Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Θέματα ιδιωτικότητας και προστασίας στο Web 2.0**
Ονοματεπώνυμο Φοιτητή	**Μαρία-Αγγελική Γρηγορίου**
Πατρώνυμο	**Επαμεινώνδας**
Αριθμός Μητρώου	**ΜΠΣΠ/08051**
Επιβλέπουσα	**Δέσποινα Πολέμη, επίκ. καθηγήτρια**

Σεπτέμβριος 2012

Τριμελής Εξεταστική Επιτροπή

Ν. Πολέμη επίκ. Καθηγήτρια	Χ. Δουληγέρης Καθηγητής	Π.Κοτζανικολάου Λέκτορας

Πίνακας περιεχομένων

Πίνακας εικόνων

1 Περίληψη (Abstract)

Το Web 2.0 αναπτύσσεται σταδιακά, παρέχοντας ένα συνεχώς αυξανόμενο πλήθος δυνατοτήτων στους χρήστες του διαδικτύου, έχοντας σαν συνέπεια την αύξηση του όγκου της πληροφορίας, της σημαντικότητας της αλλά και των κινδύνων. Είναι σημαντικό να σημειωθεί ότι η επαναστατικότητα των Web 2.0 εφαρμογών βασίζεται στην δυνατότητα διαχείρισης και μεταφοράς περιεχομένου. Στα πλαίσια της διατριβής αυτής μελετώνται τα θέματα ιδιωτικότητας στις εφαρμογές του Web 2.0 και οι τρόποι προστασίας των συμβαλλομένων μερών. Αρχικά, περιγράφεται το Web 2.0, ο τρόπος λειτουργίας του και οι εφαρμογές που το απαρτίζουν. Στην συνέχεια αναφέρονται οι απειλές που παρουσιάζονται κατά την χρήση του και στην συνέχεια οι τρόποι αντιμετώπισης τους. Επίσης, γίνεται αναφορά στο νομικό και θεσμικό πλαίσιο που ορίζει την λειτουργία του Web 2.0. Στα πλαίσια ανάλυσης του Web 2.0, υλοποιείται ένας ιστοτόπος Web 2.0, με την βοήθεια ενός εργαλείου διαχείρισης περιεχομένου. Η διατριβή ολοκληρώνεται με την παράθεση των συμπερασμάτων.

Web 2.0 is developed gradually, providing an ever increasing number of potential internet users, having as a consequence an increase in the volume of information, of its significance and its risks as well. It is important to note that the revolutionary of Web 2.0 applications is based on the capability of management and delivery of the content. This thesis studies privacy issues in Web 2.0 applications and ways to protect the parties. Firstly, Web 2.0 is described, mentioning the mode of operation and the applications that compose it. Thereafter, there are mentioned the threats encountered in its use and then ways of dealing with them. There is also a reference to the legal and institutional framework that defines the operation of Web 2.0. Analyzing Web 2.0, a site is implemented with the help of a content management tool. The thesis concludes with the summary of our conclusions.

2 Εισαγωγή – Σύντομη Περιγραφή Προβλήματος/Αντικειμένου

Οι εξελίξεις στον τομέα της πληροφορικής και ιδιαίτερα στις εφαρμογές του διαδικτύου τα τελευταία χρόνια είναι ραγδαίες. Οι μεγάλες αλλαγές σημειώθηκαν στον τρόπο χρήσης του διαδικτύου. Από την εποχή του Web 1.0, της στατικής παρουσίασης πληροφοριών με μόνη δυνατότητα την ανάγνωση, γίνεται ένα πέρασμα στο Web 2.0 και την εμφάνιση πλήρως αλληλεπιδραστικών εφαρμογών με δυνατότητα συμμετοχής και συνεισφοράς από κάθε χρήστη. Το νέο πλαίσιο δραστηριοποίησης των διαδικτυακών εφαρμογών αναπτύσσεται προς κάθε κατεύθυνση, εμφανίζοντας εφαρμογές που πριν από μερικά χρόνια αποτελούσαν σφαίρα φαντασίας.

Η ανάπτυξη των Web 2.0 εφαρμογών έφερε την ανάγκη ενός ασφαλούς περιβάλλοντος δράσης. Οι εφαρμογές και υπηρεσίες που αναπτύσσονται και παρέχονται κάνουν χρήση προσωπικών δεδομένων των χρηστών, οπότε η προστασία της ασφάλειας και της ιδιωτικότητας αποτελεί σημαντικό κομμάτι αυτών. Η διασφάλιση των προσωπικών δεδομένων αποτελεί δικαίωμα των χρηστών, και έχει προέκταση και στις διαδικτυακές συναλλαγές. Είναι σημαντικό να περιοριστούν οι κακόβουλες ενέργειες , ώστε το διαδίκτυο να αποτελεί έναν ασφαλή χώρο ανάπτυξης, έκφρασης και δημιουργίας.

Το Web 2.0 αναφέρεται σε μια υποτιθέμενη ή προτεινόμενη δεύτερη γενιά ανάπτυξης και σχεδιασμού εφαρμογών Διαδικτύου, με στόχο να διευκολύνουν την επικοινωνία, την ασφαλή ανταλλαγή δεδομένων και τη διαλειτουργικότητα στο διαδίκτυο. Οδήγησε στην ανάπτυξη εφαρμογών, που δίνουν έμφαση στην ηλεκτρονική συνεργασία, επικοινωνία και ανταλλαγή πληροφορίας μεταξύ των χρηστών. Οι νέες εφαρμογές και υπηρεσίες διευκολύνουν την κοινωνική αλληλεπίδραση, την επικοινωνία και τις συλλογικές ενέργειες για την ανάπτυξη συλλογικής γνώσης και την ανταλλαγή πλούσιου περιεχομένου πολυμέσων. Οι χρήστες αποτελούν ζωτικό παράγοντα στις Web 2.0 εφαρμογές, καθώς δεν είναι πλέον μόνο δέκτες πληροφορίας αλλά συνεισφέρουν με την δημιουργία περιεχομένου.

Τα ζητήματα ασφαλείας που προκύπτουν από τις νέες δραστηριότητες που εμφανίζονται στο διαδίκτυο εστιάζουν στη δημιουργία ενός ασφαλούς περιβάλλοντος για τον χρήστη. Σε επίπεδο διαδικτύου είναι σημαντική η δυνατότητα πιστοποίησης της ταυτότητας των χρηστών, η διασφάλιση της ακεραιότητας του περιεχομένου, η εμπιστευτικότητα και η διαθεσιμότητα των υπηρεσιών. Στις Web 2.0 εφαρμογές η διασφάλιση της ασφάλειας παρουσιάζει κάποιες ιδιαιτερότητες οι οποίες πρέπει να αντιμετωπιστούν ώστε να αποτελούν έναν φερέγγυο άξονα δράσης.

Είναι σημαντικό να αναφέρουμε ότι το Web 2.0 δεν αφορά αλλαγή σε καμία τεχνική προδιαγραφή σε σχέση με το Web 1.0. Η διαφορά έγκειται στον τρόπο με τον οποίο οι προγραμματιστές και οι χρήστες χρησιμοποιούν το διαδίκτυο. Οι επόμενες εικόνες παρουσιάζουν μια σύγκριση μεταξύ Web 1.0 και Web 2.0 σε σχέση με τον τρόπο λειτουργίας τους και τις δυνατότητες που προσφέρουν στην επεξεργασία της πληροφορίας.

Από το Web 1.0 στο Web 2.0

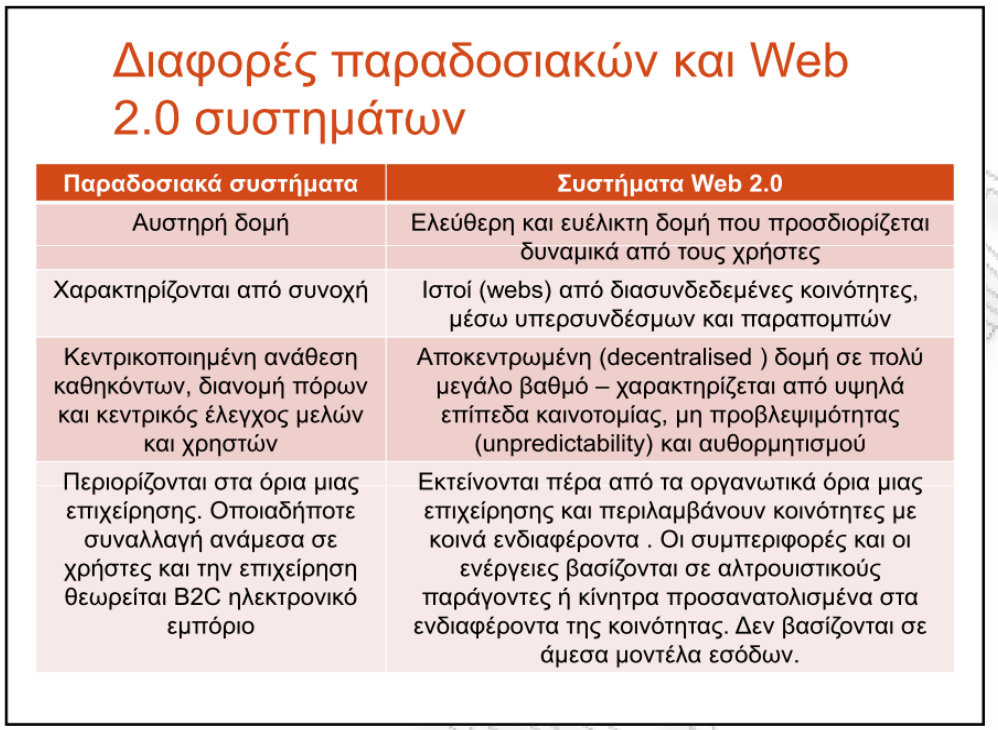
	Web 1.0	Web 2.0
Τρόπος επεξεργασίας περιεχομένου	Ανάγνωση(Read)	Συγγραφή (Write) και συνεισφορά
Μονάδα Περιεχομένου	Σελίδα	Ανακοίνωση/ανάρτηση/ εγγραφή
Κατάσταση	Στατική	Δυναμική
Εμφάνιση από	Φυλλομετρητές	Φυλλομετρητές, αναγνώστες RSS και άλλες εφαρμογές
Λειτουργικότητα φυλλομετρητή	Διεπαφή εγγράφων	Διεπαφή ανάπτυξης – προσθήκη λειτουργικών widgets
Αρχιτεκτονική	Client-server	Web services
Ανάπτυξη από	Προγραμματιστές	Όλους
Ο τομέας των	Έμπειρων χρηστών	Ερασιτεχνών
Η μορφή του Web	Παγκόσμια πηγή πληροφοριών	Παγκόσμια υποδομή πληροφοριών και ανάπτυξης εφαρμογών/υπηρεσιών

Εικόνα 2.1: Σύγκριση εφαρμογών Web 1.0 και Web 2.0

Πηγή: Κοπανάκη Εύη. Πληροφοριακά συστήματα στο διαδίκτυο.

Όπως παρουσιάζεται και στην εικόνα 1, οι διαφορές του τρόπου λειτουργίας και επεξεργασίας της πληροφορίας μεταξύ Web 1.0 και Web 2.0 είναι μεγάλες. Αρχικά, στο Web 1.0 υπήρχε η δυνατότητα για απλή ανάγνωση του περιεχομένου μιας στατικής ιστοσελίδας, δημιουργιμένης από έμπειρους προγραμματιστές. Στο Web 2.0 εμφανίζεται η δυνατότητα συμμετοχής και δυναμικής συνεισφοράς όλων των χρηστών, στην δημιουργία περιεχομένου και πληροφορίας. Το Web 1.0 αποτελούσε μια παγκόσμια πηγή πληροφοριών με διεπαφές εγγράφων μέσω των ιστοσελίδων βασισμένη στο μοντέλο πελάτη-εξυπηρετητή. Το Web 2.0 προαγεται σε μια παγκόσμια υποδομή πληροφοριών και ανάπτυξης εφαρμογών με την χρήση διαδικτυακών υπηρεσιών, ενημέρωσης, επικοινωνίας και εξυπηρέτησης.

Τα παραδοσιακά συστήματα Web 1.0, χαρακτιρίζονται από την αυστηρή δομή και την συνοχή τους. Όλες οι λειτουργίες ακολουθούν μια κεντρικοποιημένη μορφή, για την ανάθεση καθικόντων, την διανομή πόρων, τον έλεγχο μελών και χρηστών. Τα όρια ενός συστήματος Web 1.0 είναι σαφώς καθορισμένα και οποιαδήποτε συναλλαγή εκτώς των ορίων αυτών αποτελεί ηλεκτρονικό εμπόριο. Στα συστήματα Web 2.0 εφαρμόζεται μια ελεύθερη και ευέλικτη δομή, η οποία προσδιορίζεται δυναμικά από τους χρηστες. Εμφανίζεται η δημιουργία ιστών διασυνδεδεμένων κοινοτήτων με την χρήση υπερσυνδέσμων και παραπομπών. Τα συστήματα Web 2.0 παρουσιάζουν αποκέντωση των λειτουργιών τους σε μεγάλο βαθμό, ενώ είναι χαρακτηριστική η εμφάνιση καινοτομίας, μη προβλεψιμότητας και αυθορμιτισμού. Τα όρια ενός συστήματος Web 2.0 δεν είναι σαφώς καθορισμένα, καθώς περιλαμβάνουν κοινώτητες με κοινα ενδιαφέροντα και μεγάλο κύκλο δραστιριοτήτων παράλληλα με τις οικονομικές τους λειτουργίες. Η σύγκριση των δύο γενειών συστημάτων παρουσιάζεται και στην επόμενη εικόνα.



Διαφορές παραδοσιακών και Web 2.0 συστημάτων

Παραδοσιακά συστήματα	Συστήματα Web 2.0
Αυστηρή δομή	Ελεύθερη και ευέλικτη δομή που προσδιορίζεται δυναμικά από τους χρήστες
Χαρακτηρίζονται από συνοχή	Ιστοί (webs) από διασυνδεδεμένες κοινότητες, μέσω υπερσυνδέσμων και παραπομπών
Κεντρικοποιημένη ανάθεση καθηκόντων, διανομή πόρων και κεντρικός έλεγχος μελών και χρηστών	Αποκεντρωμένη (decentralised) δομή σε πολύ μεγάλο βαθμό – χαρακτηρίζεται από υψηλά επίπεδα καινοτομίας, μη προβλεψιμότητας (unpredictability) και αυθορμητισμού
Περιορίζονται στα όρια μιας επιχείρησης. Οποιαδήποτε συναλλαγή ανάμεσα σε χρήστες και την επιχείρηση θεωρείται B2C ηλεκτρονικό εμπόριο	Εκτείνονται πέρα από τα οργανωτικά όρια μιας επιχείρησης και περιλαμβάνουν κοινότητες με κοινά ενδιαφέροντα . Οι συμπεριφορές και οι ενέργειες βασίζονται σε αλτρουιστικούς παράγοντες ή κίνητρα προσανατολισμένα στα ενδιαφέροντα της κοινότητας. Δεν βασίζονται σε άμεσα μοντέλα εσόδων.

Εικόνα 2.2: Σύγκριση των παραδοσιακών συστημάτων με τα συστήματαWeb 2.0

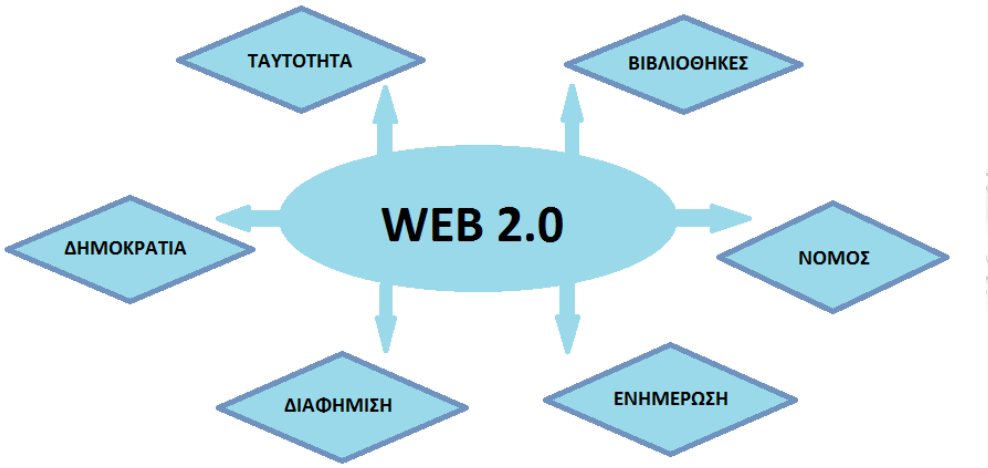
Πηγή: Κοπανάκη Εύη. Πληροφοριακά συστήματα στο διαδίκτυο.

Οι δυνατότητες δράσης που προσφέρουν οι Web 2.0 εφαρμογές, δημιουργούν το έντονο ενδιαφέρον όλο και περισσότερων χρηστών. Σε αντίθεση με το Web 1.0, υπάρχει η δυνατότητα έκφρασης, συμμετοχής, ενημέρωσης και επικοινωνίας κάθε χρήστη. Στο σημείο αυτό είναι που τίθεται και η παράμετρος της ασφάλειας των υπηρεσιών που προσφέρονται καθώς και οι τρόποι προστασίας του χρήστη στο περιβάλλον των Web 2.0 εφαρμογών.

2.1 Web 2.0

Το web 2.0 αποτελεί την νέα γενιά web, περιλαμβάνει εφαρμογές που προσφέρουν περισσότερες δυνατότητες αλληλεπίδρασης μεταξύ των χρηστών. Το Web 2.0 αποτελεί ένα απεριόριστο δίκτυο διασύνδεσης στο οποίο μπορεί να πλοηγηθεί κάθε χρήστης. Στα πλαίσια του Web 2.0 εμφανίζονται πολλές παράμετροι, καθώς αποτελεί, παράλληλα, έναν χώρο ενημέρωσης και διαφήμισης, με ευκολία στην πρόσβαση σε βιβλιοθήκες πληροφοριών, όπως και με ευκολία δημιουργίας κακόβουλων ενεργειών. Ο κάθε χρήστης χαρακτηρίζεται από μια ταυτότητα, το πλαίσιο χρήσης της όμως δεν είναι πάντα καθορισμένο.

Το Web 2.0 αποτελεί ένα νέο κοινωνικό χώρο, εικονικής δραστηριότητας. Οι έννοιες της Δημοκρατίας και η εφαρμογή τους μέσα από νομικά πλαίσια αποτελούν έναν σημαντικό παράγοντα για την εξέλιξη και τον τρόπο λειτουργίας των εφαρμογών που προσφέρονται στους χρήστες. Σε απόμενα κεφάλαια θα αναπτυχθούν οι δυνατότητες, οι απειλές και οι μηχανισμοί προστασίας στα πλαίσια του Web 2.0. Στην επόμενη εικόνα παρουσιάζονται οι παράγοντες που απαρτίζουν, αλληλεπιδρούν και επηρεάζουν το Web 2.0.



Εικόνα 2.3: Το Web 2.0 αποτελεί ένα απεριόριστο δίκτυο διασύνδεσης.

Τα τελευταία χρόνια το τοπίο και η χρήση του διαδικτύου αλλάζει με γρήγορους ρυθμούς. Μέχρι πρότινος η πληροφορία που διακινούταν μέσω του διαδικτύου κατέληγε στον εκάστοτε χρήστη ως κάτι έτοιμο και αμετάβλητο και αυτό διότι δεν υπήρχε η δυνατότητα, από την πλευρά του χρήστη, να γίνει η οποιαδήποτε παρεμβολή στη διαδικασία διακίνησης ή και δημιουργίας της πληροφορίας, εξ' αιτίας κυρίως του γεγονότος ότι οι υπηρεσίες παροχής πληροφοριών ήταν (και σε πολλές περιπτώσεις συνεχίζουν να είναι) αυστηρά «μονόδρομες», χωρίς να αφήνουν περιθώρια στον χρήστη να παρέμβει.

Στην περίοδο που διανύουμε όμως, έχει αρχίσει να δημιουργείται μια νέα τάση στη χρήση του διαδικτύου, ευρέως γνωστή ως Web 2.0. Αυτή η τάση συνίσταται στη δημιουργία και παροχή υπηρεσιών, οι οποίες έχουν έναν «αμφίδρομο» χαρακτήρα, δίνουν δηλαδή τη δυνατότητα στο χρήστη να εκφραστεί μέσω αυτών, να πει τη γνώμη του, να ψηφίσει, να βαθμολογήσει προϊόντα και ακόμα να παρέμβει στη δημιουργία της πληροφορίας.

Τέτοιες υπηρεσίες είναι, για παράδειγμα, τα blogs, τα wikis (χαρακτηριστική περίπτωση η Wikipedia), τα e-journals κ.α. Σ' αυτές τις «διαδικτυακές κοινωνίες», όπως αλλιώς χαρακτηρίζονται, ο χρήστης μπορεί πλέον από ένας παθητικός αποδέκτης να γίνει μια δραστήρια οντότητα και να παρεμβαίνει δυναμικά και συνεχώς στη διαμόρφωση και διακίνηση της πληροφορίας. Οι υπηρεσίες αυτές απαρτίζουν τα νέα συνεργατικά περιβάλλοντα.

2.2 Η γνώση του πλήθους

Η έννοια γνώση του πλήθους (wisdom of the crowd) αναφέρεται στην αναζήτηση και συλλογή της γνώσης που έχει ένα πλήθος ατόμων για ένα θέμα, σε αντίθεση με την απάντηση ενός ειδικού. Η μέθοδος αυτή δεν είναι καινούργια, εμφανίστηκε ξανά όμως μέσα από ιστοχώρους κοινωνικής πληροφόρησης όπως τα wikis. Παράδειγμα αποτελούν το Wikipedia και το Yahoo! Answers. Τα άτομα που συμμετέχουν και δίνουν πληροφορίες στα θέματα δεν είναι απαραίτητα ειδικοί, όμως με την συλλογή των απόψεων και την διασταύρωσή τους απορρέει κάτι ορθό, η «σοφία του πλήθους».

Κατά κανόνα, το σύνολο των ατόμων είναι ανομοιογενές καθώς μπορεί να απαντήσει όποιος επιθυμεί. Η ανομοιογένεια αυτή είναι που δίνει την καλύτερη πληροφορία, δεδομένου ότι όσο περισσότερες είναι οι απόψεις αρχικά, τόσο πιο σφαιρικά έχει μελετηθεί ένα θέμα. Στην περίπτωση που το πλήθος που απαντά παρουσιάζει ομοιομορφία ενδέχεται η απάντηση να μην είναι αμερόληπτη. Σε θέματα γεωγραφίας και μαθηματικών η μέθοδος αυτή λειτουργεί τέλεια, καθώς υπάρχει ορισμένη απάντηση.

Παράλληλα, η αξιοπιστία της μεθόδου αυτής εξαρτάται από τον αριθμό των ατόμων που συμμετέχουν. Όταν υπάρχει μεγάλη συμμετοχή χρηστών η εγκυρότητα της πληροφορίας είναι μεγάλη. Στις περιπτώσεις που υπάρχουν λίγοι που έχουν αναφερθεί σε ένα θέμα ή και μόνο ένας, αποτελεί απλά μια άποψη η ακρίβεια της οποίας είναι συζητήσιμη. Στα wikis συνήθως γίνεται αναφορά, προς ενημέρωση του χρήστη, στον αριθμό των ατόμων που έχουν δώσει την πληροφορία. Ενώ παράλληλα ζητείται και η γνώμη περισσότερων.

2.3 Περίληψη

Στα επόμενα κεφάλαια, έχοντας κάνει μια εισαγωγή στις Web 2.0 εφαρμογές και την αλλαγή που έχουν φέρει στον τρόπο λειτουργίας και δράσης στο διαδίκτυο, γίνεται αναφορά στα θέματα ιδιωτικότητας και προστασίας των Web 2.0 εφαρμογών.

Στο κεφάλαιο 3, αναπτύσσεται το σύγχρονο περιβάλλον στο διαδίκτυο το αποκαλούμενο Web 2.0. στο νέο πλαίσιο, εμφανίζεται η έννοια της συμμετοχικότητας, τα συνεργατικά συστήματα και τα συνεργατικά εργαλεία και εφαρμογές. Ο νέος τρόπος λειτουργίας του Web 2.0 συνεπάγεται νέες αρχιτεκτονικές δομές, οι οποίες επίσης περιγράφονται στο δεύτερο κεφάλαιο. Ιδιαίτερη σημαντικότητα δίνεται στους ιστοτόπους κοινωνικής δικτύωσης, οι οποίοι αποτελούν την επιτομή των Web 2.0 εφαρμογών.

Στο κεφάλαιο 4, γίνεται ανάλυση των προβλημάτων και των απειλών που εμφανίζονται στις Web 2.0 εφαρμογές. Η ευαίσθητη πληροφορία αποτελείται από το σύνολο των στοιχείων που πρέπει να προστατευθούν στα πλαίσια λειτουργίας των Web 2.0 εφαρμογών. Με βάση την ευαίσθητη πληροφορία, καθορίζονται οι απειλές που υπάρχουν και τα προβλήματα που δημιουργούνται κατά την χρήση των Web 2.0 εφαρμογών. Παράλληλα, επισημαίνονται τα θέματα ιδιωτικότητας που προκύπτουν, και πρέπει να διασφαλιστούν. Επιπλέον ανάλυση γίνεται για τα προσωπικά δεδομένα των χρηστών σε ιστοτόπους κοινωνικής δικτύωσης.

Στο κεφάλαιο 5, παρουσιάζονται οι μηχανισμοί προστασίας που μπορούν να διασφαλίσουν την ασφαλή λειτουργία των Web 2.0 εφαρμογών. Στο πλαίσιο αυτό αναφέρονται οι σχεδιαστικές απαιτήσεις για την προστασία των εφαρμογών στο Web 2.0 από τις απειλές. Σε συνέχεια αναφέρονται οι μηχανισμοί προστασίας σε σχέση με το πεδίο στο οποίο αναφέρονται. Από τους πιο σημαντικούς μηχανισμούς ασφαλείας που χρησιμοποιούνται στις Web 2.0 εφαρμογές, είναι η διαχείριση ταυτοτήτων. Παράλληλα, στα πλαίσια των κοινωνικών δικτύων, είναι σημαντική η χρήση μηχανισμών και συστημάτων καταγραφής της συμπεριφοράς των χρηστών.

Στο κεφάλαιο 6, γίνεται αναφορά στα πρότυπα που καθορίζουν τον τρόπο ανάπτυξης και δημιουργίας των Web 2.0 εφαρμογών. Τα πρότυπα αυτά κύριο σκοπό έχουν οι εφαρμογές να υλοποιούνται με ορισμένες προδιαγραφές, οπότε να μπορεί να γίνει αποδεκτή η λειτουργία τους. Σημαντικό κομμάτι αποτελεί η προτυποποίηση της ασφάλειας των τηλεπικοινωνιακών δικτύων. Επίσης, γίνεται αναφορά στην προτυποποίηση της πιστοποίησης της ταυτότητας καθώς και της προτυποποίησης των ηλεκτρονικών υπογραφών.

Στο κεφάλαιο 7, παρουσιάζεται το νομικό πλαίσιο που καλύπτει την λειτουργία και την χρήση των Web 2.0 εφαρμογών. Γίνεται αναφορά στο ευρωπαϊκό νομικό πλαίσιο, τις οδηγίες και τους κανονισμούς που έχουν εκδοθεί από την Ευρωπαϊκή Ένωση και ισχύουν σε ευρωπαϊκό επίπεδο. Επίσης, γίνεται αναφορά στο ελληνικό νομικό πλαίσιο, τους νόμους τις πράξεις και τα προεδρικά διατάγματα που διασφαλίζουν την χρήση των Web 2.0 εφαρμογών. Το νομικό πλαίσιο διασαφηνίζει τα δικαιώματα και τις υποχρεώσεις των μερών που σχετίζονται με τις διαδικτυακές εφαρμογές.

Στο κεφάλαιο 8, παρουσιάζεται η υλοποίηση μιας ιστοσελίδας Web 2.0 με την χρήση του Joomla έκδοση 1.7. Το Joomla είναι ένα σύστημα διαχείρισης περιεχομένου ιστοσελίδων Web 2.0 που προσφέρει την δυνατότητα διαχείρισης της πληροφορίας, της πρόσβασης και των δικαιωμάτων των χρηστών από την πλευρά του διαχειριστή. Τα κύρια χαρακτηριστικά του είναι η δυνατότητα συνεργασίας διαφορετικών χρηστών, και ο καθορισμός των δυνατοτήτων δράσης κάθε χρήστη στην ιστοσελίδα από την εφαρμογή ρόλων.

Στο κεφάλαιο 9, παρουσιάζονται τα συμπεράσματα και οι μελλοντικές εξελίξεις. Ο ρόλος του Web 2.0 συνεχώς αλλάζει, καθώς εξελίσσονται οι εφαρμογές και η χρήση του. Παράλληλα με την εξέλιξη αυτή, εμφανίζονται νέα θέματα σχετικά με την προστασία των χρηστών από κακόβουλες επιθέσεις. Η εξάλειψη των κινδύνων αυτών αποτελεί μία συνεχή πρόκληση για τους σχεδιαστές του Web 2.0 εφόσον αποτελεί τον ακρογωνιαίο λίθο της εύρυθμης λειτουργίας του.

3 Το σύγχρονο περιβάλλον στο διαδίκτυο

Οι Web 2.0 εφαρμογές προσφέρουν στον χρήστη πληθώρα δυνατοτήτων επεξεργασίας των πληροφοριών και αλληλεπίδρασης με αυτές. Η νέα τάξη υπηρεσιών στηρίζεται σε μεγάλο βαθμό στην συλλογικότητα και τη συνεργασία των χρηστών. Ανάμεσα στις τεχνικές των Web 2.0 υπηρεσιών είναι η δυνατότητα αναζήτησης (search), συγγραφής (authoring), σήμανσης (tagging), σύνδεσης (links), σηματοδότησης (signals). Τα χαρακτηριστικά των Web 2.0 υπηρεσιών συμπληρώνονται από τη μεταφερσιμότητα (portability), τη συμβατότητα (compatibility), τη διαλειτουργικότητα (interoperability) και την ολοκλήρωση (integration) που προσφέρουν στις εφαρμογές.

3.1 Η νέα εποχή της συμμετοχικότητας

Το διαδίκτυο δεν είναι πλέον σελίδες στατικού περιεχομένου. Όλο και σε μεγαλύτερο βαθμό στο διαδίκτυο αναπαρίσταται ο πραγματικός κόσμος και οι καταστάσεις μέσα από την σωστή ανάλυση και επεξεργασία κάθε αναφοράς που δημοσιεύεται. Επί της ουσίας η πληροφορία δίνεται, το πλέον σημαντικό είναι το σωστό φιλτράρισμα και οι κατάλληλες διαδικασίες επεξεργασίας μέσω υπολογιστικών συστημάτων.

Το Web 2.0 έφερε μια νέα λογική στις εφαρμογές. Οι νέες εφαρμογές δημιουργούνται για την εξυπηρέτηση όσο το δυνατόν μεγαλύτερου αριθμού χρηστών. Παράλληλα όμως με την πληροφόρηση των χρηστών, συλλέγεται πληροφορία και από αυτούς συνεισφέροντας στην συλλογική νοημοσύνη (collective intelligence). Η διαδικασία αυτή είναι που τρέφει και δυναμώνει τις νέες εφαρμογές δημιουργώντας ανεξάντλητες πηγές γνώσης [1].

Οι εφαρμογές συλλογικής νοημοσύνης βασίζονται στη διαχείριση, την επεξεργασία και την ανταπόκριση σε πραγματικό χρόνο σε μεγάλο όγκο πληροφορίας από τους χρήστες. Παράλληλα με την προσωπική συνεισφορά πληροφορίας από κάθε χρήστη, υπάρχουν και εφαρμογές που συλλέγουν πληροφορία συνεχούς ροής μέσω αισθητήρων. Τέτοιοι αισθητήρες μπορούν να συλλέξουν στοιχεία κίνησης, τοποθεσίας, ταχύτητας. Οι περισσότερες συσκευές νέας τεχνολογίας περιλαμβάνουν αισθητήρες συλλογής ανάλογων δεδομένων.

Μελετώντας τη διαδικασία ανάπτυξης συλλογικής νοημοσύνης, στη βάση βρίσκονται οι χρήστες και η προσωπική τους γνώση την οποία δημοσιεύουν στο διαδίκτυο και αποτελεί ένα ατελείωτο πεδίο γνώσης(wisdom of the crowd). Το σύνολο της προσωπικής γνώσης βρίσκεται κατανεμημένο στο διαδίκτυο και η συλλογή του γίνεται με ειδική τεχνολογία ανακάλυψης και εξόρυξης γνώσης. Με την διαδικασία αυτή η προσωπική γνώση συλλέγεται σε βάσεις γνώσης. Πολλές κοινότητες συναθροίζουν την προσωπική τους γνώση και δημιουργούν την δική τους συλλογική νοημοσύνη. Η συλλογική γνώση διαφέρει από κοινότητα σε κοινότητα καθώς εμπεριέχει τις αρχές και τα πιστεύω των μελών της[2].

3.2 Συνεργατικά συστήματα

Στα πλαίσια της συζήτησης για τα κοινωνικά δίκτυα, αναφέρονται οι έννοιες της συλλογικής νοημοσύνης (collective intelligence) και της γνώσης του πλήθους (wisdom of the crowds). Οι φράσεις αυτές αναφέρονται στην πληροφορία που παράγεται με την συνεισφορά όλων όσων προσθέτουν στοιχεία σε συνεταιριστικές εφαρμογές Web 2.0. Τέτοιες εφαρμογές αποτελούν τα Wikipedia, MySpace, Youtube, Flickr, Facebook κ.ά. Είναι η πρώτη φορά στα

[1] **Robinson, Rick.** *Enterprise Web 2.0, Part 2: Enterprise Web 2.0.* 2008 (σελ.1-2)

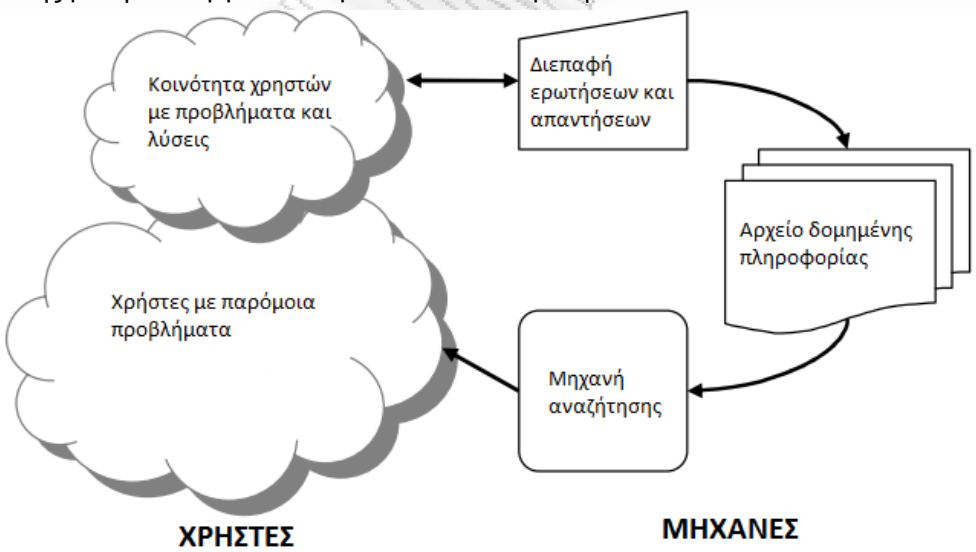
[2] **Koji Zettsu, Yasushi Kiyoki.** *Towards Knowledge Management Based on Harnessing Collective Intelligence on the Web.* 2006.(σελ.350-357)

χρονικά που δίνεται η δυνατότητα σε τόσους ανθρώπους με γνώσεις να συνδεθούν μέσω ενός αποδοτικού και παγκόσμιου δικτύου. Η δυνατότητα συνάθροισης και συνεισφοράς υπολογιστικών μέσων έδωσε τη δυνατότητα σε εταιρίες με περιορισμένους πόρους να παρουσιάσουν και να παρέχουν νέες καινοτόμες υπηρεσίες σε εκατομμύρια on-line συμμετέχοντες. Το αποτέλεσμα είναι ένα πολύ μεγάλο εύρος πληροφορίας και ποικιλομορφία στις προοπτικές, και μια κουλτούρα μαζικής συμμετοχής που συντηρεί εφαρμογές με περιεχόμενο διαθέσιμο στο κοινό[3].

Η συλλογική νοημοσύνη είναι ένα μεγάλο όραμα. Η παρούσα κατάσταση στο Social Web θα μπορούσε να χαρακτηριστεί ως «συγκεντρωμένη γνώση» (collected knowledge). Η πληροφορία που δίνεται σαν συνεισφορά του χρήστη εμφανίζεται μέσα στις συγκεκριμένες ιστοσελίδες συλλογής ενός είδους πληροφορίας (φωτογραφίες ή κείμενο ή video). Σε αυτής της μορφής τα συστήματα συλλογής πληροφορίας δεν δίνεται πραγματικά έμφαση σε νέα επίπεδα κατανόησης. Ειδικά στην περίπτωση του spam, η απλή συλλογή αναφορών από το πλήθος δεν συνεπάγεται νέα επίπεδα νοημοσύνης.

Στο σύστημα άνθρωπος – μηχανή και τα δύο μέρη συνεισφέρουν ενεργά για την απόκτηση νοημοσύνης, κάνοντας καθένας αυτό που μπορεί να κάνει καλύτερα. Οι άνθρωποι είναι οι παραγωγοί και οι πελάτες: αποτελούν την πηγή γνώσης και έχουν πραγματικά προβλήματα και ενδιαφέροντα. Οι μηχανές έχουν το ρόλο καταλύτη: αποθηκεύουν και συγκρατούν δεδομένα, αναζητούν και συνδυάζουν δεδομένα και αναπτύσσουν μαθηματικά και λογικά συμπεράσματα.

Ένα σύστημα συλλογής γνώσης (collective knowledge) μπορεί να θεωρηθεί ως ένα σύστημα ανθρώπου – υπολογιστή οπού η μηχανή επιτρέπει την συλλογή μεγάλης ποσότητας ανθρώπινης γνώσης. Ένα τέτοιο σύστημα αποτελείται από τρία μέρη: το κοινωνικό δίκτυο που επιτρέπει την ανάπτυξη ιδεών και δραστηριοτήτων στους χρήστες, μία μηχανή αναζήτησης ώστε να μπορεί να επεξεργάζεται την πληροφορία, χρήστες ικανούς να αναζητήσουν πληροφορίες στο διαδίκτυο. Στο επόμενο σχήμα φαίνεται μια απεικόνιση ενός συστήματος συλλογής γνώσης με την συνεργασία ανθρώπου – υπολογιστή.



Εικόνα 3.1: Απεικόνιση συστήματος συλλογής γνώσης.

Πηγή: Gruber, Tom. Collective Knowledge Systems: Where the Social Web meets the Semantic Web. 2007(σελ.4)

Οι κύριες ιδιότητες των συστημάτων συλλογής γνώσης είναι το περιεχόμενο που είναι δημιουργημένο από τον χρήστη, η συνεργασία ανθρώπου- μηχανής και ανάλογη αύξηση των επιδόσεων του συστήματος ως προς την αύξηση των χρηστών. Η σημαντική διαφοροποίηση όμως μεταξύ της συγκεντρωμένης γνώσης (collected knowledge) και της συλλογικής σοφίας

[3] **Audun Jøsang, Roslan Ismail, Colin Boyd.** *A Survey of Trust and Reputation Systems for Online Service Provision.* 2006.(σελ.5-7)

(collective knowledge) εξαρτάται από μια τέταρτη ιδιότητα, την Αναδυόμενη γνώση. Το σύστημα επιτρέπει επεξεργασία της συλλεγμένης πληροφορίας δημιουργώντας αποτελέσματα που δεν εμφανίζονται στις ανθρώπινες αναφορές που αποτελούν την πληροφορία του συστήματος. Το ζητούμενο δεν είναι η απλή συλλογή γνώσης, αλλά η παραγωγή γνώση[4].

3.3 Συνεργατικά εργαλεία και εφαρμογές

Το Web 2.0 προσδίδει στο διαδίκτυο ένα χαρακτήρα περισσότερο αλληλεπιδραστικό και συνεταιριστικό. Ιδιαίτερη έμφαση δίνεται στην κοινωνική αλληλεπίδραση των χρηστών και την προαγωγή της συλλογικής νοημοσύνης. Παράλληλα παρουσιάζονται νέες δυνατότητες για την αξιοποίηση του διαδικτύου, κάνοντάς το αποτελεσματικότερο για τους χρήστες. Τα τελευταία χρόνια το Web 2.0, μέσα από εφαρμογές όπως τα MySpace, Flickr, YouTube, παρέχει νέες εφαρμογές και υπηρεσίες που παλαιότερα θεωρούνταν ουτοπικές[5].

Το Web 2.0 επέτρεψε την ανάπτυξη νέων υπηρεσιών που προσφέρουν άμεση επικοινωνία στους χρήστες. Οι υπηρεσίες αυτές παρουσιάζονται στη συνέχεια. Είναι σημαντικό να αναφερθεί ότι παράλληλα με την ανάπτυξη των συγκεκριμένων υπηρεσιών εμφανίστηκαν και νέα θέματα ασφάλειας και προστασίας προσωπικών δεδομένων καθώς είναι πιθανές κακόβουλες ενέργειες, όπως δυσφήμιση και δημόσια προσβολή των χρηστών.

3.3.1 Ιστολόγια (Blogs)

Ένα ιστολόγιο (blog ή Web-log) αποτελεί ένα πολύ βασικό διαδικτυακό εργαλείο επικοινωνίας μεταξύ χρηστών. Το blog είναι μία ιστοσελίδα στην οποία χρήστες μπορούν να εισάγουν τις σκέψεις, τις ιδέες, τις προτάσεις και τα σχόλιά τους. Οι αναρτήσεις σε ένα blog (blog posts), συνήθως παρουσιάζονται σαν δημοσιεύσεις, ακολουθώντας ανάστροφη χρονολογική σειρά. Μία ανάρτηση σε blog μπορεί να περιέχει κείμενο, εικόνες ή συνδέσεις (links) με άλλα blogs και ιστοσελίδες, ή και άλλα μέσα σχετικά με το θέμα της ανάρτησης.

Τα περισσότερα blogs περιέχουν κατεξοχήν κείμενο, όμως πολλά επικεντρώνονται σε φωτογραφίες (photoblog/ photolog), video (videoblog/ videolog) ή ήχο (podcast). Ένα blog γραμμένο από μία φορητή συσκευή (pocket PC, κινητό τηλέφωνο, PDA) ονομάζεται mblog και η ανάρτηση πληροφορίας σε blog πραγματικού χρόνου ονομάζεται live blogging. Ένα ιστολόγιο μπορεί να είναι ιδιωτικό και να βρίσκεται εσωτερικά σε έναν οργανισμό ή δημόσιο και να επιτρέπεται η πρόσβαση σε οποιονδήποτε. Οι αναρτήσεις σε ένα blog συνήθως αποτελούνται από έναν τίτλο, σώμα, μόνιμο σύνδεσμο, ημερομηνία ανάρτησης, σχόλια, κατηγορία ή ετικέτα, επισήμανση ενός άλλου blog με το οποίο συνδέεται μία ανάρτηση (trackback), δυνατότητα κοινοποίησης σύνδεσης άλλου με μία ανάρτηση (pingback).

Τα blogs κατάφεραν να δώσουν μια ενδιαφέρουσα διάσταση στο διαδίκτυο προσφέροντας μια μορφή ανάπτυξης δημόσιου διαλόγου και ανταλλαγής απόψεων. Παράλληλα, με την απλότητά και την αμεσότητά του προσέλκυσε νέες ομάδες χρηστών καταρρίπτοντας την εικόνα της απρόσωπης επικοινωνίας. Η δυνατότητα συμμετοχής και διατύπωσης των προσωπικών απόψεων των χρηστών ανοίγει νέες οδούς επικοινωνίας. Μία αρνητική εκδοχή αποτελεί το ενδεχόμενο αρνητικής κριτικής και δημόσιας προσβολής. Στις Web 2.0 εφαρμογές εμφανίζονται νέα θέματα προς συζήτηση. Είναι σημαντικό να μπορεί κάθε χρήστης να παρουσιάζει τις ιδέες του ελεύθερα. Στην περίπτωση όμως που προσβάλλονται άλλα άτομα, είναι σημαντικό να υπάρχει προστασία προς αυτά.

[4] **Gruber, Tom**. *Collective knowledge systems: Where the Social Web meets the Semantic Web.* 2008.(σελ1-14)

[5] **Murugesan, San.** *Understanding Web 2.0.* 2007.(σελ.34-41)

3.3.2 Ομάδες συζητήσεων (Forums)

Το Forum είναι μια υπηρεσία όπου σε μια περιοχή ενός ηλεκτρονικού online πίνακα οι χρήστες με ένα κοινό ενδιαφέρον μπορούν να τοποθετήσουν τις απόψεις/σημειώσεις τους πάνω σε ένα θέμα. Τα φόρουμ χρησιμοποιούνται συνήθως για να υποβάλουν οι χρήστες ερωτήσεις, να μοιράζονται πληροφορίες, ή να συζητούν τις ιδέες τους.

3.3.3 Συνεργατικές βιβλιοθήκες (Wikis)

Ο όρος Wiki προήλθε από την Χαβανέζικη λέξη wikiwiki, που σημαίνει γρήγορα . Από πολλούς όμως ερμηνεύεται μερικές φορές ως ακρώνυμο για το "What I know is" δηλαδή "Αυτό που εγώ ξέρω είναι". Είναι μια χαρακτηριστική φράση για τον τρόπο λειτουργίας του Wiki: ο κάθε χρήστης που συμμετέχει στη συγγραφή κάποιου έργου προσθέτει την προσωπική του γνώση, έτσι ώστε όλοι να μπορούν να τη μοιράζονται. Όσο και αν υπάρχει το ενδεχόμενο λάθους, αποτελεί πλέον ένα πολύ διαδεδομένο εργαλείο καθώς δίνει την δυνατότητα συνεργασίας και αλληλεπίδρασης.

Μια συνεργατική βιβλιοθήκη (Wiki) είναι συνήθως μία ιστοσελίδα που επιτρέπει στους χρήστες της να προσθέσουν, να αφαιρέσουν, ή να επεξεργαστούν το περιεχόμενό της, πολύ γρήγορα και εύκολα. Οι χώροι αυτοί διευκολύνουν τη συνεργασία πολλών ατόμων για τη συγγραφή ενός έργου. Αποτελεί ένα απλό αλλά πολύ ισχυρό διαδικτυακό σύστημα συνεργατικής συγγραφής για τη δημιουργία και επεξεργασία περιεχομένου. Προσφέροντας ένα περιβάλλον διαχείρισης περιεχομένου, επιτρέπει σε οποιονδήποτε να προσθέσει νέα άρθρα ή να αναθεωρήσει υπάρχοντα μέσω ενός Web browser. Οι χρήστες παράλληλα, μπορούν να παρακολουθούν τις αλλαγές που έχουν γίνει σε ένα άρθρο.. Το πιο γνωστό ίσως wiki είναι η online παραγόμενη από τους χρήστες εγκυκλοπαίδεια Wikipedia.

Στην ουσία, ένα σύστημα wiki απλοποιεί τη διαδικασία δημιουργίας σελίδων και καταγράφει κάθε μεμονωμένη αλλαγή που εμφανίζεται κατά τη διάρκεια του χρόνου. Σε οποιαδήποτε στιγμή μια σελίδα μπορεί να επανέλθει σε κάποια από τις προηγούμενες καταστάσεις της. Το wiki περιλαμβάνει εργαλεία που επιτρέπουν στους χρήστες να παρακολουθούν την κατάστασή του. Επίσης, παρέχεται στους χρήστες χώρος για την συζήτηση θεμάτων, όπως το περιεχόμενο που προστίθεται στον ιστότοπο.

Τα περισσότερα wikis επιτρέπουν την πρόσβαση των χρηστών χωρίς κανέναν απολύτως περιορισμό. Έτσι όλοι έχουν το δικαίωμα να συμβάλουν στη συγγραφή του περιεχομένου της ιστοσελίδας χωρίς να υποβληθούν σε διαδικασία "εγγραφής" όπως συνήθως επιβάλλεται σε σελίδες συζητήσεων (forum, blogs). Αυτό σημαίνει ότι σε πολλές περιπτώσεις δεν είναι δυνατό να ελεγχθεί η εγκυρότητα των πληροφοριών που προστίθενται.

3.3.4 Ψηφιακές βιβλιοθήκες (Digital libraries)

Ψηφιακή βιβλιοθήκη είναι η βιβλιοθήκη που παρέχει όλο της το υλικό σε ψηφιοποιημένη μορφή με δυνατότητα πρόσβασης μέσω του ηλεκτρονικού υπολογιστή. Οι ψηφιακές βιβλιοθήκες μπορεί να μην υφίστανται ως φυσικά κτίρια αλλά να λειτουργούν μόνο ηλεκτρονικά μέσω διαδικτύου. Αυτές οι βιβλιοθήκες ονομάζονται εικονικές ή βιβλιοθήκες χωρίς σύνορα και ξεκίνησαν να δημιουργούνται το 1990. Παρέχουν στον χρήστη εύκολη και γρήγορη πρόσβαση στη γνώση από οποιοδήποτε σημείο χωρίς να απαιτείται φυσική παρουσία.

Από τις πρώτες ενέργειες ψηφιοποίησης στις βιβλιοθήκες ήταν η εισαγωγή του ηλεκτρονικού καταλόγου. Σε ορισμένες περιπτώσεις η βιβλιοθήκη μπορεί να διατηρείται και κτιριακά αλλά παράλληλα να διαθέτει και μέρος του υλικού της σε ψηφιοποιημένη μορφή. Η συλλογή των ψηφιακών βιβλιοθηκών μπορεί να απαρτίζεται τόσο από ψηφιοποιημένα όσο και από ψηφιακά γεννημένα τεκμήρια τα οποία οργανώνονται με εργαλεία που εξυπηρετούν τις ανάγκες για οργάνωση, πρόσβαση και διαχείριση του υλικού.

Ένα από τα βασικά πλεονεκτήματα των ψηφιακών βιβλιοθηκών είναι η μη ύπαρξη φυσικών εμπόδιων. Οι χρήστες μπορούν να έχουν πρόσβαση από οποιοδήποτε μέρος μέσω του διαδικτύου. Η πληροφορία είναι πάντοτε διαθέσιμη και οι πόρτες των ψηφιακών

οργανισμών πάντοτε ανοικτές. Παράλληλα, είναι δυνατή η πολλαπλή, ταυτόχρονη πρόσβαση, καθώς την ίδια πηγή μπορούν να τη χρησιμοποιούν πολλοί χρήστες. Οι ψηφιακές βιβλιοθήκες αποτελούν ένα από τα σημαντικότερα συνεργατικά περιβάλλοντα. Οι βιβλιοθήκες αποτελούν πηγές γνώσης. Με τη χρήση του Web 2.0 δίνεται νέα διάσταση στον τρόπο πρόσβασης και διάδοσης της γνώσης αυτής. Παράλληλα, υπάρχει η δυνατότητα διαλόγου μεταξύ ατόμων που έχουν διαβάσει το ίδιο βιβλίο ή που αναζητούν πληροφορίες στο ίδιο θέμα.

3.3.5 Τεχνολογία RSS

Η τεχνολογία RSS (Really Simple Syndication/ Rich Site Summary) αποτελεί έναν απλό τρόπο για την αποστολή πληροφοριών από μια ιστοσελίδα, χωρίς να απαιτείται από τον χρήστη να επισκέπτεται τα ανάλογα site. Το μόνο που χρειάζεται είναι να δηλώσει στο πρόγραμμα RSS -ή στην online υπηρεσία RSS- τι ακριβώς επιθυμεί να εντοπίσει στο Διαδίκτυο, και αυτομάτως αποστέλλονται οι νέες πληροφορίες.

Το RSS αποτελεί ένα σύνολο μορφών τροφοδοσίας στο διαδίκτυο που χρησιμοποιούνται για τη σύνδεση περιεχομένου μεταξύ blogs ή ιστοσελίδων. Το RSS είναι ένα αρχείο XML το οποίο συναθροίζει κομμάτια πληροφορίας και δημιουργεί συνδέσμους με τις πηγές πληροφόρησης. Η τεχνολογία αυτή ενημερώνει τους χρήστες για τις ανανεώσεις που έχουν γίνει σε blogs ή ιστοσελίδες για τις οποίες ενδιαφέρονται. Οι τροφοδοσίες RSS σε ιστοσελίδες ή blogs δηλώνονται με τη λέξη “subscribe”, ένα πορτοκαλί ορθογώνιο παραλληλόγραμμο, ή με τα γράμματα XML ή RSS σε ένα πορτοκαλί πλαίσιο.

Τα προγράμματα ανάγνωσης ειδήσεων είναι αυτόνομες εφαρμογές, οι οποίες ανακτούν και εμφανίζουν τα περιεχόμενα των καναλιών τροφοδοσίας RSS (RSS feeds) που έχουν επιλεγεί. Ένας άλλος τρόπος χρήσης της υπηρεσίας είναι η ενσωμάτωση του περιεχόμενου που ανακτάται, σε ένα blog.

Η συγκεκριμένη τεχνολογία έκανε για πρώτη φορά την εμφάνισή της στα blogs. Προσέφερε έναν τρόπο παρακολούθησης των εξελίξεων σε διάφορα θέματα, χωρίς να χρειάζεται έρευνα για ανανεώσεις. Σύντομα επεκτάθηκε και πέραν των blogs, και πλέον το περιεχόμενο των περισσότερων ιστοσελίδων κωδικοποιείται σε μορφή που επιτρέπει την ανάγνωσή του από το λογισμικό των προγραμμάτων Atom και RSS.

Σύνθεση υπηρεσιών (Mashups)

Τα Mashups (σύνθεση υπηρεσιών) δημιουργούν νέες διαδικτυακές υπηρεσίες χρησιμοποιώντας δεδομένα και στοιχεία από άλλες διαδικτυακές εφαρμογές. Πολλές φορές τα mashups επεμβαίνουν σε υπηρεσίες που απαιτούν κωδικούς πρόσβασης, τους οποίους πρέπει να δώσει ο χρήστης. Σε αυτή την περίπτωση ο χρήστης πρέπει να εμπιστεύεται σε μεγάλο βαθμό την λειτουργία του mashup καθώς επιτρέπει τόσο την πρόσβαση σε προσωπικά δεδομένα όσο και την επεξεργασία τους. Ένα κακόβουλο κομμάτι κώδικα θα ήταν αρκετό για να αντλήσει πληροφορίες παρά την θέληση του χρήστη[6].

Τα mashups παρέχουν μια ελαφριά υποδομή γεγονότος (lightweight event) που επιτρέπει στις εφαρμογές που βρίσκονται μέσα σε ένα mashup να ανταλλάσουν πληροφορία δυναμικά χωρίς να απαιτείται ανανέωση σελίδας από τον εξυπηρετητή. Τα mashups έχουν την δυνατότητα να επεξεργαστούν και να συνδυάσουν μεγάλη γκάμα πληροφορίας, όπως χάρτες και γεωγραφικά δεδομένα, πληροφορία από επιχειρησιακές βάσεις δεδομένων και εφαρμογές, ψηφιακό περιεχόμενο όπως φωτογραφίες και video, τροφοδοσία ειδήσεων. Με την επεξεργασία γραπτών πινάκων ή σχολιασμών τα mashups έχουν τη δυνατότητα να δημιουργήσουν έναν καμβά για την διαχείριση και τον συνδυασμό δεδομένων.

Εφαρμογές Mashups υπάρχουν σε διάφορους τομείς εξυπηρετώντας πολλές και διαφορετικές ανάγκες των χρηστών. Βρίσκουν χρήση στην ανίχνευση κακόβουλων μηνυμάτων στο ηλεκτρονικό ταχυδρομείο, την εύρεση πληροφοριών για την εγκληματικότητα ή τα διαφημιστικά δίκτυα που συλλέγουν πληροφορία από διάφορες πηγές και προσαρμόζουν τη λειτουργία τους με βάση τη πληροφορία αυτή.

[6] **Tim O’Reilly, John Battelle.** *Web Squared: Web 2.0 Five Years On.* 2009.(σελ.1-10)

3.3.6 Συλλογή ετικετών (Folksonomy)

Οι ετικέτες (tags) είναι λέξεις κλειδιά που προστίθενται σε άρθρα που αναρτούνται σε blogs ή ιστοσελίδες μέσω εργαλείων ετικετών κοινωνικών σελίδων όπως το del.icio.us, Technorati, Yahoo's My Web. Τα περισσότερα blogs και οι διαδικτυακές δημοσιεύσεις χρησιμοποιούν ετικέτες. Για τις ετικέτες χρησιμοποιούνται οι λέξεις tags και labels, ενώ η διαδικασία δημιουργίας ετικετών είναι γνωστή ως tagging.

Ο όρος folksonomy αναφέρεται σε δημιουργημένες από τον χρήστη ταξινομήσεις της πληροφορίας. Αποτελεί ένα ad hoc σχήμα κατηγοριοποίησης που δημιουργείται καθώς οι χρήστες χρησιμοποιούν το διαδίκτυο και κατατάσσουν το περιεχόμενο που βρίσκουν online. Το folksonomy χρησιμοποιεί συνεταιριστικά παραγμένα, ανοικτού χρόνου tags ή labels τα οποία κατηγοριοποιούν περιεχόμενο όπως ιστοσελίδες, online φωτογραφίες και διαδικτυακές συνδέσεις. Ένα ιδιαίτερο χαρακτηριστικό του folksonomy είναι η έλλειψη ιεραρχίας όπως στις επαγγελματικά αναπτυγμένες ταξινομήσεις με ελεγχόμενα λεξιλόγια και εγγενώς αορίστου χρόνου. Τα folksonomies βρίσκουν χρήση σε Web 2.0 εφαρμογές όπως το Flickr με ετικέτες για τις φωτογραφίες δημιουργημένες από τους χρήστες.

Το Folksonomy ορίζεται ως η συλλογική σήμανση (collaborative tagging) και η μέθοδος συλλογικής δημιουργίας και διαχείρισης ετικετών για τον σχολιασμό και την κατηγοριοποίηση της πληροφορίας. Τα μεταδεδομένα που συνοδεύουν κάθε πληροφορία δημιουργούνται όχι μόνο από ειδικούς αλλά και από τους δημιουργούς και τους διαχειριστές του περιεχομένου. Οι λέξεις που χρησιμοποιούνται για ετικέτες στις πληροφορίες βοηθούν στην αναζήτηση της πληροφορίας από κάθε ενδιαφερόμενο χρήστη.

Η συγκεκριμένη υπηρεσία χρησιμοποιείται σε πολλές διαδικτυακές κοινότητες. Σε αυτές, οι διατάξεις για τη δημιουργία και τη χρήση ετικετών γίνονται σε επίπεδο τοποθεσίας. Οι κοινότητες αυτές δημιουργήθηκαν ώστε να επιτρέψουν στους χρήστες τη σήμανση και το μοίρασμα πληροφορίας, όπως οι φωτογραφίες, ή τη συλλογική σήμανση ήδη υπάρχοντος περιεχομένου, όπως ιστοτόποι, βιβλία, εργασίες και καταχωρήσεις σε blog.

Το Social bookmarking είναι η διαδικασία με την οποία οι χρήστες σημαδεύουν ενδιαφέρουσες σελίδες και τις αντιστοιχίζουν σε ετικέτες. Στην συνέχεια οι χρήστες έχουν τη δυνατότητα να μοιράζονται ετικέτες που αντιστοιχούν σε σημάνσεις σελίδων. Το Social bookmarking αποτελεί μία μέθοδο συλλογής γνώσης περιεχομένου.

Ένα tag cloud αποτελεί μια οπτική απεικόνιση μίας λίστας ετικετών περιεχομένου που χρησιμοποιούνται σε μια ιστοσελίδα ή ένα blog δίνοντας έμφαση στην οπτικοποίηση της δημοτικότητας κάθε ετικέτας. Συνήθως, οι ετικέτες με τη συχνότερη χρήση παρουσιάζονται με εντονότερο τρόπο σε σχέση με τις υπόλοιπες και παρατίθενται αλφαβητικά για πιο εύκολη αναζήτηση. Επιλέγοντας μία ετικέτα μέσα από ένα tag cloud, παρουσιάζονται όλα τα στοιχεία που σχετίζονται με αυτήν.

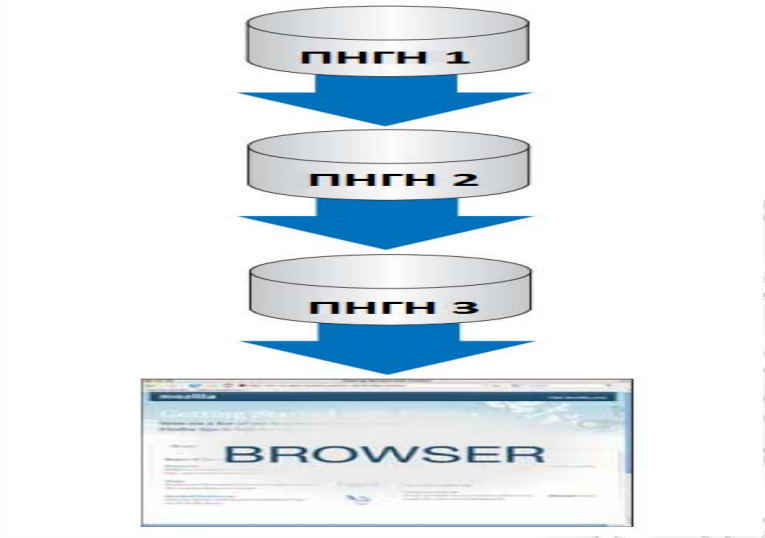
3.4 Αρχιτεκτονικές δομές Web 2.0

Οι αρχιτεκτονικές δομές στις Web 2.0 εφαρμογές ποικίλουν. Ανάλογα με τον αρχιτεκτονικό σχεδιασμό κάθε εφαρμογής και τους μηχανισμούς αναζήτησης και εμφάνισης της πληροφορίας προκύπτουν οι αρχιτεκτονικές δομές που παρουσιάζονται στη συνέχεια [7].

3.4.1 Σύνδεση πληροφορίας

Η σύνδεση της πληροφορίας (Information Syndication) γίνεται με την χρήση μηχανισμών όπως το RSS. Η πληροφορία περνάει από πολλούς εξυπηρετητές, εκδότες και παίρνει διάφορες μορφές μέχρι να φτάσει στον τελικό χρήστη. Όλη αυτή η κινητικότητα έχει αντίκτυπο στην αξιοπιστία της πληροφορίας καθώς είναι πιο εύκολη η εισαγωγή ψευδών στοιχείων σε ένα σύστημα. Στο επόμενο σχήμα απεικονίζεται η κίνηση της πληροφορίας μέχρι τον τελικό χρήστη σύμφωνα με την αρχιτεκτονική της σύνδεσης πληροφορίας .

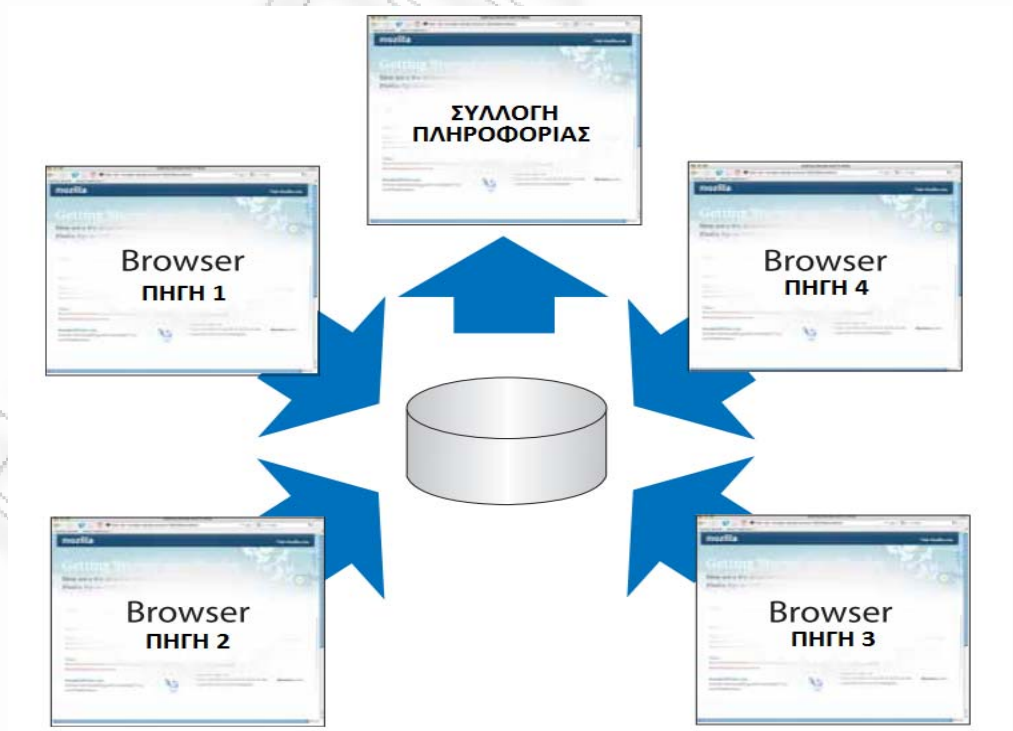
[7] **Giles Hogben, ENISA.** *Web 2.0 Security and Privacy.* 2008.(σελ.11-14)



Εικόνα 3.2: Αρχιτεκτονική δομή σύνδεσης πληροφορίας.
Πηγή: Giles Hogben, ENISA. ***Web 2.0 Security and Privacy.*** **2008.(σελ.11)**

3.4.2 Συνεργατική επεξεργασία

Η πληροφορία συλλέγεται από πολλούς χρήστες και παρουσιάζεται σαν ενιαία σαν ένα άρθρο ή πηγή προς τον τελικό χρήστη. Οι χρήστες που συμβάλουν στη συλλογή της πληροφορίας είναι συνήθως άγνωστοι και η ορθότητα της πληροφορίας που παράγεται στηρίζεται κυρίως στη φιλοσοφία της μεθόδου της γνώσης του πλήθους (wisdom of the crowds). Στο επόμενο σχήμα απεικονίζεται η συλλογή της πληροφορίας μέχρι τον τελικό χρήστη σύμφωνα με την αρχιτεκτονική της συνεργατικής επεξεργασίας (Collaborative Editing) της πληροφορίας.

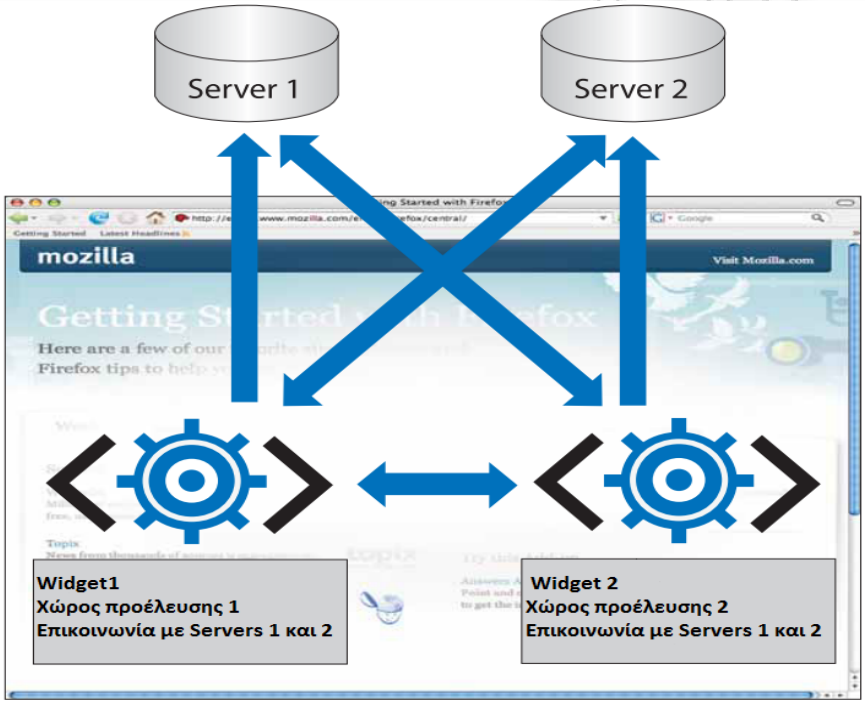


Εικόνα 3.3: Αρχιτεκτονική δομή συνεργατικής επεξεργασίας.
Πηγή: Giles Hogben, ENISA. ***Web 2.0 Security and Privacy.*** **2008.(σελ.12)**

3.4.3 Ενσωματωμένη επεξεργασία

Μια ενδιαφέρουσα παραλλαγή του τρόπου σύνδεσης της πληροφορίας στις εφαρμογές Web 2.0 αποτελεί ο widget provider. Στην ουσία είναι η πεμπτουσία των Web 2.0 εφαρμογών και όχι μια απλή εφαρμογή SOA. Το widget είναι ένα επαναχρησιμοποιήσιμο στοιχείο διεπαφής χρήστη, δημιουργημένο σε HTML, JavaScript, ή άλλη τεχνολογία Web 2.0. Χρησιμοποιείται για τη δημιουργία διεπαφής χρήστη σε μια υπηρεσία, η οποία μπορεί να περιέχει γραφικά, λογότυπα, ή ειδικούς ελέγχους. Ο πάροχος widget μονοπωλεί το ενδιαφέρον οργανισμών που θέλουν να παρέχουν πρόσβαση χρηστών σε πληροφορίες και υπηρεσίες, ενώ παράλληλα επιθυμούν να διατηρούν τον ρόλο του πάροχου υπηρεσιών και να ελέγχουν τον τρόπο παρουσίασης του περιεχομένου στους χρήστες.

Οι ιστοσελίδες συχνά περιέχουν widgets, εφαρμογές τεχνολογίας Javascript ή Ajax που προέρχονται από διάφορους εξυπηρετητές. Η λειτουργία τους πολλές φορές απαιτεί επικοινωνία με πολλούς εξυπηρετητές ή άλλα widgets της ίδιας σελίδας. Τέτοιες εφαρμογές είναι πολύ διαδεδομένες στις ιστοσελίδες κοινωνικής δικτύωσης καθώς και στην online εξατομικευμένη διαφήμιση. Στο επόμενο σχήμα απεικονίζεται η διαδραστικότητα της πληροφορίας μέσω των widgets.



Εικόνα 3.4: Αρχιτεκτονική δομή embedded widgets.

Πηγή: Giles Hogben, ENISA. *Web 2.0 Security and Privacy.* 2008.(σελ.13)

3.4.4 Συνεργατικά περιβάλλοντα

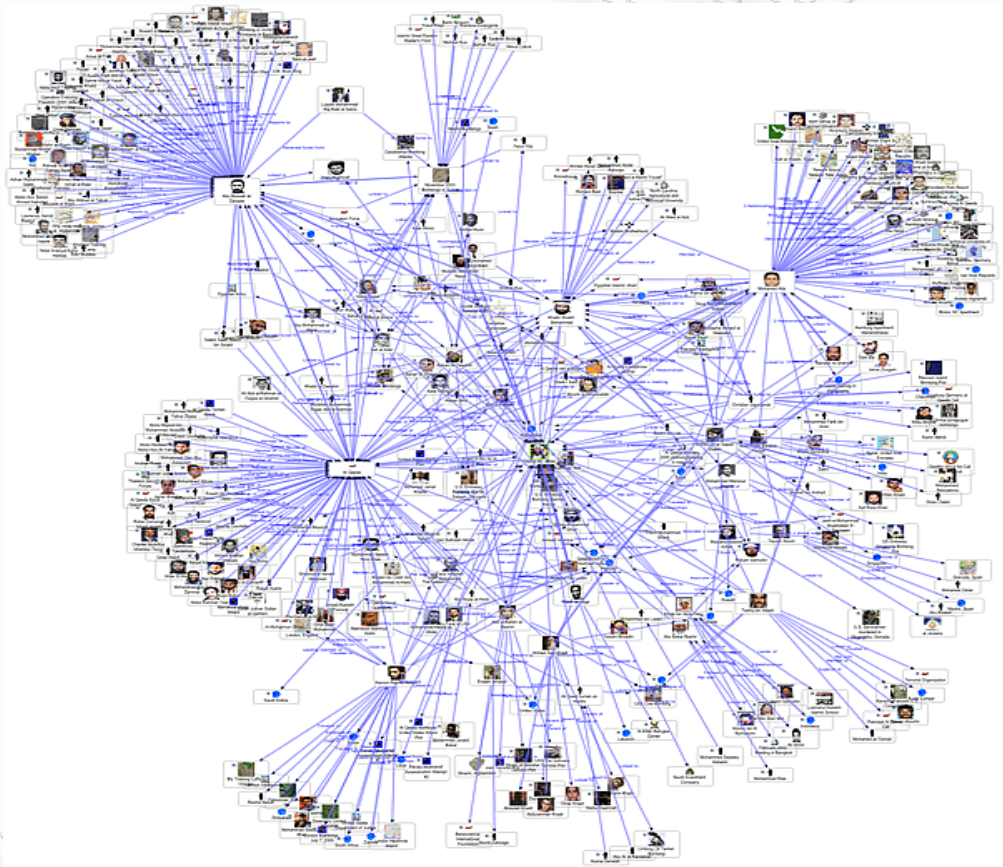
Τα συνεργατικά περιβάλλοντα (Collaborative environments) χωρίζονται σε δύο επιμέρους κατηγορίες, τα κοινωνικά δίκτυα (social networks) και τους χώρους συνεργασίας (collaborative workspaces). Η κατηγοριοποίηση γίνεται καθαρά με βάση το περιεχόμενο κάθε ιστοτόπου. Τα κοινωνικά δίκτυα περιλαμβάνουν ιστοτόπους που έχουν να κάνουν με την παρουσίαση και την διασύνδεση ατόμων, δημιουργώντας κοινωνικά σύνολα. Οι χώροι συνεργασίας περιλαμβάνουν κάθε άλλη εφαρμογή με σκοπό την εξυπηρέτηση και ενημέρωση χρηστών.

Οι χώροι συνεργασίας αποτελούνται από ένα ευρύτερο σύνολο εφαρμογών το οποίο μπορεί με την σειρά του να κατηγοριοποιηθεί σε συστήματα διαχείρισης περιεχομένου (Content Management Systems), σε μοντελοποίηση επιχειρηματικών διαδικασιών (Business Process Modeling), σε συστήματα διαχείρισης (Management Systems), σε εννοιολογικά συστήματα

(Semantics) και σε συστήματα διαχείρισης ταυτότητας και πρόσβασης (Identity and Access Management systems).

3.4.5 Κοινωνικά δίκτυα

Οι ιστότοποι κοινωνικής δικτύωσης (social networking websites) είναι χαρακτηριστικά παραδείγματα των συνεργατικών δικτύων (collaborative networks) και χρησιμοποιούν κατά κόρον υπηρεσίες διαδικτύου. Οι ιστοσελίδες αυτές, με την μορφή που έχουν σήμερα όπως είναι το Facebook και το LinkedIn έχουν γίνει αποδεκτές και χρησιμοποιούνται σε παγκόσμιο επίπεδο χαίροντας υψηλής επισκεψιμότητας και σε συνδυασμό με το γεγονός ότι ολοένα και περισσότερες υπηρεσίες αλλά και τεχνολογίες προσπαθούν να συνδεθούν με αυτές, είναι προφανές πως μια νέα εποχή για το διαδίκτυο έχει ξεκινήσει με αποτέλεσμα να αποδίδεται και η ανάλογη προσοχή σε θέματα που αφορούν τόσο άμεσες όσο και έμμεσες επιπτώσεις που προκύπτουν ή ενδεχομένως να προκύψουν μελλοντικά από την διαδραστικότητα και όχι μόνο από την οποία χαρακτηρίζεται το περιβάλλον λειτουργίας των ιστοτόπων κοινωνικής δικτύωσης[89].



Εικόνα 3.5:Απεικόνιση του ιστού ενός κοινωνικού δικτύου.

Πηγή: http://www.cosmoscience.gr/wp-content/uploads/2011/02/ SocialNetworkAnalysis_ Graph-1.gif

Στην προηγούμενη εικόνα παρουσιάζεται μια αναπαράσταση ενός κοινωνικού δικτύου, όπου κάθε οντότητα είναι συνδεδεμένη με γειτονικές της, δημιουργώντας ένα πολύπλοκο δίκτυο που δίνει την αίσθηση του ιστού. Οι ιστότοποι κοινωνικής δικτύωσης έχουν ως στόχο την δημιουργία ηλεκτρονικών διαδικτυακών κοινωνιών οι οποίες θα απαρτίζονται από άτομα

[8] **Giles Hogben, ENISA.** *Web 2.0 Security and Privacy.* 2008 (σελ.16)

[9] **Giles Hogben, ENISA.** *Security Issues and Recommendations for Online Social Networks.* 2007(σελ.6-7)

ανεξαρτήτου ηλικίας που θα μοιράζονται τα ίδια ενδιαφέροντα, θα ασχολούνται με κοινές δραστηριότητες αλλά ακόμα περισσότερο από άτομα που αρέσκονται σε αυτήν την μορφή ηλεκτρονικής επικοινωνίας μέσω διαδικτύου. Οι σελίδες αυτές παρέχουν στους χρήστες-μέλη τους τη δυνατότητα να επικοινωνούν μεταξύ τους μέσω ηλεκτρονικού ταχυδρομείου (e-mail) αλλά και με στιγμιαία μηνύματα σε πραγματικό χρόνο (instant messaging-chat).

Το social networking όπως συνηθίζεται να αποκαλείται η ενασχόληση με τέτοιου είδους ιστοσελίδες κοινωνικής φύσεως, ενθαρρύνει τους χρήστες στην ανεύρεση νέων τρόπων επικοινωνίας, ανταλλαγής πληροφοριών σε σημείο μάλιστα να έχει αναπτυχθεί παγκοσμίως μία ιδιαίτερη γλώσσα η οποία χρησιμοποιεί τα αρχικά γράμματα συγκεκριμένων εκφράσεων για λόγους συντομίας και λιγότερης χρήσης του πληκτρολογίου όπως π.χ lol,omg κ.λ.π. .

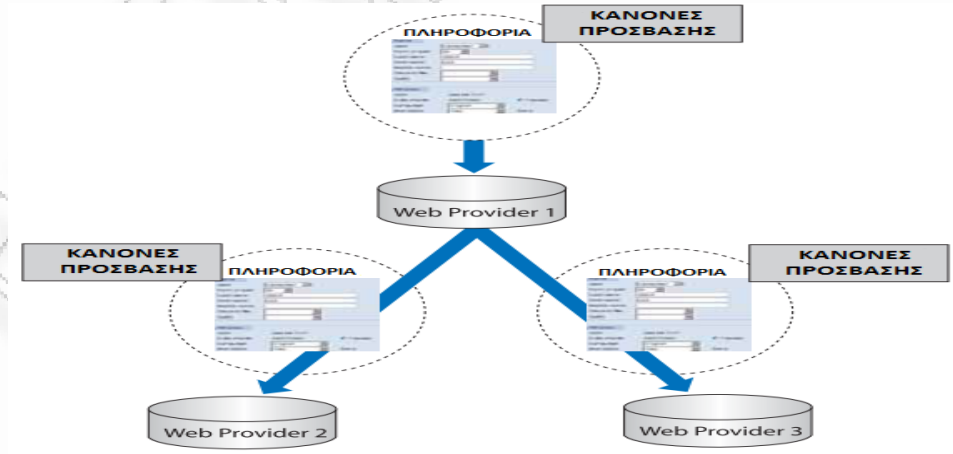
Οι ιστότοποι κοινωνικής δικτύωσης χρησιμοποιούνται ευρέως από εκατομμύρια ανθρώπους παγκοσμίως αλλά εκτός από φυσικά πρόσωπα, αναρίθμητες επιχειρήσεις και οργανισμοί ασχολούνται με αυτές τις ιστοσελίδες για επιχειρηματικούς και όχι μόνο σκοπούς απλά και μόνο γιατί είναι ένας πάρα πολύ εύκολος και οικονομικός τρόπος προσέγγισης μεγάλου αριθμού ανθρώπων μαζικά, σε όλα τα μήκη και πλάτη του πλανήτη και σε οποιαδήποτε χρονική στιγμή.

Ένα πολύ βασικό και κοινό χαρακτηριστικό σχεδόν όλων των ιστοτόπων κοινωνικής δικτύωσης είναι η δημιουργία συγκεκριμένων κατηγοριών βάσει των οποίων οι χρήστες προσπαθούν να γνωριστούν και να επικοινωνήσουν με ήδη υπάρχοντες και εγγεγραμμένους στη λίστα τους φίλους ή να κάνουν καινούριους και να επεκτείνουν έτσι την επικοινωνία τους. Τέτοιοι τρόποι αναζήτησης είναι μέσω της διεύθυνσης του ηλεκτρονικού ταχυδρομείου (e-mail) που όλοι οι χρήστες πρέπει να χρησιμοποιήσουν για να εγγραφούν σε μια τέτοιου είδους ιστοσελίδα, της χρονιάς αποφοίτησης από κάποιο σχολείο ή πανεπιστήμιο και πολλά άλλα.

Οι πιο δημοφιλείς ιστότοποι κοινωνικής δικτύωσης αυτήν τη στιγμή είναι το Facebook, το LinkedIn, και το MySpace με εκατομμύρια εγγεγραμμένους χρήστες ανά τον κόσμο. Στη συνέχεια θα ασχοληθούμε σε βάθος με όλες τις επιπτώσεις που επιφέρει η χρήση ιστοτόπων κοινωνικής δικτύωσης τόσο σε κοινωνικό όσο και σε νομικό επίπεδο.

3.4.6 Μεταφορά των δικαιωμάτων πρόσβασης

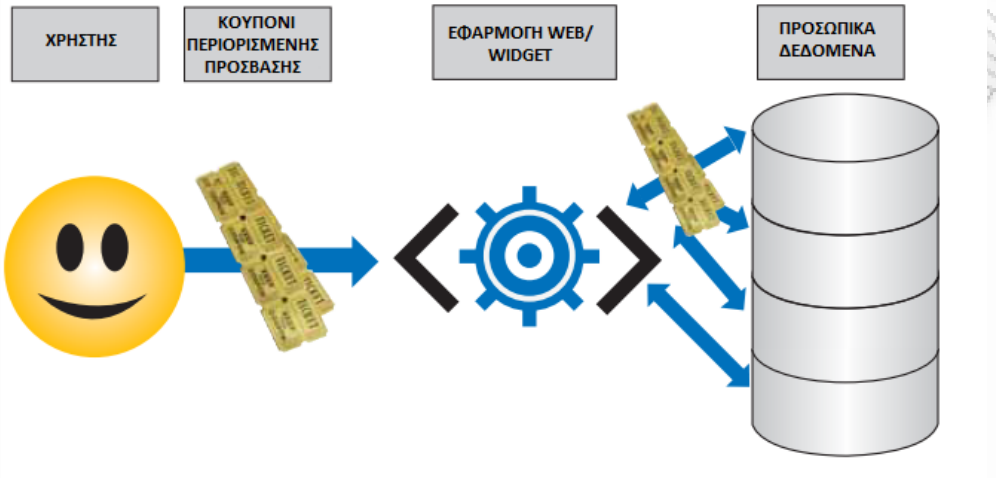
Η σύνδεση της πληροφορίας μεταξύ εφαρμογών Web 2.0 πολλές φορές επιβάλει την εφαρμογή ελέγχου πρόσβασης και κανόνων αυθεντικοποίησης. Η διαδικασία εξακρίβωσης της δυνατότητας πρόσβασης όταν πρόκειται για ευαίσθητα δεδομένα αποτελεί ένα πολύ σημαντικό κομμάτι των Web 2.0 εφαρμογών. Ο σωστός σχεδιασμός και η εφαρμογή τους συμβάλει στην δημιουργία ενός ασφαλούς περιβάλλοντος για τους χρήστες. Στο επόμενο σχήμα απεικονίζεται η διαδικασία ελέγχου και ταυτοποίησης των στοιχείων του χρήστη για την πρόσβαση στις υπηρεσίες ενός εξυπηρετητή.



Εικόνα 3.6: Απεικόνιση της διαδικασίας ελέγχου των δικαιωμάτων πρόσβασης.
Πηγή: Giles Hogben, ENISA. ***Web 2.0 Security and Privacy.*** **2008.(σελ.14)**

3.4.7 Αντιπροσωπία δικαιωμάτων πρόσβασης

Οι Web 2.0 εφαρμογές που προσφέρουν πρόσβαση σε άλλες εφαρμογές απαιτούν εξακρίβωση των δικαιωμάτων κάθε χρήστη στην προσπέλαση ευαίσθητης πληροφορίας. Στο επόμενο σχήμα απεικονίζεται η διαδικασία με την οποία ένας χρήστης μπορεί να έχει πρόσβαση σε προσωπικά δεδομένα. Εφόσον έχει στην κατοχή του ένα έγκυρο κουπόνι πρόσβασης γίνεται δυνατή η ανάκτηση των στοιχείων που επιθυμεί.



Εικόνα 3.7 : Επιβεβαίωση των δικαιωμάτων πρόσβασης με αντιπροσωπεία.
Πηγή: Giles Hogben, ENISA. ***Web 2.0 Security and Privacy.*** **2008.(σελ.14)**

4 Προβλήματα και Απειλές

Η χρήση Web 2.0 εφαρμογών έχει φέρει μεγάλη επανάσταση στην χρήση του διαδικτύου. Όπως έχει αναφερθεί και προηγουμένως, αξιοποιείται σε πολλούς τομείς και προσφέρει νέες δυνατότητες στους χρήστες. Το πλήθος των χρηστών αυξάνεται συνεχώς, ανακαλύπτοντας σε αυτό το μέσο επικοινωνίας δυνατότητες όχι μόνο ψυχαγωγίας, αλλά και επαγγελματικές. Το πρόβλημα έγκειται στην διασφάλιση της ακεραιότητας των κινήσεων ενός χρήστη στον χώρο του διαδικτύου και των Web 2.0 εφαρμογών.

Παράλληλα με την διάδοση της χρήσης των Web 2.0 εφαρμογών, εμφανίζονται και οι κακόβουλοι χρήστες που καιροφυλαχτούν για την υποκλοπή στοιχείων από ανυποψίαστους χρήστες. Η δράση τους, εάν δεν έχουν παρθεί τα απαραίτητα μέτρα, μπορεί να αποβεί καταστροφική. Τα θέματα αυτά θα παρουσιαστούν στην συνέχεια, κάνοντας αναφορά στα προβλήματα και τις απειλές που υπάρχουν στην χρήση Web 2.0 εφαρμογών.

Αρχικά, είναι σημαντικό να καθοριστεί η έννοια της ευαίσθητης πληροφορίας, η οποία αποτελεί τον στόχο των κακόβουλων ενεργειών και η οποία πρέπει να προστατευθεί. Έχοντας μια σαφή εικόνα του αντικειμένου το οποίο απειλείται, ακολουθεί η ανάλυση των απειλών που εμφανίζονται στις Web 2.0 εφαρμογές. Στην συνέχεια γίνεται αναφορά σε θέματα ιδιωτικότητας και στην σημαντικότητα ύπαρξης νομικών και θεσμικών πλαισίων για τον τρόπο δράσης των χρηστών στο διαδίκτυο. Τέλος, γίνεται ιδιαίτερη αναφορά στα προσωπικά δεδομένα των χρηστών στα πλαίσια ιστοτόπων κοινωνικής δικτύωσης, ενός χώρου που γνωρίζει ραγδαία ανάπτυξη και τα προσωπικά στοιχεία των χρηστών αποτελούν το κύριο αντικείμενό τους.

4.1 Ευαίσθητη πληροφορία

Στην προσπάθεια να καθορίσουμε τα προβλήματα και τις απειλές που προκύπτουν από την χρήση των Web 2.0 εφαρμογών, αρχικά πρέπει να οριστεί η ευαίσθητη πληροφορία. Η ευαίσθητη πληροφορία απαρτίζεται από όλα τα στοιχεία που διατρέχουν κίνδυνο στις Web 2.0 εφαρμογές. Μία από τις κατηγορίες στις οποίες μπορούμε να κατατάξουμε την ευαίσθητη πληροφορία είναι οι ιδιωτικές πληροφορίες του χρήστη. Το φλέγον ζήτημα για τις πληροφορίες αυτές είναι σε ποιο βαθμό μπορούν να κλαπούν και να χρησιμοποιηθούν για παρενόχληση, συκοφαντία ή spam. Παράλληλα, για τα οικονομικά στοιχεία ενός χρήστη πρέπει να διασφαλίζεται πόσο ασφαλή είναι στα πλαίσια των τραπεζικών συναλλαγών μέσω διαδικτύου ή σε πύλες ηλεκτρονικού εμπορίου.

Ιδιαίτερη σημασία έχει στις Web 2.0 εφαρμογές η εταιρική και η προσωπική φήμη των χρηστών εφόσον μπορούν να επηρεάσουν σε μεγάλο βαθμό τις επαφές τους. Έχοντας σαν στόχο την διασφάλιση της φήμης των χρηστών πρέπει να γίνει αναδρομή στους τρόπους αλλά και στον βαθμό που μπορεί να διαβληθεί η φήμη των οντοτήτων στις εφαρμογές. Ενώ πάντα υπάρχει και η άλλη όψη του ίδιου νομίσματος, στην δημιουργία καλής φήμης σε κακόβουλους χρήστες.

Εφόσον οι Web 2.0 εφαρμογές βρίσκουν όλο και μεγαλύτερο πεδίο δράσης στον τομέα των επιχειρήσεων, ευαίσθητη πληροφορία αποτελούν και τα εταιρικά μυστικά τους. Η πιθανότητα κλοπής τους μπορεί να προκαλέσει οικονομικές ζημιές ή και δυσφήμιση στον κλάδο στον οποίο δραστηριοποιείται η επιχείρηση. Παράλληλα, η πνευματική ιδιοκτησία αποτελεί το πλέον σημαντικό αγαθό για πολλούς ανθρώπους λόγω της φύσης της ενασχόλησής τους. Στην κατηγορία αυτή μπορούν να καταταχθούν άνθρωποι του πνεύματος, καλλιτέχνες, συγγραφείς, μουσικοί αλλά και προγραμματιστές. Η κλοπή του έργου τους μπορεί να σημαίνει μεγάλη καταστροφή τόσο οικονομική όσο και ηθική.

Οι Web 2.0 εφαρμογές εξαρτώνται σε μεγάλο βαθμό από τις μηχανές που τις υποστηρίζουν. Μείζον θέμα αποτελεί η υπερβολική αύξηση των υπολογιστικών αναγκών και η άρνηση εξυπηρέτησης των χρηστών. Ένα τέτοιο σενάριο θα μπορούσε να αναιρέσει τόσο την εμπιστοσύνη των χρηστών όσο και την επενδυτική δραστηριότητα των επιχειρήσεων σε αυτόν τον τομέα.

Κάνοντας αναφορά στην ευαίσθητη πληροφορία που μπορεί να υπάρχει στις Web 2.0 εφαρμογές, πρέπει να συμπεριληφθεί η φυσική ασφάλεια των χρηστών. Εξετάζοντας το κατά πόσο θα μπορούσε να υπάρξει τέτοιου είδους απειλή, μπορεί να αναφερθεί το ενδεχόμενο εντοπισμού των πραγματικών στοιχείων επικοινωνίας ενός χρήστη από έναν κακόβουλο χρήστη. Σε μία τέτοια περίπτωση ο χρήστης θα μπορούσε να είναι ανήλικος και τα προβλήματα να περνούν στην σφαίρα της κακοποίησης και της σεξουαλικής παρενόχλησης παιδιών.

4.2 Απειλές στις Web 2.0 εφαρμογές

Οι φυλλομετρητές (Web browsers),έχουν ανεξάντλητες δυνατότητες εκτέλεσης πολύπλοκων δικτυακών διαδικασιών. Οι δυνατότητες αυτές προσφέρουν πλούσιες σε περιεχόμενο ιστοσελίδες για την εξυπηρέτηση των χρηστών. Συγχρόνως όμως, δημιουργούν διόδους για την δράση κακόβουλων χρηστών. Στην συνέχεια αναλύονται οι απειλές που προκύπτουν στις Web 2.0 εφαρμογές[10].

4.2.1 Μη ασφαλής αρχιτεκτονική

Η αρχιτεκτονική του διαδικτύου στην οποία στηρίζονται οι εφαρμογές του web 2.0 θεωρείται μη ασφαλής κυρίως λόγω του ασθενούς μοντέλου ασφαλείας τόσο στην μεριά του πελάτη/χρήστη όσο και από τα σχεδιαστικά πρότυπα των εφαρμογών του web 2.0.

Η εκτέλεση εφαρμογών στην πλευρά του πελάτη/χρήστη περιλαμβάνει τρία διαφορετικά επίπεδα, τον κώδικα (script), τον φυλλομετρητή (browser) και το λειτουργικό σύστημα (operating system). Ο κώδικας εκτελείται μέσα στον browser, ο οποίος με την σειρά του τρέχει μέσα στα πλαίσια του λειτουργικού συστήματος.

Διαδικασίες για την εξασφάλιση της ασφάλειας στις εφαρμογές όπως η αυθεντικοποίηση και ο έλεγχος πρόσβασης χρηστών, εκτελούνται από το λειτουργικό σύστημα δίνοντας την εντύπωση ενός αξιόπιστου περιβάλλοντος.

Το πρόβλημα έγκειται στο ότι κατά την έναρξη της λειτουργίας του browser, το λειτουργικό σύστημα το θεωρεί έμπιστη εφαρμογή. Παράλληλα, έμπιστο θεωρεί και κάθε κομμάτι κώδικα που εκτελείται στον browser και του δίνει το ίδιο επίπεδο ασφάλειας άσχετα από την προέλευσή του και την λειτουργία του. Επομένως, το λειτουργικό σύστημα εμπιστεύεται οποιοδήποτε περιεχόμενο του browser, ενώ το περιεχόμενο του browser δεν ελέγχεται οπότε μπορεί να περιέχει οτιδήποτε. Ο μόνος τρόπος αποφυγής της εκτέλεσης τυχών κακόβουλου κώδικα, είναι η απενεργοποίηση της δυνατότητας εκτέλεσης κώδικα εντελώς.

4.2.2 Αναξιόπιστη πληροφορία

Οι εφαρμογές web 2.0 βασίζονται στην συνεργασία των χρηστών και την ανταλλαγή απόψεων και ιδεών. Πέρα από την ιδανική χρήση των εφαρμογών αυτών υπάρχουν και κακόβουλοι χρήστες που επωφελούνται από την ελευθερία που προσφέρεται με σκοπό οποιοδήποτε προσωπικό όφελος.

Τελικά, αναζητώντας πληροφορίες σε wikis, forums, blogs εντοπίζεται εύκολα περιεχόμενο ειδικά σχεδιασμένο για ‘ψάρεμα’ κίνησης, σελίδες με υψηλή κατάταξη σε μηχανές αναζήτησης με σκοπό οικονομικό κέρδος. Συχνά εντοπίζεται και περιεχόμενο σε μορφή ερωτήσεων με παρόμοιους σκοπούς.

Η ύπαρξη τέτοιου περιεχομένου οφείλεται στην ελλιπή αξιολόγηση της πληροφορίας που προσθέτει κάθε χρήστης, την έλλειψη φιλτραρίσματος της, αλλά και την ανοχή που δείχνουν οι χρήστες βλέποντας το όφελος της δωρεάν και εύκολα προσβάσιμης πληροφορίας που παρέχεται από το web2.0.

[10] **Giles Hogben, ENISA.** *Security Issues and Recommendations for Online Social Networks.* 2007. (σελ.8-16)

4.2.3 Παραποίηση ετικετών και δεικτών

Στις εφαρμογές web 2.0 εμφανίζονται τεχνικές όπως το tagging και το social Bookmarking λογαριασμών. Ένας κακόβουλος χρήστης μπορεί να δημιουργήσει μια πλαστή δημοτικότητα. Επίσης παρατηρείται συχνά η χρήση αρκετά διαδεδομένων bookmarking οι οποίες έχουν σαν σκοπό την διευκόλυνση της διαδικασίας εύρεσης πληροφορίας, την δημοτικότητα που φαίνεται να έχει, καθώς και την κατάταξή της με βάση την ποιότητα της πληροφορίας. Στην πράξη όμως, κακόβουλοι χρήστες χρησιμοποιούν τις τεχνικές αυτές ώστε να προωθήσουν τα προσωπικά τους συμφέροντα.

Δημιουργώντας μεγάλο αριθμό και με μεγάλη συχνότητα χρήσης λέξεων/tags ακόμη και αν είναι άσχετα προς το περιεχόμενο της εφαρμογής. Αυτές οι πράξεις εύκολα παρασύρουν πολλούς χρήστες σε spam sites καθώς εμφανίζονται στις πρώτες επιλογές που δίνονται σε μηχανές αναζήτησης.

4.2.4 Κενό της πολιτικής κοινής προέλευσης περιεχομένου

Το SOP (Same Origin Policy) αν και αποτελεί ένα μέτρο προφύλαξης για τα δεδομένα και τον κώδικα που βρίσκονται σε μια σελίδα ώστε να μην είναι προσβάσιμα από άλλες σελίδες που προέρχονται από άλλη πηγή, αντιμετωπίζει ένα σημαντικό μειονέκτημα. Υπάρχουν κάποιες εξαιρέσεις στον κανόνα απαγόρευσης της προσβασιμότητας. Σε ετικέτες όπως <script> και <img> επιτρέπεται να αναφέρονται σε άλλους χώρους, αποτελώντας ένα καλό μέσο υποβολής κακόβουλου κώδικα. Είναι σημαντικό να σημειωθεί ότι αφορά καθαρά και μόνο το domain path και όχι τις υποδιευθύνσεις, με αποτέλεσμα να μην εφαρμόζεται σε φιλοξενούμενο περιεχόμενο.

4.2.5 Επίθεση πλαστής αίτησης

Η επίθεση πλαστής αίτησης (Cross Site Request Forgery) μέσα από μια ιστοσελίδα, εκμεταλλεύεται τις αδυναμίες που παρουσιάζουν ο φυλλομετρητής αλλά και η ιστοσελίδα που αποτελεί στόχο. Ο φυλλομετρητής περιλαμβάνει αυτόματα, με αιτήματα για την ιστοσελίδα όλα τα συναφή διαπιστευτήρια, όπως τα στοιχεία συνόδου του χρήστη, την IP διεύθυνση, διαπιστευτήρια χώρου. Η διαδικασία αυτή λαμβάνει χώρα άσχετα από το σημείο του τερματικού του χρήστη στο οποίο παράχθηκε το αίτημα.

Οι κακόβουλοι χρήστες μεταμφιέζουν τις πλαστές αιτήσεις τους με ψεύτικες ετικέτες ή τις ενσωματώνουν σε φωτογραφικό υλικό ή κάτι ανάλογο. Η αδυναμία των Web 2.0 εφαρμογών έγκειται στο ότι συχνά πραγματοποιούν ενέργειες απαντώντας σε αιτήματα χρηστών, βάση αποθηκευμένων διαπιστευτηρίων στην πλευρά του πελάτη χωρίς δεύτερη επαλήθευση τους.

Στις Web 2.0 εφαρμογές οι επιθέσεις αυτού του είδους είναι πιο συχνές. Το αυξημένο περιεχόμενο που προέρχεται από χρήστες, οι περίπλοκοι κώδικες και τα αιτήματα AJAX παρέχουν στους κακόβουλους χρήστες πολύ περισσότερες ευκαιρίες για την απόκρυψη των πλαστών και κακόβουλων αιτήσεών τους.

4.2.6 Επίθεση κακόβουλου κώδικα

Η επίθεση με κακόβουλο κώδικα (Cross site scripting) μέσω μιας ιστοσελίδας, αποτελεί απειλή για το τερματικό του χρήστη. Ο δράστης επιτυγχάνει την εκτέλεση κώδικα στον φυλλομετρητή του χρήστη παρουσιάζοντας ότι προέρχεται από μια έμπιστη ιστοσελίδα. Κάθε επίθεση δημιουργείται για μια συγκεκριμένη ιστοσελίδα, αλλά ο τελικός στόχος είναι το τερματικό του χρήστη το οποίο και βρίσκεται πλήρως εκτεθειμένο στον κακόβουλο δράστη.

Όταν ο κακόβουλος κώδικας εκτελεστεί στον φυλλομετρητή του τερματικού του χρήστη, τόσο ο κώδικας όσο και ο δράστης έχουν πλήρη πρόσβαση στον υπολογιστή του χρήστη. Η δυνατότητα αυτή δίνεται από την δεδομένη ασφάλεια του υπολογιστή και η προσβασιμότητα του κακόβουλου δράστη μπορεί να επεκταθεί στα αρχεία, στις λειτουργίες και στην συνδεσιμότητα του υπολογιστή του χρήστη.

Η απειλή αυτή βρίσκει σε μεγάλο βαθμό ευάλωτους τους χρήστες Web 2.0 εφαρμογών, καθώς Web 2.0 τεχνολογίες, όπως η AJAX, απαιτούν από τα τερματικά να επιτρέπουν την εκτέλεση κώδικα σε αυτά. Σε συνδυασμό με το ασθενές μοντέλο ασφάλειας στην πλευρά του

πελάτη/χρήστη, τα τερματικά των χρηστών βρίσκονται εκτεθειμένα σε μεγάλο βαθμό σε αυτού του είδους τις επιθέσεις.

4.2.7 Σύνδεση κακόβουλου κώδικα

Στο Web 2.0 τα RSS, Blogs και Wikis αποτελούν τις σημαντικότερες φόρμες ανταλλαγής περιεχομένου. Χρησιμοποιούνται σχεδόν από κάθε σύστημα διαχείρισης γνώσης. Παράλληλα, χρησιμοποιούνται και από κακόβουλους χρήστες με σκοπό να επιτεθούν σε ανυποψίαστους χρήστες. Μέσω αυτών καταφέρνουν να διασκορπίσουν κακόβουλο κώδικα λόγω της μικρής ασφάλειας της αρχιτεκτονικής του browser.

4.3 Θέματα Ιδιωτικότητας

Η δράση των χρηστών στο διαδίκτυο και στις Web 2.0 εφαρμογές, όπως και κάθε άλλη πτυχή της ζωής, πρέπει να διασφαλίζεται από νομικά και θεσμικά πλαίσια. Τα νομικά και θεσμικά πλαίσια, μπορούν να οργανώσουν και να οριοθετήσουν τις ανεξέλεγκτες δράσεις στις Web 2.0 εφαρμογές που μπορεί να αποβούν εις βάρος ανυποψίαστων χρηστών.

Η θέσπιση και η τήρηση ενός νομικού και θεσμικού πλαισίου εμφανίζεται απαραίτητη. Το πλαίσιο αυτό θα έκανε αναφορά στα ζητήματα ασφαλείας και στα μέτρα που πρέπει να λαμβάνουν τα συμβαλλόμενα μέρη στις διαδικτυακές συναλλαγές βάση των ενδεχόμενων απειλών. Το αποτέλεσμά του θα ήταν η κάλυψη πάγιων ζητημάτων ασφαλείας στην χρήση Web 2.0 εφαρμογών. Τα ζητήματα αυτά είναι η αυθεντικοποίηση των χρηστών, η ακεραιότητα του περιεχομένου των συναλλαγών, η εμπιστευτικότητα μεταξύ των μερών και η διαθεσιμότητα των εφαρμογών.

Αναλύοντας τις απειλές που εγκυμονούν οι Web 2.0 εφαρμογές για έναν χρήστη, παρουσιάζεται η πραγματική δυσκολία της προστασίας της ιδιωτικότητας του χρήστη και του απορρήτου των πληροφοριών. Οι απειλές αυτές σχετίζονται άμεσα τόσο με νομικά όσο και με ηθικά προβλήματα.

Οι Web 2.0 εφαρμογές στηρίζονται σε αποκεντρωμένες πλατφόρμες, με ελεύθερη πρόσβαση, εντείνοντας τον κίνδυνο κακόβουλων ενεργειών. Η αποκέντρωση και η μεταφορά του μεγαλύτερου μέρους επεξεργασίας στο μέρος του χρήστη, αυξάνει την πιθανότητα δημιουργίας επιθέσεων. Η ελεύθερη ανταλλαγή πολυμεσικού υλικού αυξάνει τον κίνδυνο εξάπλωσης ιών και διείσδυσης κακόβουλων χρηστών στα τερματικά χρηστών. Η ευκολία πρόσβασης, διαχείρισης και τροποποίησης περιεχομένου στον εξυπηρετητή μπορεί να οδηγήσει σε επιθέσεις στον εξυπηρετητή. Γενικά, η χρήση των Web 2.0 εφαρμογών φαίνεται διάχυτη από κακόβουλο περιεχόμενο με δυνατότητα γρήγορης και μεγάλης εξάπλωσης.

Υπάρχει αύξηση της πιθανότητας δημιουργίας κακόβουλων και επικίνδυνων κοινοτήτων. Οι κοινότητες αυτές, κάνοντας χρήση της ανωνυμίας, μπορούν με χαμηλό κόστος να δημιουργήσουν πλατφόρμες για αλληλεπίδραση, επικοινωνία και ανταλλαγή πληροφορίας. Οι ανυποψίαστοι χρήστες μπορούν εύκολα να συμμετάσχουν σε μια τέτοια κοινότητα μη γνωρίζοντας τους πραγματικούς σκοπούς των δημιουργών της. Παράλληλα, τα κοινωνικά δίκτυα και οι κοινότητες δίνουν ιδιαίτερη αξία στους συμμετέχοντες, οδηγώντας σε κοινωνικές ανισότητες λόγω ψηφιακού αποκλεισμού.

Η δυνατότητα δημιουργίας περιεχομένου από τον χρήστη που δίνεται στις Web 2.0 εφαρμογές, προβληματίζει με την εμφάνιση υπερφόρτωσης δεδομένων, περιττής πληροφορίας, ανοργάνωτου περιεχομένου και αυξημένου κόστους και πολυπλοκότητας αναζήτησης. Η ευκολία πρόσβασης οδηγεί στη δημιουργία περιεχομένου αμφίβολης ποιότητας. Η περιττή και ανακριβής πληροφορία μπορεί να μειώσει την ποιότητα του περιεχομένου και την αξιοπιστία ειδικά σε wikis.

4.4 Τα προσωπικά δεδομένα στα κοινωνικά δίκτυα

Κάθε χρήστης ιστοτόπου κοινωνικής δικτύωσης είναι αυτόματα και χρήστης εφαρμογών Web 2.0, με αποτέλεσμα να εμφανίζονται όλα τα προβλήματα που υπάρχουν από την χρήση ανάλογων εφαρμογών. Τα δεδομένα στους ιστοτόπους κοινωνικής δικτύωσης συλλέγονται με

βασικό σκοπό την εύρεση και την επικοινωνία μεταξύ των χρηστών. Παράλληλα όμως, χρησιμοποιούνται και για άλλους, δευτερεύοντες σκοπούς, που αναφέρονται στους όρους χρήσης και με αυτό τον τρόπο γίνονται αποδεκτοί από τους χρήστες. Η χρήση που γίνεται στα δεδομένα αυτά αφορά συνήθως διαφημιστικούς σκοπούς. Παρόλα αυτά, μπορεί να χρησιμοποιηθούν νόμιμα ή μη για εμπορικούς σκοπούς, σε νομικά θέματα, ή και σε μυστικές υπηρεσίες[11].

Από την τεχνική πλευρά, η χρήση δεδομένων από χρήστες ιστοτόπων κοινωνικής δικτύωσης είναι πιο απλή σε σχέση με το παραδοσιακό ηλεκτρονικό εμπόριο. Το πιο σημαντικό στοιχείο είναι ότι οι πληροφορίες των χρηστών είναι δημόσιες και περιβάλλονται από προσδιορισμούς (semantic markup), κάνοντας την εξόρυξη τους ακόμη πιο εύκολη. Παρατηρείται ότι ενώ η νομική κάλυψη την χρηστών είναι η ίδια όπως σε άλλους ιστοτόπους, από την τεχνική πλευρά η χρήση και η κατάχρηση των πληροφοριών του χρήστη είναι πολύ πιο εύκολη.

Σε ιστοτόπους κοινωνικής δικτύωσης τα προβλήματα που εμφανίζονται είναι κυρίως ηθικής φύσης. Ένας χρήστης μπορεί να δημιουργήσει ένα λογαριασμό, δηλώνοντας στοιχεία μη πραγματικά, όμως κανείς δεν θα εμποδίσει μια τέτοια ενέργεια. Σε αυτή την περίπτωση θα μπορούσε ένα άτομο να παραποιήσει την ηλικία του, να εμφανιστεί ως ανήλικος και με αυτό τον τρόπο να προσεγγίσει ανήλικα άτομα. Μια τέτοια πράξη θεωρείται κακουργηματική και πρέπει να υπάρχει η δυνατότητα να αποδειχθεί και να διωχθεί νομικά.

Εξετάζοντας την ηθική βλάβη που θα μπορούσε να υποστεί ένας άνθρωπος, δημιουργούνται σενάρια κακόβουλης δράσης. Αρχικά, ένας οποιοσδήποτε χρήστης έχει τη δυνατότητα να εμφανίζεται σε ιστοτόπους κοινωνικής δικτύωσης με τα στοιχεία ενός άλλου ατόμου, εν αγνεία του. Θα είχε την δυνατότητα να παρουσιάζει πληροφορίες και ιδέες που να θίγουν το άτομο αυτό στο υπόλοιπο σύνολο, καταστρέφοντας την φήμη του. Λόγω της ελευθερίας που υπάρχει στην ανάρτηση περιεχομένου, σχολιασμών, φωτογραφιών ένα άτομο ακόμη και αν δεν υποκλαπεί η ταυτότητα του, να δυσφημιστεί από τον σχολιασμό άλλων. Η δυσφήμιση ενός ατόμου μπορεί να προκαλέσει αρνητικές επιπτώσεις και στην προσωπική ή και την επαγγελματική του ζωή.

[11] **Weijun Zheng, Leigh Jin.** *Online Reputation Systems in Web 2.0 Era .* 2009 (σελ.296-306)

5 Μηχανισμοί Προστασίας

Η διασφάλιση ενός ασφαλούς περιβάλλοντος στις Web 2.0 εφαρμογές αποτελεί τον σημαντικότερο στόχο κατά την υλοποίηση των εφαρμογών. Λαμβάνοντας υπόψη τα προβλήματα και τις απειλές που εγκυμονούν οι διαδικτυακές εφαρμογές, είναι απαραίτητο να δημιουργηθούν οι ανάλογοι μηχανισμοί προστασίας που να διασφαλίζουν την ιδιωτικότητα και την προστασία των χρηστών των Web 2.0 εφαρμογών .

Τα σημαντικότερα ζητήματα ασφαλείας που καλείται να καλύπτει κάθε διαδικτυακή εφαρμογή είναι η αυθεντικοποίηση των χρηστών, η ακεραιότητα του περιεχομένου, η εμπιστευτικότητα της πληροφορίας και η διαθεσιμότητα των εφαρμογών. Στα πλαίσια αυτά γίνεται αναζήτηση των βέλτιστων τεχνικών που μπορούν να χρησιμοποιηθούν για την κάλυψη της μεγαλύτερης ανάγκης των Web 2.0 εφαρμογών, της ασφάλειας.

Αναλύοντας τους μηχανισμούς προστασίας των Web 2.0 εφαρμογών , γίνεται αναφορά στις σχεδιαστικές απαιτήσεις για την προστασία από απειλές στο Web 2.0. Είναι σημαντική η ανάπτυξη ενεργών URL πραγματικού χρόνου με βάση την φήμη και φιλτράρισμα των μηνυμάτων, η προστασία από κακόβουλο κώδικα, το φιλτράρισμα και ο έλεγχος των εφαρμογών, η παρακολούθηση και η προστασία της σύνδεσης δεδομένων, η διασφάλιση ασφαλούς ανάπτυξης των proxies και caches, ο σχεδιασμός επιπέδων άμυνας και η χρήση ισχυρού συστήματος διαχείρισης και ελέγχου.

Οι μηχανισμοί προστασίας στις Web 2.0 εφαρμογές καθορίζονται από πολλούς τομείς δραστιριοποίησης. Στο πλαίσιο αυτό γίνεται αναφορά στην κυβερνητική πολιτική , τις ερευνιτικές κατευθύνσεις, την ευαισθητοποίηση των χρηστών, την προτυποποίση των μηχανισμών προστασίας, αλλά και τα θέματα που αφορούν τον πάροχο και τον κατασκευαστή.

Η διαχείρηση ταυτοτήτων αποτελεί ένα σημαντικό κομμάτι των μηχανισμών προστασίας των Web 2.0 εφαρμογών. Η διαχείρηση ταυτοτήτων στιρίζεται στην εφαρμογή ρόλων και διασφαλίζει τα επίπεδα προσβασιμότητας των χρηστών στις Web 2.0 εφαρμογές. Η πιστοποίηση της ταυτότητας των χρηστών γίνεται με την χρηση ηλεκτρονικών ταυτοτήτων και διαδικασιών ελέγχου πρόσβασης.

Η εφαρμογή μηχανισμών προστασίας είναι σημαντική και στα κοινωνικά δίκτυα. Σε εφαρμογές κοινωνικής δικτύωσης είναι σημαντική η χρήση μηχανισμών και συστημάτων καταγραφής της συμπεριφοράς των χρηστών. Η καταγραφή της συμπεριφοράς γίνεται με την χρήση μοντέλων αξιολόγησης. Τα πιο διαδεδομένα πρωτόκωλλα που χρησιμοποιούνται είναι το μοντέλο αθροιστικής ή μέσου όρου αξιολόγηση και το μοντέλο αξιολόγησης ροής.

5.1 Σχεδιαστικές απαιτήσεις προστασίας στο Web 2.0

Ο σχεδιασμός μιας εφαρμογής Web 2.0 αποτελεί ένα πολύ σημαντικό στάδιο δημιουργίας και πρέπει να δοθεί ιδιαίτερη σημασία σε αυτό. Η λειτουργικότητα του συστήματος βασίζεται σε αυτό το στάδιο. Πρέπει να πληρούνται κάποιες προϋποθέσεις και να καλύπτονται οι βασικές απαιτήσεις για την παροχή μιας ολοκληρωμένης εφαρμογής. Κατά το στάδιο αυτό πρέπει να καταλειφθούν οι σχεδιαστικές απαιτήσεις για την προστασία από τις απειλές του Web 2.0. Στην συνέχεια γίνεται ανάλυση των απαιτήσεων αυτών[12].

5.1.1 Ανάπτυξη συστημάτων φήμης

Η ύπαρξη ενός παγκόσμιου συστήματος καταγραφής συμπεριφοράς (reputation system) που να εκχωρεί την φήμη των χρηστών σε διευθύνσεις, και να επεξεργάζεται κατηγοριοποιημένες βάσεις δεδομένων, παρέχει ένα σημαντικό επίπεδο προστασίας, πολύ πιο ισχυρό από το απλό φιλτράρισμα διευθύνσεων. Ένα σύγχρονο σύστημα φήμης προστατεύει από τον κίνδυνο που εγκυμονεί η λήψη δεδομένων από έναν ιστοχώρο. Το σύστημα αυτό

[12] **Giles Hogben, ENISA.** *Web 2.0 Security and Privacy.* 2008.(σελ.19-32)

μπορεί να λειτουργήσει σε συνδυασμό με την πολιτική ασφάλειας ενός οργανισμού. Οι αποφάσεις σε αυτή την περίπτωση στηρίζονται και στις δύο πηγές πληροφόρησης. Το σύστημα φήμης παρέχει προστασία τόσο σε επίπεδο δικτύου όσο και σε επίπεδο μηνυμάτων. Αυτό είναι σημαντικό γιατί πολύ συχνά οι κακόβουλες επιθέσεις στηρίζονται σε πολλαπλά πρωτόκολλα.

5.1.2 Προστασία από κακόβουλο κώδικα

Ο έλεγχος ύπαρξης κακόβουλου υλικού πρέπει να εφαρμόζεται σε όλες τις θύρες επικοινωνίας με το διαδίκτυο. Τα συστήματα ελέγχου έχουν μηχανή προστασίας με βάση τις υπογραφές, για τον εντοπισμό γνωστών απειλών. Όμως, είναι απαραίτητοι και μηχανισμοί προστασίας από άγνωστες απειλές. Επί της ουσίας τα συστήματα πρέπει να περιλαμβάνουν εξέταση της φήμης των ιστοτόπων, ανάλυση συμπεριφοράς πραγματικού χρόνου και έλεγχο του περιεχομένου. Τα προηγούμενα συνθέτουν την ανάλυση με βάση την πρόθεση, που πρέπει να εφαρμόζεται σε κάθε μορφής κώδικα που προορίζεται να εκτελεστεί στον φυλλομετρητή του χρήστη.

5.1.3 Φιλτράρισμα και έλεγχος εφαρμογών στη θύρα εισόδου

Στις εφαρμογές που επικοινωνούν με τους χρήστες είτε με κρυπτογραφημένα είτε μη κρυπτογραφημένα πρωτόκολλα, πρέπει να γίνεται έλεγχος και προς τις δύο κατευθύνσεις. Στον έλεγχο περιλαμβάνονται ο έλεγχος πρόσβασης σε κάθε εφαρμογή, και η παρακολούθηση την συνδέσεων για τυχών εισβολή κακόβουλου υλικού ή διαρροής πληροφορίας. Δεδομένου του αυξημένου όγκου κρυπτογραφημένης πληροφορίας (https), αποτελεί επιτακτική ανάγκη η δυνατότητα επιλεκτικής αποκωδικοποίησης τέτοιου περιεχομένου στην θύρα επικοινωνίας ώστε να παρέχεται ασφάλεια με σεβασμό προς την ιδιωτική ζωή του χρήστη.

5.1.4 Παρακολούθηση της σύνδεσης δεδομένων

Η διαδικασία παρακολούθησης και προστασίας της σύνδεσης αποτελεί τον πιο σίγουρο τρόπο διασφάλισης ενός χρήστη από κακόβουλες ενέργειες. Στην ουσία περιλαμβάνει τέσσερα στάδια, τον ορισμό πολιτικών συνεργασίας και κανονισμών, τον εντοπισμό τους, την εφαρμογή τους, και την αναφορά των συμβάντων. Η διαδικασία αυτή πρέπει να εφαρμόζεται στα δεδομένα, κρυπτογραφημένα και μη, είτε αφορούν την δικτυακή κίνηση είτε τα μηνύματα. Ιδιαίτερα για τις εφαρμογές, εφαρμόζεται έλεγχος πρόσβασης και παρακολούθηση των συνδέσεων μεταφοράς δεδομένων. Για τον έλεγχο πρόσβασης είναι σημαντικό να υπάρχει η δυνατότητα επιλεκτικής αποκρυπτογράφησης κρυπτογραφημένης κίνησης στην πύλη εισόδου ώστε να παρέχεται ασφάλεια με σεβασμό στο απόρρητο ορισμένων ιστοτόπων.

5.1.5 Διασφάλιση ασφαλών εξυπηρετητών

Οποιοδήποτε αντικείμενο προσωρινής μνήμης πρέπει να εξετάζεται για τυχόν ύπαρξη κακόβουλου υλικού, για την ασφαλή καταγραφή συμπεριφοράς, και την πολιτική φιλτραρίσματος URL,πριν δοθεί στο browser του αιτούντος. Τα αντικείμενα προσωρινής μνήμης πρέπει να περνούν κάθε φορά από αυτά τα φίλτρα εφόσον η φήμη τους μπορεί να έχει αλλάξει από την στιγμή της δημιουργίας τους. Επίσης, η πολιτική ασφαλείας του αιτούντα μπορεί να είναι διαφορετική σε σχέση με άλλους αιτούντες στο θέμα της ασφαλούς φήμης, της πολιτικής φίλτρου URL και το κακόβουλο υλικό. Η ύπαρξη εξυπηρετητών που δεν φροντίζουν για την ασφάλεια γεννά τον κίνδυνο παράδοσης κακόβουλου κώδικα στον χρήστη.

5.1.6 Σχεδιασμός επιπέδων άμυνας

Οι πύλες αποτελούν ένα καίριο σημείο για την εφαρμογή πολιτικής ασφαλείας και ελέγχου. Είναι σημαντικό να διασφαλιστεί ότι οι συσκευές είναι ασφαλείς, παρέχοντας επίπεδα ασφαλείας των συσκευών. Στην πράξη η πιο αποτελεσματική άμυνα προσφέρεται με τον συνδυασμό συστημάτων άμυνας με βάση τις υπογραφές, με βάση την καταγραφή συμπεριφοράς και με βάση την πρόθεση. Η διαχείριση του κινδύνου στις δικτυακές πύλες

απαιτεί μία εφαρμογή που να συνδυάζει την ασφάλεια και τις μηχανές κρυφής μνήμης. Επιπλέον προστασία προσφέρεται με την αντικατάσταση επιμέρους λύσεων με ένα ολοκληρωμένο πακέτο προστασίας πιο λειτουργικό και πιο αποτελεσματικό. Στις δικτυακές εφαρμογές είναι το ίδιο σημαντική η προστασία εσωτερικά και εξωτερικά. Οι λύσεις που διαχειρίζονται τον κίνδυνο της κίνησης και προς τις δύο κατευθύνσεις μειώνουν το κόστος και αυξάνουν την ασφάλεια.

5.1.7 Άμεση διαχείριση και αναφορά ελέγχου

Οι επιχειρήσεις πρέπει να αναπτύξουν λύσεις που να παρέχουν αυτόματα αναφορά της κατάστασης και της υγείας του ηλεκτρονικού ταχυδρομείου και των διαδικτυακών πηλών. Παράλληλα, χρειάζεται ενημέρωση πραγματικού χρόνου για τα συμβάντα ώστε να γίνει επίλυση των προβλημάτων και ανάλυση του συμβάντος. Ένα ισχυρό σύστημα διαχείρισης και εκτενής αναφορά των συμβάντων δίνουν την δυνατότητα κατανόησης του κινδύνου, επαναπροσδιορισμό της πολιτικής και εφαρμογή των ανάλογων μέτρων.

5.2 Μηχανισμοί προστασίας στις εφαρμογές Web 2.0

Εξετάζοντας τις απειλές που εμφανίζονται στις Web 2.0 εφαρμογές, απαιτούνται ορισμένοι μηχανισμοί προστασίας για την ασφαλέστερη χρήση τους. Οι μηχανισμοί προστασίας έχουν ως στόχο την βέλτιστη λειτουργία των Web 2.0 εφαρμογών, παρέχοντας στον μεγαλύτερο δυνατό βαθμό ασφάλεια και προστασία στους χρήστες από κακόβουλες ενέργειες. Οι μηχανισμοί προστασίας αναφέρονται στην συνέχεια κατηγοριοποιημένοι με βάση την ομάδα στην οποία αφορούν. Έτσι έχουμε την κυβερνητική πολιτική η οποία πρέπει να εφαρμοστεί, τις ερευνητικές κατευθύνσεις που πρέπει να ακολουθηθούν, τους χρήστες που πρέπει να ευαισθητοποιηθούν και να ενημερωθούν, την προτυποποίηση που πρέπει να εφαρμοστεί, τις υποχρεώσεις που έχουν οι πάροχοι και οι κατασκευαστές, ώστε να επιτευχθεί ένα ολοκληρωμένο πλαίσιο λειτουργίας για τις Web 2.0 εφαρμογές[13].

5.2.1 Κυβερνητική πολιτική

Η κυβέρνηση πρέπει να προσφέρει πολιτικές κινήτρων για πρακτικές ασφαλούς ανάπτυξης εφαρμογών. Παράδειγμα τέτοιων κινήτρων αποτελεί ο σχεδιασμός περιορισμένων σε έκταση και οικονομικότερων χρηματικά εκδόσεων σχημάτων ασφαλούς πιστοποίησης (Certifications-lite), αποτελούν ιδανική λύση για μικροεφαρμογές προωθώντας παράλληλα καλύτερες πρακτικές ασφάλειας μεταξύ των παρόχων Web 2.0 εφαρμογών. Ένα άλλο χρήσιμο μοντέλο πολιτικής κινήτρων αποτελεί η Ελβετική ομοσπονδιακή πράξη προστασίας δεδομένων, σύμφωνα με την οποία καθορίζονται εθελοντικές απαιτήσεις πιστοποίησης παρακινώντας τις επιχειρήσεις να συμμορφωθούν με αυτά παρέχοντας τους απαλλαγή από ακριβές αναφορές.

Η χρηματοδότηση πιλοτικών δράσεων ενσωμάτωσης χαρακτηριστικών ασφαλείας στις Web 2.0 εφαρμογές προωθεί την δημιουργία πιο ασφαλούς περιβάλλοντος για όλους τους χρήστες. Παράλληλα, η κυβέρνηση πρέπει να επενδύσει και να απευθυνθεί στους Web 2.0 πάροχους για θέματα σχετικά με τις αντικρουόμενες υποχρεώσεις που επιφέρει η νομοθεσία. Το έργο των παρόχων πολλές φορές δυσχεραίνεται από τις διατυπώσεις του νομοθετικού και θεσμικού πλαισίου. Με την συνεργασία όμως με την κυβέρνηση μπορεί να βρεθεί μια πάγια και αποδεκτή λύση υλοποίησης της παροχής Web 2.0 εφαρμογών. Είναι επίσης σημαντικό να επιτευχθεί η απαραίτητη ισορροπία στις Web 2.0 εφαρμογές μεταξύ της αναγνώρισης από τους εμπόρους, τον νόμο και τους ιδιώτες από τη μία μεριά και από την άλλη μεριά την προστασία της ιδιωτικής ζωής και της ανωνυμίας των τελικών χρηστών.

5.2.2 Ερευνητικές κατευθύνσεις

Οι έρευνες αποτελούν πολύ σημαντικό μέρος για την ανάπτυξη και την ασφάλεια των Web 2.0 εφαρμογών. Οι Web 2.0 εφαρμογές γίνονται όλο και πιο σημαντικές, εξυπηρετούν

[13] **Giles Hogben, ENISA.** *Web 2.0 Security and Privacy.* 2008.(33-37)

περισσότερους χρήστες και παρέχουν σημαντικές υπηρεσίες. Η δημιουργία ενός ισχυρού πλαισίου ασφάλειας κατά την χρήση των εφαρμογών αυτών διασφαλίζει τους χρήστες και προωθεί τη διεύρυνση του πεδίου εφαρμογών Web 2.0.

Ένα από τα βασικά σημεία έρευνας αποτελεί το κομμάτι της χρηστικότητας των πρωτοκόλλων TLS/SSL. Τα πρωτόκολλα TLS/SSL και η κρυπτογράφηση των δεδομένων που μεταφέρονται στις Web 2.0 εφαρμογές δεν χρησιμοποιούνται ευρέως σε μεγάλο βαθμό. Η χρήση τους επιθυμείται ώστε η κρυπτογράφηση της πληροφορίας να γίνεται από άκρη σε άκρη και να βελτιωθεί η πιστοποίηση του παρόχου στις Web 2.0 εφαρμογές.

Η χρήση ισχυρότερων μηχανισμών πιστοποίησης βοηθάει στην προστασία των ευαίσθητων δεδομένων του χρήστη. Ένα από τα σημαντικότερα εμπόδια στην ευρεία χρήση της είναι η επιβάρυνση του χρήστη. Προκειμένου η ισχυρή πιστοποίηση να αποτελέσει μία εναλλακτική πρακτική στις Web 2.0 εφαρμογές, πρέπει να δοθεί λύση σε ορισμένα θέματα που προκύπτουν όπως η πολυπλοκότητα του συστήματος κουπονιών, όπου κάθε υπηρεσία χρειάζεται διαφορετικό κουπόνι. Χρειάζεται έρευνα ώστε διαφορετικές υπηρεσίες να μοιράζονται κουπόνια χωρίς απαραίτητα να μοιράζονται τα ίδια δεδομένα. Παράλληλα, η δυνατότητα εφαρμογής και χρήσης μηχανισμών ισχυρής πιστοποίησης όπως οι έξυπνες κάρτες, στις Web 2.0 εφαρμογές θα βοηθούσε στην δημιουργία ασφαλέστερων χώρων δράσης.

Σημαντικό κομμάτι για έρευνα αποτελεί η αποφυγή κακόβουλων ενεργειών προς τον τελικό χρήστη. Οι Web 2.0 εφαρμογές προσφέρουν δημόσια ανοιχτές διεπαφές για την είσοδο δεδομένων και την ανταλλαγή περιεχομένου που δημιουργείται από τον χρήστη. οι διεπαφές αυτές συχνά παρενοχλούνται από κακόβουλες ενέργειες όπως το spamming. Οι τεχνολογίες που περιορίζουν την χρήση τέτοιων πηγών με νόμιμα πρότυπα αποτελούν μια σοβαρή αδυναμία στα Web 2.0 περιβάλλοντα η οποία πρέπει να επιλυθεί ώστε να μην αποτελεί κίνδυνο για τους χρήστες.

Η διασφάλιση της σωστής λειτουργίας της έμπιστης υποδομής των ιστοτόπων κοινωνικής δικτύωσης διασφαλίζει την ασφάλεια των στοιχείων των χρηστών. Οι ιστοτόποι κοινωνικής δικτύωσης παρουσιάζουν μεγάλη πιθανότητα συλλογής έμπιστης πληροφορίας με την χρήση συστημάτων εμπιστοσύνης. Η συνολική εμπιστοσύνη που ενσωματώνεται στους βαθμούς φήμης που συλλέγονται από τους ιστοτόπους κοινωνικής δικτύωσης μπορεί να βοηθήσει στο φιλτράρισμα του περιεχομένου και την γνησιότητα των ισχυρισμών.

Επιπλέον ασφάλεια παρέχει η ανάπτυξη διαδικασιών ελέγχου της προέλευσης των πληροφοριών. Η ανάγκη έρευνας εστιάζεται στους μηχανισμούς εντοπισμού της καταγωγής και της φερεγγυότητας των πηγών πληροφόρησης. Οι απαιτήσεις των Web 2.0 εφαρμογών ως προς την ανάπτυξη των διαδικασιών αυτών περιλαμβάνουν τον σεβασμό στην ιδιωτικότητα και την πιθανή επιθυμία διατήρησης της ανωνυμίας των πηγών της πληροφορίας, την δυνατότητα εντοπισμού παρόμοιων διαδιακασιών ελέγχου, των μορφολογιών τους και την έμπιστη αξιολόγηση του περιεχομένου τους.

Η ανάπτυξη καλύτερων μοντέλων ασφαλείας στα πλαίσια των απειλών κώδικα μπορεί να διασφαλίσει τους χρήστες από πολλές κακόβουλες ενέργειες. Η Javascript θεωρείται ότι παρουσιάζει πολλά τρωτά σημεία και υπάρχουν πολλές ενέργειες προς την αντιμετώπισή τους, όμως είναι αναγκαία επιπλέον έρευνα σε αυτό το κομμάτι.

Η δημιουργία μοντέλων άδειας και συμβάσεων για τα προσωπικά δεδομένα μπορεί να διασφαλίσει την χρήση τους στις Web 2.0 εφαρμογές. Κάθε πρωτοβουλία η οποία αυξάνει τα δικαιώματα των τελικών χρηστών στην χρήση των δεδομένων τους ή περιεχομένου που παράγουν θα πρέπει να ενθαρρύνεται. Υπάρχει μικρός αριθμός έννομων μηχανισμών διαθέσιμων για τον τρόπο χρήσης προσωπικών δεδομένων εκτός εμπορικών συναλλαγών, παρά την ύπαρξη σοβαρών απειλών για την ασφάλεια των δεδομένων αυτών.

Παράλληλα με τα προηγούμενα, η ύπαρξη τρόπων μέτρησης και εξέτασης της τήρησης των κανόνων ασφάλειας στις Web 2.0 εφαρμογές μπορεί να προσφέρει στους χρήστες σημαντική πληροφορία για την εγκυρότητα των εφαρμογών και εμπιστοσύνη που μπορούν να έχουν σε αυτές. Η έρευνα πρέπει να στραφεί προς την εύρεση και ανάπτυξη πρακτικών ασφαλείας.

5.2.3 Ευαισθητοποίηση των χρηστών

Η ευαισθητοποίηση των χρηστών αποτελεί ένα πολύ σημαντικό παράγοντα για την αντιμετώπιση των περισσότερων απειλών που μπορούν να προκύψουν στις Web 2.0 εφαρμογές. Οι χρήστες είναι καλό να ενημερώνονται για προβλήματα που μπορεί να προκύψουν αλλά και για τις δυνατότητες που έχει για να προστατευθεί από κακόβουλες ενέργειες.

Υπάρχουν κάποια θέματα τα οποία είναι καλό να γνωρίζουν οι χρήστες Web 2.0 εφαρμογών. Δεδομένα τα οποία αναρτούνται από κάποιον χρήστη στο διαδίκτυο δεν χάνονται. Ακόμα και όταν διαγράφονται από τον ίδιο τα δεδομένα παραμένουν σε βάσεις δεδομένων, κρυφές μνήμες, φακέλους. Παράλληλα, τα δεδομένα χρηστών μπορεί να εμφανιστούν ως αποτελέσματα αναζήτησης.

Οι χρήστες πρέπει να είναι σωστά ενημερωμένοι για τον τρόπο λειτουργίας του ελέγχου πρόσβασης σε Web 2.0 εφαρμογές. Ο έλεγχος πρόσβασης αποτελεί την πιο σημαντική δικλείδα ασφαλείας στις διαδικτυακές εφαρμογές. Παρέχοντας ενημέρωση στους χρήστες για τα μέτρα αυτά, μαθαίνουν να τα χρησιμοποιούν πιο σωστά. Σωστή ενημέρωση είναι σημαντική και για τα πλεονεκτήματα που έχουν οι μέθοδοι ισχυρότερης αυθεντικοποίησης και ο τρόπος χρήσης τους.

Σε πολλές εφαρμογές ζητείται η ηλικία ώστε να υπάρξουν και τα απαραίτητα μέτρα προστασίας. Το πρόβλημα εμφανίζεται στο γεγονός ότι η επιβεβαίωση της πραγματικής ηλικία ενός χρήστης δεν είναι πάντα δυνατή. Οπότε πάντα οι χρήστες πρέπει να διατηρούν κάποια επιφύλαξη προς τους ισχυρισμούς άλλων χρηστών. Η ηλικία αποτελεί σημαντικό θέμα σε ευαίσθητες ομάδες, όπως ανήλικα άτομα.

Τα ανήλικα άτομα πρέπει να ενημερώνονται για να γνωρίζουν πώς να αντιδράσουν σε μη επιτρεπτές καταστάσεις. Είναι σημαντικό να μην δίνουν στοιχεία επαφής, να μην αποδεχτούν συνάντηση με άτομα που γνώρισαν μέσω διαδικτύου και χωρίς γνώση των γονέων τους, να μην απαντούν σε άσχημες συμπεριφορές, να μην δίνουν τους κωδικούς τους σε άλλους, να γνωρίζουν ότι κάποιοι χρήστες μπορεί να δίνουν ψευδής πληροφορίες.

Οι γονείς και οι δάσκαλοι πρέπει να γνωρίζουν τους κινδύνους που μπορεί να υπάρξουν για τα ανήλικα άτομα ώστε να μπορούν να τα προστατέψουν.

5.2.4 Προτυποποίηση

Η προτυποποίηση των διαδικασιών διασφαλίζει την ύπαρξη σωστών και αξιόπιστων εφαρμογών. Διαδικασίες όπως ο έλεγχος πρόσβασης και διαδικασία εξουσιοδότησης στις διαδικτυακές εφαρμογές πρέπει να αναπτύσσονται μέσα από ασφαλή πρότυπα. Είναι σημαντικό να υπάρχει ένα πλαίσιο που να καθορίζει τον τρόπο ανταλλαγής δεδομένων, την πρόσβαση σε κλήσεις λειτουργιών. Η ύπαρξη ενός πλαισίου πρόσβασης επιτρέπει την ανάθεση πρόσβασης σε εφαρμογές Web 2.0 για ορισμένο χρόνο, για ορισμένους χώρους, πρόσβαση σε ένα ορισμένο άτομο, την δυνατότητα ανίχνευσης σε περίπτωση παρενόχλησης, άμεση εμφάνιση μηνυμάτων σχετικά με την ασφάλεια.

5.2.5 Θέματα του παρόχου

Η υποδομή για τις υπηρεσίες που προσφέρει ένας πάροχος πρέπει να διακρίνεται για την πάγια εφαρμογή ισχυρότερων μηχανισμών πιστοποίησης όπου αυτό είναι απαραίτητο. Η χρήση μέτρων πιστοποίησης για την πρόσβαση σε δεδομένα πρέπει να γίνεται όπου είναι απαραίτητο. Η μεταφορά ευαίσθητων δεδομένων όπως είναι οι κωδικοί πρόσβασης και τα προσωπικά δεδομένα ενός χρήστη πρέπει να γίνεται με ασφάλεια, η οποία παρέχεται από την χρήση κρυπτογράφησης TLS/SSL.

5.2.6 Θέματα κατασκευαστή

Η δημιουργία Web 2.0 εφαρμογών καλύπτεται σε μεγάλο βαθμό από σενάρια βέλτιστων εφαρμογών τα οποία μπορούν να χρησιμοποιηθούν ως βάση για νέες εφαρμογές. Η δημιουργία ασφαλών Web 2.0 εφαρμογών πρέπει να παροτρύνεται να χρησιμοποιείται στο επίπεδο του κατασκευαστή. Στο κομμάτι της δημιουργίας λογισμικού η ασφάλεια του κώδικα

μπορεί να βελτιωθεί μόνο όταν υπάρχει η ανάλογη προσέγγιση σε όλη τη διαδικασία της δημιουργίας.

Στις Web 2.0 εφαρμογές παρατηρείται συχνά η ανάγκη χρήσης ισχυρής πιστοποίησης ενός χρήστη παράλληλα με την διατήρηση της ανωνυμίας του. Η ισχυρή πιστοποίηση έρχεται κατεξοχήν σε αντίθεση με την ανωνυμία εφόσον γίνεται άμεση σύνδεση της ταυτότητας του ατόμου με την αίτηση για υπηρεσία που έχει κάνει. Το ζητούμενο είναι μηχανισμοί οι οποίοι να πιστοποιούν την ταυτότητα του χρήστη με τέτοιο τρόπο ώστε να μην γίνεται άμεση σύνδεση της με τις συναλλαγές που έχει επιλέξει. Παραδείγματα τέτοιας τεχνολογίας αποτελούν τα Credentica και Idemix, η χρήση τους όμως δεν είναι πολύ διαδεδομένη στις Web 2.0 εφαρμογές. Στο κομμάτι αυτό υπάρχει η ανάγκη ανάπτυξης προτύπων για την σωστή χρήση τους στις Web 2.0 εφαρμογές.

5.3 Διαχείριση ταυτοτήτων

Η δημιουργία ενός συστήματος διαχείρισης ταυτότητας επιτρέπει την συμμετοχή οργανισμών στην δημιουργία ενός συστήματος εμπιστοσύνης και διαμοιρασμού ψηφιακών ταυτοτήτων και στοιχείων εργαζομένων, πελατών και προμηθευτών, παρέχοντας την δυνατότητα ενιαίας εισόδου στους χώρους των συμμετεχόντων.

Συναλλαγές που περιλαμβάνουν πολλούς οργανισμούς μπορούν να διευθετηθούν και να ολοκληρωθούν με την χρήση μιας ταυτότητας. Οι πελάτες και τα μέλη μιας ομοσπονδίας ταυτοτήτων έχουν πρόσβαση σε πολλές δικτυακές υπηρεσίες με την χρήση μόνο ενός κωδικού πρόσβασης. Οι εργαζόμενοι και οι συνεργάτες ενός οργανισμού έχουν την δυνατότητα ασφαλούς πρόσβασης σε συγκεκριμένη πληροφορία ανάλογα με τον ρόλο τους.

5.3.1 Ομοσπονδία ταυτοτήτων

Η λειτουργία της ομοσπονδίας ταυτοτήτων (identity federation) στηρίζεται στην από κοινού μεταξύ οργανισμών δημιουργία κανόνων διαμοίρασης ταυτοτήτων τηρώντας τους κανονισμούς ασφαλείας και ιδιωτικότητας. Με το σύστημα αυτό επιτρέπεται σε πολλούς φορείς η πρόσβαση στην ταυτότητα ενός ατόμου σε πολλούς ιστοτόπους, την ίδια στιγμή ώστε να επικυρωθεί η ταυτότητά του ατόμου και να εξυπηρετηθεί με ασφάλεια.

Με την δημιουργία ενός κοινού προτύπου ταυτότητας είναι πολύ πιο εύκολο να εξυπηρετηθούν οι χρήστες. Στην περίπτωση διαφορετικών ταυτοτήτων κάθε υπηρεσία πρέπει να διαχειρίζεται διαφορετικά κάθε περίπτωση χρήστη. Κάτι τέτοιο όμως, έχει μεγάλες απαιτήσεις σε χρόνο κα πώρους ενώ από ένα σημείο και μετά γίνεται ανέφικτο λόγο του αριθμού των συνεργατών.

Με την χρήση του identity federation οι οργανισμοί μπορούν να δημιουργήσουν κύκλους εμπιστοσύνης όπου ένας πάροχος περιστοιχίζεται και επικοινωνεί με άλλες επιχειρήσεις που προσφέρουν υπηρεσίες προς τους χρήστες. Όσοι συμμετέχουν στον κύκλο αυτό αποτελούν έμπιστες οντότητες, με δυνατότητα ελέγχου των στοιχείων της ταυτότητάς τους. Η εμπιστοσύνη και η ευκολία εξακρίβωση της ταυτότητας των οντοτήτων αυτών βοηθάει τις διαδικασίες παροχής υπηρεσιών σε μεγάλο βαθμό. Οι οντότητες είναι δυνατό να επικοινωνήσουν μέσω ασφαλών διαδικασιών που προάγουν ένα γενικότερο ασφαλές περιβάλλον.

5.3.2 Εφαρμογή ρόλων

Κάθε ιστοσελίδα web 2.0 μπορεί να εφαρμόσει ρόλους χρηστών. Με τον τρόπο αυτό κατηγοριοποιούνται οι χρήστες και οι δυνατότητες και οι ελευθερίες που έχουν μέσα στο site. Επίσης, διατηρώντας στοιχεία για τους χρήστες είναι ευκολότερος ο έλεγχος της ποιότητας της πληροφορίας που εισάγεται στο site. Ένας εντελώς άγνωστος και τυχαίος χρήστης θα μπορούσε να προκαλέσει σύγχυση στην πληροφορία με κακόβουλες ενέργειες.

5.3.3 Χρήση ηλεκτρονικών ταυτοτήτων

Οι ηλεκτρονικές ταυτότητες έχουν στόχο την παροχή ασφάλειας και πιστοποίησης στις συναλλαγές και τις αλληλεπιδράσεις των πολιτών στον χώρο των ηλεκτρονικών υπηρεσιών και των Web 2.0 εφαρμογών. Οι ηλεκτρονικές ταυτότητες μπορούν να παρέχουν στον χρήστη τους εγκυρότητα, σε έναν χώρο πολυσύνθετο και περίπλοκο, όπως το διαδίκτυο. Ένα τέτοιο εργαλείο διασφαλίζει την εγκυρότητα, την ασφάλεια και την μυστικότητα των δραστηριοτήτων τους.

Η λειτουργία των ηλεκτρονικών ταυτοτήτων στηρίζεται σε ορισμένες βασικές αρχές, που αντανακλούν τον τρόπο χρήσης τους. Αρχικά, παρέχεται ασφάλεια στον πλήρες κύκλο ζωής της ηλεκτρονικής ταυτότητας, από την παραγωγή της φυσικής υποστήριξης, κατά την έναρξη, την εκπομπή και τη χρήση της στις ηλεκτρονικές υπηρεσίες. Η ασφάλεια αφορά τόσο τον χρήστη που την χρησιμοποιεί, όσο και τις εφαρμογές με τις οποίες αλληλεπιδρά.

Η ηλεκτρονική ταυτότητα παρέχει πρόσβαση σε δικτυακές υπηρεσίες, φέρνοντας τις Web 2.0 εφαρμογές πιο κοντά στον χρήστη. Παρέχει στους χρήστες την ασφάλεια και τη μυστικότητα που επιθυμούν στις δραστηριότητες τους.

5.4 Συστήματα καταγραφής συμπεριφοράς σε Κοινωνικά δίκτυα

Οι υπηρεσίες που παρέχουν οι Web 2.0 εφαρμογές συχνά αναφέρονται σε συνεργαζόμενα μέρη άγνωστα μεταξύ τους, όπου μια υπηρεσία ζητείται από έναν καταναλωτή έχοντας ελλιπή πληροφόρηση για τον πάροχο της υπηρεσίας και τις υπηρεσίες του. Ο καταναλωτής επιλέγει μια υπηρεσία με ρίσκο εφόσον δεν έχει εκ των προτέρων εικόνα του αποτελέσματος. Ο πάροχος της υπηρεσίας από την άλλη μεριά, έχει πλήρη εικόνα του τι παίρνει και τι δίνει. Οι δυσλειτουργίες που προκύπτουν από την ασυμμετρία της πληροφορίας μπορούν να υπερβληθούν με την εμπιστοσύνη και την φήμη. Εφόσον ο καταναλωτής δεν μπορεί να έχει πλήρη εικόνα της υπηρεσίας, μπορεί να εμπιστευτεί τον πάροχο, ή έναν ενδιάμεσο έμπιστο κόμβο[14].

Η εμπιστοσύνη παίζει πολύ σημαντικό ρόλο στις συναλλαγές και τις υπηρεσίες του Web 2.0. Είναι όμως δύσκολη η προσέγγιση της εμπιστοσύνης μέσω υπολογιστών, μεταξύ απομακρυσμένων οντοτήτων, καθώς απομακρύνεται από τους παραδοσιακούς τρόπους συναλλαγής. Αρχικά, η ύπαρξη μιας παραδοσιακής επιχείρησης αποτελεί εγγύηση για τους καταναλωτές και έρχεται σε αντίθεση με την δημιουργία ενός ιστοτόπου ως μέσου παροχής υπηρεσιών που δεν δημιουργεί εύκολα ένα αίσθημα εμπιστοσύνης για τους καταναλωτές. Υπάρχει η ανάγκη προσδιορισμού της ποιότητας των υπηρεσιών που παρέχονται ώστε ο χρήστης να έχει μια πληροφορία για το μέρος με το οποίο πρόκειται να συνεργαστεί. Ο προσδιορισμός αυτός δεν είναι εύκολο να γίνει από τον χρήστη, όμως το θέμα της εμπιστοσύνης στις Web 2.0 υπηρεσίες αποτελεί ένα από τα πιο κρίσιμα σημεία για την ύπαρξή τους.

Τα συστήματα εμπιστοσύνης και καταγραφής συμπεριφοράς παρέχουν προστασία στους χρήστες από την παροχή κακόβουλων πηγών πληροφορίας. Η πληροφορία που παρέχουν ορισμένοι μπορεί να είναι ψευδής ή να αποπροσανατολίζει έναν χρήστη χωρίς να παραβιάζει τους παραδοσιακούς μηχανισμούς προστασίας καθώς το πρόβλημα έγκειται στο περιεχόμενο. Οι παραδοσιακοί μηχανισμοί ασφάλειας όπως η αυθεντικότητα του χρήστη και ο έλεγχος πρόσβασης αποτελούν το ‘hard security’, τα συστήματα εμπιστοσύνης και καταγραφής συμπεριφοράς αποτελούν μέρος των μηχανισμών κοινωνικού ελέγχου που αποτελούν το ‘soft security’.

Οι μηχανισμοί ασφαλείας προστατεύουν τα συστήματα και τα δεδομένα από κακόβουλους και μη εξουσιοδοτημένους χρήστες. Οι υπηρεσίες που χρησιμοποιούν τέτοιους μηχανισμούς θεωρούνται περισσότερο αξιόπιστες και κερδίζουν την εμπιστοσύνη του χρήστη. Η ασφάλεια της επικοινωνίας περιλαμβάνει την κρυπτογράφηση στο κανάλι επικοινωνίας και την κρυπτογραφημένη πιστοποίηση των ταυτοτήτων. Η πιστοποίηση παρέχει εμπιστοσύνη ως προς την ταυτότητα ενός χρήστη. Ο έμπιστος πάροχος προσφέρει τους απαραίτητους μηχανισμούς και υπηρεσίες για την επικύρωση και διαχείριση των ταυτοτήτων.

[14] **Elisabetta Carrara, Giles Hogben, ENISA.** *Reputation-based Systems: a security analysis.* 2007.(σελ.3-6)

Πέρα όμως από την επικύρωση της ταυτότητας ενός συνεργαζόμενου μέρους, υπάρχει ενδιαφέρον και για την αξιοπιστία του και την ποιότητα των υπηρεσιών που παρέχει. Η εμπιστοσύνη σε αυτό το σημείο σχετίζεται με την πρόβλεψη του αποτελέσματος της συνεργασίας και μπορεί να επιτευχθεί μόνο με τα συστήματα εμπιστοσύνης και φήμης. Σημειώνεται ότι η επικύρωση της ταυτότητας ενός έμπιστου συμβαλλόμενου μέρους δεν συνεπάγεται την γνώση των στοιχείων του. Μια έμπιστη οντότητα μπορεί να παρέχει υπηρεσίες και να συνεργάζεται με άλλες έμπιστες οντότητες, διατηρώντας την ανωνυμία της.

Τα συστήματα συνεταιριστικού φιλτραρίσματος (collaborative filtering systems) μοιάζουν πολύ με τα συστήματα φήμης. Σκοπός και των δύο είναι η συλλογή αξιολόγησης από τα μέλη μιας ομάδας. Η βασική διαφορά τους όμως είναι στο ότι τα συστήματα συνεταιριστικού φιλτραρίσματος διαφορετικοί χρήστες παρουσιάζουν διαφορετικές προτιμήσεις και αξιολογούν διαφορετικά σύμφωνα με την υποκειμενική τους άποψη. Με επεξεργασία των προτιμήσεων των χρηστών εντοπίζονται ομοιότητες μεταξύ των προτιμήσεων τους, βάση των οποίων μπορούν να τους προταθούν επιπλέον πράγματα που ίσως τους ενδιαφέρουν. Η λειτουργία αυτή καλείται σύστημα προτάσεων (recommender system).

Τα συστήματα φήμης βασίζονται στην κρίση των μελών για την ποιότητα των υπηρεσιών που έλαβαν. Στην ουσία δημιουργούν συστήματα συλλογικής επιβολής κρίσης, όπου οι υπηρεσίες κρίνονται από τους χρήστες. Προκειμένου να αποσπούν καλές κριτικές, οι πάροχοι προσφέρουν πιο ποιοτικές υπηρεσίες. Παράλληλα, οι χρήστες έχουν ένα σημείο αναφοράς για την ποιότητα της υπηρεσίας που θα έχουν.

Τα συστήματα φήμης στις Web 2.0 εφαρμογές κοινωνικής δικτύωσης, βασίζονται κυρίως στην αθροιστική ή μέσου όρου αξιολόγηση(summation or average of ratings), ενώ υπάρχουν και συστήματα που βασίζονται στο μοντέλο ροής (flow model).

5.4.1 Μοντέλο αθροιστικής ή μέσου όρου αξιολόγησης

Η απλούστερη μορφή υπολογισμού της φήμης είναι η διαφορά της άθροισης των θετικών αξιολογήσεων και των αρνητικών αξιολογήσεων. Στο μοντέλο αυτό είναι απολύτως κατανοητή η διαδικασία εξαγωγής του βαθμού αξιολόγησης της φήμης. Το μειονέκτημα είναι ότι δίνει μια φτωχή εικόνα για τους συμμετέχοντες.

Μια πιο προχωρημένη μορφή του μοντέλου αυτού υπολογίζει έναν σταθμισμένο μέσο όρο όλων των αξιολογήσεων. Η στάθμιση της αξιολόγησης γίνεται με παράγοντες όπως η αξιοπιστία και η φήμη αυτού που αξιολογεί, η παλαιότητα της αξιολόγησης, το διαφορά μεταξύ των αξιολογήσεων και του τρέχοντος βαθμού.

Παράδειγμα αθροιστικού ή μέσου όρου μοντέλου αξιολόγησης φήμης εφαρμόζεται στο e-Bay, έναν ιστοχώρο για αγοραπωλησίες. Το e-Bay δίνει την δυνατότητα στα συμβαλλόμενα μέρη μιας συναλλαγής να αξιολογήσουν ο ένας τον άλλο θετικά, αρνητικά ή ουδέτερα μετά την ολοκλήρωση της συναλλαγής. Παράλληλα, έχουν την δυνατότητα να σχολιάσουν την συναλλαγή θετικά ή αρνητικά. Το e-Bay συλλέγει και επεξεργάζεται όλη αυτή την πληροφορία και υπολογίζει τους βαθμούς των χρηστών με βάση το αθροιστικό ή μέσου όρου μοντέλο. Με σκοπό να δηλώσει την πιο πρόσφατη συμπεριφορά του συμμετέχοντος παρουσιάζει τρείς βαθμούς με χρονικό βάθος έξι μηνών, ενός μήνα και των τελευταίων επτά ημερών .

Παράλληλα, για την αποφυγή επανάληψης των ίδιων σχολίων, που θα μπορούσαν να αλλοιώσουν τις βαθμολογίες, οι συμμετέχοντες σε μια συναλλαγή επιτρέπεται να αξιολογήσουν ο ένας τον άλλο μόνο μετά από την συναλλαγή, που παρακολουθείται από το e-Bay. Η περίπτωση ψευδών συναλλαγών περιορίζεται καθώς το e-Bay χρεώνει την εισαγωγή αντικειμένων προς πώληση, οπότε υπάρχει άμεσο κόστος σε τέτοιες ενέργειες.

5.4.2 Μοντέλο αξιολόγηση ροής

Μοντέλα αξιολόγησης ροής ονομάζονται αυτά που υπολογίζουν την εμπιστοσύνη ή την φήμη μέσω μεταβατικών επαναλήψεων ή αυθαίρετων μεγάλων αλυσίδων. Σε ορισμένα μοντέλα ροής τίθεται μια αρχική τιμή εμπιστοσύνης/φήμης για όλη την κοινότητα. Τα συμβαλλόμενα μέρη μπορούν να αυξήσουν την τιμή αυτή σε κόστος άλλων. Σε ένα γενικό πλαίσιο, η φήμη ενός συμμετέχοντος αυξάνεται σαν συνάρτηση μιας ροής εισόδου και μειώνεται σαν συνάρτηση μιας ροής εξόδου.

Παράδειγμα τέτοιου μοντέλου αξιολόγησης φήμης εφαρμόζεται στο Advogato, μια κοινότητα προγραμματιστών ανοικτού κώδικα. Το μοντέλο που χρησιμοποιείται υπολογίζει την ροή φήμης μέσο ενός δικτύου όπου τα μέλη αποτελούν τους κόμβους και οι ενώσεις συνιστούν τις αναφορές μεταξύ των κόμβων. Κάθε μέλος-κόμβος λαμβάνει χωρητικότητα μεταξύ 800 και 1, ανάλογα με την απόστασή του από τον αρχικό κόμβο. Ο αρχικός κόμβος έχει χωρητικότητα 800 και όσο πιο μακριά από αυτόν βρίσκεται ένας κόμβος, τόσο μικρότερη χωρητικότητα έχει. Τα μέλη διαβαθμίζονται με βάση την χωρητικότητα τους σε τρεις κατηγορίες (χαμηλού επιπέδου, μεσαίου επιπέδου και ανώτατου επιπέδου). Ένα ξεχωριστό γράφημα ροής υπολογίζεται για κάθε τύπο αναφοράς.

6 Πρότυπα

Τα πρότυπα δημιουργούνται για να καθορίζουν τις διαδικασίες υλοποίησης Web 2.0 εφαρμογών. Αποτελούν τον γνώμονα για τον τρόπο με τον οποίο πρέπει να δημιουργηθεί μία εφαρμογή και διασφαλίζει τον τρόπο λειτουργίας τους. Εφόσον μια εφαρμογή λειτουργεί σύμφωνα με τα καθορισμένα πρότυπα, καλύπτει τόσο τα θέματα διαλειτουργικότητας όσο και ασφάλειας και μπορεί να θεωρηθεί ασφαλής από τους χρήστες. Στην συνέχεια, γίνεται αναφορά στα πρότυπα που σχετίζονται με την δημιουργία και την λειτουργία Web 2.0 εφαρμογών, σε όλα τα επίπεδα της εξέλιξής τους.

Η προτυποποίηση της ασφάλειας των τηλεπικοινωνιακών δικτύων καλύπτει τις προδιαγραφές σε επίπεδο δικτύου σε κύριο στόχο την σωστή και ασφαλή λειτουργία των Web 2.0 εφαρμογών. Το συγκεκριμένο πρότυπο αναφέρει επίσης, αναλυτικά, τις υπηρεσίες ασφαλείας και τους μηχανισμούς ασφαλείας. Επιπλέον, σημαντικό κομμάτι στην διασφάλιση της ιδιωτικότητας και της προστασίας των χρηστών στις Web 2.0 εφαρμογές αποτελεί η προτυποποίηση πιστοποίησης ταυτότητας και η προτυποποίηση των ηλεκτρονικών υπογραφών.

6.1 Προτυποποίηση ασφάλειας τηλεπικοινωνιακών δικτύων

Ένας σημαντικός τομέας προστασίας είναι αυτός του δικτύου. Το πρότυπο για την ασφάλεια των τηλεπικοινωνιακών δικτύων είναι το ISO 7498-2. Σε αυτό περιέχονται καθορισμένες περιγραφές για υπηρεσίες ασφαλείας και αντίστοιχους μηχανισμούς. Σύμφωνα με το πρότυπο αυτό, ο κύκλος ζωής της ασφάλειας ενός συστήματος περιλαμβάνει καταρχήν τον καθορισμό της πολιτικής ασφάλειας. Στην συνέχεια είναι απαραίτητη η ανάλυση των απειλών ασφάλειας, σε σχέση με την πολιτική ασφαλείας που έχει καθοριστεί. Τα επόμενα βήματα περιέχουν τον προσδιορισμό των υπηρεσιών ασφάλειας και των μηχανισμών ασφαλείας. Τέλος, απαιτείται συνεχής διαχείριση της ασφάλειας για την κάλυψη των νέων αναγκών ή για κάποια αλλαγή στα υπάρχοντα.

Οι βασικές απειλές που αντιμετωπίζει ένα σύστημα είναι οι παρακάτω:

- Η διαρροή πληροφοριών
- Η παραβίαση της ακεραιότητας των πληροφοριών
- Η άρνηση εξυπηρέτησης
- Η παράνομη χρήση διαφόρων υπολογιστικών ή δικτυακών πόρων

Η πραγματοποίηση οποιασδήποτε από τις απειλές που αναφέρονται παραπάνω, μπορεί να γίνει με κάποια από τεχνικές επίθεσης, όπως η μεταμφίεση ταυτότητας, η παράκαμψη ελέγχων, η παραβίαση εξουσιοδότησης, η χρήση δούρειου ίππου ή η παγίδα.

6.1.1 Υπηρεσίες Ασφάλειας

Το ISO 7498-2 καθορίζει πέντε κύριες κατηγορίες υπηρεσιών ασφάλειας. Αυτές οι κατηγορίες αναφέρονται παρακάτω:

- Πιστοποίηση ταυτότητας και προέλευσης

Η πιστοποίηση της ταυτότητας μιας οντότητας απαντά στο ερώτημα αν μια οντότητα είναι πραγματικά αυτή η οποία ισχυρίζεται πως είναι. Συνήθως αυτό γίνεται στην αρχή μιας σύνδεσης, προκειμένου να αντιμετωπιστούν απειλές από επιθέσεις μεταμφίεσης ταυτότητας και επανάληψης. Η πιστοποίηση ταυτότητας της προέλευσης προσφέρει επαλήθευση της πηγής των δεδομένων, αλλά δεν προστατεύει από επιθέσεις επανάληψης ή/και σκόπιμης καθυστέρησης.

- Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης αποτελεί θεμελιώδη όρο στην ασφάλεια κάθε πληροφοριακού συστήματος, καθώς καθορίζει τα μέτρα και τις τεχνικές που παρέχουν προστασία ενάντια σε μη εξουσιοδοτημένη χρήση πόρων, συμπεριλαμβανομένων και της χρήσης επικοινωνιακών πόρων, της ανάγνωσης, εγγραφής ή διαγραφής πόρων πληροφοριών αλλά και της επεξεργασίας πληροφοριών.

- Εμπιστευτικότητα δεδομένων

Η εμπιστευτικότητα προσφέρει προστασία ενάντια στη μη εξουσιοδοτημένη αποκάλυψη πληροφοριών, στοχεύοντας στην αποφυγή ακούσιας ή εκούσιας διαρροής πληροφοριών και περιλαμβάνει την εμπιστευτικότητα σύνδεσης, την εμπιστευτικότητα μη-σύνδεσης, την εμπιστευτικότητα επιλεκτικού πεδίου και την εμπιστευτικότητα ροής πληροφοριών.

- Μη-αποποίηση

Η μη-αποποίηση προστατεύει από έναν αποστολέα δεδομένων ο οποίος αρνείται το γεγονός ότι τα δεδομένα εστάλησαν από αυτόν (μη-αποποίηση προέλευσης), αλλά και από έναν παραλήπτη δεδομένων ο οποίος αρνείται ότι τα δεδομένα παρελήφθησαν από αυτόν (μη-αποποίηση παραλαβής). Σε περιπτώσεις όπως οι χρηματιστηριακές συναλλαγές που εκτελούνται με ηλεκτρονικά μέσα, η εξασφάλιση αυτή είναι πρωταρχικής σημασίας.

6.1.2 Μηχανισμοί Ασφάλειας

Άλλο ένα σημαντικό κομμάτι του προτύπου ISO 7498-2, είναι οι μηχανισμοί ασφάλειας που αποτελούν την τεχνική υλοποίηση των υπηρεσιών ασφαλείας. Οι μηχανισμοί αυτοί, διαιρούνται σε δύο κατηγορίες, στους συγκεκριμένους μηχανισμούς ασφάλειας και στους γενικούς μηχανισμούς.

Οι συγκεκριμένοι μηχανισμοί ασφάλειας αναφέρονται και επεξηγούνται παρακάτω:

- Μηχανισμοί κρυπτογράφησης

Οι μηχανισμοί κρυπτογράφησης σχετίζονται με τη χρήση των απαραίτητων κρυπτογραφικών αλγορίθμων προκειμένου να προσφέρουν εμπιστευτικότητα τόσο στα δεδομένα τα οποία διακινούνται, όσο και στη ροή τους. Επίσης, οι μηχανισμοί αυτοί αποτελούν τη βάση για τους μηχανισμούς ανταλλαγής για πιστοποίηση ταυτότητας.

- Μηχανισμοί ψηφιακών υπογραφών

Οι ψηφιακές υπογραφές προσφέρουν ταυτόχρονα υπηρεσίες ακεραιότητας, πιστοποίησης προέλευσης και μη-αποποίησης σε ένα μήνυμα. Οι ψηφιακές υπογραφές, χρησιμοποιούνται, επίσης, στους μηχανισμούς ανταλλαγής για πιστοποίηση ταυτότητας.

- Μηχανισμοί ελέγχου πρόσβασης

Οι μηχανισμοί ελέγχου πρόσβασης είναι αυτοί που καθορίζουν αν ένας χρήστης που χρησιμοποιεί ένα πρόγραμμα πελάτη μπορεί να έχει πρόσβαση σε συγκεκριμένες πληροφορίες οι οποίες παρέχονται από ένα πρόγραμμα εξυπηρετητή και πολλές φορές και το αντίστροφο.

- Μηχανισμοί ακεραιότητας δεδομένων

Οι μηχανισμοί ακεραιότητας προσφέρουν υπηρεσίες προστασίας ενάντια στην τροποποίηση των δεδομένων καθώς και υπηρεσίες πιστοποίησης της προέλευσης ενός μηνύματος. Χωρίζονται σε δύο τύπους ανάλογα με το αν σχετίζονται με την ακεραιότητα μια και μόνο μονάδας δεδομένων ή αν σχετίζονται με την ακεραιότητα μιας πλήρους ακολουθίας δεδομένων.

- Μηχανισμοί ανταλλαγής για πιστοποίηση ταυτότητας

Οι μηχανισμοί αυτοί προσφέρουν τις αντίστοιχες υπηρεσίες πιστοποίησης ταυτότητας μιας οντότητας και είναι επίσης γνωστές σαν πρωτόκολλα πιστοποίησης. Τα πρωτόκολλα αυτά καθορίζονται από μια σειρά κρυπτογραφημένων μηνυμάτων, τα οποία ανταλλάσσουν μεταξύ τους ένα ζεύγος επικοινωνουσών οντοτήτων, καθώς και από συγκεκριμένους κανόνες για την επεξεργασία αυτών των μηνυμάτων.

- Μηχανισμοί παραγεμίσματος κυκλοφορίας

Οι συγκεκριμένοι μηχανισμοί χρησιμοποιούνται για την απόκρυψη του πραγματικού όγκου των δεδομένων που διακινούνται μέσα από ένα δίκτυο υπολογιστών. Αν και η τεχνική του παραγεμίσματος κυκλοφορίας χρησιμοποιείται από τους μηχανικούς δικτύων και για άλλους σκοπούς, μπορεί ωστόσο να αποτρέψει -σε συνδυασμό με τη χρήση των μηχανισμών

κρυπτογράφησης- έναν επιτιθέμενο από το να εξάγει συμπεράσματα σχετικά με το είδος της κίνησης των δεδομένων.

- Μηχανισμοί ελέγχου δρομολόγησης

Οι συγκεκριμένοι μηχανισμοί χρησιμοποιούνται κυρίως για να αποτρέψουν τη χρήση ανασφαλών καναλιών για τη μεταφορά ευαίσθητων δεδομένων. Σε ορισμένες περιπτώσεις χρειάζεται η διακίνηση δεδομένων να γίνει μόνο από συγκεκριμένα (φυσικά) στοιχεία του δικτύου.

- Μηχανισμοί συμβολαίων

Η χρήση μιας έμπιστης τρίτης οντότητας, όπως είδαμε και στο κεφάλαιο της κρυπτογραφίας, η οποία λειτουργεί σαν «συμβολαιογράφος» μπορεί να εγγυηθεί την ακεραιότητα, την προέλευση ή/και τον προορισμό των δεδομένων. Ο συμβολαιογράφος προκαλεί μια (κρυπτογραφική) αλλαγή στα δεδομένα, παρέχοντας έτσι κοινά αποδεκτές υπηρεσίες μη-αποποίησης.

Οι γενικοί μηχανισμοί ασφαλείας αποτελούνται από τους παρακάτω πέντε τύπους μηχανισμών:

- Έμπιστη λειτουργικότητα

Κάθε δραστηριότητα η οποία βοηθά στη λειτουργικότητα ενός συστήματος και η οποία προσφέρει ή έχει πρόσβαση σε μηχανισμούς ασφάλειας πρέπει να είναι αξιόπιστη. Η υλοποίηση τέτοιων μηχανισμών συμπεριλαμβάνει συνδυασμό λογισμικού και υλικού.

- Ετικέτες ασφάλειας

Κάθε δικτυακός ή υπολογιστικός πόρος είναι εξασφαλισμένο ότι μπορεί να σχετίζεται με μια ετικέτα ασφάλειας η οποία θα καθορίζει την ευαισθησία του.

- Ανακάλυψη γεγονότων

Η ανακάλυψη γεγονότων περιλαμβάνει την καταγραφή κάθε απόπειρας παραβίασης της πολιτικής ασφάλειας αλλά και κάθε νόμιμης δραστηριότητας που σχετίζεται με την ασφάλεια ενός συστήματος. Η λειτουργία αυτή μπορεί να χρησιμοποιηθεί για να δώσει το έναυσμα για αναφορά γεγονότων.

- Ακολουθία αρχείων καταγραφής περιστατικών ασφάλειας

Ο μηχανισμός αυτός είναι πολύ σημαντικός, καθώς καταγράφει και αποθηκεύει τα παρελθόντα αλλά και τα τρέχοντα γεγονότα που σχετίζονται με την ασφάλεια. Παράλληλα, επιτρέπει την αναγνώριση και την εξέταση παρελθόντων γεγονότων που παραβίασαν (ή επιχείρησαν να παραβιάσουν) την πολιτική ασφάλειας.

- Ανάκαμψη ασφάλειας

Ο μηχανισμός ανάκαμψης ασφάλειας χειρίζεται τις αιτήσεις για ανάκαμψη από περιπτώσεις αποτυχίας των μέτρων ασφάλειας. Αυτό επιτυγχάνεται με ενέργειες όπως η άμεση ματαίωση εργασιών ή η ακύρωση μίας οντότητας.

Αυτά είναι τα βασικά χαρακτηριστικά του προτύπου ISO 7498-2 που πλαισιώνουν τις υπηρεσίες και τους μηχανισμούς διαχείρισης της ασφάλειας σε ένα σύστημα. Είναι πολύ σημαντικό να λαμβάνονται αυτά τα μέτρα για την σωστή λειτουργία ενός συστήματος.

6.2 Προτυποποίηση πιστοποίησης ταυτότητας

Το ISO/IEC 9798 καθορίζει μια ποικιλία από πρότυπα πρωτόκολλα πιστοποίησης ταυτότητας καθώς και διάφορα πρωτόκολλα διανομής κλειδιών. Η χρήση του προορίζεται για διάφορες εφαρμογές που απαιτούν πιστοποίηση ταυτότητας. Ο σχεδιασμός του επιτρέπει την προσαρμογή του ανάλογα με τις απαιτήσεις που υπάρχουν στις διάφορες εφαρμογές.

6.3 Προτυποποίηση ηλεκτρονικών υπογραφών

Η διεθνής προτυποποίηση παίζει σημαντικό ρόλο στη διευκρίνιση των απαιτήσεων της οδηγίας για τις ηλεκτρονικές υπογραφές. Η Ευρωπαϊκή Επιτροπή πρόκειται να υιοθετήσει και να δημοσιεύσει τους αριθμούς αναφοράς προτύπων σχετικά με τα προϊόντα των ηλεκτρονικών υπογραφών στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων. Γι' αυτό το έργο έχει επιφορτιστεί μια επιτροπή με τους αντιπροσώπους από τα κράτη μέλη της ΕΕ.

Ένα μεγάλο μέρος των ενεργειών προτυποποίησης προκύπτει από το πρόγραμμα EESSI το οποίο αποτελεί μια από κοινού προσπάθεια των Ευρωπαϊκών οργανισμών προτυποποίησης ETSI(SEC ESI WG) και CEN (WS/ E- Sign). Ο οργανισμός ETSI έχει υποβάλλει τις εξής τεχνικές προδιαγραφές:

TS 101 456	Απαιτήσεις πολιτικής για αρχές πιστοποιητικών για την έκδοση έγκυρων πιστοποιητικών
TS 101 733	Τύποι ηλεκτρονικών υπογραφών
TS 101 861	Πρότυπο χρονοσφραγίδας
TS 101 862	Πρότυπο έγκυρου πιστοποιητικού
TS 102 023	Απαιτήσεις πολιτικής για τις αρχές χρονοσφραγίδας
TS102 042	Απαιτήσεις πολιτικής αρχών πιστοποίησης για την παροχή πιστοποιητικών δημόσιου κλειδιού
TS 101 903	Προηγμένες ηλεκτρονικές υπογραφές XML
TR 102 041	Αναφορά πολιτικής των υπογραφών
TS 102 030	Πρόβλεψη για την κατάσταση των πληροφοριών στην εναρμονισμένη παροχή υπηρεσιών εμπιστευτικότητας

Εικόνα 6.1 : Τεχνικές προδιαγραφές ETSI για τις ηλεκτρονικές υπογραφές.

Οι αντίστοιχες δημοσιεύσεις της Ευρωπαϊκής επιτροπής προτυποποίησης CEN στην περιοχή αυτή, είναι έγγραφα CWA (CEN Working Agreements - Συμφωνίες Εργασιών CEN). Η επιτροπή έχει εγκρίνει τα ακόλουθα έγγραφα:

CWA 14167-1	Απαιτήσεις ασφάλειας για αξιόπιστα συστήματα διαχείρισης πιστοποιητικών ηλεκτρονικών υπογραφών: Μέρος 1 – Απαιτήσεις ασφάλειας συστήματος
CWA 14167-2	Απαιτήσεις ασφάλειας για αξιόπιστα συστήματα διαχείρισης πιστοποιητικών ηλεκτρονικών υπογραφών: Μέρος 1 – Μηχανισμοί κρυπτογράφησης για τις διαδικασίες υπογραφής CSP – Πρότυπο προστασίας (MCSO-PP)
CWA 14168	Ασφαλείς συσκευές δημιουργίας υπογραφών, έκδοση EAL 4
CWA 14169	Ασφαλείς συσκευές δημιουργίας υπογραφών, έκδοση EAL 4+
CWA 14170	Απαιτήσεις ασφάλειας για συστήματα δημιουργίας υπογραφών
CWA 14171	Διαδικασίες επιβεβαίωσης ηλεκτρονικών υπογραφών
CWA 14172-1	Οδηγός καθοδήγησης επιβεβαίωσηςEESSI:Μέρος 1 – Γενικά στοιχεία
CWA 14172-2	Οδηγός καθοδήγησης επιβεβαίωσηςEESSI:Μέρος 2- Υπηρεσίες και διαδικασίες αρχών πιστοποίησης
CWA 14172-3	Οδηγός καθοδήγησης επιβεβαίωσηςEESSI:Μέρος 3 – Αξιόπιστα συστήματα διαχείρισης πιστοποιητικών ηλεκτρονικών υπογραφών
CWA 14172-4	Οδηγός καθοδήγησης επιβεβαίωσηςEESSI:Μέρος 4 – Εφαρμογές δημιουργίας υπογραφών και διαδικασίες επιβεβαίωσης ηλεκτρονικών υπογραφών
CWA 14172-5	Οδηγός καθοδήγησης επιβεβαίωσηςEESSI:Μέρος 5 – Συσκευές ασφαλούς δημιουργίας υπογραφών
CWA 14255	Οδηγίες για την εφαρμογή των συσκευών δημιουργίας ασφαλών υπογραφών

Εικόνα 6.2 : Συμφωνίες Εργασιών CEN για τις ηλεκτρονικές υπογραφές.

6.3.1 Πρότυπο ηλεκτρονικής υπογραφής XML

Το πρότυπο υπογραφών XML, (XML-DSig) καθορίζει τον τρόπο εφαρμογής των ηλεκτρονικών υπογραφών σε μέρη ενός XML εγγράφου, αλλά και γενικότερα σε διαδικτυακούς πόρους. Το πρότυπο αυτό ορίζει απόλυτα την σύνταξη και την βασική σημασιολογία των

υπογραφών XML. Το μήνυμα μιας υπογραφής καθορίζεται από μια λίστα με αναφορές, προς διαδικτυακούς πόρους ή μέρος ενός εγγράφου XML. Κάθε μέρος που αναφέρεται στο μήνυμα, υποβάλετε σε μια συνάρτηση κατακερματισμού (hush) και η λίστα με τις αναφορές στις πληροφορίες υπογράφονται με το παραδοσιακό σχέδιο ψηφιακών υπογραφών, με την χρήση των κρυπτογραφικών αλγόριθμων DSA ή RSA, μετά την εφαρμογή της συνάρτησης κατακερματισμού.

Το πρότυπο υπογραφών XML καθορίζει μόνο την βασική σημασιολογία για τις υπογραφές. Καθορίζει δηλαδή, την σημασιολογία για την συσχέτιση μιας κρυπτογραφικής υπογραφής με ένα μήνυμα. Ειδικότερα, η σημασιολογία αυτή περιλαμβάνει την ακεραιότητα και τις ιδιότητες επικύρωσης μηνυμάτων της κρυπτογραφικής υπογραφής. Αυτό επιτρέπει μόνο στον πραγματικό κάτοχο του κλειδιού της υπογραφής να δημιουργεί την υπογραφή, οπότε τα υπογεγραμμένα μηνύματα προστατεύονται από τυχόν αλλαγές αναρμόδιας τρίτης οντότητας

Η επικύρωση των υπογραφόντων υποστηρίζεται από τις ψηφιακές υπογραφές XML με επιπλέον προσθήκες, αλλά δεν περιλαμβάνεται στο πρότυπο. Η σημασιολογία εμπιστοσύνης αναπτύσσεται στις εφαρμογές. Η επεκτασιμότητα της σημασιολογίας του προτύπου υπογραφής XML, χρησιμοποιείται για τις μεθόδους μεταφοράς της σημασιολογίας απόδειξης στην σημασιολογία της υπογραφής XML.

7 Νομικό πλαίσιο

Στα πλαίσια μελέτης των θεμάτων που σχετίζονται με την ιδιωτικότητα και τη προστασία στο Web 2.0 , είναι σημαντικό να αναφερθεί το ισχύων νομικό πλαίσιο. Μέσα από το νομοθετικό πλαίσιο καθορίζεται ο έγκριτος τρόπος δράσης των συναλλασσομένων μελών με την διάταξη νόμων, οδηγιών και κανονισμών. Στην συνέχεια γίνεται αναφορά στο ευρωπαϊκό και ελληνικό νομικό πλαίσιο.

7.1 Ευρωπαϊκό νομικό πλαίσιο

Η Ευρωπαϊκή Ένωση μέσα από σχέδια δράσης, πιλοτικά προγράμματα και την θέσπιση οδηγιών και αποφάσεων, προωθεί την εξέλιξη της ηλεκτρονικής ολοκλήρωσης του δημόσιου τομέα όλων των χωρών. Θέτει στόχους, και δίνει τα πλαίσια μέσα στα οποία πρέπει να γίνονται οι μεταβολές. Ο τελικός σκοπός είναι ολοκληρωμένα συστήματα ηλεκτρονικής διακυβέρνησης σε κάθε χώρα μέλος, που θα έχουν κοινή βάση ώστε να μπορεί να υπάρχει διαλειτουργικότητα μεταξύ των εφαρμογών.

Οι οδηγίες και οι αποφάσεις αποτελούν τα ακριβή πλαίσια προδιαγραφών για εφαρμογές που λαμβάνουν χώρα. Με την συλλογή στοιχείων από παρόμοιες εφαρμογές, προβλήματα που δημιουργούνται και τρόπους που επιλύονται η Ευρωπαϊκή Ένωση είναι σε θέσει να καθορίσει τον τρόπο δράσης για τις χώρες μέλη.

Οδηγία 95/46/EC

Η πρώτη ολοκληρωμένη νομική πράξη σε Ευρωπαϊκό επίπεδο, για την προστασία των προσωπικών δεδομένων τέθηκε με την Οδηγία 95/46/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995. Η οδηγία αυτή αποτελεί μια προσπάθεια αναγνώρισης του δικαιώματος για μυστικότητα και στοχεύει στον εναρμονισμό των αντίστοιχων εθνικών νόμων. Αναφέρεται στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και στην ελεύθερη κυκλοφορία των δεδομένων αυτών.

Η οδηγία 95/46/EC, αποτελεί κείμενο αναφοράς σε ευρωπαϊκό επίπεδο όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα . Δημιουργεί ένα κανονιστικό πλαίσιο που αποσκοπεί στην επικράτηση ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης. Ως συνέχεια της οδηγίας αυτής το 1997 ψηφίστηκε η Οδηγία 97/66/EC. Σε αυτήν γίνεται αναφορά στην προστασία δεδομένων που διακινούνται μέσω δικτύων και τηλεπικοινωνιακών συστημάτων.

Στην συνέχεια υπογράφηκε σύμβαση στην οποία συμπεριλαμβάνεται η έννοια του εγκλήματος με ηλεκτρονικό υπολογιστή. Στη σύμβαση αναφέρονται οι ηλεκτρονικές παραβάσεις και τα μέτρα που υπάρχουν σε εθνικό επίπεδο στις χώρες της Ευρωπαϊκής Ένωσης. Μεταξύ των σημαντικότερων παραβάσεων είναι οι ακόλουθες:

- Παράνομη πρόσβαση (illegal access)
- Παράνομη υποκλοπή (illegal interception)
- Παρεμβολή σε δεδομένα (data interference)
- Παρεμβολή σε συστήματα (system interference)
- Κακή χρήση συσκευών (misuse of devices)
- Κλοπή που σχετίζεται με υπολογιστή (computer-relatedforgery)
- Απάτη που σχετίζεται με υπολογιστή (computer-related fraud)
- Προστασία πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών (offences related to copyrights)

Στην ίδια σύμβαση γίνεται αναφορά στην διεθνή συνεργασία μεταξύ των χωρών. Περιγράφονται οι ανάγκες για τη λήψη κατάλληλων μέτρων που αφορούν στη σχέση μεταξύ εγκλημάτων που γίνονται με τον παραδοσιακό τρόπο αλλά και εκείνων που γίνονται με τη βοήθεια υπολογιστή. Αναλυτικότερα, προβλέπονται δυο τρόποι συνεργασίας:

- Χωρίς νομική βάση συνεργασίας μεταξύ των χωρών που εμπλέκονται

- Με νομική βάση συνεργασίας μεταξύ των χωρών που εμπλέκονται

Παράλληλα, προβλέπεται η δημιουργία ενός Δικτύου Συνεργασίας, το οποίο θα επιτυγχάνει τη βέλτιστη δυνατή συνεργασία μεταξύ των μερών που υπογράφουν τη συγκεκριμένη σύμβασης.

Οδηγία 2002/58/ΕΚ

Προστασία των δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών

Η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, αναφέρεται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Οι νέες τεχνολογίες απαιτούν την επιβολή ειδικών όρων για τη διασφάλιση του δικαιώματος σεβασμού της ιδιωτικής ζωής.

Η οδηγία 2002/58/ΕΚ αποτελεί μέρος της δέσμης ρυθμίσεων για τις τηλεπικοινωνίες και συνιστά τη νέα νομοθετική πράξη που καλύπτει τον τομέα των ηλεκτρονικών επικοινωνιών και αντικαθιστά την υφιστάμενη νομοθεσία που διέπει τον τομέα των τηλεπικοινωνιών. Η δέσμη ρυθμίσεων για τις τηλεπικοινωνίες περιλαμβάνει τέσσερις ακόμη οδηγίες για το γενικό πλαίσιο , για την πρόσβαση και τη διασύνδεση, για τις γενικές και ειδικές άδειες, καθώς και για την καθολική υπηρεσία. Παράλληλα, η οδηγία προσεγγίζει ορισμένα θέματα, όπως η φύλαξη των δεδομένων σύνδεσης από τα κράτη μέλη για την εξυπηρέτηση της αστυνομικής επιτήρησης, η αποστολή αυτόκλητων ηλεκτρονικών μηνυμάτων, η χρήση «cookies» και η αναγραφή προσωπικών δεδομένων στους δημόσιους καταλόγους συνδρομητών.

- **Απόρρητο των επικοινωνιών**

Η οδηγία υπενθυμίζει ως βασική αρχή ότι τα κράτη μέλη οφείλουν να εγγυώνται, μέσω της εθνικής νομοθεσίας, το απόρρητο των επικοινωνιών που πραγματοποιούνται μέσω δημόσιου δικτύου ηλεκτρονικών επικοινωνιών. Οφείλουν, ειδικότερα, να απαγορεύουν σε κάθε άλλο πρόσωπο εκτός των χρηστών την ακρόαση, την υποκλοπή, την αποθήκευση των επικοινωνιών χωρίς τη συγκατάθεση των ενδιαφερόμενων χρηστών.

- **Διατήρηση των δεδομένων**

Όσον αφορά το ευαίσθητο θέμα της διατήρησης των δεδομένων, η οδηγία ορίζει ότι τα κράτη μέλη δεν επιτρέπεται να αίρουν την προστασία των δεδομένων παρά μόνον όταν πρόκειται για τη διενέργεια ερευνών ποινικού χαρακτήρα ή για τη διαφύλαξη της εθνικής ασφάλειας, της εθνικής άμυνας και της δημόσιας ασφάλειας. Ένα τέτοιο μέτρο μπορεί να θεσπιστεί μόνον όταν αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο στο πλαίσιο της δημοκρατικής κοινωνίας.

- **Αυτόκλητα ηλεκτρονικά μηνύματα**

Η οδηγία υιοθετεί μια προσέγγιση συγκατάθεσης έναντι των αυτόκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα, σύμφωνα με την οποία οι χρήστες οφείλουν να παρέχουν τη συγκατάθεσή τους προτού λάβουν τα εν λόγω μηνύματα. Αυτό το σύστημα συγκατάθεσης καλύπτει επίσης τα σύντομα μηνύματα και τα λοιπά ηλεκτρονικά μηνύματα που λαμβάνονται σε οποιοδήποτε σταθερό ή κινητό τερματικό.

Οδηγία 2006/24/ΕΚ

Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών.

Τον Μάρτιο του 2006, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσαν οδηγία για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με

την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ.

Η οδηγία αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών μελών σχετικά με τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών όσον αφορά τη διατήρηση των δεδομένων. Σκοπός είναι να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα προκειμένου να διερευνώνται, να διαπιστώνονται και να διώκονται οι παραβάσεις. Ορίζει συγκεκριμένα τις κατηγορίες διατηρούμενων δεδομένων, το χρονικό διάστημα διατήρησης δεδομένων, τους όρους αποθήκευσης για τα διατηρούμενα δεδομένα και τις αρχές που πρέπει να τηρούνται όσον αφορά την ασφάλεια των δεδομένων.

Κανονισμός (ΕΚ) αριθ. 45/2001

Ο Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων.

Ο κανονισμός αυτός αποσκοπεί στη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των οργάνων και των οργανισμών της ΕΕ. Το κείμενο περιλαμβάνει διατάξεις που εγγυώνται υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα, τα οποία διαχειρίζονται τα όργανα και οι οργανισμοί της Κοινότητας. Παράλληλα, διασαφηνίζεται η δημιουργία ανεξάρτητου οργάνου εποπτείας, επιφορτισμένου με τον έλεγχο της εφαρμογής των εν λόγω διατάξεων.

Απόφαση 2004/387/ΕΚ: Πρόγραμμα IDABC (2005-2009)

Η απόφαση 2004/387/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Απριλίου 2004, αναφέρεται στην διαλειτουργική παροχή πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης στις δημόσιες διοικήσεις, τις επιχειρήσεις και τους πολίτες (IDABC). Το πρόγραμμα IDABC (*Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens*) αποσκοπεί στην παροχή πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης στις δημόσιες διοικήσεις, τις επιχειρήσεις και τους πολίτες. Στόχος είναι να βελτιωθεί η αποτελεσματικότητα των ευρωπαϊκών δημόσιων διοικήσεων και η μεταξύ τους συνεργασία.

Το πρόγραμμα IDABC αποσκοπεί να υποστηρίξει και να προωθήσει την ανάπτυξη των πανευρωπαϊκών υπηρεσιών ηλεκτρονικής δημόσιας διοίκησης, καθώς και τα διαλειτουργικά τηλεματικά δίκτυα που τις υποστηρίζουν. Μέσα στις επιδιώξεις του προγράμματος είναι να δημιουργήσει τη δυνατότητα ανταλλαγής πληροφοριών μεταξύ των δημόσιων διοικήσεων, καθώς και μεταξύ των εν λόγω δημόσιων διοικήσεων και των κοινοτικών οργάνων. Ακόμα, στοχεύει στην διευκόλυνση της παροχής πανευρωπαϊκών υπηρεσιών στις επιχειρήσεις και τους πολίτες, λαμβάνοντας υπόψη τις ανάγκες τους. Παράλληλα, είναι σημαντική και η επίτευξη της διαλειτουργικότητας μεταξύ των διάφορων τομέων πολιτικής, κυρίως βάσει ενός ευρωπαϊκού διαλειτουργικού πλαισίου.

Απόφαση 1719/1999/ΕΚ

Η Απόφαση 1719/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 1999, σχετικά με σειρά κατευθύνσεων, συμπεριλαμβανομένης της ταυτοποίησης προγραμμάτων κοινού ενδιαφέροντος, όσον αφορά τα διευρωπαϊκά δίκτυα ηλεκτρονικής ανταλλαγής δεδομένων μεταξύ διοικήσεων (IDA) [Επίσημη Εφημερίδα L 203 της 3ης Αυγούστου 1999].

Απόφαση 1720/1999/ΕΚ

Η Απόφαση 1720/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 1999, για τη θέσπιση μιας σειράς δράσεων και μέτρων με σκοπό την εξασφάλιση της διαλειτουργικότητας των διευρωπαϊκών δικτύων ηλεκτρονικής ανταλλαγής δεδομένων

μεταξύ διοικήσεων (IDA) και της πρόσβασης σ' αυτά [Επίσημη Εφημερίδα L 203 της 3ης Αυγούστου 1999].

COM(2005) 425: Ηλεκτρονική προσβασιμότητα

Η ηλεκτρονική προσβασιμότητα καθορίζει καταρχήν τις πρωτοβουλίες με τις οποίες θα εξασφαλισθεί για όλους τους πολίτες πρόσβαση στις υπηρεσίες της κοινωνίας των πληροφοριών. Το θέμα είναι δηλαδή να αρθούν οι τεχνικοί, οι νομικοί ή άλλοι φραγμοί στους οποίους μπορούν να προσκρούσουν ορισμένα άτομα όταν χρησιμοποιούν υπηρεσίες που συνδέονται με τις ΤΠΕ. Πρόκειται ιδίως για τους ανάπηρους και ορισμένα ηλικιωμένα άτομα. Το θέμα είναι επίσης να προωθηθεί σε αυτά τα άτομα η χρήση των ΤΠΕ και του Διαδικτύου και να ευαισθητοποιηθούν όσον αφορά τις προοπτικές που μπορούν να τους προσφέρουν.

Απαιτήσεις και πρότυπα προσβασιμότητας

Η έκδοση ευρωπαϊκών προτύπων για την ηλεκτρονική προσβασιμότητα θα συμβάλει στην ομαλή λειτουργία της ενιαίας ευρωπαϊκής αγοράς.

Σχεδιασμός για όλους (DFA)

Ο DFA επιτρέπει πληρέστερο συνυπολογισμό των απαιτήσεων προσβασιμότητας κατά το σχεδιασμό ενός προϊόντος ή μιας υπηρεσίας.

Προσβασιμότητα στους ιστοτόπους

Η Επιτροπή και τα κράτη μέλη, με τη βοήθεια μιας ομάδας εμπειρογνωμόνων ηλεκτρονικής προσβασιμότητας, ελέγχουν τις πρωτοβουλίες που αναλαμβάνονται για την δημιουργία ιστοτόπων. Μια ομάδα εργασίας της Ευρωπαϊκής Επιτροπής Τυποποίησης ασχολείται με την εξεύρεση κατάλληλων λύσεων στην εκπόνηση συστημάτων πιστοποίησης της προσβασιμότητας.

Σημεία αναφοράς και παρακολούθηση

Για να είναι δυνατή η περαιτέρω ανάπτυξη κατάλληλων ευρωπαϊκών πολιτικών ηλεκτρονικής προσβασιμότητας είναι απαραίτητο να υπάρχουν διαθέσιμα ευρωπαϊκά δεδομένα, τα οποία να είναι συγκρίσιμα μεταξύ κρατών μελών.

Πιστοποίηση της προσβασιμότητας

Ισχύουν ήδη ή καταρτίζονται πολλά πρότυπα που ορίζουν τον τρόπο με τον οποίο μπορούν τα προϊόντα και οι υπηρεσίες να καταστούν προσβάσιμες. Ωστόσο, σήμερα δεν υπάρχουν αξιόπιστα μέσα για την αξιολόγηση της συμμόρφωσης των προϊόντων με αυτά τα πρότυπα προσβασιμότητας. Η καθιέρωση μηχανισμών πιστοποίησης της προσβασιμότητας θα βοηθήσει να προσανατολισθούν οι καταναλωτές και οι πελάτες που επιθυμούν προσβάσιμα προϊόντα και υπηρεσίες.

Κανονισμός (ΕΚ) αριθ. 460/2004: Δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών

Προκειμένου να εξασφαλισθεί υψηλό και ουσιαστικό επίπεδο ασφάλειας δικτύων και πληροφοριών εντός της Κοινότητας και να αναπτυχθεί η αντίληψη της ασφάλειας δικτύων και πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα της Ευρωπαϊκής Ένωσης, συμβάλλοντας έτσι στην ομαλή λειτουργία της εσωτερικής αγοράς, δημιουργείται ο ευρωπαϊκός οργανισμός για την ασφάλεια δικτύων και πληροφοριών.

Ο Οργανισμός παρέχει συνδρομή και δίνει συμβουλές στην Επιτροπή και στα κράτη μέλη σχετικά με θέματα που αφορούν την ασφάλεια δικτύων και πληροφοριών, τα οποία εμπίπτουν στις αρμοδιότητές του κατά τα οριζόμενα στον παρόντα κανονισμό. Με αφετηρία τις εθνικές και τις κοινοτικές προσπάθειες, αναπτύσσει υψηλό επίπεδο ειδικών γνώσεων. Ο Οργανισμός χρησιμοποιεί αυτές τις ειδικές γνώσεις για την προώθηση ευρείας συνεργασίας μεταξύ παραγόντων του δημόσιου και του ιδιωτικού τομέα.

Συμμετοχή τρίτων χωρών

Ο Οργανισμός είναι ανοικτός στη συμμετοχή χωρών που έχουν συνάψει συμφωνίες με την Ευρωπαϊκή Κοινότητα, δυνάμει των οποίων έχουν υιοθετήσει και εφαρμόζουν την κοινοτική νομοθεσία στον τομέα που καλύπτει ο παρών κανονισμός.

Οδηγία 1999/93/ΕΚ

Κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές

Η Οδηγία 1999/93/ΕΚ στοχεύει στην διευκόλυνση της χρήσης ηλεκτρονικών υπογραφών καθώς και στη νομική αναγνώρισή τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς.

Πρόσβαση στην αγορά

Τα κράτη μέλη δύνανται να διατηρούν μηχανισμούς εθελοντικής διαπίστευσης που αποσκοπούν στην επίτευξη βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης. Όλες οι προϋποθέσεις που συνδέονται με τους εν λόγω μηχανισμούς πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες και να μην οδηγούν σε διακρίσεις. Η Επιτροπή καθορίζει τα κριτήρια βάσει των οποίων τα κράτη μέλη ορίζουν τους φορείς. Εάν διαπιστωθεί ότι η δημιουργία υπογραφών συμμορφώνεται προς τις απαιτήσεις της οδηγίας, είναι αναγνωρίσιμη από όλα τα κράτη μέλη.

Αρχές της εσωτερικής αγοράς

Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει για παρόχους υπηρεσιών πιστοποίησης εγκατεστημένους στην επικράτειά του, καθώς και για τις υπηρεσίες που αυτοί παρέχουν. Τα κράτη μέλη διασφαλίζουν ότι τα προϊόντα ηλεκτρονικής υπογραφής που συμμορφώνονται με την παρούσα οδηγία επιτρέπεται να κυκλοφορούν ελεύθερα στην εσωτερική αγορά.

Έννομες συνέπειες των ηλεκτρονικών υπογραφών

Τα κράτη μέλη διασφαλίζουν ότι οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρούνται επί χάρτου, και γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.

Ευθύνη

Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι με την έκδοση πιστοποιητικού ως αναγνωρισμένου πιστοποιητικού στο κοινό ή με την εγγύηση τέτοιου πιστοποιητικού στο κοινό, ο πάροχος υπηρεσιών πιστοποίησης υπέχει ευθύνη για την προκληθείσα ζημία έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου που ευλόγως βασίζεται στο πιστοποιητικό.

Διεθνείς πτυχές

Τα κράτη μέλη διασφαλίζουν ότι τα πιστοποιητικά που εκδίδονται στο κοινό ως αναγνωρισμένα πιστοποιητικά από πάροχο υπηρεσιών πιστοποίησης, εγκατεστημένο σε τρίτη χώρα, θεωρούνται νομικώς ισοδύναμα με πιστοποιητικά που εκδίδονται από πιστοποιημένο πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Κοινότητα.

Προστασία δεδομένων

Τα κράτη μέλη διασφαλίζουν ότι οι πάροχοι υπηρεσιών πιστοποίησης και οι εθνικοί φορείς, αρμόδιοι για πιστοποίηση ή εποπτεία, συμμορφώνονται προς τις απαιτήσεις που καθορίζονται στην 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.

Κοινοποίηση

Για την σωστή λειτουργία του συστήματος ηλεκτρονικών υπογραφών και την αποφυγή δυσπιστίας έναντι κάποιου πιστοποιητικού, τα κράτη μέλη πρέπει να κοινοποιούν στην Επιτροπή αλλά και στα υπόλοιπα κράτη μέλη πληροφορίες σχετικά με εθνικά συστήματα εθελοντικής διαπίστευσης. Πρέπει να είναι ευρέως γνωστές και οι ονομασίες και οι διευθύνσεις των εθνικών φορέων που είναι αρμόδιοι για διαπίστευση και επίβλεψη των ηλεκτρονικών υπογραφών. Πρέπει να ανακοινώνονται οι ονομασίες και οι διευθύνσεις όλων των διαπιστευμένων εθνικών παρόχων υπηρεσιών πιστοποίησης.

7.2 Ελληνικό νομικό πλαίσιο

Η Ελλάδα, ακολουθώντας την γραμμή που δίνεται από την Ευρωπαϊκή Ένωση, δημιουργεί το ανάλογο θεσμικό και νομικό πλαίσιο. Λαμβάνοντας τις οδηγίες και τις αποφάσεις που παίρνονται από το συμβούλιο της Ευρωπαϊκής Ένωσης, τις προσαρμόζει στον ελληνικό νόμο, εξελίσσοντας τον έτσι ώστε να συμπεριληφθούν και τα νέα δεδομένα που δημιουργούνται με την ανάπτυξη της τεχνολογίας.

Από την στιγμή που αναπτύσσονται ραγδαία, οι ηλεκτρονικές υπηρεσίες και επηρεάζονται πολλοί τομείς ακόμα και της καθημερινής ζωής των πολιτών, είναι αναγκαία η προσαρμογή της νομοθεσίας ώστε να καλύπτει και να διασφαλίζει την ομαλή αλληλεπίδραση των μερών. Είναι αναγκαία η διασφάλιση της ακεραιότητας και της αυθεντικότητας των ηλεκτρονικών συναλλαγών.

Στην συνέχεια αναφέρονται οι διατάξεις που σχετίζονται με την λειτουργία και την χρήση των στοιχείων πιστοποίησης της ταυτότητας των χρηστών.

Ποινικός κώδικας- Άρθρο 370Β

Το άρθρο 370Β του ποινικού κώδικα εξετάζει περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε απόρρητα δεδομένα ηλεκτρονικών υπολογιστών.

«Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτο ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστο τριών μηνών.

Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστο ενός έτους. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.»

(Άρθρο 370Β, παράγραφοι 1,2,3)

Το άρθρο αυτό είναι ιδιαίτερα σημαντικό, καθώς περικλείει ποινές για μια πλειάδα εγκληματικών πράξεων όπως, μη εξουσιοδοτημένη πρόσβαση σε συστήματα υπολογιστών, μη εξουσιοδοτημένη αντιγραφή απόρρητων δεδομένων, μη εξουσιοδοτημένη διακίνηση απόρρητων δεδομένων. Τα οποία είναι από τους σημαντικότερους περιορισμούς που πρέπει να λαμβάνονται υπόψη.

Το άρθρο 370Β του ποινικού κώδικα σχετίζεται, μεταξύ άλλων, με:

- Το άρθρο 2, παράγραφος 4, εδάφιο Β του νόμου 1599/1986 «Σχέσεις κράτους-πολίτη, καθιέρωση νέου δελτίου ταυτότητας κ.ά. διατάξεις»
- Το άρθρο 16 του νόμου 146/1914 «Περί αθέμιτου ανταγωνισμού» 26 Το άρθρο 3708 προστέθηκε με το άρθρο 3 του νόμου 1805/1988
- Το άρθρο 35, παράγραφος 1, του νόμου 2172/1993 «Για την προστασία της κοινωνίας από το οργανωμένο έγκλημα»
- Το νόμο 2068/1992 «Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα»
- Άρθρο 18, παράγραφος 4 και άρθρο 22, παράγραφοι 1-8, του νόμου 2472/1997 «προστασία του ατόμου από την επεξεργασία δεδομένων Προσωπικού χαρακτήρα»

Ποινικός κώδικας - Άρθρο 370Γ

Ανάλογες περιπτώσεις εξετάζονται και στο Άρθρο 370Γ, στο οποίο καλύπτονται και θέματα παράνομης αντιγραφής και διακίνησης προστατευμένου λογισμικού (software).

«Όποιος χωρίς δικαίωμα αντιγράψει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μηνών και με χρηματική ποινή εκατό χιλιάδες έως δυο εκατομμυρίων δραχμών. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε

υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφ' όσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τριών μηνών ή με χρηματική ποινή τουλάχιστο δέκα χιλιάδων δραχμών. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση αρμόδιου υπαλλήλου του.»

(Άρθρο 370Γ, παράγραφοι 1,2,3)

Το άρθρο 370Γ του ποινικού κώδικα σχετίζεται, μεταξύ άλλων, με:

- Το άρθρο 16, του νόμου 146/1914 («Περί αθέμιτου ανταγωνισμού»)
- Το άρθρο 30, του νόμου 1806/1988 («Τροποποίηση νομοθεσίας για τα
- Χρηματιστήρια και άλλες διατάξεις»)
- Το άρθρο 35, παράγραφος 1, του νόμου 2172/1993 (ο οποίος αντικατέστησε το άρθρο 12 του νόμου 1916/1990 «Για την προστασία της κοινωνίας από το οργανωμένο έγκλημα»)
- Το νόμο 2068/1992 («Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα»)
- Το άρθρο 18, παράγραφος 4 καθώς και το άρθρο 22, παράγραφοι 1-8, του νόμου 2472/1998 («Για την, προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»)

Νόμος 2472/1997

Προστασία Του ατόμου από την επεξεργασία δεδομένων Προσωπικού χαρακτήρα

Σύμφωνα με το νόμο αυτό, ως δεδομένα προσωπικού χαρακτήρα ορίζονται «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων». Ο συγκεκριμένος νόμος περιλαμβάνει τις επόμενες έννοιες:

- Χαρακτηριστικά δεδομένων προσωπικού χαρακτήρα
- Προϋποθέσεις Επεξεργασίας
- Γνωστοποίηση αρχείων
- Επεξεργασία ευαίσθητων δεδομένων
- Απαλλαγή υποχρέωσης γνωστοποίησης και λήψης άδειας
- Διασύνδεση Αρχείων
- Διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα
- Απόρρητο και ασφάλεια της επεξεργασίας

Επίσης, ο νόμος περιγράφει τα δικαιώματα που έχει στα δεδομένα ο κάτοχός τους, ορίζοντας το δικαίωμα ενημέρωσης, πρόσβασης, αντίρρησης και το δικαίωμα προσωρινής δικαστικής προστασίας.

Νόμος 3471

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του νόμου 2472/1997.

Ο νόμος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Με τον νόμο αυτό γίνεται ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002.

Ο σκοπός των διατάξεων του νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών. Οι ορισμοί που περιλαμβάνονται στον νόμο αυτό συμπληρώνουν τους ορισμούς του νόμου 2472/1997, ενώ παράλληλα λαμβάνονται υπόψη οι ορισμοί του νόμου 3431/2006 περί ηλεκτρονικών επικοινωνιών.

Η εφαρμογή του νόμου αυτού γίνεται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών. Η ακρόαση, η υποκλοπή, η αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης απαγορεύονται. Εξαίρεση αποτελεί κάθε περίπτωση που προβλέπεται διαφορετικά από το νόμο.

Η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, απαγορεύεται, ιδίως με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων. Από τον νόμο επίσης καθορίζονται οι κανόνες επεξεργασίας βάσει των οποίων πρέπει να λειτουργεί ένα σύστημα. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων και των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της.

Επιτρέπεται η επεξεργασία δεδομένων θέσης, που αφορούν τους χρήστες ή συνδρομητές δικτύων ή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, για την παροχή υπηρεσίας προστιθέμενης αξίας, μόνον εφόσον αυτά καθίστανται ανώνυμα με την κατάλληλη κωδικοποίηση ή με τη ρητή συγκατάθεση του χρήστη ή του συνδρομητή, στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μίας υπηρεσίας προστιθέμενης αξίας.

Ο νόμος 3471 ορίζει επίσης τις αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει και ως προς την τήρηση των διατάξεων του παρόντος νόμου τις αρμοδιότητες που προβλέπονται από το ν. 2472/1997. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) έχει ως προς την τήρηση των διατάξεων του παρόντος νόμου, που αναφέρονται σε αυτήν, τις αρμοδιότητες που προβλέπονται από το νόμου 3115/2003, όπως εκάστοτε ισχύει.

Με τον νόμο αυτό ορίζονται τα ευαίσθητα δεδομένα και τα δεδομένα προσωπικού χαρακτήρα. Ως ευαίσθητα δεδομένα, ορίζονται τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Ως Αρχείο δεδομένων προσωπικού χαρακτήρα ορίζεται κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια.

Νόμος 2672/1998

Ο Νόμος 2672 του 1998 καθορίζει στο άρθρο 14 τους όρους χρήσης μιας ψηφιακής υπογραφής. Το άρθρο αυτό ασχολείται κυρίως με θέματα που προκύπτουν από την χρήση του ηλεκτρονικού ταχυδρομείου. Οι κανόνες δέσμευσης μεταξύ του αποδέκτη ενός μηνύματος (π.χ. ένας δημόσιος υπάλληλος) και ένας αποστολέας (π.χ. ένας υπάλληλος) είναι επίσης καθορισμένοι. Με την αποστολή ενός μηνύματος δεν συνεπάγεται ότι θα γίνει παραλαβή από τον αποδέκτη, εκτός εάν υπάρχουν τρόποι επιβεβαίωσης. Από την άλλη μεριά, εάν ο αποστολέας ζητά μια τέτοια επιβεβαίωση, ο αποδέκτης πρέπει να δώσει μια επιβεβαίωση, εάν δεν είναι διαθέσιμος ένας αυτόματος μηχανισμός.

Ο νόμος αυτός καλύπτει ως ένα βαθμό την ανάγκη αναγνώρισης ταυτότητας, πιστοποίησης ταυτότητας και σχετικών μηχανισμών ασφαλείας. Οι μηχανισμοί αυτοί είναι απαραίτητοι για τις αλληλεπιδράσεις των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Οι διασφαλίσεις αυτές αφορούν ιδιαίτερα τις υπηρεσίες που βρίσκονται στα στάδια της κάθετης και της οριζόντιας ολοκλήρωσης, οπότε και υπάρχει ουσιαστική αλληλεπίδραση.

Νόμος 3389/2005

Ο νόμος αυτός έχει έμμεση σχέση με την χρήση των ηλεκτρονικών ταυτοτήτων και την υλοποίηση τους, καθώς προσδιορίζει το θεσμικό πλαίσιο για τις συμπράξεις του δημοσίου με τον ιδιωτικό τομέα. Ο νόμος αυτός ψηφίστηκε το 2005 και ενσωματώνει την οδηγία 18/2004. Με την ψήφιση του νόμου αυτού επιτρέπεται στις δημόσιες υπηρεσίες να συνεργάζονται με εταιρίες του ιδιωτικού τομέα για την ανάπτυξη έργων.

Η χρηματοδότηση αυτών των έργων γίνεται με ιδιωτικά κυρίως κεφάλαια ενώ μετά την υλοποίηση τους παραχωρούνται προς εκμετάλλευση στον ιδιωτικό τομέα για προκαθορισμένο χρονικό διάστημα ώστε να γίνει απόσβεση του κόστους υλοποίησης, καθώς και η απαιτούμενη απόδοση των επενδυμένων κεφαλαίων. Σε περίπτωση που το δημόσιο είναι ο κύριος και μοναδικός χρήστης του έργου τότε θα καταβάλει ένα τακτικό μίσθωμα στον ιδιωτικό φορέα για επίσης προκαθορισμένο χρονικό διάστημα. Ο λόγος για τον οποίο γίνεται αναφορά στον συγκεκριμένο νόμο είναι η δυνατότητα υλοποίησης σημαντικών έργων, όπως οι ηλεκτρονικές ταυτότητες.

7.3 Πράξεις και προεδρικά διατάγματα

Προεδρικό Διάταγμα Ν342

Το προεδρικό διάταγμα Ν342 που εκδόθηκε την 22^{η} Νοεμβρίου 2002, καθορίζει τις καταστάσεις, στις οποίες μια ψηφιακή υπογραφή είναι απαραίτητη. Δηλώνει ξεκάθαρα ότι μια ψηφιακή υπογραφή είναι απαραίτητη σε ένα ηλεκτρονικό έγγραφο εάν αυτό το έγγραφο έχει νομική συνέπεια. Αυτό σημαίνει ότι μόνο έγγραφα χωρίς συνέπειες μπορούν να παραδοθούν στους δημόσιους διαχειριστές, ενώ σχεδόν όλες οι σημαντικές συναλλαγές πρέπει να χρησιμοποιούν ένα μηχανισμό ψηφιακής υπογραφής.

Προεδρικό Διάταγμα 150/2000

Το Προεδρικό Διάταγμα. 150/2000 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. Έγινε καθορισμός του πλαισίου μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά κάτω από ορισμένες συνθήκες, έχουν την ίδια δέσμευση όπως με τις παραδοσιακές συναλλαγές.

Επιπλέον, με το Προεδρικό Διάταγμα 150/2000,καθόριστηκαν οι όροι που πρέπει να ισχύουν σε ψηφιακά πιστοποιητικά για να θεωρούνται αναγνωρισμένα πιστοποιητικά και τους όρους που πρέπει να πληρούν οι Πάροχοι Υπηρεσιών Πιστοποίησης για να παρέχουν αναγνωρισμένα πιστοποιητικά. Τέθηκαν οι αρχές λειτουργίας της εσωτερικής αγοράς όσον αφορά την παροχή ψηφιακών υπηρεσιών πιστοποίησης. Παράλληλα, τέθηκαν οι προϋποθέσεις νομικής αναγνώρισης εντός των χωρών της Ευρωπαϊκής Ένωσης των αναγνωρισμένων πιστοποιητικών που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης εγκατεστημένους σε χώρες εκτός της Ευρωπαϊκής Ένωσης.

Επιπλέον, ορίστηκαν και οι αρμοδιότητες της Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ). Η ΕΕΤΤ είναι η αρμόδια αρχή για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής καθώς και για την διαπίστωση της συμμόρφωσης προς τις «ασφαλείς διατάξεις δημιουργίας υπογραφής». Παράλληλα η ΕΕΤΤ είναι αρμόδια για τον ορισμό και την εποπτεία ιδιωτικών ή δημόσιων φορέων για την διαπίστευση των παρόχων πιστοποίησης όσο και για την διαπίστωση της συμμόρφωσης προς τις «ασφαλείς διατάξεις δημιουργίας υπογραφής».

Απόφαση 248/71 ΕΕΤΤ

Με την υπ. αρ. 248/71 Απόφασή της ΕΕΤΤ ορίζεται ο κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής. Η απόφαση αυτή ρυθμίζει ζητήματα των

αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.

Την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, οι οποίοι εκδίδουν αναγνωρισμένα ή μη πιστοποιητικά ή παρέχουν άλλες σχετικές με την ηλεκτρονική υπογραφή υπηρεσίες πιστοποίησης. Σύμφωνα με το άρθρο 10, η ΕΕΤΤ τηρεί μητρώο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης

Με μια σειρά Αποφάσεών της μέσα στο 2003 η ΕΕΤΤ δημιούργησε το θεσμικό πλαίσιο α) για τον ορισμό και τη λειτουργία των εντεταλμένων φορέων για την Εθελοντική Διαπίστευση (των παρόχων υπηρεσιών πιστοποίησης) και τον έλεγχο των προϊόντων (ασφαλών διατάξεων δημιουργίας υπογραφής και ασφαλών κρυπτογραφικών μονάδων) και β) για την Εθελοντική Διαπίστευση των παρόχων υπηρεσιών πιστοποίησης.

Πράξη συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002

Η πράξη του Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002 καθορίζει το πλαίσιο επίβλεψης των συστημάτων πληρωμών. Ειδικότερα περιλαμβάνονται οι ορισμοί των εννοιών ηλεκτρονικής πληρωμής, ηλεκτρονικού χρήματος, πιστωτικού κινδύνου, διαχειριστή συστημάτων πληρωμών και άλλων βασικών εννοιών. Παράλληλα ορίζεται το σύστημα πληρωμών ως σύστημα που συνίσταται σε σύνολο μέσων και τραπεζικών διαδικασιών που χρησιμοποιούνται, με βάση συμβάσεις και σύμφωνα με τους σχετικούς κανονισμούς λειτουργίας, από ομάδα προσώπων και οργανισμών για να εξυπηρετηθεί, διευκολυνθεί και διασφαλισθεί η ομαλή μεταφορά κεφαλαίων και κυκλοφορία του χρήματος σε μία περιοχή.

Με την έννοια αυτή το σύστημα πληρωμών περιλαμβάνει τα πιστωτικά ιδρύματα και τους πιστωτικούς οργανισμούς, τα μη πιστοποιητικά ιδρύματα που παρέχουν υπηρεσίες για την διενέργεια πληρωμών, την τεχνική υποδομή, το δίκτυο διασύνδεσης των φορέων που μεσολαβούν στις πληρωμές, τις διαδικασίες εκκαθάρισης, συμψηφισμού και διακανονισμού των πληρωμών και τους κανόνες που διέπουν τα μέσα πληρωμής και την εν γένει λειτουργία του συστήματος.

Πράξη Διοικητή 2501/31.10.2002

Η Πράξη Διοικητή 2501/31.10.2002 ρυθμίζει την ενημέρωση των συναλλασσόμενων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές τους. Στην πράξη αυτή γίνεται ειδική αναφορά για τις διενεργούμενες μέσω του διαδικτύου τραπεζικές συναλλαγές και ρυθμίζεται η πληροφορία που παρέχεται από τα τραπεζικά ιδρύματα προκειμένου να συμμορφώνεται με τις απαιτήσεις της πράξης. Αυτό, σύμφωνα με την πράξη, επιτυγχάνεται είτε με την άμεση γνωστοποίηση στο διαδίκτυο των σχετικών στοιχείων είτε με παραπομπή σε εναλλακτικό τρόπο παροχής της σχετικής πληροφόρησης σε επίπεδο καταστήματος.

8 Πρακτική εργασία – Δημιουργία ιστοτόπου Cook it

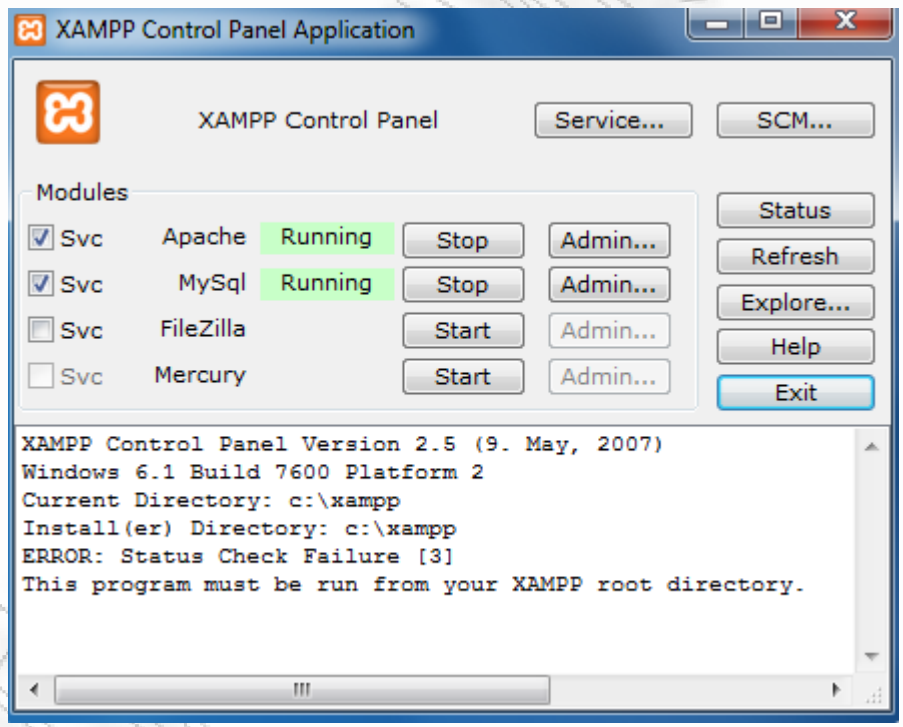
Στα πλαίσια της μελέτης της ιδιωτικότητας και της προστασίας στο Web 2.0, δημιουργήθηκε ένας ιστοτόπος με την χρήση του Joomla. Το Joomla αποτελεί ένα εργαλείο διαχείρισης περιεχομένου ανοικτού κώδικα. Προσφέρει την δυνατότητα διαχείρισης περιεχομένου και καθορισμού των ρόλων των χρηστών στα πλαίσια του ιστοτόπου. Ως εργαλείο ανοικτού κώδικα, προσφέρεται για χρήση σε όποιον το επιθυμεί, ενώ παράλληλα υπάρχει πληθώρα εφαρμογών που μπορούν να εξυπηρετήσουν ανάγκες των χρηστών.

8.1 Χρήση Joomla

Χρησιμοποιήθηκε η έκδοση Joomla 1.7 η οποία παρέχει τη δυνατότητα δημιουργίας αλυσίδας κατηγοριών και υποκατηγοριών, απεριόριστου βάθους, διευκολύνοντας την ταξινόμηση των άρθρων. Η δημιουργία κατηγοριών και υποκατηγοριών διευκολύνει την εννοιολογική αποκόνηση του περιεχομένο του ιστοτόπου αλλά και τον ορισμό της προσβασιμότητας των χρηστών.

8.1.1 Εγκατάσταση του τοπικού server XAMPP

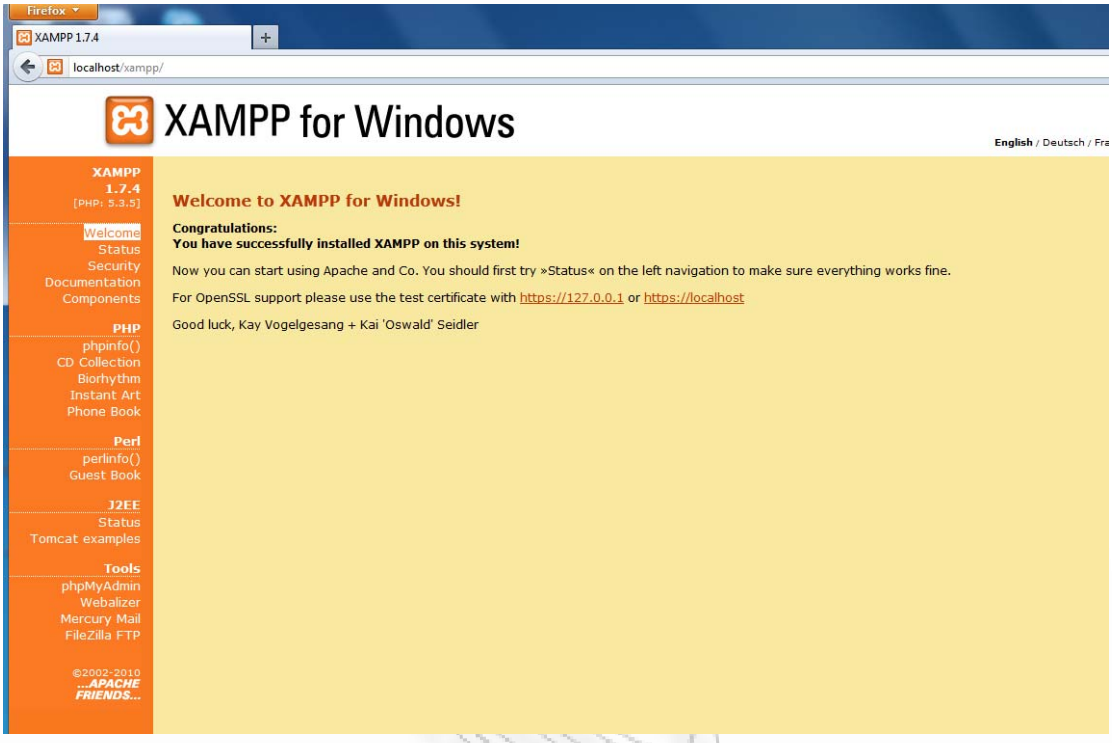
Αρχικά, γίνεται η εγκατάσταση του τοπικού server, του XAMPP. Το αρχείο εγκατάστασης του XAMPP βρίσκεται στην διεύθυνση www.apachefriends.org, από όπου γίνεται η λήψη του αρχείου. Στην συνέχεια γίνεται εγκατάσταση του προγράμματος στον υπολογιστή. Η ενεργοποίηση του τοπικού server XAMPP γίνεται από το control panel.



Εικόνα 8.1 Το control panel του XAMPP

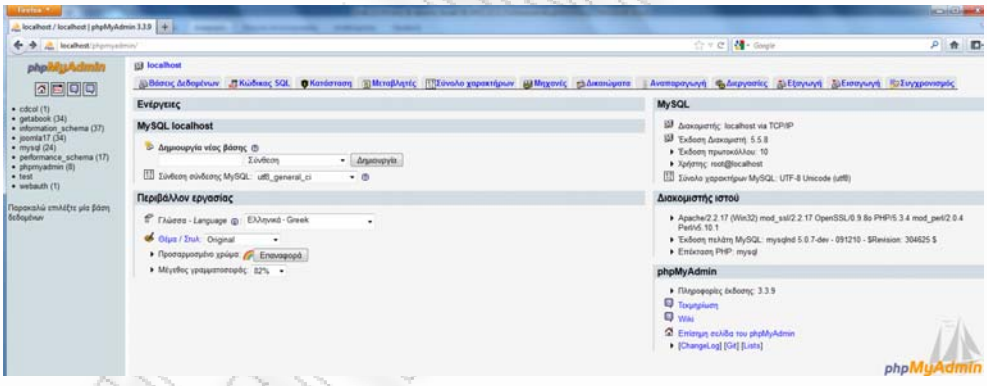
8.1.2 Δημιουργία βάσης δεδομένων της ιστοσελίδας

Εφόσον έχει ενεργοποιηθεί ο τοπικός server, η διαχείρηση όλων των παραμέτρων γίνεται μέσω φυλλομετρητή, πληκτρολογώντας την διεύθυνση: http://localhost/xampp/.



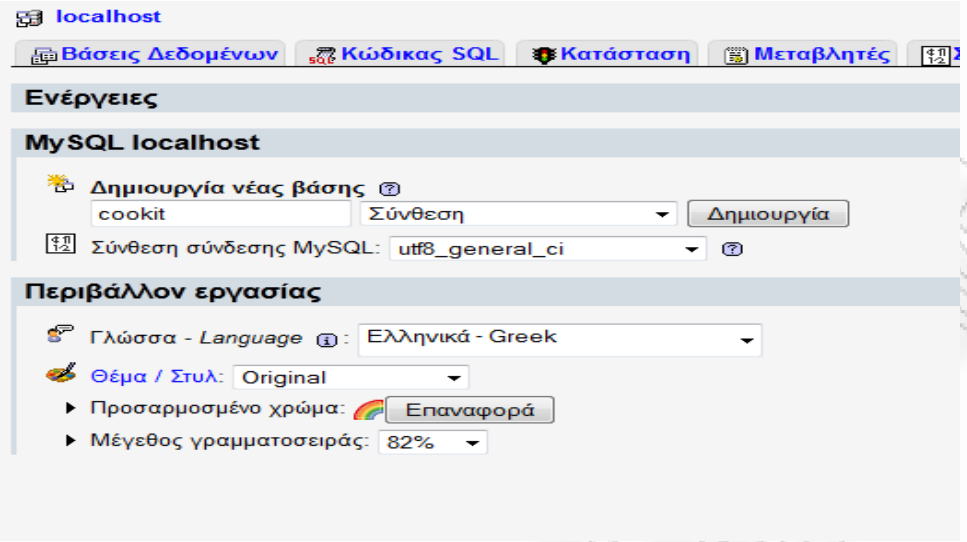
Εικόνα 8.2 Η διαχείριση του τοπικού server XAMPP

Επιλέγοντας το phpMyAdmin εμφανίζεται η σελίδα δημιουργίας και διαχείρισης της βάσης δεδομένων .



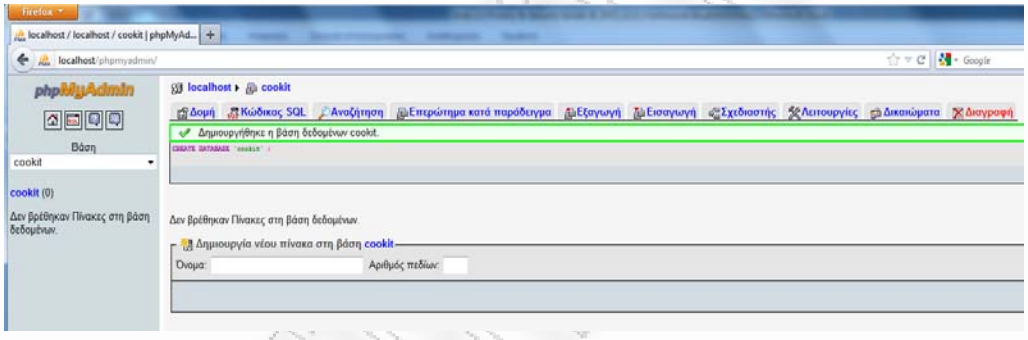
Εικόνα 8.3 Η σελίδα διαχείρισης της βάσης δεδομένων

Για την δημιουργία μίας νέας βάσης δεδομένων, δίνεται το όνομα της βάσης, η κωδικοποίηση που θα χρησιμοποιηθεί και η γλώσσα. Με το πάτημα του πλήκτρου ‘Δημιουργία’, δημιουργείται η βάση δεδομένων.



Εικόνα 8.4 Συμπλήρωση των στοιχείων για τη δημιουργία της βάσης δεδομένων

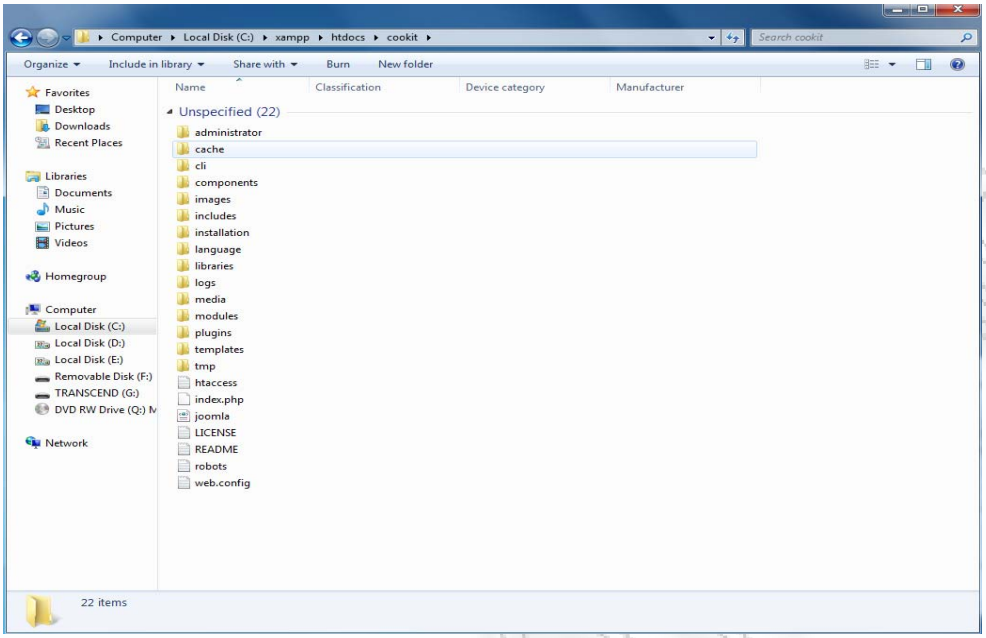
Με το πάτημα του πλήκτρου ‘Δημιουργία’, δημιουργείται η βάση δεδομένων.



Εικόνα 8.5 Δημιουργία βάσης δεδομένων.

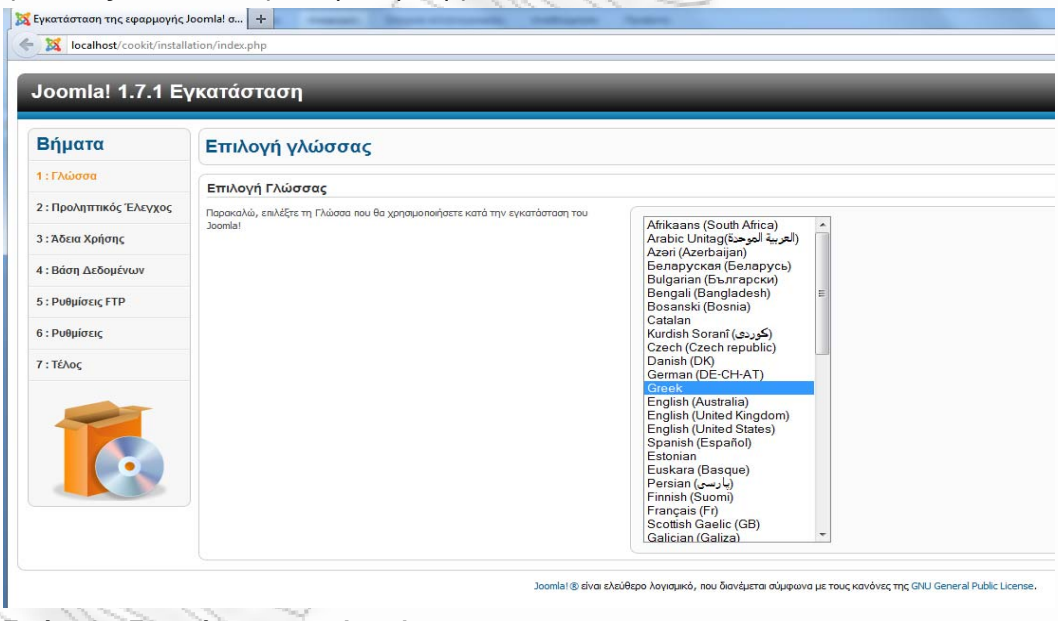
8.1.3 Εγκατάσταση προγράμματος JOOMLA

Το αρχείο του προγράμματος Joomla βρίσκεται στη διεύθυνση http://www.Joomla.org, από όπου γίνεται η λήψη του αρχείου Joomla_1.7.1-Stable-Full_Package, για την έκδοση Joomla 1.7 . Στην συνέχεια, γίνεται αποσυμπίεση και αντιγραφή όλων των αρχείων του Joomla στον φάκελο C:/xampp/htdocs/cookit.



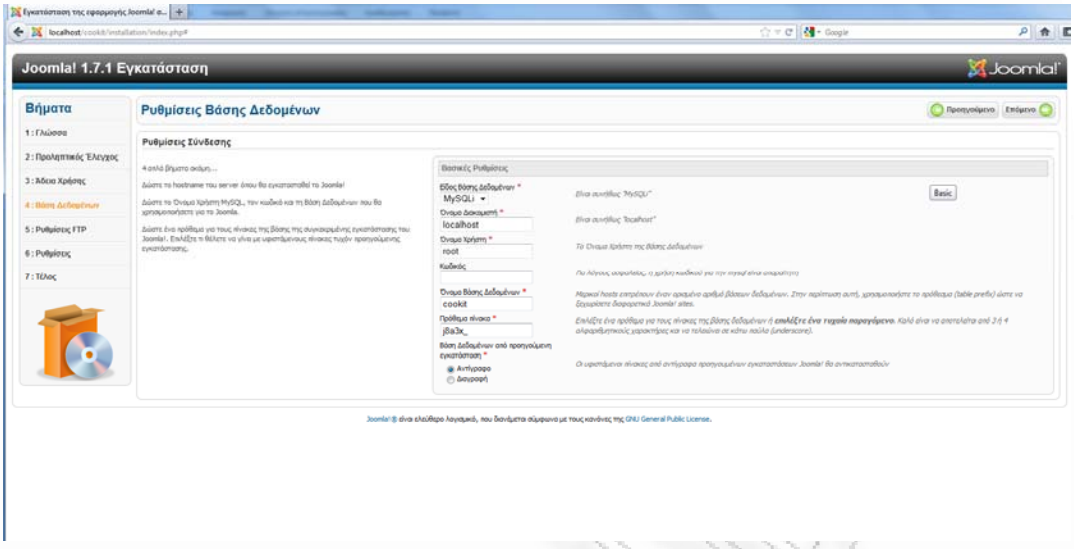
Εικόνα 8.6 Εισαγωγή των αρχείων Joomla στον τοπικό server

Η εγκατάσταση του Joomla ολοκληρώνεται σε 7 βήματα μέσα από τον φυλλομετρητή, δίνοντας την διεύθυνση http://localhost/cookit/. Στο πρώτο βήμα της εγκατάστασης γίνεται η επιλογή γλώσσας, όπου επιλέγεται η ελληνική γλώσσα.



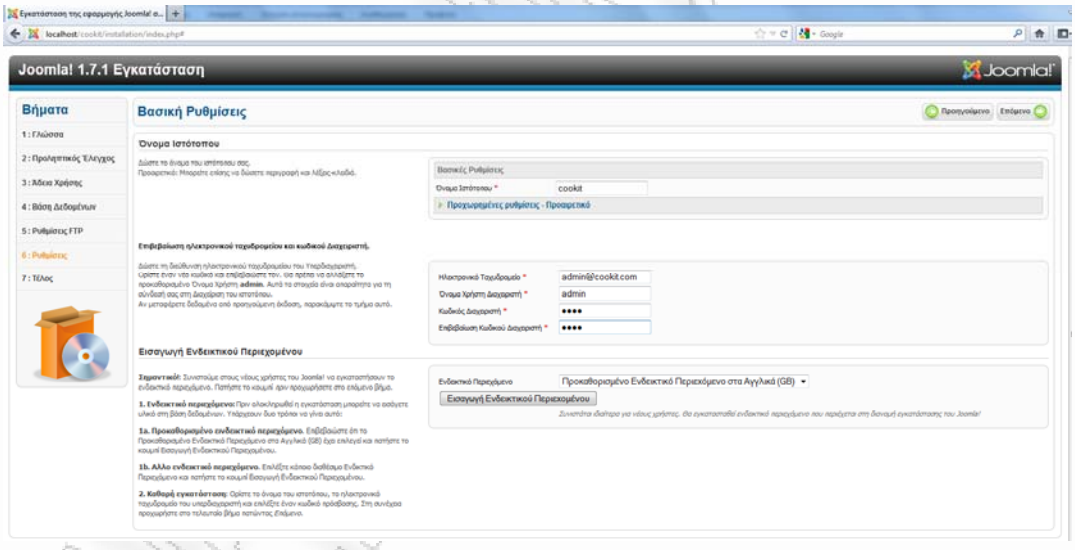
Εικόνα 8.7 Εγκατάσταση του Joomla.

Στο δεύτερο βήμα, εκτελείται προληπτικός έλεγχος για την ορθή λειτουργία της εφαρμογής και στο τρίτο βήμα γίνεται αναφορά στην άδεια χρήσης. Στο τέταρτο βήμα, γίνεται η σύνδεση της ιστοσελίδας με την βάση δεδομένων.



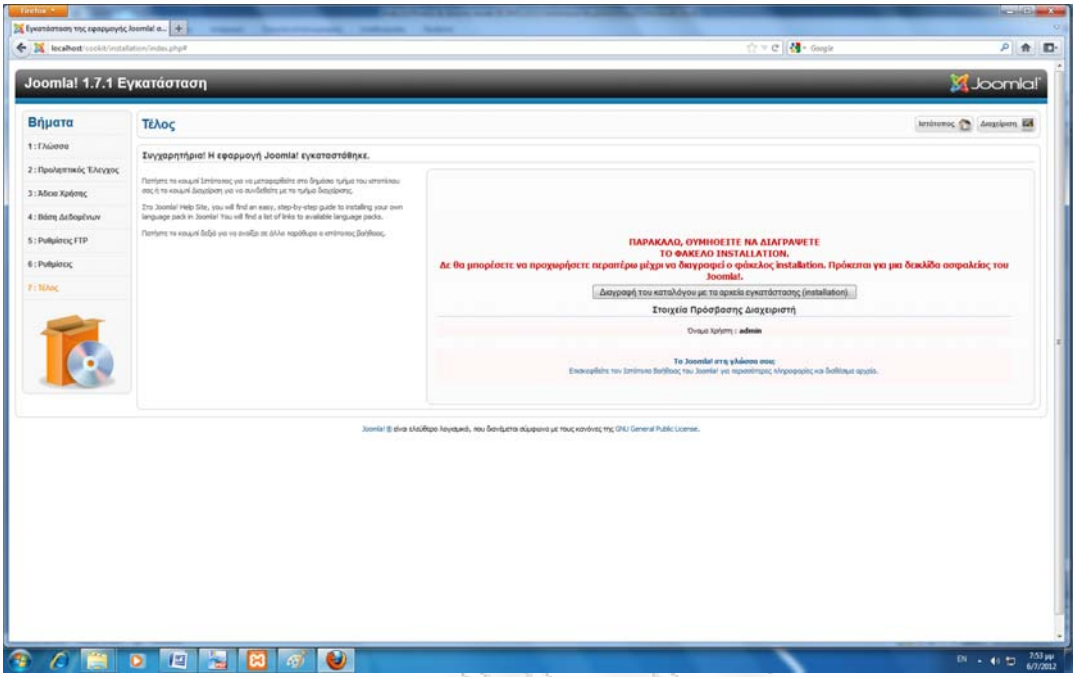
Εικόνα 8.8 Σύνδεση της ιστοσελίδας με την βάση δεδομένων.

Το πέμπτο βήμα είναι προαιρετικό, και αφορά ρυθμίσεις FTP. Στο έκτο βήμα, γίνονται οι βασικές ρυθμίσεις της σελίδας, δίνεται η ονομασία, και ορίζονται τα στοιχεία του διαχειριστή.



Εικόνα 8.9 Ορισμός βασικών ρυθμίσεων σελίδας

Στο έβδομο βήμα, ολοκληρώνεται η εγκατάσταση του Joomla 1.7 και επισημαίνεται ένα βασικό στάδιο της διαδικασίας εγκατάστασης, η διαγραφή του φακέλου installation από τα αρχεία του Joomla 1.7 για την ιστοσελίδα cookit.



Εικόνα 8.10 ολοκλήρωση της εγκατάστασης του Joomla 1.7.

Στην συνέχεια, είναι δυνατή η πρόσβαση τόσο στο κομμάτι της διαχείρισης της ιστοσελίδας όσο και στην ιστοσελίδα ως τελικός χρήστης.

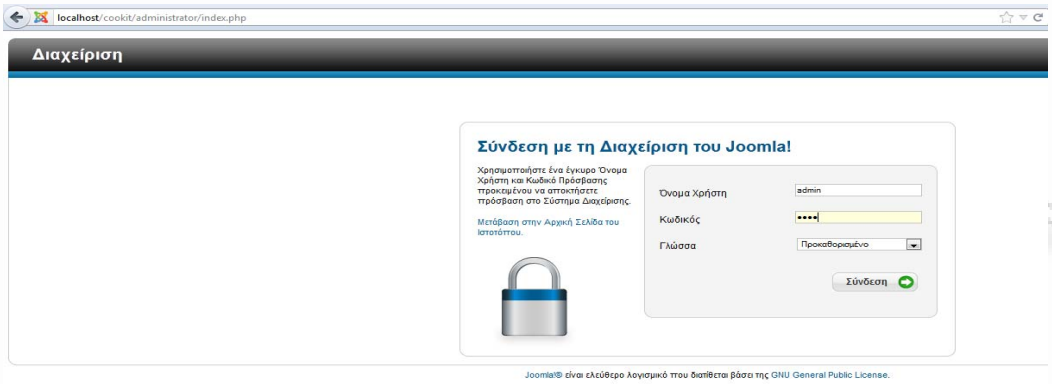
8.1.4 Εγκατάσταση της ελληνικής γλώσσας

Η αρχική γλώσσα του Joomla είναι η αγγλική, όμως διατίθενται αρχεία για αλλαγή της γλώσσας τόσο στο περιβάλλον του διαχειριστή όσο και στην ιστοσελίδα. Η ανάκτηση του αρχείου για την ελληνική γλώσσα γίνεται από την διεύθυνση http://www.Joomla.org, και γίνεται επιλογή του αρχείου για την έκδοση Joomla 1.7 (αρχείο el_GR_joomla_lang_full_1.7.0v2). Η εγκατάσταση της ελληνικής γλώσσας γίνεται μέσα από το διαχειριστικό κομμάτι του Joomla 1.7.. Εισάγουμε δύο ξεχωριστά αρχεία, ένα για το περιβάλλον διαχείρισης και ένα για την ιστοσελίδα. Από το περιβάλλον διαχείρισης γίνεται και η ενεργοποίηση τους, οπότε και όλες οι επιλογές εμφανίζονται στην ελληνική γλώσσα.

Μετά την ολοκλήρωση της εγκατάστασης του Joomla, αρχίζει το στάδιο δημιουργίας του ιστοτόπου.

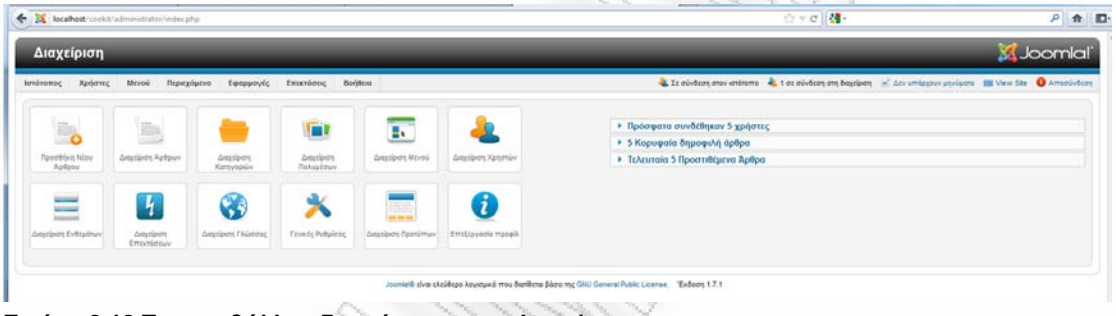
8.2 Είσοδος στην διαχείριση του ιστοτόπου Cook it

Το Joomla υποστηρίζει σύνδεση των διαχειριστών στο διαχειριστικό κομμάτι. Η είσοδος γίνεται με την συμπλήρωση των στοιχείων του διαχειριστή, στην ειδική φόρμα.



Εικόνα 8.11 Φόρμα εισόδου στη διαχείριση

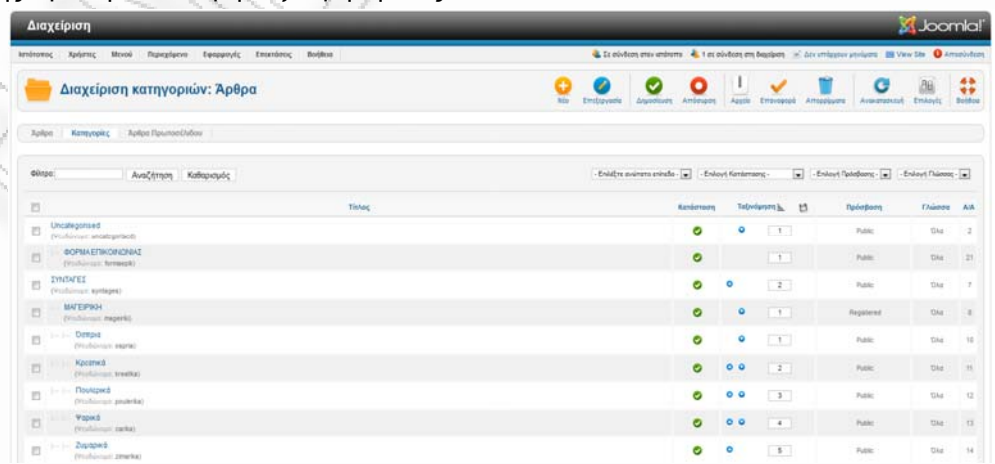
Κατά την εισαγωγή στη διαχείριση, εμφανίζεται το φιλικό περιβάλλον διαχείρισης του Joomla,εμφανίζονται οι κατηγορίες δράσης, δημιουργίας, μορφοποίησης περιεχομένου, όπως φαίνεται στην επόμενη εικόνα.



Εικόνα 8.12 Το περιβάλλον διαχείρησης του Joomla

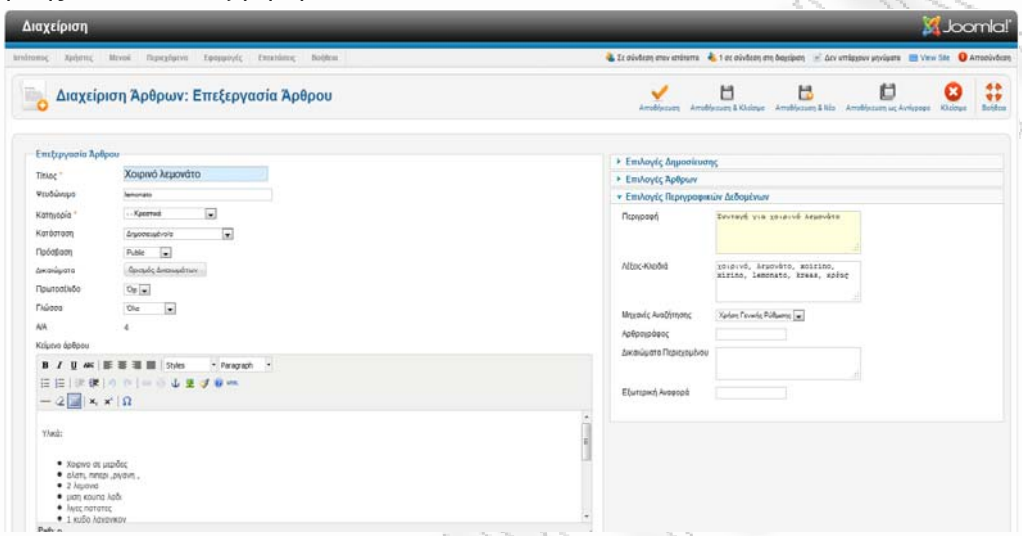
Οι επιλογές που προσφέρονται στον διαχειριστή είναι η καρτέλα ιστοτόπος, για τις ρυθμίσεις, τη συντήρηση και τον πίνακα ελέγχου, η καρτέλα χρήστες από όπου γίνεται η διαχείριση χρηστών, οι ομάδες χρηστών και τα επίπεδα πρόσβασης για κάθε ομάδα. Η καρτέλα μενού παραπέμπει στην δημιουργία μενού για πιο εύκολη πλοήγηση στον ιστότοπο για την ανεύρεση πληροφορίας. Η καρτέλα περιεχόμενο συγκεντρώνει τις επιλογές για την δημιουργία, διαχείριση και κατηγοριοποίηση των άρθρων. Η καρτέλα εφαρμογές, συγκεντρώνει το πλήθος των εφαρμογών που χρησιμοποιούνται στον ιστοτόπο. Οι επεκτάσεις, αποτελούν το κέντρο διαχείρισης εφαρμογών, προτύπων, ενθεμάτων και προσθέτων. Από τις επεκτάσεις είναι δυνατή η εισαγωγή στον ιστοτόπο νέου υλικού, δημιουργημένου από άλλους χρήστες. Επίσης, υπάρχει η καρτέλα βοήθειας, για την καλύτερη επεξήγηση του τρόπου λειτουργίας του Joomla.

Για τη δημιουργία του ιστοτόπου Cook it, δημιουργήθηκαν οι βασικές κατηγορίες, Μαγειρική και Ζαχαροπλαστική, και στην συνέχεια υποκατηγορίες που δηλώνουν το είδος της συνταγής, για την καλύτερη ταξινόμηση τους.



Εικόνα 8.13 Δημιουργώντας κατηγορίες και υποκατηγορίες

Η προσθήκη συνταγών γίνεται με την δημιουργία άρθρων, και την καταχώρησή τους στην ανάλογη κατηγορία και υποκατηγορία. Κατά την δημιουργία ενός άρθρου ορίζονται όλες οι απαραίτητες παράμετροι. Για καλύτερη και ευκολότερη αναζήτηση, προστίθενται στο πεδίο λέξεις κλειδιά, με ελληνικούς και λατινικούς χαρακτήρες προνοώντας τον τρόπο που μπορεί ένας χρήστης να κάνει αναζήτηση.



Εικόνα 8.14 Δημιουργία νέας συνταγής από το διαχειριστικό μέρος

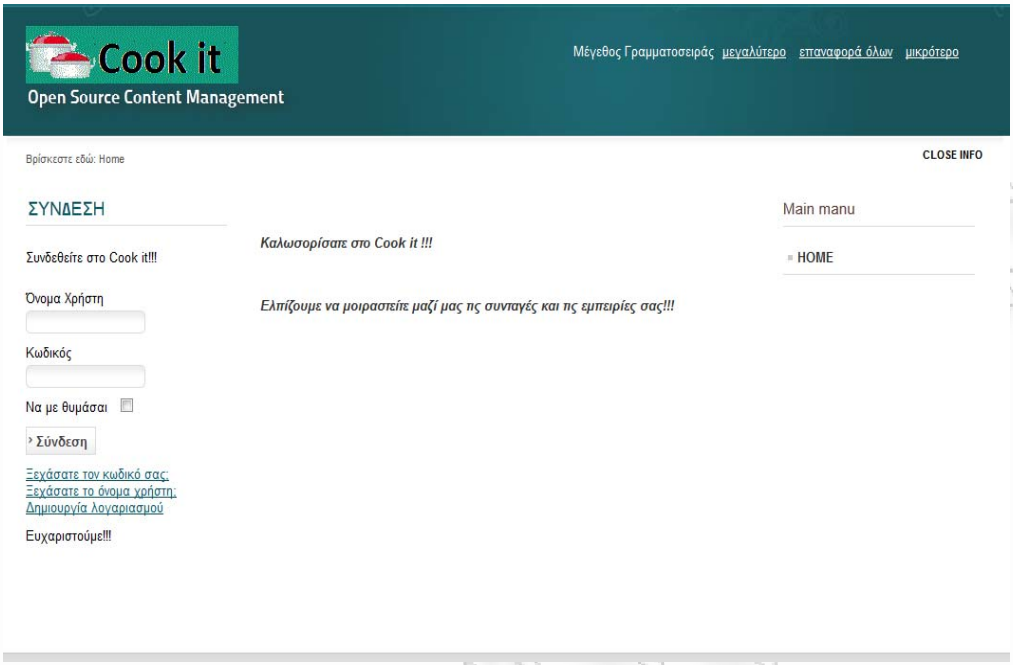
Το Joomla είναι ένα πρόγραμμα ανοικτού λογισμικού και σε πολλούς ιστότοπους υπάρχουν έτοιμα δημιουργημένα στοιχεία που μπορεί κάθε χρήστης να προσθέσει στον ιστότοπό του. Ένα ενδιαφέρον στοιχείο είναι το MobiRate το οποίο προστέθηκε στον ιστότοπο Cook it. Το συγκεκριμένο ένθεμα, επιτρέπει στους χρήστες να βαθμολογήσουν και να σχολιάσουν τις συνταγές του ιστοτόπου. Παραμετροποιώντας το ένθεμα αυτό, ορίζονται οι σελίδες στις οποίες θα εμφανίζεται αλλά και οι χρήστες που θα μπορούν να το χρησιμοποιήσουν. Ένας απλός χρήστης μπορεί απλά να διαβάσει τα σχόλια άλλων χρηστών και να δει την βαθμολογία που έχουν βάλει. Ένας χρήστης εξουσιοδοτημένος από τον διαχειριστή, έχει τη δυνατότητα να συμπληρώσει και τις δικές του απόψεις.

8.3 Είσοδος χρήστη στον ιστότοπο Cook it

Έχοντας δημιουργήσει τον ιστότοπο από το διαχειριστικό κομμάτι, μπορούμε να τον επισκεπτούμε ως χρήστες. Η αρχική σελίδα του ιστοτόπου εμφανίζει πολύ περιορισμένες επιλογές. Μόνο εγγεγραμμένοι χρήστες μπορούν να πλοηγηθούν στον ιστότοπο και στις συνταγές.

8.3.1 Είσοδος μη εγγεγραμμένου χρήστη στο Cook it

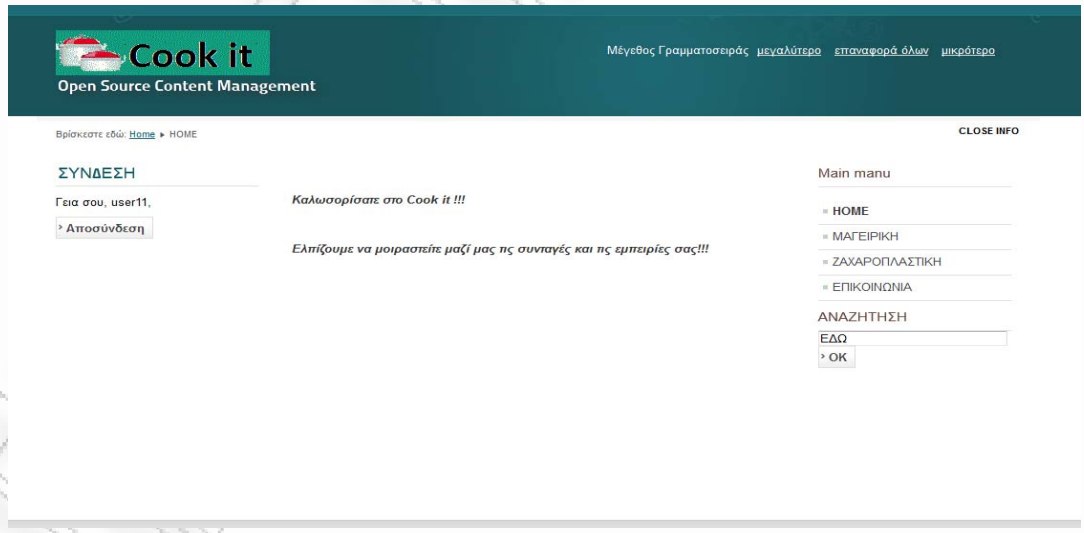
Ως μη εγγεγραμμένος χρήστης, υπάρχει η δυνατότητα εμφάνισης της αρχικής σελίδας και της φόρμας σύνδεσης χρηστών, οπότε μόνο εγγεγραμμένοι χρήστες να μπορούν να έχουν πρόσβαση στην πληροφορία. Στην φόρμα σύνδεσης προβλέπεται επιλογή για τον χρήστη όταν έχει ξεχάσει τον κωδικό ή το όνομα για την είσοδό του. Επίσης, υπάρχει η δυνατότητα δημιουργίας λογαριασμού από για ένα νέο χρήστη.



Εικόνα 8.15 Η αρχική σελίδα του ιστοτόπου

8.3.2 Είσοδος απλού χρήστη στο Cook it

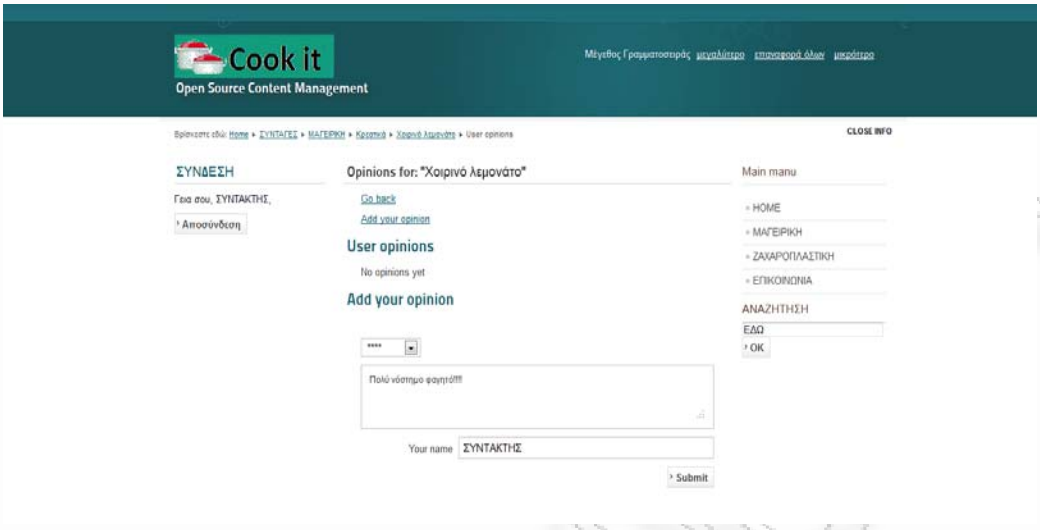
Ένας έγκυρος χρήστης, θα δώσει τα σωστά στοιχεία και θα εισαχθεί με επιτυχία στον ιστότοπο. Με την εισαγωγή του ως έγκυρος χρήστης, έχει δυνατότητα να πλοηγηθεί στον ιστότοπο, να διαβάσει τα άρθρα που έχουν δημοσιευθεί και τις βαθμολογίες και τους σχολιασμούς άλλων χρηστών. Επίσης υπάρχει η δυνατότητα να επικοινωνήσει με τον διαχειριστή μέσα από την φόρμα επικοινωνίας. Στην επόμενη εικόνα φαίνεται η είσοδος του εγγεγραμμένου χρήστη στον ιστοτόπο.



Εικόνα 8.16 Είσοδος εγγεγραμμένου χρήστη στον ιστοτόπο

8.3.3 Είσοδος χρήστη με δικαίωμα σχολιασμού στο Cook it

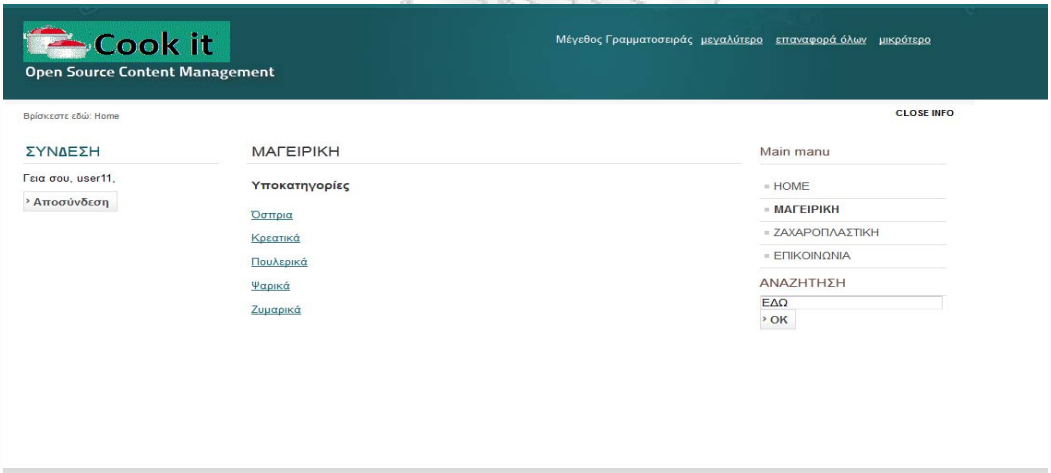
Οι χρήστες που έχουν και δικαίωμα σχολιασμού των άρθρων, βλέπουν τις ίδιες σελίδες με τους απλά εγγεγραμμένους χρήστες, με την διαφορά ότι έχουν το δικαίωμα να σχολιάσουν και να βαθμολογήσουν τις συνταγές. Στην επόμενη εικόνα παρουσιάζουμε την είσοδο ενός χρήστη με δικαιώματα.



Εικόνα 8.17 Δυνατότητα βαθμολόγησης και σχολιασμού των συνταγών

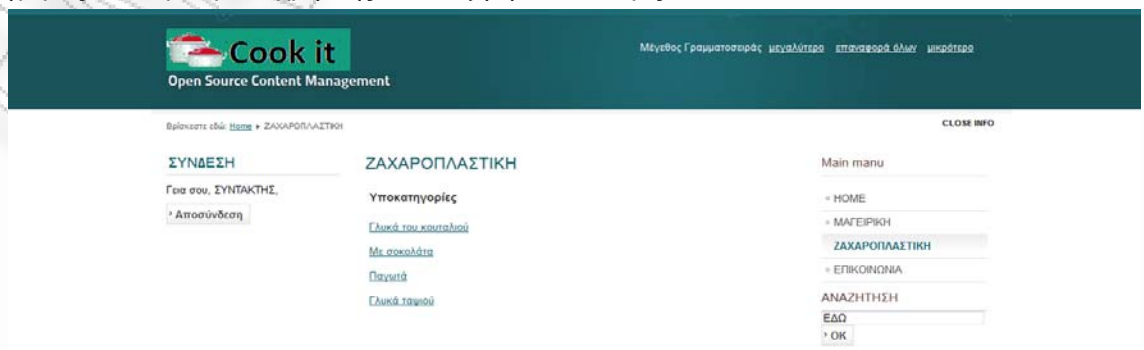
8.3.4 Περιήγηση χρηστών στον ιστότοπο Cook it

Ένας εγγεγραμμένος χρήστης μπορεί να περιηγηθεί στον ιστότοπο, επιλέγοντας συνταγές μέσα από τις κατηγορίες και τις υποκατηγορίες στις οποίες είναι ταξινομημένες. Στην επόμενη εικόνα φαίνονται οι υποκατηγορίες για την κατηγορία Μαγειρική.



Εικόνα 8.18 Περιήγηση στο μενού του Cook it, επιλογή της κατηγορίας Μαγειρική

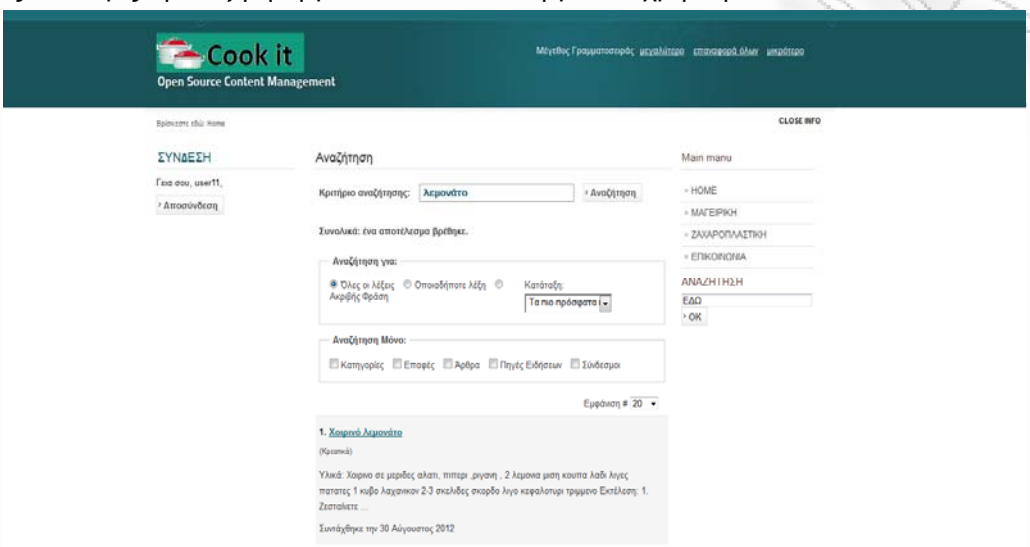
Με τον ίδιο τρόπο είναι δομημένη και η κατηγορία Ζαχαροπλαστική, αναφέροντας τις υποκατηγορίες όπου μπορεί ο χρήστης να αναζητήσει συνταγές.



Εικόνα 8.19Περιήγηση στο μενού, επιλογή της κατηγορίας Ζαχαροπλαστική

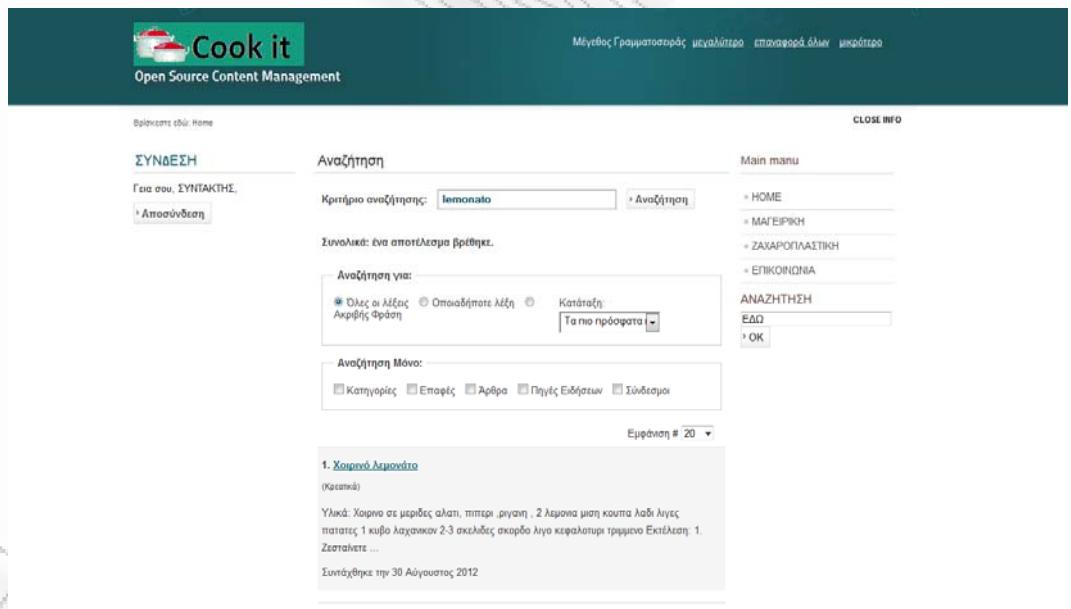
8.3.5 Χρήση της αναζήτησης

Στον ιστοτόπο Cook it, ένας χρήστης μπορεί να αναζητήσει μία συνταγή πληκτρολογώντας στο πεδίο της αναζήτησης μια λέξη σχετική με την συνταγή που αναζητεί. Έχοντας οργανώσει σωστά τον ιστοτόπο, και έχοντας ενημερώσει με τις κατάλληλες λέξεις-κλειδιά τις συνταγές, η αναζήτηση γίνεται πολύ εύκολη για τον χρήστη.



Εικόνα 8.20 Χρήση της αναζήτησης και εμφάνιση των αποτελεσμάτων

Το ίδιο αποτέλεσμα θα είχε ο χρήστης που έκανε αναζήτηση την λέξη «λεμονάτο», ακόμη και αν έγγραφε με λατινικούς χαρακτήρες «lemonato».

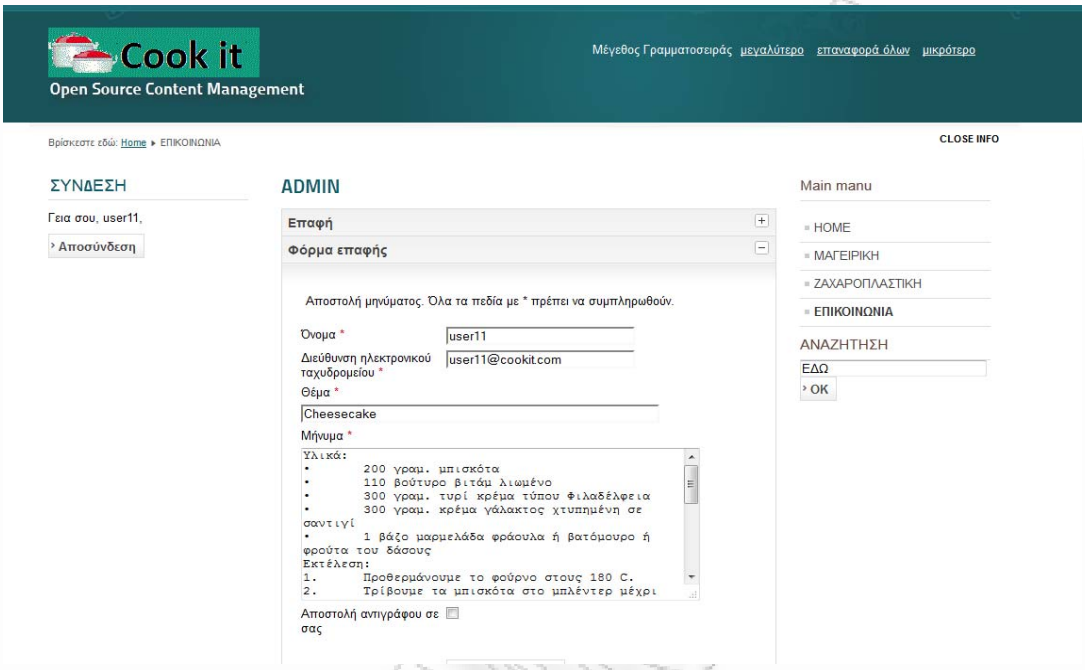


Εικόνα 8.21 Αναζήτηση συνταγών με λατινικούς χαρακτήρες

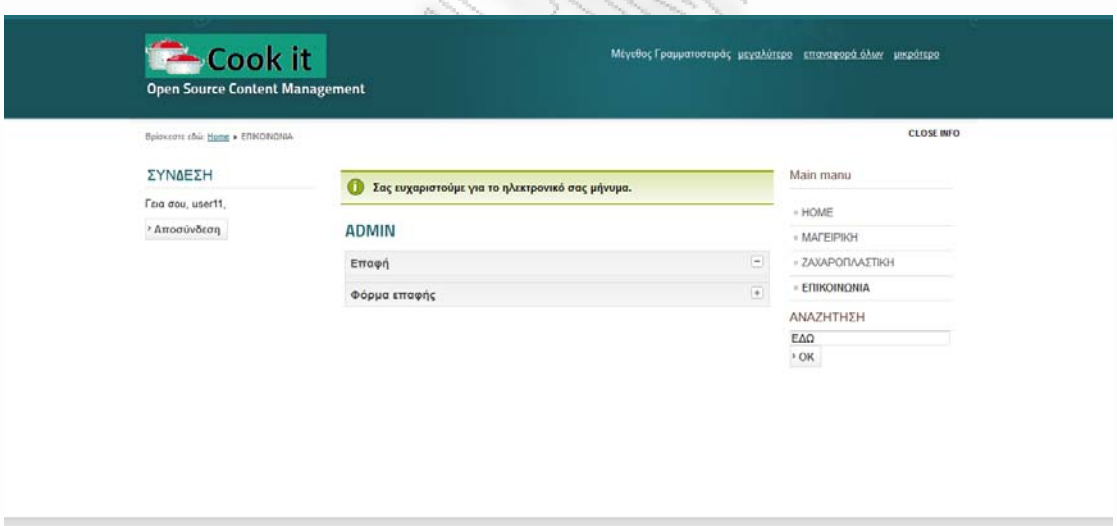
8.3.6 Φόρμα επικοινωνίας με τον διαχειριστή

Στον ιστότοπο Cook it προσφέρεται μια φόρμα για επικοινωνία με τον διαχειριστή, την οποία μπορούν να χρησιμοποιήσουν όλοι οι εγγεγραμμένοι χρήστες. Μέσω της φόρμα αυτής οι χρήστες μπορούν να ενημερώνουν τον διαχειριστή για οποιδήποτε πρόβλημα τους παρουσιαστεί, ενώ ο διαχειρηστής μπορεί να τους απαντήσει στον διεύθυνση ηλεκτρονικού ταχυδρομείου που δηλώνουν. Ακόμα, απλοί χρήστες μπορούν να ζητήσουν να αναβαθμιστούν,

ώστε να μπορούν να συμμετέχουν στην βαθμολόγηση και τον σχολιασμό των συνταγών. Επίσης είναι δυνατή η αποστολή νέων συνταγών προς ανάρτηση από τον διαχειριστή που λαμβάνει το μήνυμα.



Εικόνα 8.22 Δημιουργία μηνύματος από εγγεγραμμένο χρήστη προς τον διαχειριστή



Εικόνα 8.23 Επιβεβαίωση της αποστολής του μηνύματος

Λαμβάνοντας την επιβεβαίωση της ορθής αποστολής, ο χρήστης έχει ολοκληρώσει την αποστολή του μηνύματος.

Στα πλαίσια του ιστοτόπου Cook it, οι εγγεγραμμένοι χρήστες μπορούν να απολαμβάνουν την πλοήγησή τους στις συνταγές. Παράλληλα, έχουν την δυνατότητα να τις βαθμολογούν και να τις σχολιάζουν δημιουργώντας διαλόγους και επικοινωνώντας μεταξύ τους.

9 Συμπεράσματα –Μελλοντικές εξελήξεις

Η ανάπτυξη των Web 2.0 εφαρμογών αποτελεί μια πολύ θετική κοινωνική και τεχνολογική εξέλιξη που δημιουργεί πολλές δυνατότητες στην επικοινωνία και συναλλαγή τόσο στον επιχειρηματικό όσο και στον ιδιωτικό τομέα. Η εξέλιξη εμφανίζεται μέσα από το πλήθος και την ποιότητα των προσφερόμενων στους χρήστες επιλογών. Επιπλέον χαρακτηριστικό αποτελεί η αποδοχή που υπάρχει από το κοινωνικό σύνολο, το οποίο ανταποκρίνεται θετικά, και παροτρύνει με την στάση του την περαιτέρω ανάπτυξη. Εφόσον υπάρχει χρησιμότητα των εφαρμογών, υπάρχει και η εξέλιξή τους.

Οι Web 2.0 εφαρμογές υποστηρίζουν σε μεγάλο βαθμό επίσης, την ύπαρξη ανοικτού λογισμικού, παρέχοντας πρόσβαση στην γνώση άσχετα από την κοινωνική και οικονομική κατάσταση κάθε χρήστη. Το χαρακτηριστικό αυτό συνεισέφερε στην αποδοχή από τους χρήστες και παράλληλα βοήθησε στην δημιουργία πρόσθετου υλικού και την εμφάνιση περισσότερων νέων ιδεών τόσο σε επίπεδο σχεδίασης όσο και σε επίπεδο εφαρμογής της τεχνολογίας. Η τεχνολογία ανοικτού κώδικα, δεν απαιτεί την διάθεση μεγάλων ποσών για τον εκσυγχρονισμό των μέσων, δημιουργώντας περισσότερες ευκαιρίες ανάπτυξης ιδεών.

Η πρόσβαση σε υπηρεσίες μέσω διαδικτύου αποδεσμεύτηκε από την στασιμότητα ενός υπολογιστή. Ένα οποιοδήποτε τερματικό με πρόσβαση στο διαδίκτυο είναι αρκετό για έναν χρήστη για να χρησιμοποιήσει Web 2.0 εφαρμογές. Με την παράλληλη εξέλιξη της τεχνολογίας στα μικροκυκλώματα, η πρόσβαση είναι δυνατή ακόμα και από ένα κινητό τηλέφωνο. Ενώ η ύπαρξη προτύπων και μηχανισμών ασφαλείας, επιτυγχάνεται η ανάπτυξη εμπιστοσύνης από την πλευρά των χρηστών, άρα και η χρησιμοποίηση των εφαρμογών.

Η εφαρμογή των κατάλληλων μέτρων σε κάθε επίπεδο λειτουργίας των εφαρμογών Web 2.0, τα προβλήματα που αφορούν στην εμφάνιση απειλών ως προς την ασφάλεια των εφαρμογών, μπορούν να καταπολεμηθούν σε μεγάλο βαθμό ανοίγοντας νέους δρόμους στην τεχνολογία αυτή. Όμως οι απειλές εξελίσσονται μαζί με την τεχνολογία, κάνοντας την επίτευξη ασφαλών εφαρμογών ένα συνεχές και αδιάκοπο αγώνα. Η αναγκαιότητα του όμως είναι επακόλουθο και της αυξανόμενης χρήσης των Web 2.0 εφαρμογών.

Οι μελλοντικές εξελίξεις στις διαδικτυακές εφαρμογές προδιαγράφονται ραγδαίες με εφαρμογή σε ακόμη περισσότερους τομείς και εκφάνσεις της καθημερινής ζωής. Εμφανίζει μεγάλο ενδιαφέρον η πορεία που θα διαγράψουν οι Web 2.0 εφαρμογές αλλά και οι μέθοδοι που θα χρησιμοποιηθούν για να προσπεραστούν τα εμπόδια που εμφανίζονται σήμερα ως απροσπέλαστα. Νέες έννοιες εμφανίζονται στο προσκήνιο, εμβαθύνοντας ακόμα περισσότερο στην χρήση μεταδεδομένων και στην περιγραφή του περιεχομένου, ώστε να παρέχεται όσο το δυνατόν μεγαλύτερη συσχέτιση και αξιοποίηση της πληροφορίας που διαχέεται στο διαδίκτυο.

10 Βιβλιογραφία

1. **Tim O'Reilly, John Battelle.** *Web Squared: Web 2.0 Five Years On.* 2009.

2. **Robinson, Rick.** Enterprise Web 2.0, Part 2: Enterprise Web 2.0. 2008.

3. **John Musser, Tim O'Reilly, O'Reilly Radar Team.** *Web 2.0 Principles and Best Practices.* 2006.

4. **Levy, Moria.** WEB 2.0 implications on knowledge management. 2007.

5. **Murugesan, San.** *Understanding Web 2.0.* 2007.

6. **Koji Zettsu, Yasushi Kiyoki.** Towards Knowledge Management Based on Harnessing Collective Intelligence on the Web. 2006.

7. **Peter Dolog, Markus Kr¨otzsch, Sebastian Schaffert and Denny Vrande˘ci´**. *Social Web and Knowledge Management.* 2009.

8. **Kapetanios, Epaminondas.** Quo Vadis computer science: From Turing to personal computer, personal content and collective intelligence. 2008.

9. **Smith, Earl.** A confused critique of identity federation. 2010.

10. **Aniket Kittur, Robert E. Kraut.** Harnessing the Wisdom of Crowds in Wikipedia: Quality Through Coordination . 2008.

11. **Giles Hogben, ENISA.** Security Issues and Recommendations for Online Social Networks. 2007.

12. **Gruber, Tom.** Collective Knowledge Systems: Where the Social Web meets the Semantic Web. 2007.

13. **Gruber, Tom**. Collective knowledge systems: Where the Social Web meets the Semantic Web. 2008.

14. **Audun Jøsang, Roslan Ismail, Colin Boyd.** A Survey of Trust and Reputation Systems for Online Service Provision. 2006.

15. **Soren Preibusch, Bettina Hoser , Seda Gurses, Bettina Berendt.** Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling. 2007.

16. **Elisabetta Carrara, Giles Hogben, ENISA.** *Reputation-based Systems: a security analysis.* 2007.

17. **Weijun Zheng, Leigh Jin.** Online Reputation Systems in Web 2.0 Era . 2009.

18. **Shine, Sean.** Web 2.0 and the Next Generation of Public Service. 2009.

19. **Giles Hogben, ENISA.** *Web 2.0 Security and Privacy.* 2008.

20. Kiran Maraju, CISSP, CEH, ITIL, ISO27001, SCJP. *Web 2.0 Attacks Revealed .* 2008.

21. **McAfee.** Seven Design Requirements for Web 2.0 Threat Prevention. 2009.

22. **ALAG, SATNAM.** Collective Intelligence in Action. 2009.

10.1 Ιστότοποι

- **Web 2.0 Security and Privacy 2010:** http://w2spconf.com/2010/
- **IBM, Web 2.0 Security:** http://domino.research.ibm.com/comm/research_projects.nsf/pages/web_2.0_security.index.html
- **Microsoft, Safety & Security Center:** http://www.microsoft.com/security/default.aspx
- **Κοινωνικά δίκτυα η εξέλιξη του Web 1.0 στο Web 2.0:** http://karafatme.blogspot.com/2009/02/web-10-web-20.html
- **Mule Framework Guideline:** http://www.scribd.com/doc/17128541/Mule-Framework-Guideline
- **Social Networking: Commission brokers agreement among major web companies:**

http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4672

- **Facebook, Data Use Policy:** http://www.facebook.com/policy.php?ref=pf
- **Web 2.0: Conceptual foundations and marketing issues:** http://www.palgrave-journals.com/dddmp/journal/v9/n3/full/4350098a.html

Λήψη αρχείου τοπικού server XAMPP: http://www.apachefriends.org

Λήψη αρχείου Joomla: http://www.Joomla.org