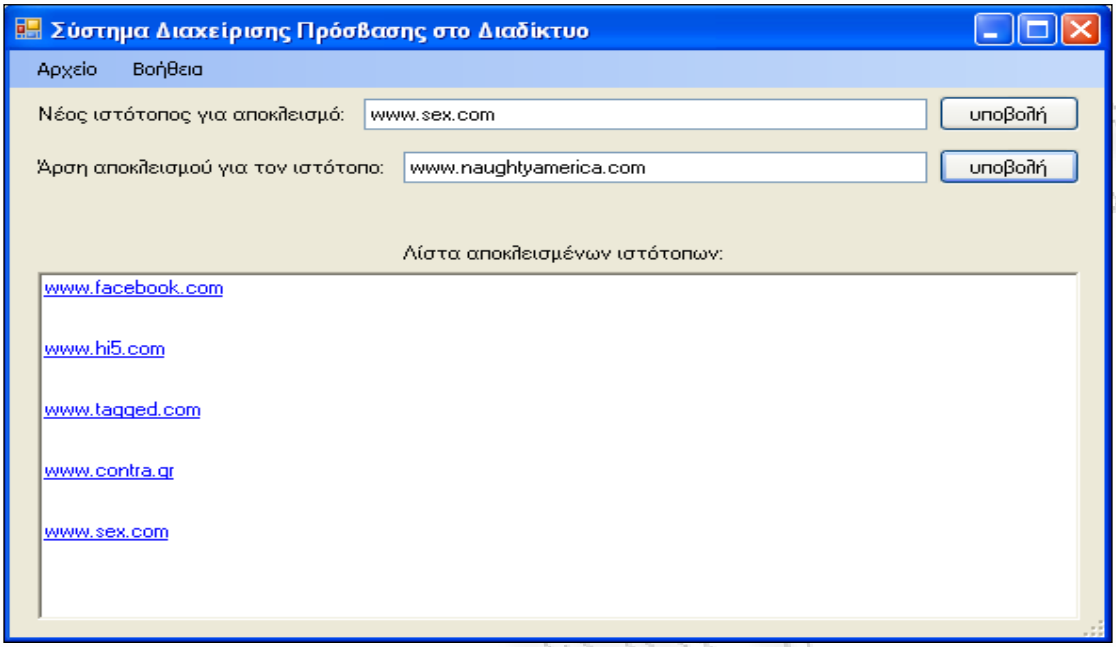
Αν επιλέξουμε Αρχείο → Προσθήκη ιστότοπου, τότε θα ενεργοποιηθεί το αντίστοιχο textbox που μπορούμε να πληκτρολογήσουμε το «απαγορευμένο» URL, όπως φαίνεται παρακάτω. Το ίδιο ισχύει και για την επιλογή Αρχείο → Άρση αποκλεισμού.... και για την επιλογή Αρχείο → Προβολή λίστας...



Εικόνα 8



Εικόνα 9



Εικόνα 10

Τέλος μπορούμε να ζητήσουμε εκ νέου την έναρξη της υπηρεσίας ή την έξοδο από την εφαρμογή με τις αντίστοιχες επιλογές Αρχείο→εκκίνηση υπηρεσίας και Αρχείο → έξοδος.

6. SPAMMING

Spam είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Το Spam συχνά έχει την μορφή ενημερωτικών ή διαφημιστικών μηνυμάτων για προϊόντα ή υπηρεσίες τα οποία φθάνουν στο γραμματοκιβώτιο μας χωρίς να έχουμε ζητήσει την εν λόγω πληροφόρηση. Η αλληλογραφία αυτή λοιπόν μπορεί να χαρακτηριστεί ως **απρόκλητη** ή **ανεπιθύμητη αλληλογραφία,** δύο όρους που χρησιμοποιούμε για την απόδοση στη γλώσσα μας του όρου Spam. [39]

Το spamming ή ανεπιθύμητη αλληλογραφία, αποτελείται από e-mail που στέλνονται ταυτόχρονα μέσω συστημάτων σε χιλιάδες διευθύνσεις μαζί. Κύριο μέλημα των spammers είναι να βρουν όσο το δυνατόν περισσότερες διευθύνσεις e-mail μπορούν και γι' αυτόν το λόγο χρησιμοποιούν ειδικά προγράμματα που σαρώνουν το διαδίκτυο και αναζητούν διευθύνσεις λογαριασμών ηλεκτρονικής αλληλογραφίας. Η εξέλιξη της τεχνολογίας βοηθάει στην παραγωγή τέτοιων προγραμμάτων αναζήτησης, διευκολύνοντας έτσι τους spammers να συλλέγουν και να αποθηκεύουν σε τεράστιες λίστες διευθύνσεις e-mail τις οποίες θα χρησιμοποιήσουν για τους δικούς τους σκοπούς. Εκτός από τα προγράμματα αναζήτησης διευθύνσεων υπάρχουν και άλλα πιο εξελιγμένα τα οποία μπορούν να μαντεύουν ηλεκτρονικές διευθύνσεις e-mail, είτε βασιζόμενοι σε domain names, είτε σε εφαρμογές που χρησιμοποιούν προγράμματα λεξικών. Συμπλήρωση μιας μεγάλης λίστας από διευθύνσεις e-mail αποτελεί και την πιο δύσκολη δουλειά για έναν spammer. Γι' αυτό το λόγο τέτοιες λίστες πωλούνται και σε άλλους επαγγελματίες του χώρου.

Το περιεχόμενο αυτών των μηνυμάτων e-mail που απαρτίζουν το spamming είναι από μόνο του ελκυστικό. Έτσι πολλές φορές ειδικά οι αρχάριοι και μη ενημερωμένοι σχετικά με τους κινδύνους χρήστες του διαδικτύου, πέφτουν θύματα αυτού. Έτσι λοιπόν, κάθε χρήστης του διαδικτύου και του ηλεκτρονικού ταχυδρομείου θα πρέπει να είναι ιδιαίτερα επιφυλακτικός με τέτοιου είδους μηνύματα.

[39] *http://en.wikipedia.org/wiki/Spam_%28electronic%29*

Ας δούμε τώρα ποια είναι τα κυριότερα σημεία που χαρακτηρίζουν το spamming. Πρώτα απ' όλα το spamming είναι απρόκλητο υπό την έννοια ότι δεν υπάρχει κάποια σχέση μεταξύ αποστολέα και παραλήπτη που θα μπορούσε να προκαλέσει αυτήν την επικοινωνία. Αυτήν την απρόκλητη επικοινωνία την εκβιάζει ο αποστολέας-spammer. Δεύτερο χαρακτηριστικό είναι ότι το spamming είναι εμπορικό, αφού τις περισσότερες φορές τα μηνύματα αυτά αποσκοπούν στην προβολή και διαφήμιση προϊόντων και υπηρεσιών με σκοπό την προσέλκυση πελατών και την πραγματοποίηση πωλήσεων. Και τρίτων, το spamming είναι μαζικό αφού εξ' ορισμού το spamming είναι η μαζική αποστολή μηνυμάτων από τον αποστολέα-spammer σε πολλούς παραλήπτες μαζί.

6.1 ΕΙΔΗ ΗΛΕΚΤΡΟΝΙΚΟΥ SPAMMING

- **ΔΙΑΦΗΜΙΣΗ**

Τα e-mail που περιέχουν διαφημιστικό περιεχόμενο είναι η πιο συνηθισμένη μορφή του spamming. Τα εν λόγω spamming e-mail επίσημα ονομάζονται "μη ζητηθείσα εμπορική επικοινωνία" (unsolicited e-mail). Αρκετά συχνά τα εισερχόμενα μηνύματα του λογαριασμού ηλεκτρονικού ταχυδρομείου μας είναι γεμάτα από e-mail που διαφημίζουν προϊόντα, ιστοσελίδες και υπηρεσίες, γεγονός που είναι αρκετά ενοχλητικό. Σύμφωνα με το νόμο 2774/1999, η μη ζητηθείσα εμπορική αλληλογραφία κρίνεται παράνομη και πιο συγκεκριμένα το άρθρο 9 του νόμου 2774/1999 περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα αναφέρει: *Η με οποιοδήποτε τηλεπικοινωνιακό μέσο απ' ευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών επιτρέπεται μόνον στην περίπτωση συνδρομητών, οι οποίοι έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους.* [40]

Σύμφωνα με αυτόν τον νόμο η τακτική που ακολουθείται από μερικές επιχειρήσεις που προσπαθούν να διαφημίσουν και να πουλήσουν τα προϊόντα τους με χρήση του spamming, είναι παράνομη και θα έπρεπε να τιμωρείται. Έτσι λοιπόν, θα πρέπει να είμαστε ιδιαίτερα προσεκτικοί για το που δίνουμε τα προσωπικά μας στοιχεία, διότι σε πολλές περιπτώσεις εταιρείες προωθούν αυτά τα στοιχεία έναντι αμοιβής και σε άλλες επιχειρήσεις οι οποίες με τη σειρά τους χρησιμοποιούν το spamming για την προώθηση των προϊόντων τους.

[40] *www.sch.gr/.../about**Spam**/index.php*

- **ΔΙΑΔΟΣΗ ΒΛΑΒΕΡΟΥ ΛΟΓΙΣΜΙΚΟΥ**

Ένα είδος του ηλεκτρονικού spam είναι και η μετάδοση ιών. Η τακτική που ακολουθούν σε αυτήν την περίπτωση οι ηλεκτρονικοί εγκληματίες, είναι η αποστολή e-mail που περιέχουν συνημμένα αρχεία, τα οποία περιέχουν ιούς και προγράμματα με βλαβερό κώδικα. Συνηθισμένη είναι και η περίπτωση που όταν λάβει κάποιος χρήστης ένα τέτοιο συνημμένο αρχείο και το ανοίξει, εκτός από το δικό του λογισμικό θα διαδώσει τον ιό και σε όλες τις επαφές ηλεκτρονικού ταχυδρομείου που έχει αποθηκευμένα στο λογαριασμό του. Γι' αυτό το λόγο η συμβουλή "μην ανοίγετε συνημμένα από άγνωστους αποστολείς" πρέπει να τηρείται κατά γράμμα.

- **ΕΞΑΚΡΙΒΩΣΗ E-MAIL**

Μια συνήθης τακτική που ακολουθούν οι spammer, είναι η αποστολή e-mail που περιέχουν ένα ειδικό πρόγραμμα το οποίο καταλαβαίνει εάν είναι ενεργός ο λογαριασμός ηλεκτρονικού ταχυδρομείου στον οποίο έχει σταλθεί. Στην περίπτωση που καταλάβουν ότι ο λογαριασμός είναι ενεργός, τότε συνεχίζουν να το βομβαρδίζουν με spam-email και συμπληρώνουν τη λίστα με τις διευθύνσεις e-mail.

- **ΑΠΑΤΗ**

Οι ηλεκτρονικοί εγκληματίες χρησιμοποιούν το spamming για την εξαπάτηση των χρηστών. Ο ηλεκτρονικός εγκληματίας στέλνει spam-email που δείχνουν να προέρχονται από γνωστές εταιρίες αφού περιέχουν λογότυπα, επίσημα κείμενα με σκοπό να καταφέρει να αποσπάσει από το χρήστη τον αριθμό του προσωπικού του λογαριασμού. Συνήθως οι hacker επικαλούνται εταιρίες όπως τράπεζες ή ηλεκτρονικά καταστήματα, προκειμένου ο χρήστης να πειστεί να εισάγει τα στοιχεία του. Βεβαίως όσοι δεν καταλαβαίνουν ότι πρόκειται περί απάτης, βλέπουν τα χρήματα τους να κάνουν φτερά μέσα από τους λογαριασμούς τους.

- **ΦΑΡΣΑ**

Πολλοί επιτήδειοι χρησιμοποιούν τα spam-email προκειμένου να διαδώσουν μια φήμη που σκοπό θα έχει να τρομοκρατήσει τους χρήστες του διαδικτύου. Μάλιστα σε αυτά τα email παρακινούν τους παραλήπτες να τα στείλουν και αυτοί με τη σειρά τους σε άλλους, δίνοντας έτσι μεγαλύτερη διάσταση στη φάρσα τους. Τέτοιες φάρσες συχνά στέλνονται μέσω των messengers με σκοπό να σπείρουν τον τρόμο ανάμεσα στους χρήστες.

- **ΠΡΟΣΗΛΙΤΙΣΜΟΣ**

Πολλά spam-email έχουν σαν στόχο τη διάδοση μιας ρατσιστικής ακραίας ή θρησκευτικού περιεχομένου ιδεολογίας. Έτσι, αυτή η μορφή του spamming αποτελεί κίνδυνο για τις κοινωνικές σχέσεις και αντιλήψεις.

- **FLOODING**

Στόχος αυτής της μορφής spamming είναι να πλημυρίσει τους λογαριασμούς ηλεκτρονικού ταχυδρομείου με κενά email. Με αυτόν τον τρόπο οι spammer καταφέρνουν να παραλείψουν ένα δίκτυο ή ένα email provider.

6.2 ΙΣΤΟΡΙΑ ΤΟΥ SPAM ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το 1978, παρουσιάστηκε η πρώτη μορφή τεκμηριωμένου “spam”. Ήταν ένα μήνυμα που διαφήμιζε τη διαθεσιμότητα ενός νέου μοντέλου υπολογιστών του Digital Equipment Corporation που εστάλη σε 393 παραλήπτες στις Η.Π.Α. στο ARPANET, παρόλο που δεν του είχε αποδοθεί ο χαρακτηρισμός “spam”. [41]

Το 1988, εστάλη το πρώτο γνωστό “chain letter” με τίτλο “Make Money Fast”. Πολλαπλά ηλεκτρονικά μηνύματα αποστέλλονταν από τους συμμετέχοντες παιχνιδιών πολλαπλών παικτών (multi-user games) σαν φάρσα προκειμένου να γεμίσουν τους λογαριασμούς των αντιπάλων με αυτά τα ανεπιθύμητα μηνύματα.

Το 1994, πραγματοποιήθηκε το πρώτο εμπορικό spam. Ένα ζευγάρι δικηγόρων χρησιμοποίησε τη μαζική αποστολή μηνυμάτων USENET για να διαφημίσει της υπηρεσίες του νόμου μετανάστευσης. Το γεγονός παραμένει γνωστό ως “Green Card Spam”.

[41] www.sansimera.gr/articles/440

Το 1994, επίσης, το spam λειτουργεί κάτω από το κωδικό όνομα “Serdar Argic”, όπου το περιεχόμενο των μηνυμάτων που αποστέλλονταν, αφορούσε στην άρνηση της αρμένικης γενοκτονίας, όποτε γίνονταν η αναζήτηση της λέξης “Τουρκία”. Μέσα σε μερικά χρόνια και μέχρι σήμερα, το spamming εστιάζεται στην ηλεκτρονική αλληλογραφία (e-mails).

6.3 ΝΟΜΟΣ ΥΠ’ ΑΡΙΘΜ. 2251/1994

Ο Νόμος 2251 του 1994 αποτελεί τον πιο σημαντικό νόμο που ρυθμίζει ζητήματα **προστασίας του καταναλωτή**. Περιέχει ορισμούς των εννοιών του καταναλωτή, του προμηθευτή, της σύμβασης από απόσταση και άλλων. Για την περίπτωση του spam ενδιαφέρον παρουσιάζει το άρθρο 9 και πιο συγκεκριμένα οι παράγραφοι: 10, 11, 12 και 13. [42]

Άρθρο 9 (Διαφήμιση)

Παράγραφος 10. Η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή μέσω τηλεφώνου, τηλεομοιοτυπίας (φαξ), ηλεκτρονικού ταχυδρομείου, αυτόματης κλήσης ή άλλου ηλεκτρονικού μέσου επικοινωνίας επιτρέπεται μόνο αν συναινεί ρητά ο καταναλωτής.

Παράγραφος 11. Ανεξάρτητα από τον περιορισμό της προηγούμενης παραγράφου, η μετάδοση διαφημιστικού μηνύματος απευθείας στον καταναλωτή με οποιονδήποτε τρόπο άμεσης επικοινωνίας (άμεση διαφήμιση) επιτρέπεται μόνο αν ο προμηθευτής ή άλλος για λογαριασμό του προμηθευτή κάνει χρήση στοιχείων ή πληροφοριών προσωπικού χαρακτήρα του καταναλωτή που περιήλθαν σε γνώση του από τις προηγούμενες συναλλακτικές σχέσεις του με τον καταναλωτή, από γενικά προσιτές πηγές, όπως κατάλογο ή άλλα δημοσιευμένα στοιχεία, ή από άλλο φυσικό ή νομικό πρόσωπο, εφόσον ο καταναλωτής εγκρίνει ρητά τη μεταβίβαση των προσωπικών του στοιχείων για το σκοπό της άμεσης διαφήμισης. Ο διαφημιστής είναι υποχρεωμένος να αναφέρει στον καταναλωτή τον τρόπο με τον οποίο περιήλθαν σε γνώση του τα προσωπικά στοιχεία του καταναλωτή.

Παράγραφος 12. Στις περιπτώσεις των παραγράφων 10 και 11, ο προμηθευτής οφείλει να διακόψει κάθε μορφή άμεσης διαφήμισης και να διαγράψει τα προσωπικά στοιχεία του καταναλωτή, εφόσον το ζητήσει ο καταναλωτής.

[42] Ο Νόμος 2251 του 1994 αποτελεί τον πιο σημαντικό νόμο που ρυθμίζει ζητήματα **προστασίας του καταναλωτή**

Παράγραφος 13. Η άμεση διαφήμιση θα πρέπει να γίνεται με τρόπο που να μην προσβάλλει την ιδιωτική ζωή του καταναλωτή.

6.4 ΟΔΗΓΙΑ 2002/58 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (12-7-2002)

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). [43]

Άρθρο 13

Αυτόκλητες κλήσεις

- Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), φαξ ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνο στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους.
- Παρά την παράγραφο 1, αν ένα φυσικό ή νομικό πρόσωπο αποκτά από τους πελάτες του στοιχεία επαφής του ηλεκτρονικού ταχυδρομείου τους στο πλαίσιο της πώλησης ενός προϊόντος ή μιας υπηρεσίας, σύμφωνα με την οδηγία 95/46/ΕΚ, μπορεί να χρησιμοποιεί τα εν λόγω στοιχεία για την απευθείας εμπορική προώθηση των δικών του παρόμοιων προϊόντων ή υπηρεσιών, υπό την προϋπόθεση ότι οι πελάτες του έχουν σαφώς και ευδιάκριτα την ευκαιρία να αντιτάσσονται, δωρεάν και εύκολα, σε αυτή τη συλλογή και χρησιμοποίηση ηλεκτρονικών στοιχείων επαφής, και αυτό με κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει με αυτή τη χρήση.

  Τα κράτη μέλη λαμβάνουν τα ενδεδειγμένα μέτρα προκειμένου να εξασφαλίζεται, ατελώς, ότι οι αυτόκλητες κλήσεις με σκοπό την

[43] ΟΔΗΓΙΑ 2002/58 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (12-7-2002)

απευθείας εμπορική προώθηση, σε άλλες, εκτός των προβλεπόμενων στις παραγράφους 1 και 2, περιπτώσεις, δεν επιτρέπονται χωρίς τη συγκατάθεση των ενδιαφερομένων συνδρομητών ή όταν πρόκειται για συνδρομητές οι οποίοι δεν επιθυμούν να λαμβάνουν αυτές τις κλήσεις. Η σχετική επιλογή καθορίζεται από την εθνική μονοθεσία.

- Εν πάση περιπτώσει, απαγορεύεται η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την άμεση εμπορική προώθηση, τα οποία συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, ή δίχως έγκυρη διεύθυνση στην οποία ο αποδέκτης να μπορεί να ζητεί τον τερματισμό της επικοινωνίας αυτής.
- Οι παράγραφοι 1 και 3 ισχύουν για τους συνδρομητές που είναι φυσικά πρόσωπα. Τα κράτη μέλη εξασφαλίζουν επίσης, στο πλαίσιο του κοινοτικού δικαίου και της εφαρμοστέας εθνικής νομοθεσίας, ότι προστατεύονται επαρκώς τα έννομα συμφέροντα των συνδρομητών που δεν είναι φυσικά πρόσωπα σε ό, τι αφορά τις αυτόκλητες κλήσεις.

6.5 ΔΕΚΑ ΤΡΟΠΟΙ ΝΑ ΑΠΟΦΥΓΕΤΕ ΤΟ SPAM:

- Χρησιμοποιήστε το λιγότερο 2 ηλεκτρονικές διευθύνσεις (e-mail). Την μία θα πρέπει να την χρησιμοποιείτε αποκλειστικά και μόνο για την προσωπική σας αλληλογραφία, ενώ την δεύτερη (κοινόχρηστη) θα μπορείτε να την χρησιμοποιείτε σε δημόσια προσβάσιμες εφαρμογές, όπως για παράδειγμα καταχώρηση στοιχείων σε ομάδες συζητήσεων (forums), χώρους συζητήσεων (chat rooms), εγγραφές σε λίστες αλληλογραφίας κτλ. [44]

[44] *http://noc.chania.teicrete.gr/index.php?Itemid=52&id=14&option=com_content&task=view*

- Μην δημοσιεύετε ποτέ το προσωπικό σας e-mail σε δημόσια προσβάσιμες εφαρμογές.
- Χρησιμοποιείστε ως προσωπική σας διεύθυνση ένα συνδυασμό από το όνομα και το επίθετο σας αντί για απλά ονόματα που περιέχονται σε λεξικά π.χ. bill, mary. Οι αποστολείς spam χρησιμοποιούν συνδυασμούς ονομάτων, λέξεων και αριθμών για να δημιουργήσουν πιθανές διευθύνσεις.
- Αν πρέπει οπωσδήποτε να κοινοποιήσετε το προσωπικό σας e-mail ηλεκτρονικά, καμουφλάρετε το, ώστε να δυσκολέψετε το έργο των spammers. Για παράδειγμα το Joe.Smith@yahoo.com, είναι εύκολο να βρεθεί από τις ειδικές μηχανές αναζήτησης (robots), όπως εύκολο είναι και το Joe.Smith at yahoo.com. Δοκιμάστε να το γράψετε Joe-dot-Smith-at-yahoo-dot-com. Επίσης αν πρέπει απαραίτητα να δημοσιεύσετε το προσωπικό σας e-mail σε κάποια ιστοσελίδα (το οποίο δεν συστήνεται), κάντε το ως αρχείο γραφικών ή εικόνα και όχι link.
- Αντιμετωπίστε το «κοινόχρηστο» e-mail σας, ως προσωρινό. Οι πιθανότητες οι spammers να το βρουν είναι μεγάλες, συνεπώς μην διστάζετε να το αλλάζετε συχνά.
- Να χρησιμοποιείτε πάντα το «κοινόχρηστο» e-mail για την καταχώρηση στοιχείων σε ομάδες συζητήσεων, χώρους συζητήσεων, για εγγραφή σε λίστες αλληλογραφίας. Επίσης θα μπορούσατε να χρησιμοποιείτε πολλές διαφορετικές «δημόσιες» (κοινόχρηστες) διευθύνσεις, ώστε να εντοπίσετε ποιες υπηρεσίες/ οργανισμοί, πωλούν διευθύνσεις σε spammers.
- Μην απαντάτε ποτέ σε μηνύματα spam. Οι περισσότεροι spammers επαληθεύουν με τον τρόπο αυτό την λήψη της αλληλογραφίας και άρα την ύπαρξη της συγκεκριμένης διεύθυνσης e-mail. Όσο περισσότερο απαντάτε, τόσο περισσότερη ανεπιθύμητη αλληλογραφία θα λαμβάνετε.
- Μην επισκέπτεστε συνδέσμους με σκοπό την διαγραφή σας από μία λίστα στην οποία δεν θέλετε να ανήκετε, από ύποπτες/ αμφισβητήσιμες πηγές. Οι spammers στέλνουν τέτοια παραπλανητική αλληλογραφία, σε μία προσπάθεια να συλλέξουν ενεργές διευθύνσεις. Αν η διεύθυνση σας χαρακτηριστεί ως «ενεργή», θα αυξηθεί ο αριθμός των ανεπιθύμητων e-mail που λαμβάνετε.
- Αν αντιληφθείτε πως το e-mail σας είναι γνωστό σε spammers, αλλάξτε το. Μπορεί να είναι άβολο/δύσκολο, αλλά είναι ένας τρόπος για να αποφύγετε το spam- έστω και για λίγο διάστημα.

- Σιγουρευτείτε ότι το e-mail σας, φιλτράρεται από κατάλληλο λογισμικό anti-spam. Μπορείτε επίσης να εγκαταστήσετε στον υπολογιστή σας, κάποιο λογισμικό προστασίας από spam.

7. Firewalls

Γενικά η λέξη firewall αποδίδεται σε πυρίμαχους τοίχους που εμποδίζουν την εξάπλωση της φωτιάς από δωμάτιο σε δωμάτιο ή μεταξύ διαμερισμάτων. Στην περίπτωση των δικτύων υπολογιστών, τα firewalls αποτελούν την αναγκαία λύση προστασίας τους, καθώς αυτά συνδέονται ολοένα και περισσότερο σε μεγαλύτερα δίκτυα τα οποία επίσης είναι συνδεμένα στο διαδίκτυο. Από τη στιγμή που ένα δίκτυο αποκτήσει σύνδεση στο Internet, ανοίγει ένα κανάλι αμφίδρομης επικοινωνίας: οι χρήστες του δικτύου, insiders, αποκτούν επαφή με τον έξω κόσμο, αλλά ταυτόχρονα και οι outsiders, δηλαδή οι εξωτερικοί χρήστες ως προς αυτό το δίκτυο, αποκτούν πλέον δυνατότητα πρόσβασης σε αυτό. Ο τρομακτικός ρυθμός αύξησης του διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά δίκτυα που συνδέονται μαζί του. Για τη προστασία τους από διάφορες εισβολές απαιτείται ένας κατάλληλος φράκτης. Ο φράκτης αυτός που καλείται firewall, πρέπει να είναι ικανός να επεξεργάζεται όλη τη κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet. Στην πραγματικότητα ένα σύστημα firewalll ανορθώνει ένα εξωτερικό τοίχο ασφάλειας, οριοθετώντας μια περίμετρο προστασίας. Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο-εσωτερικό δίκτυο ενός οργανισμού το οποίο θεωρείται ασφαλές και έμπιστο και στο εξωτερικό διαδίκτυο το οποίο θεωρείται μη ασφαλές και μη έμπιστο. Ο πρωταρχικός σκοπός των firewalll δηλαδή είναι να προστατεύσουν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντας τους τα δικαιώματα προσπέλασης σε αυτό, χωρίς να περιορίζουν την προσπέλαση στον εξωτερικό περιβάλλον. [45]

Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει την προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Έτσι ένα τυπικό σύστημα firewall μπορεί να επιτρέπει επιλεκτικά τη πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε ονόματα επικρατειών (domain names). Ο κύριος σκοπός του δηλαδή είναι να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευμένο περιβάλλον.

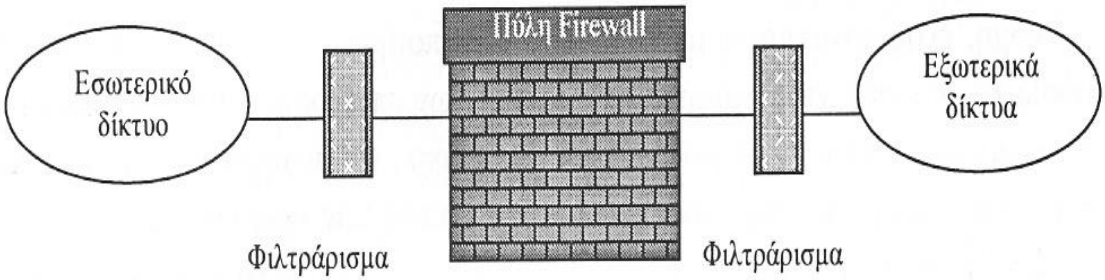
Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει τη κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή

[45] el.wikipedia.org/wiki/**Firewall**

τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της πολιτικής ελέγχου που υποστηρίζει και εξαρτάται από την συγκεκριμένη διαμόρφωσή του. Ένα σύστημα firewall δεν είναι απλά και μόνο ένας δρομολογητής, ένας διανομέας ή διακομιστής, ένας οικοδεσπότης ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, ώστε να αποτελούν αντικείμενο για παραπέρα εξέταση και καταγραφή από αυτό.

Μια τυπική διάταξη firewalls παρουσιάζεται στην ακόλουθη εικόνα:

Σχήμα 1.



.

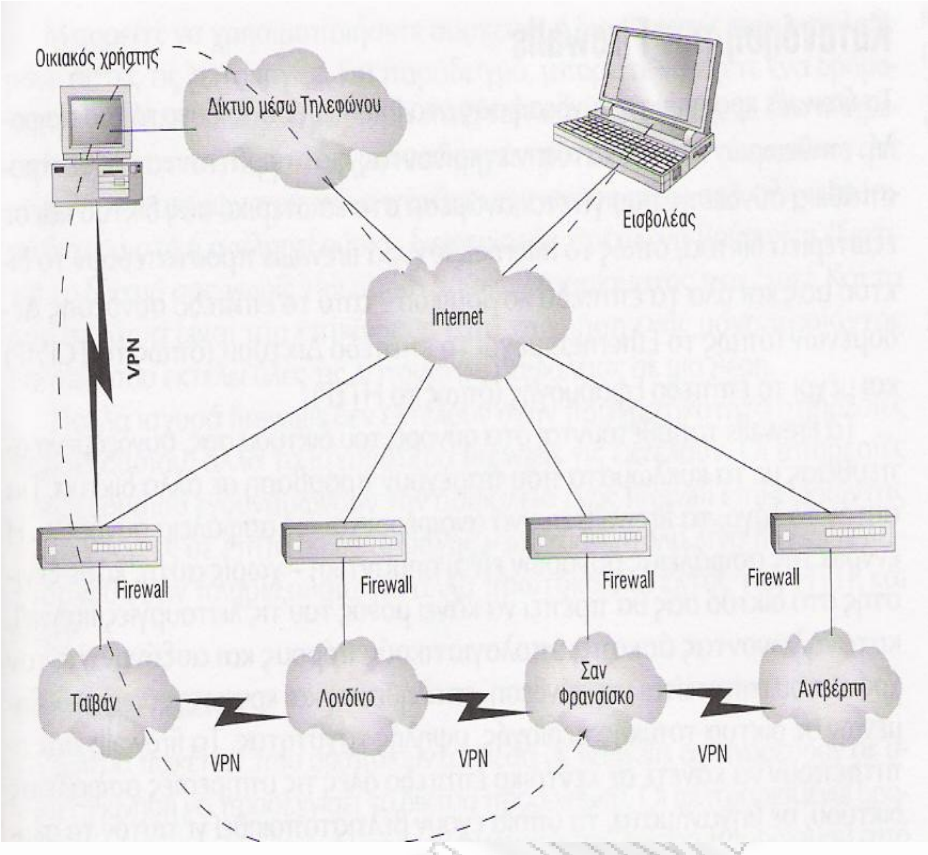
Τα firewalls κρατούν τη σύνδεση στο Internet όσο το δυνατό πιο ασφαλή, επιθεωρώντας και κατόπιν εγκρίνοντας ή απορρίπτοντας κάθε προσπάθεια σύνδεσης που γίνεται ανάμεσα στο εσωτερικό δίκτυο μιας εταιρείας και σε εξωτερικά δίκτυα, όπως το Internet. Ισχυρά firewalls προστατεύουν ένα δίκτυο υπολογιστών και όλα τα επίπεδα λογισμικού - από το επίπεδο σύνδεσης Δεδομένων όπως το Ethernet μέχρι το επίπεδο Δικτύου όπως το TCP/IP και μέχρι το επίπεδο Εφαρμογής όπως το HTTP. [46]

[46] www.go-online.gr

Τα firewalls τοποθετούνται στα σύνορα του δικτύου, συνδεόμενα απευθείας με τα κυκλώματα που παρέχουν πρόσβαση σε άλλα δίκτυα. Για αυτόν το λόγο, τα firewalls συχνά αναφέρονται ως ασφάλεια συνόρων. Η έννοια της ασφάλειας συνόρων είναι σημαντική αφού χωρίς αυτή, κάθε ξενιστής στο δίκτυο θα πρέπει να κάνει μόνος του τις λειτουργίες firewall, καταναλώνοντας άσκοπα υπολογιστικούς πόρους και αυξάνοντας τον χρόνο που απαιτείται για σύνδεση, επαλήθευση και κρυπτογράφηση δεδομένων σε δίκτυα τοπικής περιοχής, υψηλής ταχύτητας. Τα firewalls επιτρέπουν να γίνονται σε κεντρικό επίπεδο όλες τις υπηρεσίες ασφάλειας δικτύου, σε μηχανήματα, τα οποία έχουν βελτιστοποιηθεί γι' αυτόν το σκοπό και είναι αφοσιωμένα σε αυτήν την εργασία.

Από τη φύση τους, τα firewalls δημιουργούν συνωστισμούς ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο, όπως φαίνεται και από το Σχήμα 2. επειδή όλη η κίνηση που κινείται ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο πρέπει να περάσει από ένα μόνο σημείο ελέγχου. Αυτό είναι ένα μικρό τίμημα που πρέπει να πληρώσει κανείς για να έχει ασφάλεια. Εφόσον οι εξωτερικές συνδέσεις μισθωμένων γραμμών είναι σχετικά αργές σε σχέση με την ταχύτητα των σύγχρονων υπολογιστών, η υστέρηση που προκαλείται από τα firewalls μπορεί να είναι τελείως διαφανής.

Σχήμα 2. Τοποθέτηση Firewall πίσω από μηχανήματα με εκτεταμένη σύνδεση στο Διαδίκτυο



Καθώς τα τοπικά δίκτυα συνδέονται στο Internet, αποτελεί ζήτημα μεγάλης σημασίας η διασφάλιση της κανονικής λειτουργίας τους από τους νόμιμους και παράνομους χρήστες τους. Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο μιας επιχείρησης και το διαδίκτυο, παρέχει δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη σύνδεσή του με το διαδίκτυο, προστατεύοντας εκ μέρους της επιχείρησης τους πόρους της από φθορά, κατάχρηση, ή κλοπή, την υπόληψή της από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου της καθώς και την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του διαδικτύου από τους εργαζομένους της.

Ο πιο συνηθισμένος πάντως λόγος ύπαρξης ενός συστήματος firewall σε έναν οργανισμό ή μια επιχείρηση, είναι η παροχή ενός μηχανισμού ελέγχου προσπέλασης πρώτου επιπέδου, για τον Web Server. Ένα firewall πρέπει να ελέγχει και να καταγράφει την ροή των επικοινωνιών που διέρχονται μέσα από τον διακομιστή Web. Δηλαδή πρέπει να παρεμβάλλεται και να αποκόπτει όλη την κίνηση των δεδομένων ανάμεσα στον Web Server και το Internet. Έτσι είναι σε θέση να προστατεύει τα δεδομένα που δημοσιεύονται από ανεπιθύμητες

αλλαγές και να ελέγχει τη πρόσβαση στον διακομιστή Web, αποκλείοντας τους μη-εξουσιοδοτημένους χρήστες από ευαίσθητους πόρους του δικτύου.

Ακόμη, μια επιχείρηση μπορεί να χρησιμοποιήσει ένα firewall για να απομονώσει τις επικοινωνίες ανάμεσα στα δίκτυα των επιμέρους τμημάτων της. Για παράδειγμα ένα νοσοκομείο ενδεχομένως να θελήσει να διαχωρίσει το δίκτυο διακίνησης των δεδομένων των ασθενών από το δίκτυο των οικονομικών στοιχείων του. Ένα ή περισσότερα firewalls μπορούν να χρησιμοποιηθούν για να παρέχουν απομόνωση και ελεγχόμενη προσπέλαση ανάμεσα στα διάφορα μέρη ενός οργανισμού ή μιας επιχείρησης.

Ως ένα σύστημα firewall μπορεί να θεωρηθεί μια διάταξη δρομολόγησης, ένας προσωπικός υπολογιστής, ένας διακομιστής, ή ένα σύνολο από διακομιστές, διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία ή ένα υποδίκτυο από πρωτόκολλα και υπηρεσίες, όπως οι υπηρεσίες FTP, HTTP, e-mail, οι οποίες μπορούν να προσβληθούν από διακομιστές εκτός του υποδικτύου. Η συνηθισμένη θέση του είναι ως πύλη υψηλού επιπέδου ακριβώς στο σημείο σύνδεσης της επιχείρησης με το Internet.

Η εγκατάσταση επιπλέον συστημάτων firewall ως διαχωριστικά των επιμέρους τμημάτων μιας επιχείρησης, προσφέρει δυνατότητες διαχωρισμού των εξουσιοδοτήσεων που προσφέρονται στους εσωτερικούς χρήστες, λεπτομερέστερη επίβλεψή τους και γενικότερα υποστήριξη υπευθυνότητας με περισσότερη διακριτότητα. Με άλλα λόγια, παρέχει μέτρα προστασίας από τους νόμιμους και εσωτερικούς χρήστες του δικτύου, που σύμφωνα και με τις περισσότερες έρευνες αποτελούν τον σημαντικότερο κίνδυνο για την ασφάλεια μιας επιχείρησης.

7.1 Τεχνικές Ασφαλείας με Firewalls

Υπάρχουν τέσσερις βασικές τεχνικές προστασίας:

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

Μια ολοκληρωμένη υπηρεσία firewall συνήθως παρέχεται με συνδυασμό των παραπάνω βασικών τεχνικών φιλτραρίσματος.

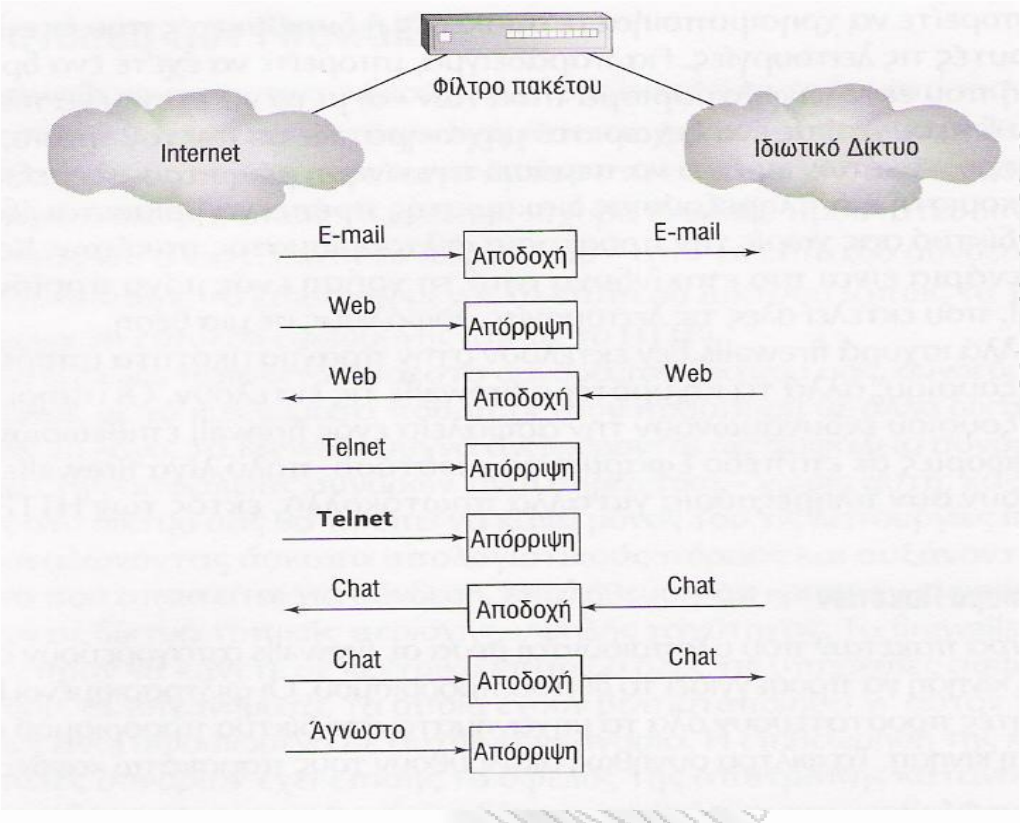
7.1.1 Πύλες Φιλτραρίσματος Πακέτων :

Οι πύλες φιλτραρίσματος πακέτων παρέχουν έναν εύκολο και φθηνό τρόπο υλοποίησης ενός βασικού επιπέδου φιλτραρίσματος με πραγματοποίηση ελέγχων των IP πακέτων ενός δικτύου. Ένα πακέτο είναι μια μικρή μονάδα επικοινωνίας, συνήθως μερικές εκατοντάδες bytes. Ένας δρομολογητής μπορεί να διοχετεύσει χιλιάδες πακέτα μέσα σε ένα δευτερόλεπτο. [47]

Αυτή η τεχνική φιλτραρίσματος είναι η πρώτη που εμφανίστηκε ως συνοδευτικό εργαλείο λογισμικού για τη υποστήριξη επιπλέον ρυθμίσεων στον αρχικά απλό εξοπλισμό των διατάξεων ή συσκευών δρομολόγησης που δεν είχαν δυνατότητες φιλτραρίσματος των πακέτων.

Σχήμα 3. Φιλτράρισμα Πακέτων

[47] www.webopedia.com



Το φίλτρο πακέτων όπως φαίνεται και στο Σχήμα 3. διενεργεί τον έλεγχο εφαρμόζοντας ένα σύνολο κανόνων οι οποίοι έχουν οριστεί από το διαχειριστή του firewall κατά τη διαμόρφωσή του και οι οποίοι υλοποιούν μια προαποφασισμένη πολιτική ασφάλειας. Κάθε κανόνας έχει δυο βασικά τμήματα το πεδίο της ενέργειας και το πεδίο των κριτηρίων επιλογής. Οι δυνατές ενέργειες είναι δύο, επιτρέπω ή σταματώ. Τα κριτήρια επιλογής των πακέτων για τα οποία θα ισχύσει η αντίστοιχη ενέργεια, βασίζονται στην διεύθυνση προέλευσης και προορισμού των πακέτων, στον αριθμό θυρίδας προέλευσης και προορισμού, στο πρωτόκολλο, αν είναι για παράδειγμα TCP (Transmission Control Protocol), ICMP (Internet Control Message Protocol) ή UDP (User Datagram Protocol) καθώς και στην κατεύθυνση, δηλαδή στο αν εισέρχεται το πακέτο στο ιδιωτικό δίκτυο ή αν εξέρχεται από αυτό. Η τεχνολογία φιλτραρίσματος πακέτων παρουσιάζει όμως και αρκετούς περιορισμούς:

- Ο έλεγχος που πραγματοποιείται, αφορά κυρίως το είδος της κυκλοφορίας του δικτύου, αφού εξετάζονται μόνο οι IP-επικεφαλίδες κάθε πακέτου. Εκεί υπάρχουν οι πληροφορίες δρομολόγησης όπως η προέλευση και ο προορισμός του κάθε πακέτου. Το περιεχόμενο του κάθε πακέτου δεν εξετάζεται, γι' αυτό και η τεχνολογία αυτή είναι κατάλληλη για απλές σχετικά πολιτικές ασφαλείας.
- Δεν προσφέρει επαρκείς μηχανισμούς επίβλεψης (auditing) και ειδοποίησης κινδύνου (alerting).
- Δεν υποστηρίζει εύκολη διαχείριση γιατί υπάρχει περιορισμένος αριθμός κανόνων οι οποίοι μάλιστα απαιτούν κατανόηση των ιδιαιτεροτήτων των πρωτοκόλλων επικοινωνίας. Έτσι είναι αρκετά σύνθετο και δύσκολο έργο η ορθή διαμόρφωσή τους για την εφαρμογή μιας πολιτικής ασφάλειας.
- Δεν διαθέτουν συνήθως μηχανισμούς αυθεντικοποίησης σε επίπεδο χρήστη (user level authentication).
- Δεν προστατεύουν από επιθέσεις πλαστογραφίας σε IP και DNS διευθύνσεις (IP & DNS address spoofing). Η βασική αδυναμία των μηχανισμών φιλτραρίσματος πακέτων είναι ότι στηρίζονται στις IP διευθύνσεις, οι οποίες όμως δεν είναι απόλυτα ασφαλείς γιατί συνήθως δεν προστατεύονται.

Σε γενικές γραμμές το επίπεδο ασφάλειας που προσφέρουν είναι χαμηλού επιπέδου. Από την άλλη μεριά πάλι, είναι απλοί, ταχύτατοι, ευέλικτοι και χαμηλού κόστους. Έτσι θεωρούνται ιδανικοί για περιβάλλοντα χαμηλής επικινδυνότητας. Βεβαίως οι υπηρεσίες που προσφέρουν είναι σημαντικότατες για αυτό και θεωρούνται αναπόσπαστο τμήμα ενός ολοκληρωμένου συστήματος firewall.

7.1.2 **Πύλες Κυκλωμάτων** :

Η χρήση των πυλών κυκλωμάτων σε διατάξεις firewalls αναβαθμίζει σημαντικά την ασφάλεια των δικτύων. Επιτρέπουν τη χρήση εφαρμογών που βασίζονται στα πρωτόκολλα επικοινωνίας TCP και UDP, όπως για παράδειγμα WWW και Telnet χωρίς να αφήνουν να γίνονται όλα σε επίπεδο πρωτοκόλλου επικοινωνίας.

Οι πύλες κυκλωμάτων λειτουργούν ως εκπρόσωποι των πρωτοκόλλων επικοινωνίας, μεταβιβάζοντας την δικτυακή κίνηση μεταξύ δυο υπολογιστών που

είναι συνδεδεμένοι μεταξύ τους μέσω ενός ιδεατού κυκλώματος του δικτύου. Ένας εσωτερικός χρήστης, για παράδειγμα, μπορεί να συνδέεται σε μια θύρα της πύλης η οποία στη συνέχεια μπορεί να συνδέεται σε μια άλλη θύρα ενός υπολογιστή που βρίσκεται σε ένα εξωτερικό δίκτυο. Η πύλη απλά αντιγράφει bytes από την μια θύρα στην άλλη. Κανονικά η πύλη μεταβιβάζει τα δεδομένα χωρίς να τα εξετάζει, αλλά συνήθως διατηρεί μια καταγραφή της ποσότητας των μεταβιβαζόμενων δεδομένων και του προορισμού τους. Σε μερικές περιπτώσεις η σύνδεση μεταβίβασης, η οποία με αυτό τον τρόπο διαμορφώνει τελικά ένα "κύκλωμα", λειτουργεί αυτόματα. Άλλες φορές πάλι, χρειάζεται να καθορισθεί στην πύλη η επιθυμητή θύρα προορισμού.

Ένα από τα μειονεκτήματα αυτών των συστημάτων είναι ότι οι εφαρμογές των πελατών πρέπει να μετατραπούν πριν να καταστούν έτοιμες για να λειτουργήσουν με μια συγκεκριμένη πύλη κυκλωμάτων.

7.1.3 **Πύλες Εφαρμογών** :

Οι πύλες κυκλωμάτων και οι πύλες εφαρμογών αναφέρονται και ως proxy servers, καθώς και οι δυο συμπεριφέροντε ως εκπρόσωποι του υποτιθέμενου πελάτη. Όμως οι πύλες εφαρμογών προχωρούν ακόμη παραπέρα, σε ότι αφορά την ασφάλεια των δικτύων. Λειτουργούν στο υψηλότερο στρώμα επικοινωνίας, γνωστό ως το επίπεδο εφαρμογής. Έτσι έχουν πρόσβαση σε περισσότερες πληροφορίες από ότι τα συστήματα με απλό φιλτράρισμα πακέτων και μπορούν να προγραμματιστούν πιο έξυπνα κάνοντάς τα ικανά να υποστηρίξουν σύνθετες πολιτικές ασφάλειας.

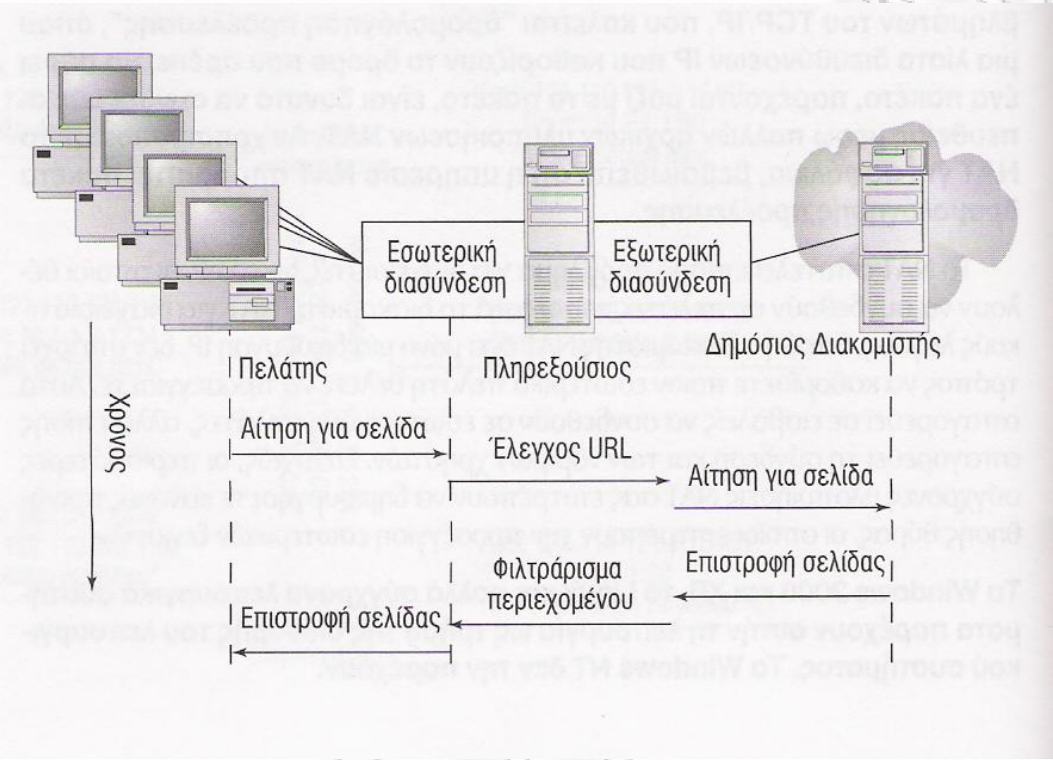
Όλα τα IP-πακέτα που φτάνουν ή που πρέπει να φύγουν, εξετάζονται πρώτα ως προς το περιεχόμενό τους και ανάλογα προωθούνται ή απορρίπτονται. Για το σκοπό αυτό χρησιμοποιούνται προγράμματα που εκτελούνται ως εφαρμογές, οι οποίες ονομάζονται proxies. Κάθε TCP/IP υπηρεσία που θέλουμε να ελέγχεται από το firewall, έχει το δικό της proxy, δηλαδή μια υπηρεσία διαμεσολαβητή. Για παράδειγμα, ένας χρήστης προερχόμενος από το Internet, για να αποκτήσει πρόσβαση στην υπηρεσία FTP ενός μηχανήματος του προστατευμένου δικτύου, θα πρέπει πρώτα να συνδεθεί με τη αντίστοιχη proxy εφαρμογή, να ακολουθήσει η αναγνώριση - πιστοποίησή του και στη συνέχεια, αν η πολιτική ασφάλειας του firewall περιέχει για το συγκεκριμένο και αναγνωρισμένο χρήστη τις κατάλληλες εξουσιοδοτήσεις, θα προωθηθεί η σύνδεση με την υπηρεσία FTP που ζήτησε.

Κάθε υπηρεσία proxy, είναι ένα λογισμικό δυο κατευθύνσεων που δρα ταυτόχρονα και σαν εξυπηρετητής και σαν πελάτης. Στους εσωτερικούς χρήστες απαντάει σαν να είναι η εξωτερική σύνδεση που ζήτησαν, ενώ στους εξωτερικούς χρήστες αποκρίνεται σαν να είναι η εσωτερική υπηρεσία που θα χρειαστούν.

Πρόκειται δηλαδή για Υπηρεσίες Πληρεξουσίου Οι πληρεξούσιοι επιπέδου εφαρμογής επιτρέπουν την πλήρη αποσύνδεση της ροής πρωτοκόλλων επιπέδου Δικτύου μέσω του firewall και τον περιορισμό της κίνησης μόνο σε πρωτόκολλα υψηλότερου επιπέδου, όπως τα HTTP για υπηρεσίες Web, FTP για αποστολή αρχείων και SMTP για e-mail. Όταν γίνεται μια σύνδεση μέσω ενός πληρεξουσίου διακομιστή, ο πληρεξούσιος διακομιστής δέχεται τη σύνδεση, εξάγει το πρωτόκολλο υψηλού επιπέδου, όπως το HTTP, τα εξετάζει και παίρνει αποφάσεις για το περιεχόμενό του με βάση την πολιτική ασφαλείας που έχει καθορίσει. Ο πληρεξούσιος διακομιστής δημιουργεί κατόπιν μια νέα σύνδεση TCP στη δημόσια διασύνδεση προς τον τελικό προορισμό και στέλνει το πρωτόκολλο υψηλού επιπέδου μέσω της νέας σύνδεσης. Επειδή τα πρωτόκολλα επιπέδου Εφαρμογής και επιπέδου Δικτύου αναπαράγονται πλήρως, επιθέσεις που βασίζονται σε λάθος διαμορφωμένα πακέτα TCP/IP σε λάθος διαμορφωμένα μηνύματα Web ή e-mail εξαλείφονται.

Οι πληρεξούσιοι συνδέουν δύο δίκτυα, τα οποία δεν συνδέονται μέσω δρομολογητών. Όταν ένας πελάτης στο προστατευμένο δίκτυο κάνει μια σύνδεση προς ένα διακομιστή στη δημόσια πλευρά, ο πληρεξούσιος δέχεται την αίτηση σύνδεσης και μετά κάνει τη σύνδεση για λογαριασμό του προστατευμένου πελάτη. Κατόπιν, ο πληρεξούσιος προωθεί την απάντηση από το δημόσιο διακομιστή προς το εσωτερικό δίκτυο. Το παρακάτω γραφικό παρουσιάζει τη διαδικασία αυτή με λεπτομέρειες.

Σχήμα 4: Πληρεξούσιοι Επιπέδου Εφαρμογής



Οι πληρεξούσιοι είναι καλά παραδείγματα του πώς ένα ενδιάμεσο σύστημα ανάμεσα στο δίκτυο μιας επιχείρησης και όχι μόνο, και σε ένα άλλο τελικό σύστημα μπορεί να κάνει κάθε είδος επεξεργασίας - με ή χωρίς την άδειά των διαχειριστών του δικτύου. Ένας κακόβουλος πληρεξούσιος κρυμμένος ανάμεσα σε έναν πελάτη και ένα διακομιστή μπορεί να κάνει μια επίθεση ενδιάμεσου.

Στην πραγματικότητα, δηλαδή, ένα τέτοιου τύπου firewall ή συστατικό ενός firewall, εκτελώντας ψευδοεφαρμογές, παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας προκειμένου να ελέγχει τη νομιμότητα των επικοινωνιών. Καμιά άλλη υπηρεσία δεν μπορεί απευθείας να στείλει ή να λάβει δεδομένα. Αυτός είναι άλλωστε και ο ρόλος του συστήματος firewall, να

λειτουργεί δηλαδή ως ένα ισχυρό τείχος ασφαλείας αλλά και ικανό να προσαρμόζεται εύκολα στις ανάγκες επικοινωνίας ενός δικτύου. Η τεχνολογία αυτή προσφέρει ολοκληρωμένη ασφάλεια με τους ισχυρούς μηχανισμούς αυθεντικοποίησης χρηστών και συστημάτων, καταγραφής και υποστήριξης υπευθυνότητας που διαθέτει.

7.1.4 Πύλες μετάφρασης διευθύνσεων Δικτύου:

(Network Address Translation-NAT)

Η Μετάφραση Διευθύνσεων Δικτύου επιτρέπει την πολύπλεξη μιας δημόσιας διεύθυνσης IP επάνω σε ένα ολόκληρο δίκτυο. Πολλές μικρές εταιρείες βασίζονται στις υπηρεσίες ενός παρόχου υπηρεσιών Internet, ο οποίος μπορεί να είναι απρόθυμος να παρέχει μεγάλα μπλοκ διευθύνσεων, επειδή και ο δικός του χώρος διευθύνσεων είναι περιορισμένος. Ίσως να υπάρχει όμως η ανάγκη κάποιος χρήστης να μοιραστεί μια μόνο διεύθυνση μέσω τηλεφωνικής κλήσης ή διεύθυνσης μέσω καλωδιακού μόντεμ, χωρίς να ενημερώσει για αυτό τον πάροχο υπηρεσιών. Αυτές οι επιλογές είναι δυνατές με τη χρήση Μετάφρασης Διευθύνσεων Δικτύου.

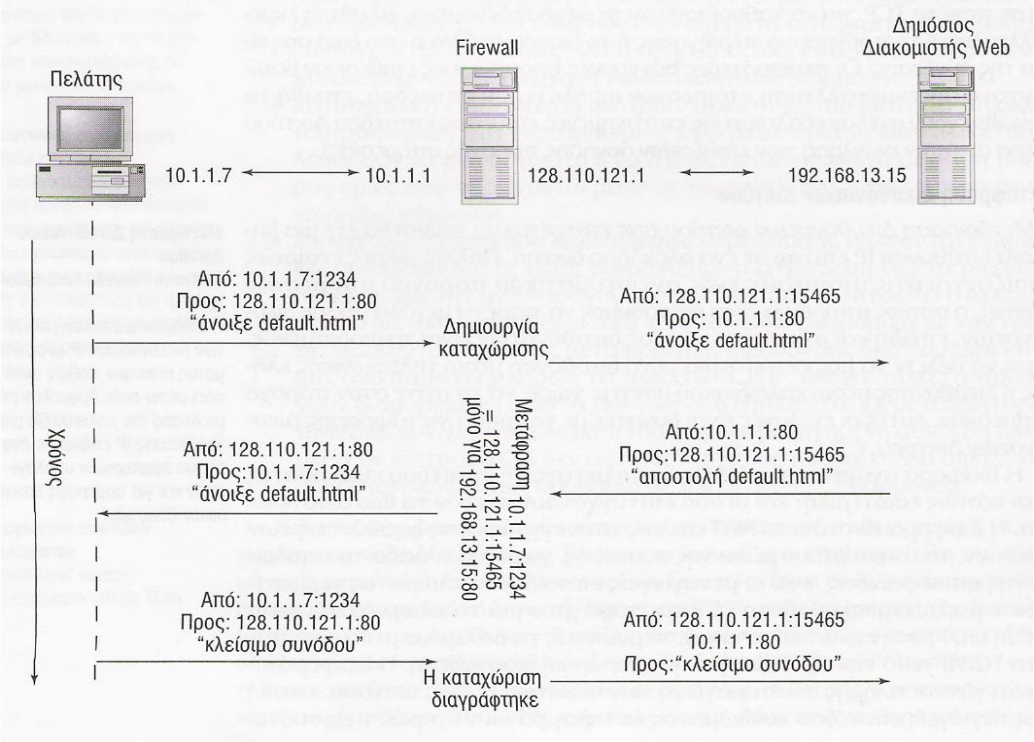
Η διαφορά ανάμεσα στο NAT και στη μεταγωγή επιπέδου κυκλώματος είναι κάπως εσωτερική και οι δύο επιτυγχάνουν σχεδόν το ίδιο αποτέλεσμα. Η διαφορά είναι ότι το NAT απλώς επανεγγράφει τις διευθύνσεις των πακέτων, τα οποία ρέουν μέσω της συσκευής, χωρίς να αλλάζει το υπόλοιπο της επικεφαλίδας, ενώ οι μεταγωγείς επιπέδου κυκλώματος τερματίζουν την εξωτερική σύνδεση TCP και παράγουν μια τελείως νέα σύνδεση TCP (ή UDP) στην ιδιωτική πλευρά, περνώντας τα δεδομένα μέσα στα πακέτα TCP/IP από την εξωτερική στην εσωτερική διασύνδεση. Η διαφορά είναι ότι γίνεται πλήρης αναπαραγωγή των πακέτων TCP/IP. Ωστόσο, επειδή οι μεταγωγείς επιπέδου κυκλώματος καταλαμβάνουν σαφώς περισσότερους πόρους για να κάνουν περίπου την ίδια λειτουργία, οι συσκευές NA T έχουν γίνει πιο δημοφιλείς. Οι μεταγωγείς επιπέδου κυκλώματος παραμένουν όμως πιο ασφαλείς, επειδή φράσσουν τις επιθέσεις λάθος διαμορφωμένων πακέτων, που μπορούν να ρέουν μέσω ενός NAT και δεν προσβάλλονται από επιθέσεις δρομολόγησης προέλευσης, οι οποίες μπορούν να ρέουν μέσω NAT, που δεν ελέγχουν για την ύπαρξή τους.

Το NAT αρχικά αναπτύχθηκε επειδή ήταν δύσκολο να πάρει ένας χρήστης και ακόμα περισσότερο μια επιχείρηση με κάποιο δίκτυο υπολογιστών, μεγάλα μπλοκ δημόσιων διευθύνσεων IP και τα δίκτυα συχνά εξαντλούσαν την εκχωρημένη τους δεξαμενή πριν να μπορέσουν να ζητήσουν περισσότερες διευθύνσεις από το InterNIC. Το InterNIC άρχισε να εξοικονομεί διευθύνσεις, όταν άρχισε η επανάσταση του Internet, επειδή η δεξαμενή των διαθέσιμων διευθύνσεων εξαντλήθηκε γρήγορα. Περιπλέκοντας μια μόνο δημόσια διεύθυνση με αρκετούς εσωτερικούς ξενιστές μέσα σε μια ιδιωτική περιοχή IP, μια εταιρεία μπορούσε να έχει μόνο μια δημόσια διεύθυνση IP.

Ευτυχώς, η Μετάφραση Διευθύνσεων Δικτύου λύνει επίσης το πρόβλημα της απόκρυψης εσωτερικών ξενιστών. Το NAT είναι στην πραγματικότητα ένας πληρεξούσιος επιπέδου Δικτύου: Στο Internet, φαίνεται ως ένας μόνο ξενιστής να κάνει αιτήσεις εκ μέρους όλων των εσωτερικών ξενιστών, και έτσι κρύβεται η ταυτότητα από το δημόσιο δίκτυο.

Το NAT κρύβει τις εσωτερικές διευθύνσεις IP, μετατρέποντας όλες τις εσωτερικές διευθύνσεις ξενιστών στη δημόσια διεύθυνση του firewall. Το firewall κατόπιν μεταφράζει τη διεύθυνση του εσωτερικού ξενιστή από την δική του διεύθυνση, χρησιμοποιώντας τον αριθμό θύρας TCP για να παρακολουθεί ποιες συνδέσεις στη δημόσια πλευρά αντιστοιχούν με ποιους ξενιστές στην ιδιωτική πλευρά. Για το Internet, όλη η κίνηση στο δίκτυο φαίνεται να προέρχεται από έναν εξαιρετικά απασχολημένο υπολογιστή.

Σχήμα 5 : Μετάφραση Διευθύνσεων Δικτύου



Το NAT στην ουσία κρύβει όλες τις πληροφορίες επιπέδου TCP/IP που αφορούν εσωτερικούς ξενιστές από αδιάκριτους μέσα στο Internet. Η μετάφραση διευθύνσεων επιτρέπει επίσης την χρησιμοποίηση οποιασδήποτε περιοχής διευθύνσεων IP θέλει ο διαχειριστής ενός εσωτερικού δίκτυο, ακόμη και αν αυτές οι διευθύνσεις χρησιμοποιούνται και κάπου αλλού μέσα στο Internet. Αυτό σημαίνει ότι μια επιχείρηση δεν χρειάζεται να πάρει ένα μεγάλο μπλοκ διευθύνσεων από το InterNIC ή να εκχωρήσει εκ νέου αριθμούς δικτύου που χρησιμοποιούσε πριν να συνδεθεί το δίκτυό της στο Internet.

Το μειονέκτημα είναι ότι το NAT υλοποιείται μόνο σε επίπεδο TCP/IP. Αυτό σημαίνει ότι πληροφορίες κρυμμένες μέσα στο ωφέλιμο φορτίο δεδομένων της κίνησης TCP/IP μπορούν να μεταδοθούν σε μια υπηρεσία υψηλότερου επιπέδου και να χρησιμοποιηθούν για να γίνει εκμετάλλευση αδυναμιών σε κίνηση υψηλότερου επιπέδου ή για επικοινωνία με ένα Δούρειο ίππο.

Τέλος, πολλά πρωτόκολλα περιλαμβάνουν επίσης τη διεύθυνση IP μέσα στο ωφέλιμο φορτίο δεδομένων, οπότε όταν ξαναγράφεται μια διεύθυνση, ενώ περνά μέσω του NAT, η διεύθυνση μέσα στο ωφέλιμο φορτίο δεν είναι πλέον έγκυρη. Αυτό συμβαίνει με FTP ενεργού τρόπου λειτουργίας και με σχεδόν κάθε άλλο πρωτόκολλο, που βασίζεται στον καθορισμό ενός δευτερεύοντος ρεύματος επικοινωνίας ανάμεσα στον πελάτη και στο διακομιστή. Επίσης δεν είναι δυνατό

να γίνει σύνδεση με έναν ξενιστή μέσα στο ιδιωτικό δίκτυο, επειδή δεν υπάρχει τρόπος να απευθυνθεί κάποιος σε ξενιστές απευθείας από το Internet. Οι περισσότερες υλοποιήσεις NAT επιλύουν αυτό το πρόβλημα για τα συγκεκριμένα πρωτόκολλα “κρατώντας ανοικτή την πόρτα” για τη διαδρομή επιστροφής των πρωτοκόλλων, για τα οποία γνωρίζουν ότι πρόκειται να επιστρέψουν, όπως συμβαίνει με το FTP. Επειδή η σύνδεση ξενιστή εξήλθε μέσω του μεταφραστή, γνωρίζει ότι πρέπει να περιμένει μια προσπάθεια επιστροφής σύνδεσης από αυτά τα πρωτόκολλα και γνωρίζει για ποιο εσωτερικό υπολογιστή θα μεταφράσει το κανάλι επιστροφής. Οπότε εφόσον μια συσκευή NAT γνωρίζει αυτά τα προβληματικά πρωτόκολλα, μπορεί να τα χειριστεί. Νέα πρωτόκολλα ή εφαρμογές μπορούν να έχουν προβλήματα υλοποίησης μέσω NAT γι' αυτόν το λόγο.

Χρησιμοποιώντας ένα απαρχαιωμένο χαρακτηριστικό αντιμετώπισης προβλημάτων του TCP/IP, που καλείται "δρομολόγηση προέλευσης", όπου μια λίστα διευθύνσεων IP που καθορίζουν το δρόμο που πρέπει να πάρει ένα πακέτο, παρέχονται μαζί με το πακέτο, είναι δυνατό να συνδεθεί κανείς απευθείας μέσω πολλών αρχικών υλοποιήσεων NAT.

Το NAT αποτελεί επίσης πρόβλημα για διαχειριστές δικτύων, οι οποίοι θέλουν να συνδεθούν σε πελάτες πίσω από το διακομιστή NAT για διαχειριστικούς λόγους. Επειδή ο διακομιστής NAT έχει μόνο μια διεύθυνση IP, δεν υπάρχει τρόπος να καθοριστεί ποιον εσωτερικό πελάτη θέλει κάθε φορά να προσεγγίσει. Αυτό απαγορεύει σε εισβολείς να συνδεθούν σε εσωτερικούς πελάτες, αλλά επίσης απαγορεύει τη σύνδεση και των νόμιμων χρηστών. Ευτυχώς, οι περισσότερες σύγχρονες υλοποιήσεις NAT επιτρέπουν την δημιουργία κανόνων προώθησης θύρας, οι οποίοι επιτρέπουν την προσέγγιση εσωτερικών ξενιστών.

Τα Windows 2000 και XP, το Unix και πολλά σύγχρονα λειτουργικά συστήματα παρέχουν αυτήν τη λειτουργία ως τμήμα της διανομής του λειτουργικού συστήματος. Τα Windows NT δεν την παρέχουν.

7.2 Σύγχρονες Τεχνολογίες Firewalls - Υβριδικές Πύλες

Είναι γενική αίσθηση των διαχειριστών firewalls, ότι για ολοκληρωμένη προστασία απαιτείται η συνδυασμένη δράση των τεχνολογιών επιπέδου πακέτων και επιπέδου εφαρμογής. Έτσι, παρατηρείται μια τάση υιοθέτησης της

σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστημάτων firewall για περιβάλλοντα μεσαίας έως υψηλής επικινδυνότητας.

Ο όρος υβριδικές ή σύνθετες πύλες χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα firewall που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών τύπων, προχωρούν ακόμη ένα βήμα παραπέρα. Δύο είναι οι σύγχρονες εναλλακτικές υλοποιήσεις, ο συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών και η τεχνολογία Stateful Inspection.

7.3 Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών:

Έχει ήδη τονιστεί ότι ο σχετικά πρωτόγονος έλεγχος αποκλειστικά των IP επικεφαλίδων, είναι μια λειτουργία που κάθε firewall χρειάζεται, γιατί σε αρκετές περιπτώσεις αυτός είναι ο πιο κατάλληλος και πιο γρήγορος τρόπος ελέγχου. Έτσι ακόμη και τα καθαρά proxy firewalls διαθέτουν λογισμικό που προσομοιώνει έναν δρομολογητή φιλτραρίσματος. Επειδή όμως αυξάνει κατά πολύ η ασφάλεια ενός συστήματος όταν δεν είναι συγκεντρωμένη η άμυνά του σε ένα μοναδικό σημείο, πολλές φορές ένα proxy-based σύστημα firewall συνδυάζεται με μια επιπλέον διάταξη φίλτρου πακέτων. Το υβριδικό αυτό σύστημα αποκτά παράλληλα ακόμη πιο γρήγορο και πιο αξιόπιστο φιλτράρισμα πακέτων, αφού είναι επιπέδου hardware. Η σύνδεσή τους πρέπει φυσικά να γίνει εν σειρά έτσι ώστε οι επικοινωνίες να διέρχονται και από τα δύο αυτά συστατικά μέρη του firewall.

7.4 Τεχνολογία Stateful Inspection:

Πρόκειται για μια νέα τεχνολογία, κατηγορίας packet filtering. Όμως εδώ επεκτείνεται το απλό IP φιλτράρισμα δίνοντας δυνατότητα να εξετάζεται το κάθε πακέτο στο εσωτερικό του και μάλιστα όχι το κάθε ένα ξεχωριστά και απομονωμένα αλλά ο έλεγχος να γίνεται σε σχέση με προηγούμενες επικοινωνίες. Δημιουργείται δηλαδή μια εσωτερική βάση δεδομένων με πληροφορίες προηγούμενων πακέτων που συνεχώς ενημερώνεται. Με αυτό τον τρόπο είναι δυνατόν να καταγράφονται πληροφορίες κατάστασης και συναφείς πληροφορίες για κάθε επικοινωνία, οπότε, από τον έλεγχό τους και με συνεχή τροφοδοσία από την εξελισσόμενη βάση δεδομένων, επιτρέπεται ή απαγορεύεται μια επικοινωνία με δυναμικό τρόπο.

Ο χώρος δράσης ενός τέτοιου «έξυπνου» firewall εκτείνεται και στα χαμηλά επίπεδα δικτυακής επικοινωνίας, όπου φιλτράρονται τα πακέτα, αλλά και στο επίπεδο εφαρμογής. Σε αυτό το επίπεδο γίνεται η διαχείριση και ο καθορισμός της πολιτικής ασφαλείας μέσω πάλι υπηρεσιών proxy, διαφορετικής όμως κατασκευής από τα firewalls τύπου application gateway. Αυτός ο συνδυασμός δράσης υπερέχει σημαντικά έναντι των υπολοίπων, αφού συγκεντρώνει όλα τα πλεονεκτήματα των δυο βασικών τεχνολογιών. Όπως και στα προηγούμενου τύπου firewalls, η εγκατάσταση μιας ξεχωριστής διάταξης δρομολόγησης έχει νόημα μόνο ως κίνηση διασποράς των σημείων αμύνης.

7.5 Αρχιτεκτονικές Συστημάτων Firewalls

Ένα ολοκληρωμένο σύστημα firewall μπορεί να αποτελείται από αρκετά συστατικά, χωρίς να είναι και όλα απαραίτητα. Πέντε διαφορετικά μέρη μπορεί κανείς να διακρίνει στη σχεδίαση ενός τέτοιου συστήματος:

- Μηχανισμό φίλτρου πακέτων για να εμποδίζεται η πορεία των διακινούμενων πακέτων δεδομένων ανάμεσα στο Internet και το ιδιωτικό δίκτυο και να επιτρέπεται η κίνησή τους μέσω του firewall μόνο σε όσα πακέτα ανήκουν σε αποδεκτούς τρόπους επικοινωνίας.
- Λογισμικό υλοποίησης πυλών σε επίπεδο εφαρμογής ικανό να εμποδίζει τη κυκλοφορία των δεδομένων και να αυθεντικοποιεί τους χρήστες σε επίπεδο εφαρμογών TCP/IP όπως οι υπηρεσίες εξυπηρέτησης HTTP, FTP.
- Υπηρεσία ονομασίας επικρατειών (Domain Name Service-DNS) ικανή για την απόκρυψη των εσωτερικών IP διευθύνσεων του ιδιωτικού δικτύου από τους χρήστες του διαδικτύου.
- Μηχανισμό διαχείρισης ηλεκτρονικών γραμμάτων για να διασφαλίζεται ότι η ανταλλαγή ηλεκτρονικών γραμμάτων διεκπεραιώνεται μέσω firewall.
- Ασφαλές λειτουργικό σύστημα ως βάση του όλου συστήματος.

Τα συστήματα firewall συναντώνται με διάφορους τρόπους διαμόρφωσης και αρχιτεκτονικής. Παρέχουν έτσι και διαφορετικά επίπεδα ασφάλειας με το ανάλογο κόστος εγκατάστασης και λειτουργίας. Μερικά τέτοια συστήματα αναφέρονται στη συνέχεια.

- Multi-Homed Host

Είναι ένας διακομιστής / οικοδεσπότης που διαθέτει περισσότερες από μια κάρτες δικτύου. Κάθε κάρτα είναι συνδεδεμένη σε ένα τμήμα δικτύου που είναι λογικά και φυσικά διαχωρισμένο. Η πιο διαδεδομένη μορφή της είναι με δυο κάρτες δικτύου (dual-homed host).

Σε ένα dual-homed firewall, η μια κάρτα είναι συνδεμένη στο εξωτερικό και μη έμπιστο διαδίκτυο, ενώ η άλλη κάρτα συνδέεται με το εσωτερικό και θεωρούμενο ασφαλές δίκτυο. Σημείο προσοχής σε αυτή την αρχιτεκτονική είναι ότι δεν πρέπει να επιτρέπεται η άμεση δρομολόγηση των πακέτων των δεδομένων ανάμεσα στα δύο δίκτυα. Η επικοινωνία τους πρέπει να γίνεται μόνο μέσω του λογισμικού firewall του διακομιστή.

- Screened Host

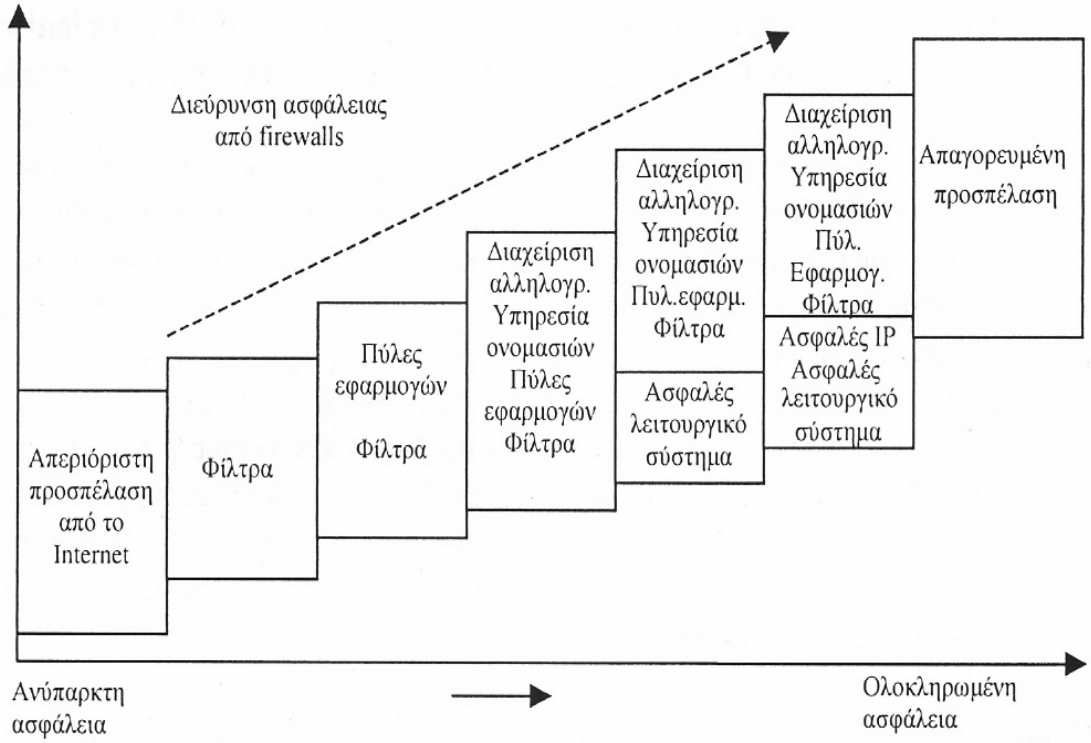
Αυτή η αρχιτεκτονική χρησιμοποιεί έναν διακομιστή που καλείται οχυρό ή bastion host και έναν δρομολογητή φιλτραρίσματος. Ο δρομολογητής αυτός είναι έτσι διαμορφωμένος ώστε να στέλνει αποκλειστικά στον bastion host όλες τις προερχόμενες από το εξωτερικό δίκτυο αιτήσεις, όποιον προορισμό και αν είχαν αυτές μέσα στο εσωτερικό δίκτυο. Όλοι λοιπόν οι εξωτερικοί διακομιστές, υποχρεωτικά περνούν μέσω του λογισμικού firewall στο διακομιστή-οχυρό.

- Screened Subnet

Πρόκειται ουσιαστικά για την προηγούμενη αρχιτεκτονική μορφή, όπου επιπρόσθετα χρησιμοποιείται ένας δεύτερος δρομολογητής φιλτραρίσματος προκειμένου να διαχωρίσει τον bastion host και το δίκτυο που αυτός βρίσκεται, το οποίο καλείται περιμετρικό δίκτυο, από το υπόλοιπο εσωτερικό δίκτυο. Έτσι παρέχεται ακόμη ένα επίπεδο προστασίας.

Η διαβάθμισης της ασφάλειας που παρέχεται από ένα από τα παραπάνω συστήματα firewall εικονίζονται στο Σχήμα 6.

Σχήμα 6: Διαβάθμιση ασφάλειας παρεχόμενης από firewall



7.6 Γενικές Κατευθύνσεις Πολιτικής Ασφάλειας μέσω Firewalls

Τα κύρια σημεία μιας πολιτικής ασφάλειας μέσω firewalls είναι ότι πρέπει:

- Ένα firewall να διαμορφώνεται έτσι ώστε να αποτελεί τη μόνη ορατή διεύθυνση διακομιστή προς το έξω δίκτυο, ενώ ταυτόχρονα να απαιτεί όλες οι συνδέσεις προς και από το εσωτερικό δίκτυο να διέρχονται μέσα από αυτό.

- Οι ισχυροί μηχανισμοί πιστοποίησης χρηστών να εφαρμόζονται σε επίπεδο εφαρμογής.
- Οι υπηρεσίες διαμεσολάβησης (proxy) να παρέχουν λεπτομερείς πληροφορίες καταγραφής σε επίπεδο εφαρμογής.
- Να μην επιτρέπεται η άμεση προσπέλαση στις δικτυακές υπηρεσίες του εσωτερικού δικτύου. Όλες οι αιτήσεις που φτάνουν για υπηρεσίες, όπως TELNET, FTP, HTTP, e-mail κλπ, να διέρχονται μέσω της κατάλληλης υπηρεσίας proxy στο firewall, ανεξάρτητα από το ποιος εσωτερικός διακομιστής είναι ο τελικός προορισμός τους.
- Όλες οι νεοεισερχόμενες υπηρεσίες οφείλουν να διεκπεραιώνονται από υπηρεσίες proxy του firewall. Αν μια νέα υπηρεσία ζητηθεί, αυτή δεν θα είναι διαθέσιμη μέχρι να διατεθεί το αντίστοιχο λογισμικό proxy και να γίνουν οι έλεγχοι από το διαχειριστή ασφάλειας.
- Όλη η διαχείριση του συστήματος firewall να διενεργείται από ένα τοπικό τερματικό. Δεν επιτρέπεται προσπέλαση στο λογισμικό λειτουργίας του firewall, από απομακρυσμένη τοποθεσία. Η φυσική προσπέλαση προς το τερματικό του firewall να επιτρέπεται μόνο στο διαχειριστή του και στον εφεδρικό διαχειριστή.
- Ένας διαχειριστής συστημάτων firewall οφείλει να έχει πολύ καλή εμπειρία στα δικτυακά ζητήματα ασφάλειας, καθώς και στη σχεδίαση και υλοποίηση firewalls. Έτσι μπορεί να επιτύχει τη σωστή ρύθμιση και εγκατάστασή του, ενώ ακόμη μπορεί να το διαχειρίζεται με ασφαλή τρόπο. Επιπλέον, οι διαχειριστές οφείλουν σε περιοδική βάση, να επιμορφώνονται και να ενημερώνονται πάνω σε πρακτικές ασφάλειας δικτύων και λειτουργίας συγχρόνων διατάξεων firewalls.
- Να δημιουργούνται σε καθημερινή, εβδομαδιαία και μηνιαία βάση ασφαλή εφεδρικά αντίγραφα του λογισμικού και των δεδομένων του συστήματος firewall, δηλαδή του λογισμικού συστήματος, των αρχείων ρυθμίσεων, των αρχείων της βάσης δεδομένων, των αρχείων καταγραφής, κ.ά., έτσι ώστε σε περίπτωση αποτυχίας του συστήματος να υπάρχει η δυνατότητα αποκατάστασης της λειτουργίας του χωρίς σημαντικές απώλειες. Τα εφεδρικά αρχεία να φυλάσσονται με ασφάλεια σε αξιόπιστα μέσα που κατόπιν μπορούν να χρησιμοποιηθούν μόνο για ανάγνωση, για να αποφευχθεί η ακούσια διαγραφή / καταστροφή τους. Μόνο το κατάλληλο προσωπικό να έχει φυσική πρόσβαση σε αυτά.

- Τουλάχιστον ένα ακόμη σύστημα firewall, έτοιμο προς χρήση και με τις σωστές ρυθμίσεις να κρατείται εκτός λειτουργίας ως εφεδρεία.

8. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στις μέρες μας η ραγδαία εξάπλωση της τεχνολογίας και των δυνατοτήτων που μας προσφέρει, έχουν σαν αποτέλεσμα η τεχνολογία και το δίκαιο να μην συμβαδίζουν, δηλαδή το δίκαιο δεν είναι ικανό να προβλέψει κάθε απότομη αλλαγή στις κοινωνικές, οικονομικές, πολιτισμικές και τεχνολογικές συνθήκες.

Η εξέλιξη της τεχνολογίας πρόσφερε τη δυνατότητα να δημιουργηθεί ένα νέο είδος εγκλήματος, το ηλεκτρονικό έγκλημα. Δηλαδή το έγκλημα που γίνεται με τη βοήθεια των υπολογιστών και κυρίως μέσω του διαδικτύου. Σήμερα το ηλεκτρονικό έγκλημα οργανώνεται και εξαπλώνεται ολοένα και περισσότερο καθώς οι «ηλεκτρονικοί εγκληματίες» βρίσκουν πρόσφορο έδαφος στο διαδίκτυο αφού τους δίνει τη δυνατότητα να δρουν αποτελεσματικά και να κρύβονται εύκολα.

Από τα πρώτα δευτερόλεπτα που θα συνδεθούμε στο διαδίκτυο θα πρέπει να γνωρίζουμε ότι κάποιος άλλος χρήστης, ανεξάρτητα από την πρόθεση που έχει, έχει την ικανότητα και τη δυνατότητα να εισέλθει στον υπολογιστή μας, να αντιγράψει όλα μας τα δεδομένα ακόμα και να κάνει όποια ζημιά αυτός θέλει. Αυτό έχει σαν αποτέλεσμα στο διαδίκτυο να έχουν χαθεί οι έννοιες του προσωπικού και του ιδιωτικού. Έτσι ο «παγκόσμιος εγκληματίας» έχει εγκατασταθεί στα καλώδια των προσωπικών υπολογιστών μας.

Το διαδίκτυο είναι ένα παγκόσμιο δίκτυο υπολογιστών, ένα δίκτυο χωρίς κεντρική εξουσία ή κεντρική διαχείριση. Κανένας δεν είναι υπεύθυνος για τη λειτουργία του. Έτσι από τη στιγμή που κανείς δεν είναι σε θέση να ελέγξει το περιεχόμενο του το διαδίκτυο αποτελεί τον παράδεισο της παρανομίας της φάρσας και της απάτης.

Αυτό που προκύπτει από τα παραπάνω είναι ότι κανείς δεν έχει τη δυνατότητα να γλιτώσει τα προσωπικά του δεδομένα όσο και αν προσπαθήσει από τη στιγμή που θα αποφασίσει να συνδεθεί και να περιπλανηθεί στο διαδίκτυο. Σκοπός της παρακολούθησης και της καταγραφής των προσωπικών μας δεδομένων είναι η σκιαγράφηση του καταναλωτικού μας προφίλ. Από την άλλη μεριά αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν και από τις διωκτικές

αρχές για τον εντοπισμό των κακοποιών που παρανομούν στο διαδίκτυο ή επικοινωνούν μέσω του διαδικτύου.

Συμπερασματικά, η απώλεια προσωπικών δεδομένων στο διαδίκτυο αποτελεί μια από τις μεγαλύτερες μη υπολογιζόμενες ζημιές για μια σύγχρονη κοινωνία. Η θετική πλευρά του θέματος είναι ότι δεν υπάρχει το τέλειο έγκλημα, ευτυχώς ούτε και στο διαδίκτυο. Τα «ηλεκτρονικά αποτυπώματα» που αφήνουν οι δράστες καθώς περιηγούνται στο διαδίκτυο αποτελούν και την επικήρυξη τους. Από κει αρχίζει η εξιχνίαση που οδηγεί τελικά στη σύλληψη τους.

Έτσι το τελικό συμπέρασμα που προκύπτει από την παραπάνω έρευνα είναι ότι προτεραιότητα κάθε χρήστη του διαδικτύου είναι η προστασία των προσωπικών δεδομένων από εξωτερικούς ή και εσωτερικούς κινδύνους.

ΠΡΟΤΑΣΕΙΣ - ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ

Η προστασία των καταναλωτών στο διαδίκτυο είναι σαφώς ένα αντικείμενο που η ανάγκη για περαιτέρω έρευνα και αναζήτηση μεθόδων προστασίας είναι επιτακτική. Η καταπάτηση των δικαιωμάτων του καταναλωτή στο διαδίκτυο αποτελεί μείζον πρόβλημα στη σημερινή κοινωνία αφού μεγάλο πλήθος καταναλωτών πέφτει θύμα εξαπάτησης στο διαδίκτυο. Έτσι δημιουργείται η ανάγκη για περισσότερη έρευνα και βαθύτερη αναζήτηση των αιτιών του προβλήματος έτσι ώστε η εύρεση των τρόπων και μεθόδων αντιμετώπισης να γίνει πιο εύκολη.

Ο τρόπος αντιμετώπισης αυτού του νέου είδους εγκλήματος βρίσκεται στην ίδια του τη ρίζα, την ανάπτυξη της τεχνολογίας. Η τεχνολογία μπορεί να βοηθήσει στην ανάπτυξη νέων τεχνικών και μεθόδων, οι οποίες θα δημιουργήσουν ένα τοίχος προστασίας για τον καταναλωτή. Σίγουρα τέτοιες προσπάθειες έχουν γίνει αλλά τα αποτελέσματα δείχνουν ότι δεν είναι επαρκή, έτσι οι προγραμματιστές πρέπει να επικεντρωθούν στη δημιουργία τέτοιου είδους λογισμικών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) Ιγγλεζάκης Ιωάννης, "Το δίκαιο του ηλεκτρονικού εμπορίου – Επιτομή", Αθήνα , 2008.

2) Καραδημητρίου Κοσμάς, "Η ηλεκτρονική υπογραφή", Αθήνα, 2008.

3) Νούσκαλης Γεώργιος, "Ποινική προστασία προγράμματος ηλεκτρονικού υπολογιστή, Αθήνα, 2003.

4) Αλεξανδρίδου Ελίζα, "Το δίκαιο του ηλεκτρονικού εμπορίου: ελληνικό και κοινοτικό", Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2004.

5) Καράκωστας Κ. Ιωάννης, "Δίκαιο και Ίντερνετ – Νομικά ζητήματα του διαδικτύου", Εκδόσεις Δίκαιο και Οικονομία Π.Ν. ΣΑΚΚΟΥΛΑΣ, Αθήνα, 2003.

6) Σιδηρόπουλος Θεόδωρος, "Το δίκαιο του διαδικτύου", Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2003.

7) ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΙΚΩΝ ΚΟΙΝΟΤΗΤΩΝ, πράσινο βιβλίο για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στο πλαίσιο των οπτικοακουστικών υπηρεσιών και των υπηρεσιών πληροφόρησης, Βρυξέλλες, 1996.