



# ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

«ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

ΠΜΣ – Κατεύθυνση: “Ψηφιακές Επικοινωνίες & Δίκτυα”

**ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**ΘΕΜΑ: Αξιολόγηση Ηλεκτρονικών Υπηρεσιών**

**ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Σωκράτης Κ. Κάτσικας**

**ΕΠΙΜΕΛΕΙΑ: Χρήστος Λέων, Α.Μ: ΜΕ/0644**

**2011**

## ΠΕΡΙΕΧΟΜΕΝΑ

<b>ΠΕΡΙΛΗΨΗ</b> .....	4
<b>ΕΙΣΑΓΩΓΗ</b> .....	6
<b>ΚΕΦΑΛΑΙΟ 1</b>	
<b>ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ</b> .....	8
<b>1.1</b> Βασικά Χαρακτηριστικά.....	8
<b>1.2</b> Τεχνική Ανάλυση.....	9
<b>1.2.1</b> Πλεονεκτήματα Ηλεκτρονικών Υπηρεσιών.....	10
<b>1.2.2</b> Μειονεκτήματα Ηλεκτρονικών Υπηρεσιών.....	11
<b>1.3</b> Πρωτόκολλα Επικοινωνίας.....	13
<b>1.4</b> Δομή Ηλεκτρονικών Υπηρεσιών.....	14
<b>1.4.1</b> Μοντέλο των Ηλεκτρονικών Υπηρεσιών.....	15
<b>1.4.2</b> Microsoft .NET.....	16
<b>1.4.3</b> Πρωτοβουλίες σε Java.....	17
<b>1.4.4</b> XML - eXtensible Markup Language.....	18
<b>1.5</b> Πρωτόκολλα των Ηλεκτρονικών Υπηρεσιών.....	23
<b>1.5.1</b> WSDL - Web Services Description Language.....	24
<b>1.5.2</b> UDDI - Universal Description, Discovery and Integration.....	26
<b>1.5.3</b> SOAP - Simple Object Access Protocol.....	27
<b>1.6</b> Εφαρμογές των Ηλεκτρονικών Υπηρεσιών και Παραδείγματα.....	31
<b>1.7</b> Βιβλιογραφία 1 <sup>ου</sup> Κεφαλαίου.....	34
<b>ΚΕΦΑΛΑΙΟ 2</b>	
<b>ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ</b> .....	36
<b>2.1</b> Βασικά Χαρακτηριστικά.....	37
<b>2.2</b> Ασφάλεια Δικτύων.....	39
<b>2.3</b> Φιλτράρισμα Πακέτων (Packet Filtering).....	42
<b>2.4</b> Τείχος Προστασίας (Firewall).....	43
<b>2.5</b> Αποστρατικοποιημένη Περιοχή (DMZ - Demilitarized Zone).....	45
<b>2.6</b> Αυτοματοποιημένη Ανίχνευση Επιθέσεων (IDS - Intrusion Detection Systems).....	45
<b>2.7</b> Ασφάλεια Διαδικτυακών Υπηρεσιών.....	50
<b>2.8</b> Ηλεκτρονικές Υπηρεσίες και Ασφάλεια.....	52
<b>2.9</b> Αδυναμίες και Απειλές.....	54
<b>2.10</b> Μέθοδοι Ασφαλείας.....	55
<b>2.10.1</b> Τεχνικές Δοκιμής Διείσδυσης.....	56
<b>2.11</b> Εργαλεία Ελέγχου Ασφαλείας.....	56
<b>2.12</b> Βιβλιογραφία 2 <sup>ου</sup> Κεφαλαίου.....	57

**ΚΕΦΑΛΑΙΟ 3****ΠΟΙΟΤΗΤΑ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ.....60**

<b>3.1</b>	Βασικά Χαρακτηριστικά Ποιότητας.....	60
<b>3.2</b>	Το Μοντέλο SERVQUAL (Service Quality).....	61
<b>3.3</b>	Το Μοντέλο SERVPERFORM.....	68
<b>3.4</b>	International Organization for Standardization (ISO) .....	68
	<b>3.4.1</b> ISO 27001: Το Πρότυπο για την Διαχείριση Ασφάλειας Πληροφοριών....	69
	<b>3.4.2</b> ISO Πρότυπα Ηλεκτρονικών Υπηρεσιών.....	70
<b>3.5</b>	Αξιολόγηση Ηλεκτρονικών Υπηρεσιών.....	70
	<b>3.5.1</b> Τρόποι Αξιολόγησης.....	70
	<b>3.5.2</b> Παράμετροι Αξιολόγησης.....	71
<b>3.6</b>	Μέθοδοι Αξιολόγησης.....	72
<b>3.7</b>	Βιβλιογραφία 3 <sup>ου</sup> Κεφαλαίου.....	76

**ΚΕΦΑΛΑΙΟ 4****ΕΡΓΑΛΕΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ.....77**

<b>4.1</b>	Εισαγωγή.....	77
<b>4.2</b>	Ανάλυση και Αξιολόγηση Επισκεψιμότητας.....	77
<b>4.3</b>	Εφαρμογή σε Ιστοσελίδες.....	81
	<b>4.3.1</b> Μεθοδολογία Ανάλυσης.....	81
	<b>4.3.2</b> Περιγραφή Ιστοσελίδων.....	82
<b>4.4</b>	Στατιστική.....	84
<b>4.5</b>	Εργαλείο Ανάλυσης Επισκεψιμότητας Ιστοσελίδων – WebTrends.....	102
	<b>4.5.1</b> Στατιστικά Στοιχεία Δημοτικότητας ενός Web Site.....	102
	<b>4.5.2</b> Γενικά Κριτήρια Αναλυτικής Αξιολόγησης Ιστοσελίδων.....	105
	<b>4.5.3</b> Περιγραφή του εργαλείου WebTrends Analysis Series 7.0.....	106
	<b>4.5.4</b> Παραδείγματα Αναφοράς Επισκεψιμότητας μέσω του εργαλείου WebTrends Analysis Series 7.0.....	109
	<b>4.5.5</b> Συμπεράσματα Αναφοράς Επισκεψιμότητας του εργαλείου WebTrends Analysis Series 7.0.....	111
<b>4.6</b>	Βιβλιογραφία 4 <sup>ου</sup> Κεφαλαίου.....	113

**ΕΠΙΛΟΓΟΣ.....114****ΒΙΒΛΙΟΓΡΑΦΙΑ.....117**

## ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματεύεται την Αξιολόγηση των Ηλεκτρονικών Υπηρεσιών. Οι Ηλεκτρονικές Υπηρεσίες, αποτελούν μία αρχιτεκτονική καταναμημένων συστημάτων κατασκευασμένη από πολλά διαφορετικά υπολογιστικά συστήματα τα οποία επικοινωνούν μέσω δικτύου, ώστε να δημιουργήσουν ένα σύστημα. Αποτελούνται, από σύνολο προτύπων τα οποία επιτρέπουν στους υπεύθυνους για την ανάπτυξη (προγραμματιστές - developers) να υλοποιήσουν καταναμημένες εφαρμογές - χρησιμοποιώντας διαφορετικά εργαλεία από διαφορετικούς προμηθευτές - ώστε να κατασκευάσουν εφαρμογές που χρησιμοποιούν σε συνδυασμό με ενότητες λογισμικού (software modules) οι οποίες χρησιμοποιούνται από συστήματα που ανήκουν σε διαφορετικά τμήματα ενός οργανισμού ή και σε διαφορετικούς οργανισμούς.

Στο πρώτο κεφάλαιο της εργασίας, γίνεται εισαγωγή στις Ηλεκτρονικές Υπηρεσίες, αναφέροντας βασικά χαρακτηριστικά, καθώς και τα πλεονεκτήματα και τα μειονεκτήματα των ηλεκτρονικών υπηρεσιών. Στην συνέχεια, αναφέρονται τα πρωτόκολλα επικοινωνίας (SOAP, UDDI, WSDL) και αναλύεται η δομή των Ηλεκτρονικών Υπηρεσιών, λαμβάνοντας υπόψη την σχέση που έχει ο πάροχος της υπηρεσίας, ο κατάλογος των υπηρεσιών και ο πελάτης. Επίσης, γίνεται εκτενής αναφορά στα πρωτόκολλα Ηλεκτρονικών Υπηρεσιών με βασικές εφαρμογές.

Η αξία της πληροφορίας που συγκεντρώνεται στο διαδίκτυο αποκτά τεράστιες διαστάσεις και γίνεται ένα θέμα που ολοένα και περισσότερο απασχολεί. Σε πολλές περιπτώσεις μάλιστα, ολόκληρη η πληροφορία είναι αποθηκευμένη σε ψηφιακά μέσα, χωρίς να υπάρχει σε έντυπη ή αναλογική μορφή. Η εξάρτηση από τα συστήματα αυτά, και το γεγονός ότι η λειτουργικότητα και η φιλικότητα των υπολογιστικών συστημάτων έχουν αυξηθεί σημαντικά, οδηγούν σε μια ενισχυμένη πολυπλοκότητα των συστημάτων αυτών. Η πολυπλοκότητα αυτή, ανάγεται σε μια πληθώρα αδυναμιών και προβλημάτων στην ασφάλεια των συστημάτων και των δεδομένων, είτε από προγραμματιστικά λάθη, είτε από κακές ρυθμίσεις, ή από τις σχέσεις εμπιστοσύνης που δημιουργούνται.

Στο δεύτερο κεφάλαιο της εργασίας, αναλύεται η έννοια της ασφάλειας των ηλεκτρονικών υπηρεσιών. Αρχικά, περιγράφονται βασικά χαρακτηριστικά, όπως είναι η Απειλή (Threat), οι Μηχανισμοί προστασίας, οι Μηχανισμοί κρυπτογράφησης και η Επίθεση (Attack). Αφού αναφέρονται οι μορφές επίθεσης σε ένα δίκτυο και την κατανομή δικαιωμάτων πρόσβασης των χρηστών, εν συνεχεία αναλύονται τα επίπεδα ασφαλείας που μπορεί να έχει ένα δίκτυο όπως είναι το Φιλτράρισμα Πακέτων (Packet Filtering), το Τείχος Προστασίας (Firewall) και η Demilitarized Zone (DMZ). Τα web services παρέχουν πολλά πλεονεκτήματα στις εφαρμογές αλλά επίσης εκθέτουν σημαντικούς νέους κινδύνους στην ασφάλεια. Η δημιουργία και η διατήρηση ενός ασφαλούς περιβάλλοντος ηλεκτρονικών υπηρεσιών, περιλαμβάνει και τη διαχείριση διαφόρων μηχανισμών για το διαδίκτυο, την γλώσσα XML και τις ίδιες τις ηλεκτρονικές υπηρεσίες.

Βασικό κριτήριο στην ασφάλεια δικτύων, είναι ο ανθρώπινος παράγοντας. Επομένως, πολλές επιθέσεις είτε ακούσια ή κακόβουλα γίνονται στο εσωτερικό του δικτύου. Η ασφάλεια δικτύων αποτελεί μια συνεχώς μεταβαλλόμενη διαδικασία. Οι διαχειριστές των δικτύων κάθε επιχείρησης, πρέπει να έχουν άριστη γνώση της δομής του δικτύου που επιβλέπουν και να παρακολουθούν στενά τις εξελίξεις στο χώρο της ασφάλειας δεδομένων, για να ικανοποιούν τις άμυνές τους.

Στο τρίτο κεφάλαιο της εργασίας αναλύεται η ποιότητα και η αξιολόγηση των ηλεκτρονικών υπηρεσιών. Δίνεται ο ορισμός της Ποιότητας και παρατίθενται τα βασικά χαρακτηριστικά της.

Στην συνέχεια παρουσιάζεται το μοντέλο 'SERVQUAL', που αποτελεί εργαλείο ανάλυσης, ανάπτυξης και μέτρησης της ποιότητας των υπηρεσιών, που μπορεί να προσφέρει ένας οργανισμός προς τους πελάτες του προκειμένου αυτοί να είναι ικανοποιημένοι από τις υπηρεσίες που παρέχονται. Γίνεται αναφορά και στο μοντέλο SERVPERFORM παραθέτοντας βασικά χαρακτηριστικά γνωρίσματα.

Σε αυτό το σημείο, κρίθηκε σκόπιμο να περιγραφεί το πρότυπο ISO (International Organization for Standardization), που αποτελεί τεκμηριωμένες έγγραφες συμφωνίες, που περιχέουν τεχνικές προδιαγραφές ή ακριβή κριτήρια για να χρησιμοποιηθούν ως κανόνες, οδηγίες ή ορισμοί χαρακτηριστικών. Παρουσιάζονται το πρότυπο ISO 27001 που αφορά το πρότυπο για την Διαχείριση της Ασφάλειας Πληροφοριών και αναφέρονται τα ISO πρότυπα των Ηλεκτρονικών Υπηρεσιών. Στο τέλος, δίνεται ο ορισμός της Αξιολόγησης των Ηλεκτρονικών Υπηρεσιών καθώς επίσης οι τρόποι, οι παράμετροι και οι μέθοδοι Αξιολόγησης.

Στο τέταρτο κεφάλαιο της εργασίας, αναλύεται η επισκεψιμότητα ιστοχώρου, και τα εργαλεία αξιολόγησης των ηλεκτρονικών υπηρεσιών. Η διαδικασία της ανάλυσης επισκεψιμότητας αποτελείται από την συλλογή δεδομένων (data collection), την προεπεξεργασία των δεδομένων (data preprocessing) και της ανακάλυψης γνώσης (knowledge discovery). Η διαδικασία ολοκληρώνεται, με την στατιστική ανάλυση των δεδομένων.

Στην συνέχεια, ακολουθεί μία εφαρμογή που υποστηρίχθηκε με την μέθοδο του ερωτηματολογίου. Οι ιστοσελίδες που χρησιμοποιήθηκαν στην ανάλυση, είναι οι επίσημοι ιστοχώροι των Περιφερειακών Επιχειρησιακών Προγραμμάτων (Π.Ε.Π). Τα Π.Ε.Π συμβάλουν στην κάλυψη των εθνικών στρατηγικών στόχων με έμφαση στα ιδιαίτερα χαρακτηριστικά και στις ανάγκες κάθε Περιφέρειας. Οι ιστοχώροι αυτοί, περιέχουν πολυποίκιλα μενού, επιτρέπουν την πρόσβαση σε πληθώρα πληροφοριών διαφορετικών θεμάτων και έχουν επισκεψιμότητα σε ημερήσια βάση. Στο ερωτηματολόγιο, 19 ερωτήσεων, περιέχονται ερωτήματα που καλύπτουν στοχευμένη πληροφόρηση σχετικά με την ασφάλεια, την ποιότητα και την αξιολόγηση των ιστοχώρων αυτών, κάνοντας χρήση του μοντέλου SERVQUAL.

Με την Περιγραφική Στατιστική και την Στατιστική Συμπερασματολογία, γίνεται έλεγχος της σημαντικότητας της πληροφορίας και της συσχέτισης των πληροφοριών, με απώτερο σκοπό την ποσοτικοποίηση της ικανοποίησης των χρηστών των ιστοσελίδων χρησιμοποιώντας το στατιστικό πακέτο SPSS.

Τέλος, παρουσιάζεται το εργαλείο WebTrends Analysis Series 7.0 που αναλύει την επισκεψιμότητα, εξάγοντας γενικά και αναλυτικά αποτελέσματα για όλο τον ιστοχώρο. Η WebTrends παρέχει στατιστικά στοιχεία σχετικά με σελίδες δικτυακών τόπων, τους οποίους οι χρήστες ιστοσελίδων επισκέπτονται με μεγαλύτερη συχνότητα και για περισσότερο χρονικό διάστημα. Αυτή η πληροφόρηση, παρέχει στις εταιρίες σημαντικές πληροφορίες με σκοπό, να βελτιώσουν τον δικτυακό τους τόπο, τις πληροφορίες για τις υπηρεσίες και τα προϊόντα που παρέχουν μέσω αυτού. Επίσης, δίνονται αποτελέσματα μέσω διαγραμμάτων και πινάκων για το Π.Ε.Π της Στερεάς Ελλάδας και παρουσιάζεται ένας συγκεντρωτικός πίνακας των οχτώ (8) ιστοσελίδων με γενικά στοιχεία που εξάχθηκαν μέσω του εργαλείου WebTrends Analysis Series 7.0.

## ΕΙΣΑΓΩΓΗ

Σε αντίθεση με τα καλά ορισμένα και αμετάβλητα σύνορα μιας χώρας, τα σύνορα του Διαδικτύου είναι σε μια συνεχή κατάσταση ροής και ανανέωσης. Το Διαδίκτυο (Internet), σαν εικονικό κομμάτι λογισμικού, computing και networking, είναι απείρως ανανεώσιμο και ευπροσάρμοστο, με αποτέλεσμα να μεγαλώνει και να αλλάζει καθημερινά.

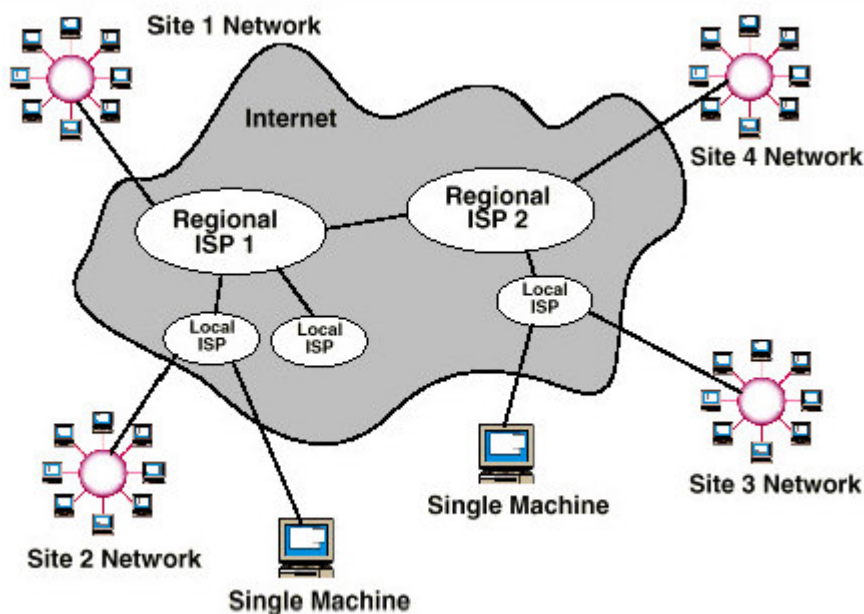
Ο ευμετάβλητος χαρακτήρας του Internet και η διείδυση του σε κάθε γωνιά της υφηλίου, έχουν δημιουργήσει ένα πλούσιο και συχνά απρόβλεπτο περιβάλλον στο οποίο τα κοινά ενδιαφέροντα και η εμπειρία είναι μερικές φορές περισσότερο σημαντικά από τα γεωπολιτικά και κοινωνικά σύνορα που διαχωρίζουν τους χρήστες του. Αυτή η μίξη έχει δημιουργήσει μια συλλογή από παγκόσμια χωριά με την ασυνήθιστη ιδιότητα ότι πολλοί άνθρωποι στο Internet μένουν σε περισσότερα από ένα παγκόσμια χωριά κάθε χρονική στιγμή. Η εμβέλεια, η πολυπλοκότητα και η μεγαλοπρέπεια του συστήματος που έχουμε σήμερα δεν είχε ποτέ προβλεφθεί.

Κοιτάζοντας το Internet του σήμερα, ακόμα με τα μάτια της δεκαετίας του '90, θα μπορούσε κανείς μόνο να αναρωτηθεί για αυτή του την εξέλιξη. Όπως και η σύνθετη ζωή σχηματίζεται από απλούστερες, μέσα από γενετικά πειράματα, έτσι και το Internet είναι ένα αναπτυσσόμενο και συστηματοποιημένο εικονικό περιβάλλον. Αλλά, με τη ματιά του σήμερα, αποτελεί επίσης και μία επανάσταση γιατί μεταμορφώνει την κουλτούρα μας. Η ελευθερία της έκφρασης και πρόσβασης σε πληροφορίες στο Internet είναι επαναστατική. Κατά κάποιο τρόπο, το Internet έχει κάνει κάθε δημιουργό, εκδότη δίνοντας ένα νέο νόημα στη φράση «desktop publishing». Οι κοινωνικές και επιχειρηματικές μας ενέργειες επηρεάζονται ορατά. Το εκπαιδευτικό μας σύστημα μπορεί να υποβληθεί σε αλλαγές καθώς εργαλεία για παραγωγή και διαμοίραση γνώσης αναμειγνύονται με νέους τρόπους σφυρηλάτησης μαθητών σε μαθησιακές εμπειρίες.

Υπάρχουν βέβαια μειονεκτήματα όσον αφορά τη ροή της πληροφορίας στο Internet. Το πιο προφανές είναι η δυσκολία της εύρεσης απλών αντικειμένων στον απέραντο πλούτο του διαθέσιμου υλικού. Οι δέκτες της πληροφορίας πρέπει να είναι πραγματικά επιλεκτικοί και σκεπτόμενοι ταξιδιώτες, να ταξινομούν και να αποτιμούν την πληροφορία που τους είναι διαθέσιμη ασταμάτητα, καθώς «πλέουν στους ηλεκτρονικούς ωκεανούς» και ψάχνουν για πολύτιμο περιεχόμενο. Πράγματι, το πολύτιμο περιεχόμενο του Internet είναι τεράστιο σε ποσότητα αλλά δύσκολο να βρεθεί και ακόμη περισσότερο γιατί αυτό αναπαράγεται καθημερινά. Το browsing δίνει νέα ώθηση σε προσπάθειες για εύρεση και τοποθέτηση νέων επιχειρηματικών ευκαιριών στον κατάλογο της πληροφορίας.

Η ανάπτυξη των τεχνολογιών του Διαδικτύου έχει αλλάξει σημαντικά τον τρόπο με τον οποίο λειτουργούν οι επιχειρήσεις. Οι εταιρίες «εξάγουν» τις κύριες λειτουργίες τους στον Παγκόσμιο Ιστό προσδοκώντας επιπλέον αυτοματοποίηση, αποδοτικότερες επιχειρησιακές διαδικασίες και καθολική ορατότητα των λειτουργιών τους. Για να επιζήσουν οι εταιρίες στις συνθήκες του πολύ σκληρού ανταγωνισμού που έχει δημιουργηθεί πρέπει να επιλέξουν τις σωστότερες και πιο ευέλικτες επιχειρησιακές λύσεις που θα τους επιτρέψουν αφενός να χρησιμοποιήσουν τις υπάρχουσες εφαρμογές με τον καλύτερο δυνατό τρόπο και αφετέρου θα τους επιτρέψουν να εξελίσσονται και να αλλάζουν.

Στις μέρες μας, υπάρχει μια αλλαγή κατεύθυνσης, όσον αφορά την συνεργασία εφαρμογών, από τα στενά συνεργαζόμενα συστήματα, όπως για παράδειγμα, DCOM[DCOM] σε συστήματα με πιο χαλαρά συνδεδεμένες και δυναμικά προσαρμοζόμενες συνιστώσες όπως είναι τα Jini[JINI], Enterprise Java Beans[EJB] με τελευταία παρουσία σε αυτή την κατηγορία το παράδειγμα των Ηλεκτρονικών Υπηρεσιών.



Εικόνα 1: Το Μοντέλο Διαδικτύωσης του Internet

Οι Ηλεκτρονικές Υπηρεσίες είναι αυτόνομες (self-contained) και αρθρωτές (modular) εφαρμογές, προσβάσιμες μέσω του Παγκόσμιου Ιστού παρέχοντας ένα σύνολο από λειτουργικότητες σε επιχειρήσεις ή άτομα. Αυτό που κάνει τις Ηλεκτρονικές Υπηρεσίες να ξεχωρίζουν σαν πρόταση είναι η δυνατότητα ανακάλυψης Ηλεκτρονικών Υπηρεσιών που να ταιριάζουν στις απαιτήσεις μίας εφαρμογής, η δυνατότητα διαπραγμάτευσης των συμβολαίων χρήσης τους και η καθολική προσβασιμότητα τους από οποιοδήποτε σημείο, οποιαδήποτε στιγμή.

Στοιχεία όπως η ενθουλάκωση, το πέρασμα μηνυμάτων και η δυναμική δέσμευση υπηρεσιών, είναι πρωτεύουσες σημασίες. Εντούτοις οι ηλεκτρονικές υπηρεσίες επεκτείνονται πέρα από τις απλές «υπογραφές μεθόδων» (method signatures) αφού η περιγραφή (ή διεπαφή) μιας Ηλεκτρονικής Υπηρεσίας περιλαμβάνει πληροφορία για την λειτουργικότητα της υπηρεσίας (τι κάνει), την τοποθεσία της υπηρεσίας (που είναι), τον τρόπο με τον οποίο επικαλείται η υπηρεσία, την ποιότητα της υπηρεσίας (quality of service) και τις πολιτικές ασφάλειας που σχετίζονται με αυτήν. Αυτά τα χαρακτηριστικά αποδίδουν στις Ηλεκτρονικές Υπηρεσίες τον χαρακτηρισμό αυτοπεριγραφόμενες (self-describing). Αντίστοιχα, οι Ηλεκτρονικές Υπηρεσίες μπορούν να θεωρηθούν και σαν επέκταση του παραδείγματος συνιστωσών λογισμικού, αφού κάθε Ηλεκτρονική Υπηρεσία μπορεί να θεωρηθεί σαν μία συνιστώσα, ανεξάρτητη πλατφόρμας που δίνει την δυνατότητα χαλαρής σύνδεσης (loose coupling) με εφαρμογές ή άλλες Ηλεκτρονικές Υπηρεσίες.

## ΚΕΦΑΛΑΙΟ 1

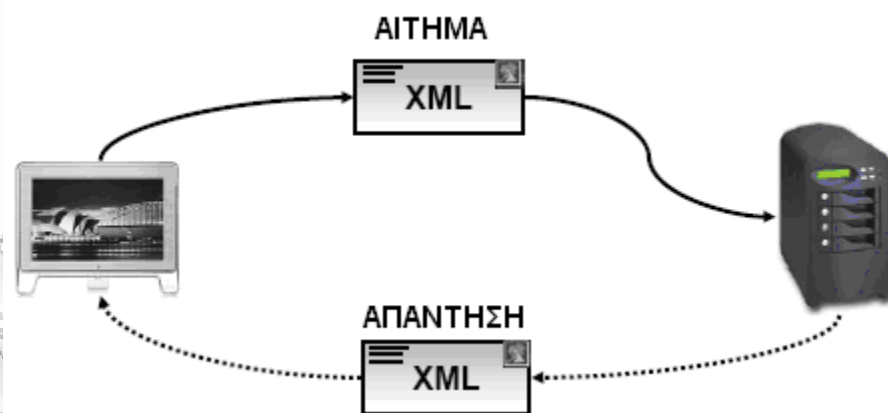
### ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

#### 1.1 Βασικά Χαρακτηριστικά

Ένας πολύ καλός ορισμός έρχεται από την IBM<sup>1</sup>: *Τα web services είναι μια τεχνολογία που επιτρέπει στις εφαρμογές να επικοινωνούν μεταξύ τους ανεξαρτήτως πλατφόρμας και γλώσσας προγραμματισμού. Ένα web service είναι μια λογισμική διάσυνδεση (software interface) που περιγράφει μια συλλογή από λειτουργίες οι οποίες μπορούν να προσεγγιστούν από το δίκτυο μέσω πρότυπων μηνυμάτων XML. Χρησιμοποιεί πρότυπα βασισμένα στη γλώσσα XML για να περιγράψει συγκεκριμένες λειτουργίες (operation) προς εκτέλεση και τα δεδομένα προς ανταλλαγή με διαφορετική εφαρμογή. Μια ομάδα από web services οι οποίες αλληλεπιδρούν μεταξύ τους καθορίζει μια εφαρμογή web services.*

Η Microsoft μέσα από το MSDN της καταλήγει ότι όλα τα web services έχουν τρία (3) κοινά χαρακτηριστικά<sup>2</sup>:

- ✓ Τα web services εκθέτουν χρήσιμη λειτουργικότητα σε χρήστες του διαδικτύου μέσα από ένα πρότυπο δικτυακό πρωτόκολλο. Στις περισσότερες περιπτώσεις αυτό το πρωτόκολλο είναι το SOAP (Simple Object Access Protocol).
- ✓ Τα web services παρέχουν ένα τρόπο να περιγράφουν τις διεπαφές τους με αρκετή λεπτομέρεια ώστε να επιτρέψουν στο χρήστη τους να “χτίσει” μια εφαρμογή η οποία να επικοινωνήσει μαζί τους. Η περιγραφή συνήθως παρέχεται σε ένα έγγραφο XML το οποίο ονομάζεται έγγραφο WSDL (Web Services Description Language).
- ✓ Τα web services καταχωρούνται ώστε οι δυνητικοί χρήστες να μπορούν να διαθέτουν εύκολη προσβασιμότητα. Αυτό γίνεται με το UDDI (Universal Discovery Description and Integration).



Εικόνα 2: Γενική Μορφή Ηλεκτρονικής Υπηρεσίας

Οι Ηλεκτρονικές Υπηρεσίες, αποτελούν μία αρχιτεκτονική καταναμημένων συστημάτων κατασκευασμένη από πολλά διαφορετικά υπολογιστικά συστήματα τα οποία επικοινωνούν μέσω δικτύου, ώστε να δημιουργήσουν ένα σύστημα. Αποτελούνται, από σύνολο προτύπων τα οποία επιτρέπουν στους υπεύθυνους για την ανάπτυξη (προγραμματιστές - developers) να



υλοποιήσουν καταναμημένες εφαρμογές - χρησιμοποιώντας διαφορετικά εργαλεία από διαφορετικούς προμηθευτές - ώστε να κατασκευάσουν εφαρμογές που χρησιμοποιούν συνδυασμό από ενότητες λογισμικού (software modules) οι οποίες καλούνται από συστήματα που ανήκουν σε διαφορετικά τμήματα ενός οργανισμού ή σε διαφορετικούς οργανισμούς.

## 1.2 Τεχνική Ανάλυση

Οι γλώσσες προγραμματισμού στην πληροφορική συνεχώς εξελίσσονται. Στις προηγούμενες δεκαετίες, υπήρξε η ιδέα της function στην οποία παρέχει μερικές παραμέτρους, εκτελεί μια λειτουργία με αυτές τις παραμέτρους, και επιστρέφει μια τιμή βασισμένη στους υπολογισμούς που έγιναν. Τελικά, αυτή η πρώτη έννοια, εξελίχθηκε σε αντικείμενο (object) όπου κάθε αντικείμενο είχε όχι απλώς έναν αριθμό από λειτουργίες (functions) που μπορεί να εκτελέσει αλλά και τις δικές του μεταβλητές (private data variables), αντί να στηρίζεται σε εξωτερικές μεταβλητές του συστήματος που προηγουμένως έκαναν πιο περίπλοκη την ανάπτυξη εφαρμογών. Δεδομένου ότι οι εφαρμογές άρχισαν να επικοινωνούν μεταξύ τους, η έννοια του καθορισμού καθολικών διεπαφών (universal interfaces) για αντικείμενα έγινε σημαντική, επιτρέποντας αντικείμενα σε διαφορετικές πλατφόρμες να επικοινωνούν ακόμη και αν είχαν αναπτυχθεί σε διαφορετικές γλώσσες προγραμματισμού και εκτελούνταν σε διαφορετικά λειτουργικά συστήματα.

Πρόσφατα, τα web services προχώρησαν μπροστά με την έννοια των διεπαφών και επικοινωνιών καθορισμένων με XML (Extensible Markup Language), ενώνοντας τελικά κάθε είδους εφαρμογή με οποιαδήποτε άλλη, όπως και παρέχοντας την ελευθερία στις εφαρμογές να αλλάξουν και να εξελιχθούν με το χρόνο, αρκεί να είναι σχεδιασμένες σύμφωνα με την κατάλληλη διεπαφή. Η μεταβλητότητα της XML, είναι αυτό που κάνει τα web services διαφορετικά από τεχνολογίες προηγούμενων γενεών. Επιτρέπει το διαχωρισμό της γραμματικής δομής (syntax) και της γραμματικής έννοιας (semantics), και του πώς αυτά υποβάλλονται σε επεξεργασία και κατανοούνται από μία υπηρεσία και το περιβάλλον μέσα στο οποίο υπάρχει. Έτσι, τα αντικείμενα μπορούν να καθοριστούν σαν υπηρεσίες, οι οποίες επικοινωνούν με άλλες υπηρεσίες σε γραμματική καθορισμένη σε XML, με την οποία κάθε υπηρεσία μεταφράζει και αναλύει το μήνυμα σύμφωνα με το περιβάλλον της. Κατά συνέπεια, μια δικτυακή εφαρμογή μπορεί πραγματικά να συντεθεί από πολλαπλές οντότητες διαφόρων υλοποιήσεων και σχεδιασμών εφόσον προσαρμόζονται στους κανόνες που καθορίζονται από την προσανατολισμένη στις υπηρεσίες αρχιτεκτονική τους.

Οι βασικοί άξονες επιτρέπουν :

- ✓ Την αλληλεπίδραση μεταξύ υπηρεσιών σε οποιαδήποτε πλατφόρμα, γραμμένες σε οποιαδήποτε γλώσσα προγραμματισμού.
- ✓ Να αντιληφθεί κανείς, λειτουργικές εφαρμογές ως εργασίες, οδηγούμενος σε ανάπτυξη και ροές εργασιών προσανατολισμένες σε εργασίες. Αυτό επιτρέπει μια υψηλότερη αφαίρεση του λογισμικού το οποίο μπορεί να υιοθετηθεί από λιγότερο τεχνικά καταρτισμένους χρήστες.
- ✓ Τη χαλαρή συνδεσιμότητα μεταξύ εφαρμογών, πράγμα που σημαίνει ότι αλληλεπιδράσεις μεταξύ υπηρεσιών δε θα απομονώνονται κάθε φορά που υπάρχει κάποια αλλαγή.
- ✓ Την προσαρμογή ήδη υπάρχουσών εφαρμογών στις μεταβαλλόμενες επιχειρησιακές συνθήκες και ανάγκες των πελατών.

- ✓ Εισαγωγή άλλων διοικητικών λειτουργιών ή λειτουργίες διαχείρισης διαδικασιών, όπως η αξιοπιστία, υπευθυνότητα, ασφάλεια, ανεξάρτητες της αρχικής λειτουργίας μιας εφαρμογής, αυξάνοντας κατά συνέπεια, τη μεταβλητότητα και τη χρησιμότητά της στο επιχειρησιακό περιβάλλον.

### 1.2.1. Πλεονεκτήματα Ηλεκτρονικών Υπηρεσιών

Η αρχιτεκτονική των web services παρέχει αρκετά πλεονεκτήματα μερικά από τα οποία αναφέρονται παρακάτω<sup>15, 16</sup> :

- ✓ **Διαλειτουργικότητα:** Ένα web service παρέχει ανεξαρτησία τόσο από το λειτουργικό σύστημα όσο και από το hardware. Οποιοδήποτε πρόγραμμα που συμβαδίζει με αυτή τη τεχνολογία μπορεί πολύ εύκολα να προσπελάσει μία τέτοια υπηρεσία. Επίσης, ένα web service επιτρέπει ένα πρόγραμμα σε έναν υπολογιστή να καλέσει μία λειτουργία σε έναν άλλο υπολογιστή χωρίς να δίνει σημασία στο Λειτουργικό Σύστημα, στην Γλώσσα Προγραμματισμού, στον Κατασκευαστή.
- ✓ **Ενσωμάτωση:** Σε ένα υπάρχον λογισμικό σύστημα που λειτουργεί μέσα στο Internet, η δημιουργία ενός web service δεν απαιτεί αλλαγές στον μηχανισμό του συστήματος. Τα web services υλοποιούνται σαν επέκταση ενός Web Server, και χρησιμοποιούν το standard http πρωτόκολλο. Ακόμα, αντί να ζητούν (request) μία σελίδα, ζητούν την κλήση μίας λειτουργίας χρησιμοποιώντας 'GET', 'POST' ή το 'SOAP' και αντί να επιστρέφεται μία σελίδα, επιστρέφεται το αποτέλεσμα της λειτουργίας είτε ως απλό περιεχόμενο είτε ως περιεχόμενο σε SOAP (Web service implementation).
- ✓ **Διαθεσιμότητα και δημοσίευση:** Οι πληροφορίες για τα web services δημοσιεύονται, οπότε η εύρεση και η χρήση τους μπορεί να είναι ταχύτερες και φυσικά η πρόσβαση των πληροφοριών είναι συνεχής και οι χρήστες μπορούν να εξυπηρετούνται ταυτόχρονα.
- ✓ **Επέκταση:** Ένα έτοιμο web service είναι δυνατό να ανανεωθεί με εύκολο τρόπο παρέχοντας έτσι επιπρόσθετες υπηρεσίες στους χρήστες του.
- ✓ **Μικρό κόστος δημιουργίας και χρήσης:** Εφόσον σε ένα λογισμικό σύστημα υπάρχει ήδη κάποια διαδικασία που χρειάζεται να επεκταθεί σε on-line υπηρεσία, η δημιουργία του web service κοστίζει ελάχιστα. Η δημιουργία Web Services είναι εύκολη, γρήγορη και απλή, το data schema είναι εύκολα αναγνώσιμο από τον άνθρωπο, και μπορεί να χρησιμοποιηθεί οποιαδήποτε προγραμματιστική γλώσσα. Επίσης, το κόστος ενσωμάτωσης ενός web service σε κάποιο website ή σε δικτυακή εφαρμογή, είναι πάρα πολύ μικρό. Ακόμα και στις περιπτώσεις που η χρήση κάποιου web service γίνεται με ενοικίαση, σίγουρα το συνολικό κόστος της χρήσης είναι αρκετά πιο μικρό από το κόστος δημιουργίας της υπηρεσίας αυτής.
- ✓ **Χρήση λογισμικών συστημάτων:** Όλα τα λογισμικά συστήματα και ειδικότερα τα web sites που χρησιμοποιούν έτοιμες υπηρεσίες, γίνονται πιο λειτουργικά και πιο φιλικά αφού παρέχουν περισσότερες υπηρεσίες στους χρήστες, διαρκή ενημέρωση των εφαρμογών, χωρίς να απαιτείται καμιά ενέργεια από τους χρήστες καθώς και αμεσότητα πρόσβασης των δεδομένων χωρίς να χρειάζονται εγκατάσταση και διαμόρφωση. Επίσης, υπάρχει η ευκολία δοκιμής και χρήσης αφού υπάρχουν δοκιμαστικές εκδόσεις, ειδικά για ακριβά λογισμικά.
- ✓ **Συγκεντρωμένα δεδομένα:** Ένα από τα πλεονεκτήματα, που κάνει πιο εύκολη την αποθήκευση των δεδομένων και την δημιουργία αντιγράφων ασφαλείας. Οι εταιρίες αποθηκεύουν τα δεδομένα με σύγχρονα μέσα και μεθόδους σε server farms, όπως αυτά

λέγονται, μειώνοντας τον κίνδυνο απώλειας αυτών, από ότι αν ήταν τοπικά σε κάθε χρήστη. Ακόμα έχουμε λιγότερα τεχνικά προβλήματα, όσον αφορά το software αλλά και το hardware, και τυχόν προβλήματα που παρουσιάζονται λύνονται πολύ πιο γρήγορα από ότι αν ήταν εγκατεστημένα τοπικά). Επίσης, έχουμε μικρότερες απαιτήσεις μνήμης από ότι τοπικά εγκατεστημένα προγράμματα.

- ✓ **Ελάττωση της πολυπλοκότητας λόγω ενθυλάκωσης:** Σε ένα περιβάλλον Ηλεκτρονικών Υπηρεσιών, όλες οι συνιστώσες είναι Ηλεκτρονικές Υπηρεσίες. Σημασία έχει, η «συμπεριφορά» που έχει η υπηρεσία και όχι ο τρόπος που είναι υλοποιημένη αυτή η συμπεριφορά. Αυτό το στοιχείο ενθυλάκωσης, η εικόνα δηλαδή των Ηλεκτρονικών Υπηρεσιών σαν «μαύρα κουτιά» με συγκεκριμένη συμπεριφορά, διευκολύνει κατά πολύ το έργο των προγραμματιστών που δεν ασχολούνται πλέον με τις λεπτομέρειες των εφαρμογών που επικαλούνται. Έτσι, η πολυπλοκότητα της ανάπτυξης Ηλεκτρονικών Υπηρεσιών ελαττώνεται σημαντικά.

### 1.2.2 Μειονεκτήματα Ηλεκτρονικών Υπηρεσιών <sup>30, 31, 32, 33</sup>

Τα μειονεκτήματα των Ηλεκτρονικών Υπηρεσιών, που αναφέρονται κυρίως στο σχεδιασμό τους και στις γλώσσες που χρησιμοποιούν, είναι:

- ✓ **Μη πιστοποιημένη είσοδος:** Δεδομένα που προέρχονται από αιτήματα μέσω δικτύου, δεν πιστοποιούνται πριν χρησιμοποιηθούν από μια web εφαρμογή. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν αυτή τη διαρροή ασφαλείας για να επιτεθούν στα στοιχεία που την απαρτίζουν, μέσα από μια εφαρμογή.
- ✓ **Έλεγχος πρόσβασης:** Περιορισμοί σχετικά με τις επιτρεπόμενες ενέργειες των πιστοποιημένων χρηστών, δεν επιβάλλονται όπως θα έπρεπε. Οι επιτιθέμενοι μπορούν να ανακαλύψουν τα κενά αυτά για να αποκτήσουν πρόσβαση στους λογαριασμούς άλλων χρηστών, να δουν ευαίσθητα δεδομένα ή να κάνουν χρήση εντολών για τις οποίες δεν έχουν δικαιώματα.
- ✓ **Διαχείριση προσβάσεων και συνδέσεων:** Ιδιότητες των λογαριασμών και συνδέσεις που έχουν γίνει, δεν προστατεύονται επαρκώς. Επιτιθέμενοι που μπορούν να χρησιμοποιήσουν κωδικούς, κλειδιά, session cookies, ή άλλα κερκημένα, μπορούν να ξεπεράσουν τη διαδικασία πιστοποίησης και τους περιορισμούς που αυτή επιβάλλει και να συνδεθούν υποδύομενοι άλλους χρήστες.
- ✓ **Διαρροές μέσω Cross Site Scripting (XSS):** Η web εφαρμογή μπορεί να χρησιμοποιηθεί σαν ένας μηχανισμός μεταφοράς επιθέσεων, στον browser του τελικού χρήστη. Μια επιτυχημένη επίθεση μπορεί να κρατήσει ανοιχτή τη σύνδεση ενός χρήστη, να μπει στο τοπικό μηχάνημα ή να αλλάξει δεδομένα και περιεχόμενα, για να ξεγελάσει τον χρήστη.
- ✓ **Υπερχείλιση των Buffer:** Τα στοιχεία μιας web εφαρμογής σε μερικές γλώσσες που δεν επικυρώνουν την είσοδο μπορεί να τεθούν εκτός και, σε μερικές περιπτώσεις, να χρησιμοποιηθούν για να πάρει ένας επιτιθέμενος τον έλεγχο της εφαρμογής. Τα στοιχεία αυτά μπορεί να περιλαμβάνουν CGI, βιβλιοθήκες, οδηγούς συσκευών και στοιχεία διακομιστών web εφαρμογών.
- ✓ **Διαρροές μέσω Injection:** Οι web εφαρμογές περνούν παραμέτρους όταν παίρνουν πρόσβαση σε εξωτερικά συστήματα ή σε τοπικά λειτουργικά συστήματα. Αν ένας επιτιθέμενος μπορέσει να εμβολιάσει κακόβουλες εντολές μέσα σε αυτές τις

παραμέτρους, το εξωτερικό σύστημα θα εκτελέσει τις εντολές αυτές για λογαριασμό της εφαρμογής.

- ✓ **Μη αρμόζουσα διαχείριση λαθών:** Καταστάσεις λάθους που προκύπτουν κατά τη διάρκεια κανονικών λειτουργιών δεν διαχειρίζονται ορθά. Εάν ένας επιτιθέμενος μπορεί να προκαλέσει σφάλματα για να δώσει την εικόνα ότι η εφαρμογή δεν συμπεριφέρεται σωστά, μπορεί να συλλέξει λεπτομερείς πληροφορίες σχετικές με το σύστημα, να προκαλέσει άρνηση παροχής υπηρεσιών, να "ρίξει" μηχανισμούς ασφαλείας ή να θέσει εκτός τον server.
- ✓ **Μη ασφαλής αποθήκευση:** Οι Web εφαρμογές συχνά χρησιμοποιούν εντολές κρυπτογράφησης για να προστατεύσουν πληροφορίες και πιστοποιητικά. Οι εντολές αυτές και ο κώδικας που τις ενοποιεί έχει αποδειχθεί ότι είναι δύσκολο να κωδικοποιηθούν σωστά. Το γεγονός αυτό, συχνά μας οδηγεί σε αδύναμα μέτρα ασφαλείας.
- ✓ **Άρνηση παροχής Υπηρεσιών (DoS):** Οι επιτιθέμενοι μπορούν να καταναλώσουν πόρους της web εφαρμογής σε σημείο που άλλοι νόμιμοι χρήστες να μην μπορούν πλέον να έχουν πρόσβαση σε αυτή. Οι επιτιθέμενοι μπορούν επίσης να κλειδώσουν τους λογαριασμούς άλλων χρηστών ή ακόμη να προκαλέσουν την κατάρρευση ολόκληρης της εφαρμογής.
- ✓ **Μη ασφαλής διαχείριση της παραμετροποίησης:** Το να υπάρχει ένα ισχυρό πρότυπο παραμετροποίησης των διακομιστών, είναι σημαντικό για την ασφάλεια των web εφαρμογών. Οι διακομιστές αυτοί, έχουν πολλές επιλογές παραμετροποίησης που επηρεάζουν την ασφάλεια.
- ✓ **Ευάλωτες σε επιθέσεις hackers:** Οι hackers πλέον δεν αποτελούν μια μικρή εξειδικευμένη κοινότητα. Υπάρχουν πίνακες ανακοινώσεων και ομάδες συζητήσεων, όπου ο καθένας μπορεί να βρει έτοιμο υλικό και πληροφορίες για την πραγματοποίηση διαφόρων ειδών επιθέσεων. Η απόλυτη πλειοψηφία των επιθέσεων προέρχεται από αυτή την κατηγορία. Για το λόγο αυτό θα πρέπει να γίνονται τακτικοί έλεγχοι στο σύνολο των εφαρμογών, να επαναλαμβάνονται σε κάθε νέα εγκατάσταση και κάθε φορά που γίνεται μια επέκταση, προσθήκη ή αναβάθμιση.
- ✓ **Standards-transactions-performance:** Στα Web services, τα πρότυπα (standards) για χαρακτηριστικά όπως οι συναλλαγές (transactions) είναι προς το παρόν ανύπαρκτα ή ακόμη σε πολύ βασικά στάδια σε αντίθεση με πολύ ωριμότερα ανοικτά πρότυπα καταναμημένων συστημάτων, όπως για παράδειγμα η CORBA. Εν συνεχεία, τα Web services έχουν χαμηλότερες επιδόσεις (performance) σε σύγκριση με άλλες προσεγγίσεις καταναμημένων συστημάτων όπως για παράδειγμα οι RMI, CORBA, ή DCOM. Αυτό είναι ένα κοινό μειονέκτημα των text-based formats, καθώς στους σχεδιαστικούς στόχους της XML δεν συγκαταλέγεται ούτε η σαφήνεια της κωδικοποίησης ούτε η αποτελεσματικότητα της λεκτικής ανάλυσης (parsing). Ακόμα, με τη χρησιμοποίηση του HTTP, τα web services μπορούν να αποφύγουν τα υπάρχοντα μέτρα ασφαλείας (firewall) οι κανόνες των οποίων προορίζονται για να εμποδίσουν ή να ελέγξουν την επικοινωνία μεταξύ των προγραμμάτων από κάθε πλευρά του firewall.
- ✓ **Γλώσσες scripting:** Οι περισσότερες γλώσσες scripting δεν έχουν τυπική σύνταξη και δεν συμβάλλουν στην καλή προγραμματιστική μέθοδο (εννοώντας τον καλό τρόπο γραφής προγραμμάτων). Οι γλώσσες scripting είναι γενικά πιο αργές από αυτές που χρειάζονται compiler (μερικές φορές και περισσότερο από 100 φορές). Έτσι, τα Scripts πολλές φορές οδηγούν σε βάσεις κώδικα που είναι δύσκολο να διαχειριστούν καθώς το

μέγεθος τους αυξάνει, μειώνοντας συνεπώς την απόδοση της εφαρμογής. Αποτέλεσμα αυτού, είναι το γεγονός ότι είναι δύσκολο (αλλά όχι αδύνατο) να γραφούν μεγάλες και multi-tier εφαρμογές σε γλώσσες scripting, διότι τα επίπεδα presentation, application and data βρίσκονται στο ίδιο μηχάνημα με αποτέλεσμα να περιορίζεται η κλιμάκωση και η ασφάλεια τους. Οι περισσότερες γλώσσες scripting από τη φύση τους, δεν υποστηρίζουν remote μεθόδους και κλήσεις web υπηρεσιών, πράγμα που κάνει δύσκολη την επικοινωνία με application servers και εξωτερικές web υπηρεσίες.

Για τη δημιουργία και τη λειτουργία ενός Website, στο οποίο τρέχουν web εφαρμογές, γίνεται χρήση ενός μεγάλου συνόλου διαφορετικών τεχνολογιών και προϊόντων. Η αλληλεπίδραση μεταξύ αυτών προκαλεί ένα απέραντο πλήθος προβλημάτων ασφαλείας. Από την ύπαρξη και την εκμετάλλευση αυτών των αδυναμιών, ένας επιτιθέμενος μπορεί να προκαλέσει μεγάλη ζημιά.

### 1.3 Πρωτόκολλα Επικοινωνίας

Τα web services, χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το SOAP. Το πρωτόκολλο αυτό, είναι πολύ πιο απλό από πρωτόκολλα παλαιότερων τεχνολογιών όπως αυτά που χρησιμοποιούνταν από τα καταναμημένα περιβάλλοντα CORBA, DCOM, RPC. Έτσι, το να δημιουργήσει κανείς μια υλοποίηση SOAP που υπόκειται στα πρότυπα (standards - compliant) είναι πολύ πιο εύκολο. Μπορεί εύκολα να βρει κανείς, υλοποιήσεις του SOAP από μεγαλύτερες εταιρίες πληροφορικής αλλά ακόμη και από μεμονωμένους προγραμματιστές, πράγμα αδιανόητο για παλαιότερες καταναμημένες τεχνολογίες<sup>2</sup>. Τα web services λειτουργούν με πρότυπες γλώσσες και πρωτόκολλα όπως η XML, το HTTP και το TCP/IP. Η πλειονότητα των εταιριών, έχουν ήδη την δικτυακή υποδομή και το κατάλληλο προσωπικό που τη συντηρούν. Έτσι, το κόστος για την εφαρμογή των web services είναι σημαντικά μικρότερο από αυτό των προηγούμενων τεχνολογιών<sup>2</sup>.

Με τις προηγούμενες τεχνολογίες η συνεργασία μεταξύ εταιριών ήταν ένα θέμα, διότι καταναμημένες τεχνολογίες όπως CORBA και DCOM χρησιμοποιούσαν μη πρότυπες πόρτες. Σαν αποτέλεσμα η συνεργασία σήμαινε άνοιγμα «οπών» στα τείχη προστασίας (firewalls) κάτι που πολλές φορές δεν ήταν αποδεκτό από τους ανθρώπους της πληροφορικής σε μια εταιρία, αφού έθετε σε κίνδυνο στην ασφάλεια των συστημάτων. Το γεγονός αυτό, δεν επέτρεπε δυναμική συνεργασία λόγω του ότι απαιτούσε μια χειροκίνητη διαδικασία για τη συνεργασία μιας εταιρίας με τους συνεργάτες της. Τα web services μπορούν να χρησιμοποιήσουν (μεταξύ άλλων) το HTTP ως πρωτόκολλο μεταφοράς και τα περισσότερα τείχη προστασίας επιτρέπουν την πρόσβαση μέσω της θύρας 80 (πρότυπη θύρα για το HTTP). Με αυτόν τον τρόπο, δημιουργούνται ευκολότερες συνεργασίες μεταξύ των συστημάτων των εταιριών<sup>4</sup>.

Σε ένα υψηλότερο εννοιολογικό επίπεδο, μπορεί κανείς να δει τα web services σαν μονάδες εργασίας (units of work). Αυτές οι μονάδες μπορούν να συνδυαστούν σε εργασίες επιχειρησιακού προσανατολισμού, για να χειριστούν συγκεκριμένες επιχειρησιακές λειτουργίες. Αυτό με τη σειρά του επιτρέπει σε μη τεχνικούς ανθρώπους να σχεδιάσουν εφαρμογές οι οποίες μπορούν να χειριστούν τα επιχειρησιακά ζητήματα, συνδυάζοντας τα web services σε ροές εργασίας. Σε μία αναλογία από τον χώρο των αυτοκινήτων, ο αρχιτέκτονας των επιχειρησιακών διαδικασιών μπορεί να συνδυάσει ολόκληρο τον κινητήρα με το πλαίσιο, τη μετάδοση και τα υπόλοιπα υποσυστήματα παρά να ασχοληθεί με τα εσωτερικά κομμάτια του κινητήρα.

Επιπλέον, η δυναμική πλατφόρμα σημαίνει ότι ο κινητήρας μπορεί να συνεργαστεί με τη μετάδοση ή άλλα υποσυστήματα διαφορετικών κατασκευαστών.

Αυτό που προκύπτει από αυτή την πτυχή, είναι ότι τα web services βοηθούν στην καλύτερη γεφύρωση του κενού που υπάρχει ανάμεσα στους ανθρώπους του επιχειρείν και τους ανθρώπους της πληροφορικής σε ένα οργανισμό. Οι άνθρωποι του επιχειρείν, μπορούν να περιγράψουν γεγονότα και δραστηριότητες και οι τεχνικοί μπορούν να τα συνδέσουν με τις κατάλληλες υπηρεσίες.

Με καθορισμένες διεπαφές και καλά σχεδιασμένες λειτουργίες, γίνεται επίσης εύκολο να επαναχρησιμοποιηθούν αυτές οι λειτουργίες, άρα και οι εφαρμογές που αντιπροσωπεύουν. Η επαναχρησιμοποίηση μιας εφαρμογής λογισμικού σημαίνει καλύτερη απόδοση της επένδυσης (return on investment), διότι μπορεί να παράγει περισσότερα με τους ίδιους πόρους. Επιτρέπει, τη χρησιμοποίηση μιας ήδη υπάρχουσας εφαρμογής με ένα διαφορετικό τρόπο ή το ενδεχόμενο προσφοράς αυτής σε ένα συνεργάτη με διαφορετικό τρόπο, αυξάνοντας ενδεχομένως τις επιχειρησιακές συναλλαγές μεταξύ των συνεργατών.

Επομένως, τα κύρια ζητήματα που τα web services προσπαθούν να λύσουν είναι τα ζητήματα ολοκλήρωσης (integration) δεδομένων και εφαρμογών και αυτά της μεταμόρφωσης των τεχνικών λειτουργιών σε υπολογιστικές λειτουργίες επιχειρησιακού προσανατολισμού<sup>4</sup>.

#### 1.4 Δομή Ηλεκτρονικών Υπηρεσιών

Για να γίνουν κατανοητές οι τεχνολογίες που απαιτούνται για τα web services πρέπει πρώτα να γίνει αντιληπτό, μία τυπική αλληλεπίδραση των web services.

Δίνεται ένα παράδειγμα – σενάριο αλληλεπίδρασης των web services. Έτσι, στο παράδειγμα αυτό χρειάζεται να εντοπίσουμε ένα συγκεκριμένο φαρμακείο στην περιοχή μας το οποίο έχει και ιστοσελίδα στο διαδίκτυο. Θα βγαίναμε στο δρόμο και θα ρωτούσαμε κάθε άτομο που θα συναντούσαμε για την ταχυδρομική διεύθυνση του φαρμακείου. Αντί για αυτό θα μπορούσαμε να αναφερθούμε στην ιστοσελίδα του φαρμακείου στο διαδίκτυο. Αν γνωρίζαμε την ηλεκτρονική διεύθυνση της ιστοσελίδας θα πλοηγούμασταν κατευθείαν σε αυτή και θα βρίσκαμε την ταχυδρομική διεύθυνση για την οποία ενδιαφερόμαστε. Αν δεν γνωρίζαμε την ηλεκτρονική διεύθυνση του φαρμακείου θα πλοηγούμασταν σε μια μηχανή αναζήτησης και θα πληκτρολογούσαμε το όνομα του φαρμακείου στη γλώσσα την οποία η μηχανή αναζήτησης αναγνωρίζει. Αφού βρίσκαμε την ιστοσελίδα, θα πλοηγούμασταν σε αυτήν και στη συνέχεια θα βρίσκαμε την ταχυδρομική διεύθυνση.

Η δομή των web services είναι παραπλήσια. Κοιτάζοντας προσεκτικά το προηγούμενο παράδειγμα, υπάρχει ένας αιτούντος ή καταναλωτής: εμείς. Υπάρχει επίσης μία υπηρεσία : το φαρμακείο. Η κεντρική βάση δεδομένων είναι το διαδίκτυο, μέσω της οποίας βρίσκουμε την τοποθεσία του φαρμακείου. Στο παράδειγμα, όταν εκτελείται μία αναζήτηση στη μηχανή αναζήτησης, η αίτησή τοποθετείται σε μία δομή, της οποίας η γλώσσα είναι προκαθορισμένη και τοπική και τότε περνιέται στον εξυπηρετητή της μηχανής αναζήτησης.

Στα web services το SOAP, UDDI και WSDL αντιπροσωπεύουν τους ρόλους που αναφέρθηκαν στα παραπάνω βήματα:

- ✓ Το SOAP (Simple Object Access Protocol), είναι η μέθοδος με την οποία στέλνονται μηνύματα σε διαφορετικές ενότητες λογισμικού (software modules). Είναι παρόμοιο με το πώς επικοινωνούμε με τη μηχανή αναζήτησης.
- ✓ Το UDDI (Universal Description, Discovery and Integration) είναι η καθολική βάση αναζήτησης για τον εντοπισμό των υπηρεσιών. Στο προηγούμενο παράδειγμα, είναι

ανάλογη της υπηρεσίας ευρετηρίου της μηχανής αναζήτησης, στην οποία όλες οι ιστοσελίδες καταχωρούνται και σχετίζονται με λέξεις κλειδιά. Διατηρεί ένα κατάλογο με όλα τα φαρμακεία της χώρας.

- ✓ Η WSDL (Web Services Definition Language) είναι ο τρόπος με τον οποίο διαφορετικές υπηρεσίες περιγράφονται στο UDDI. Αυτή αντιστοιχεί στην πραγματική μηχανή αναζήτησης<sup>5</sup>.

Για το SOAP, UDDI και WSDL παρακάτω γίνεται μεγαλύτερη περιγραφή.

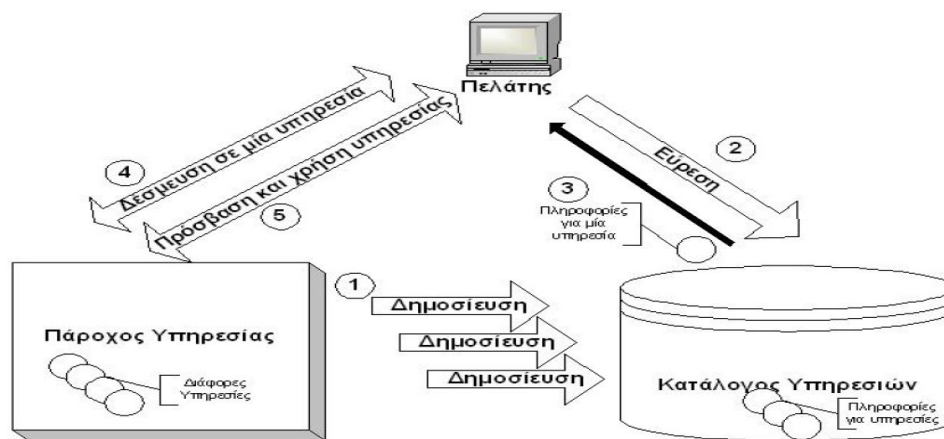
### 1.4.1 Μοντέλο των Ηλεκτρονικών Υπηρεσιών<sup>20</sup>

Το μοντέλο των web services ακολουθεί το παράδειγμα δημοσίευση (publish), εύρεσης (find) και σύνδεσης (bind). Στο πρώτο βήμα, ο προμηθευτής της υπηρεσίας δημοσιεύει την υπηρεσία σε ένα κατάλογο υπηρεσιών. Στο δεύτερο βήμα, ο πελάτης ο οποίος ψάχνει για μία υπηρεσία η οποία να καλύπτει τις απαιτήσεις του την αναζητεί στον κατάλογο. Αφού επιτυχημένα βρει πολλαπλές υπηρεσίες επιλέγει μία, βάσει των προτιμήσεών του. Τότε μεταφορτώνει την περιγραφή της υπηρεσίας και συνδέεται (δεσμεύεται) με αυτήν, ώστε να μπορέσει να καλέσει και να εκτελέσει την υπηρεσία<sup>4</sup>.

Η εφαρμογή που παρέχει την υπηρεσία και η εφαρμογή-πελάτης η οποία χρησιμοποιεί την υπηρεσία συνδέονται μεταξύ τους σε μια κοινή γλώσσα. Έπειτα, οι δύο εφαρμογές χρειάζονται ένα τρόπο να εντοπίζουν η μία την άλλη πριν ξεκινήσουν να «συνεργάζονται» μεταξύ τους. Αυτό αληθεύει ακόμη παραπάνω για τις καταναμημένες εφαρμογές, όπου μία εφαρμογή δεν έχει καμία γνώση της θέσης της άλλης.

Μετά τα παραπάνω, μια βασική αρχιτεκτονική για web services πρέπει να παρέχει<sup>5</sup>:

- ✓ Έναν πρότυπο τρόπο επικοινωνίας.
- ✓ Ένα ομοίμορφο μηχανισμό για περιγραφή και ανταλλαγή των δεδομένων.
- ✓ Μια πρότυπη περιγραφική γλώσσα (meta language) για την περιγραφή των υπηρεσιών που προσφέρονται.
- ✓ Ένα μηχανισμό καταχώρησης και εντοπισμού των εφαρμογών που βασίζονται σε web services.



Εικόνα 3: Μοντέλο των Ηλεκτρονικών Υπηρεσιών<sup>6</sup>

Επίπεδα: Τα επίπεδα του προγραμματιστικού μοντέλου των υπηρεσιών ιστού είναι:

**1ο Επίπεδο:** Το επίπεδο δικτύου (network) είναι το δομικό επίπεδο του προγραμματιστικού μοντέλου των υπηρεσιών ιστού. Όλες οι υπηρεσίες ιστού πρέπει να είναι διαθέσιμες μέσω του δικτύου. Το δίκτυο βασίζεται συνήθως στο πρωτόκολλο HyperText Transport Protocol (HTTP protocol), αλλά μπορούν να χρησιμοποιηθούν και άλλα πρωτόκολλα.

**2ο Επίπεδο:** Πάνω από το επίπεδο δικτύου, είναι το επίπεδο XML μηνυμάτων που παρέχει την επικοινωνία μεταξύ των υπηρεσιών ιστού και των πελατών που τα καλούν. Αυτό το επίπεδο επικοινωνίας βασίζεται στο πρωτόκολλο Simple Object Access Protocol (SOAP).

**3ο Επίπεδο:** Το πρωτόκολλο SOAP είναι ένα XML πρωτόκολλο που παρέχει τις λειτουργίες δημοσίευσης (publish), εύρεσης (find) και σύνδεσης (bind). Πάνω από το επίπεδο XML μηνυμάτων είναι το επίπεδο περιγραφής υπηρεσιών. Αυτό το επίπεδο βασίζεται στην προδιαγραφή Web Services Description Language (WSDL), που περιγράφει σε μορφή XML εγγράφων διαθέσιμες υπηρεσίες ιστού για τους πελάτες.

Αυτά τα 3 επίπεδα είναι υποχρεωτικά για τη δημιουργία διαλειτουργικών (interoperable) υπηρεσιών ιστού και τη δημοσίευση τους στο Internet. Τα ακόλουθα επίπεδα είναι προαιρετικά και χρησιμοποιούνται όταν απαιτείται ανάλογα με τις επιχειρησιακές ανάγκες.

**4ο Επίπεδο:** Στο επίπεδο δημοσίευσης μιας υπηρεσίας ιστού περιλαμβάνεται η ενέργεια που εκτελεί ο προμηθευτής μιας υπηρεσίας για να κάνει το έγγραφο WSDL (περιγραφή της υπηρεσίας) διαθέσιμο στους πιθανούς αιτούντες της υπηρεσίας. Αυτό το επίπεδο βασίζεται στη προδιαγραφή Universal, Description, Discovery and Integration (UDDI). Για παράδειγμα, η αποστολή του εγγράφου WSDL (ή της διεύθυνσης URL του εγγράφου) με ένα e-mail σε κάποιον, θεωρείται δημοσίευση της υπηρεσίας. Επίσης, η δημοσίευση του εγγράφου WSDL μιας υπηρεσίας σε μια αποθήκη UDDI, ώστε να είναι διαθέσιμο στους αιτούντες υπηρεσίας, αποτελεί τη δημοσίευση της υπηρεσίας.

**5ο Επίπεδο:** Παρόμοια, στο επίπεδο ανακάλυψης μιας υπηρεσίας ιστού περιλαμβάνεται κάθε ενέργεια που εκτελείται ώστε ο αιτώντος υπηρεσίας να προσπελάσει το WSDL έγγραφο της υπηρεσίας. Αυτό το επίπεδο, βασίζεται στη προδιαγραφή Universal, Description, Discovery and Integration (UDDI). Η ενέργεια μπορεί να είναι απλή, όπως η προσπέλαση του εγγράφου WSDL ή η επίσκεψη της διεύθυνσης που βρίσκεται το έγγραφο WSDL ή πολύπλοκη, όπως είναι η αναζήτηση σε μια αποθήκη UDDI και η χρήση των εγγράφων WSDL για την επιλογή ενός ή περισσότερων υπηρεσιών.

**6ο Επίπεδο:** Το επίπεδο ροής υπηρεσιών (service flow layer) παρέχει τη σύνθεση των υπηρεσιών ιστού σε ροές εργασίας (workflows) και την αναπαράσταση αυτής της συσσώρευσης των υπηρεσιών ως μια υπηρεσία ιστού υψηλότερου επιπέδου. Για αυτό το επίπεδο, η IBM έχει προτείνει την τυποποίηση Web Services Flow Language (WSFL) και η Microsoft την τυποποίηση XLANG. Η προδιαγραφή Business Process Execution Language for Web Services (BPEL4WS) αποτελεί μια προσπάθεια για ενοποίηση των προδιαγραφών WSFL και XLANG, συνδυάζοντας τα προτερήματα της κάθε μιας προσέγγισης, με στόχο την τυποποίησή (standard) της για τη σύνθεση υπηρεσιών ιστού.

Σε όλα τα επίπεδα του προγραμματιστικού μοντέλου των υπηρεσιών ιστού, πρέπει να ληφθεί υπόψη η ασφάλεια των υπηρεσιών, η διαχείριση των υπηρεσιών και η διαχείριση της ποιότητας παροχής υπηρεσιών.

## 1.4.2 Microsoft .NET <sup>29</sup>

Το .NET της Microsoft, αποτελεί μια από τις καλύτερα ανεπτυγμένες WS πρωτοβουλίες. Η τεχνολογία ξεκίνησε να αναπτύσσεται από την Microsoft παράλληλα με το Windows Distributed



Internet Architecture πρόγραμμα το 1997. Το .NET χρησιμοποιεί πρότυπα βασισμένα σε XML, και αυτό το κάνει ανεξάρτητο πλατφόρμας. Επιπροσθέτως, αποτελείται από μεγάλο πλήθος στοιχείων κλειδιών, που κάνει το .NET ανεξάρτητο και από γλώσσα.

Για παράδειγμα η Προδιαγραφή Κοινής Γλώσσας (Common Language Specification), είναι ένα σύνολο από κανόνες με σκοπό την ανάδειξη της διαλειτουργικότητας της γλώσσας. Επίσης, το περιβάλλον πολύ - γλωσσικότητας Κοινής Γλώσσας Χρόνου Εκτέλεσης (Common Language Runtime Multilanguage Environment), κάνει χρήση ενός μεταγλωττιστή - just in time compiler - για να επιτρέπει στον κώδικα να γράφεται σε οποιαδήποτε από ένα πλήθος γλωσσών, όπως Cobol και C#, και παραδίδει τα WS μέσω XML.

Το .NET είναι μια προσπάθεια να ενσωματωθούν όλες οι δημοφιλείς προγραμματιστικές γλώσσες σε ένα runtime και αναπτυξιακό σύστημα. Το εργαλείο ανάπτυξης της πρωτοβουλίας αυτής είναι το Visual Studio .NET. Το .NET My Services, αναπαριστά ένα σύνολο από βασισμένες σε XML υπηρεσίες, που οι χρήστες μπορούν να καλέσουν για να προτυποποιήσουν και να απλουστεύσουν το e-commerce και άλλες διαδικτυακές εφαρμογές. Για παράδειγμα, η .NET Profile υπηρεσία περιλαμβάνει πληροφορία όπως το όνομα του χρήστη και διεύθυνση και η .NET Wallet περιλαμβάνει προτιμώμενους μηχανισμούς πληρωμής. Η Microsoft, έχει προσθέσει ακόμα στο .NET επιπρόσθετες υπηρεσίες, όπως το Passport σύστημα αναγνώρισης χρηστών.

### 1.4.3 Πρωτοβουλίες σε Java <sup>28</sup>

Οι υπόλοιπες προσπάθειες άλλων εταιρειών επάνω σε Java WSs, είναι παρόμοιες με τις προαναφερθείσες. Η ουσιαστική διαφορά είναι, ότι κάθε μια κάνει χρήση της προτεινόμενης J2EE υλοποίησης της εκάστοτε εταιρείας και λειτουργεί καλύτερα με την δικιά της DBMS.

**BEA:** Αποτελεί ένα από τους κορυφαίους προμηθευτές εξυπηρετητών εφαρμογών. Η BEA προτείνει τον δικό της server για J2EE WS, τον WebLogic Server 6.1.

**HP:** Η πρωτοβουλία της HP για πλατφόρμα WS, ξεκίνησε με το ελεύθερης διανομής πρόγραμμα του e-Speak, το οποίο αρχικά είχε σχεδιαστεί για να εξυπηρετεί Web Services κάνοντας χρήση τεχνολογιών της HP. Παρόλα αυτά, η συνεχής αποδοχή της XML για την εξυπηρέτηση WS, έκαναν το e-Speak λιγότερο σημαντικό. Πλέον η HP χρησιμοποιεί WS κάνοντας χρήση προδιαγραφών βασισμένων σε XML, και την Bluestone J2EE μηχανή ως τον κεντρικό εξυπηρετητή εφαρμογών.

**IBM:** Η IBM έχει συμπεριλάβει τα WS στον Web-Sphere εξυπηρετητή εφαρμογών μέσω του Web Service Toolkit. Αυτό αποτελεί ένα πρόγραμμα ανάπτυξης λογισμικού που συμπεριλαμβάνει runtime environment, αρχιτεκτονικά προσχέδια (architectural blueprints), εργαλεία, και παραδείγματα για να βοηθάει στον σχεδιασμό και εκτέλεση WS εφαρμογών.

**Oracle:** Η εταιρεία για να μπορέσει να παρέχει WS, ανέπτυξε τον Oracle9iAS εξυπηρετητή εφαρμογών WS. Επίσης προχώρησε στην δημιουργία του Jdeveloper, ένα εργαλείο ανάπτυξης, που μπορεί να θεωρηθεί ως ένα παρόμοιο πακέτο με το Visual Studio.NET βασισμένο σε Java.

Η XML, σε αντίθεση με το δυαδικό ΠΟΡ, βασίζεται σε κείμενο και άρα δημιουργεί περισσότερα δεδομένα που τα συστήματα πρέπει να επεξεργαστούν. Για αυτό τον λόγο η XML, τρέχει με πιο αργό ρυθμό επάνω σε HTTP. Η προσθήκη ενός πρωτοκόλλου ασφαλείας όπως το SSL (Secure Socket Layer), επιβραδύνει την απόδοση ακόμα περισσότερο. Αυτό κάποιες φορές, αποτελεί τροχοπέδη για δραστηριότητες WS σε χαμηλής ταχύτητας συνδέσεις, όπως τα dial-up modem.

Ακολουθώς, επειδή τα WS δεν έχουν ενσωματωμένο μοντέλο ασφάλειας, πρέπει να βασίζονται στο SSL, στα εικονικά ιδιωτικά δίκτυα, ή σε άλλα εξωγενή μέτρα. Γενικά, η δημόσια υποδομή και το SSL, παρέχουν ικανοποιητική ασφάλεια. Παρόλα αυτά, αναπτυξιακές εταιρείες όπως οι Netegrity, Oblix και Open Network Technologies, έχουν επεξεργαστεί μοντέλα για διαχείριση της ασφάλειας των Web Services μέσω επικύρωσης ή κωδικοποίησης.

Επιπροσθέτως, ο Οργανισμός για την Βελτιστοποίηση των Προτύπων Δομημένων Δεδομένων, ανέπτυξε την SAML (Security Assertion Markup Language), ουδέτερο format ως προς τους προμηθευτές, για την επικύρωση των συναλλαγών των WS.

#### 1.4.4 XML - eXtensible Markup Language

Η eXtensible Markup Language (XML), είναι μια γλώσσα ανεξάρτητη από σύστημα και υλικό για την αναπαράσταση δεδομένων και της μορφής τους σε ένα έγγραφο XML (XML document). Ένα έγγραφο XML, στην πιο απλή του μορφή είναι ένα αρχείο κειμένου το οποίο περιέχει δεδομένα μαζί με σήμανση η οποία καθορίζει τη δομή των δεδομένων .

Η XML, είναι μια παγκοσμίως συμφωνημένη μεταγλώσσα σήμανσης που χρησιμοποιείται πρώτιστα για την ανταλλαγή πληροφοριών. Η ομορφιά της XML βρίσκεται στο γεγονός ότι είναι επεκτάσιμη. Απλά, η XML είναι ένα σύνολο προκαθορισμένων κανόνων (συντακτικό πλαίσιο) που πρέπει να ακολουθήσουμε κατά τη δόμηση των δεδομένων μας .

Για ένα μεγάλο χρονικό διάστημα, οι προγραμματιστές και οι προμηθευτές εφαρμογών κατασκεύαζαν εφαρμογές και συστήματα εγκατεστημένα σε μια επιχείρηση τα οποία επεξεργάζονταν δεδομένα τα οποία μπορούσαν να με το δικό τους ιδιωτικό τρόπο. Αλλά καθώς η ανταλλαγή πληροφορίας μεταξύ εφαρμογών και συστημάτων στις επιχειρήσεις επικρατούσε, έγινε πολύ δύσκολη η ανταλλαγή δεδομένων διότι τα συστήματα δε σχεδιάστηκαν ώστε να δέχονται δεδομένα από εξωτερικά, άγνωστα συστήματα .

Η XML παρέχει μία πρότυπη και κοινή δομή για τη διανομή δεδομένων μεταξύ ανόμοιων συστημάτων. Επιπλέον, η XML έχει ενσωματωμένο ένα μηχανισμό επικύρωσης δεδομένων, ο οποίος εγγυάται ότι η δομή των δεδομένων που λαμβάνεται είναι έγκυρη .

Εδώ παρατίθεται ένα παράδειγμα, για το πώς αναπαριστάνουμε τα δεδομένα με την βοήθεια της XML.

---

```
<employee>
<shift id= "counter" time="8-12">
<phone id = "1"> All phone information
<number>3444333</number >
</phone>
</shift >
<shift id="help_desk" time="1-5">
<phone id = "2"> All phone information
<number>332333</number >
</phone>
</shift >
...
<home-address>
<street>3434 Norwalk street</street>
```

```
<city>New York</city>
<state>NY</state>
</home-address>
</employee>
```

Στο παραπάνω παράδειγμα, αναπαρίστανται οι προσωπικές πληροφορίες και οι πληροφορίες σχετικά με τις βάρδιες ενός υπαλλήλου σε ένα οργανισμό.

Η XML χρησιμοποιεί τις διακριτικές ετικέτες “<>” και “</>” παρόμοια με τις ετικέτες που χρησιμοποιούνται στην HTML. Αυτό συμβαίνει, γιατί η XML είναι μια γλώσσα σήμανσης σαν την HTML.

Η κύρια διαφορά της XML με την HTML είναι ως προς τον σκοπό της κάθε μίας:

- ✓ Η XML, σχεδιάστηκε για να περιγράφει δεδομένα και να εστιάσει στο τί είναι αυτά τα δεδομένα.
- ✓ Η HTML σχεδιάστηκε για να προβάλλει δεδομένα και να εστιάσει στο πώς φαίνονται αυτά τα δεδομένα.

Στο παραπάνω παράδειγμα, τα δεδομένα είναι καθαρά: ένας υπάλληλος (employee) έχει παραπάνω από μία βάρδιες (shift), για παράδειγμα το πρωί εργάζεται στο ταμείο (counter) και το μεσημέρι στο γραφείο βοήθειας (helpdesk) και διευθύνσεις.

Οι δύο αρχικές δομικές μονάδες XML που χρησιμοποιούνται στο προηγούμενο παράδειγμα είναι τα elements (στοιχεία) και τα attributes (ιδιότητες) <sup>5</sup>.

### Στοιχεία (Elements)

Τα στοιχεία (elements) είναι ετικέτες, όπως και στην HTML, που περιέχουν τιμές. Επιπλέον, τα elements είναι δομημένα δένδροειδή στοιχεία. Ως εκ τούτου τα στοιχεία είναι οργανωμένα με ένα ιεραρχικό τρόπο με ένα στοιχείο-πατέρα και στοιχεία-παιδιά. Τα στοιχεία-παιδιά μπορούν να περιέχουν και αυτά άλλα στοιχεία-παιδιά και ούτω καθεξής <sup>5</sup>.

Στο προηγούμενο παράδειγμα, το στοιχείο <employee> είναι το γονικό στοιχείο και έχει το στοιχείο <shift> σαν στοιχείο-παιδί. Παρακάτω το στοιχείο <phone> είναι στοιχείο-παιδί του γονικού στοιχείου <shift>.

Τα στοιχεία έχουν συγκεκριμένα χαρακτηριστικά. Ορισμένα από αυτά είναι <sup>5</sup>:

- ✓ Τα στοιχεία μπορεί να περιέχουν δεδομένα, όπως το στοιχείο <number> στο παράδειγμα.
- ✓ Αντίστροφα, τα στοιχεία μπορεί να μην περιέχουν δεδομένα αλλά μόνο ιδιότητες, όπως το στοιχείο <shift>.
- ✓ Εναλλακτικά, τα στοιχεία μπορεί να περιέχουν ταυτόχρονα και ιδιότητες αλλά και δεδομένα, αλλά επίσης και στοιχεία-παιδιά, όπως το στοιχείο <phone>.

Επίσης, τα στοιχεία έχουν κάποιους κανόνες <sup>8</sup>:

- ✓ Όλα τα στοιχεία πρέπει να έχουν ετικέτα κλεισίματος αντίθετα με την HTML όπου υπάρχουν και ετικέτες που δε χρειάζονται κλείσιμο όπως για παράδειγμα η <br>.
- ✓ Οι ετικέτες των στοιχείων είναι case sensitive, δηλαδή υπάρχει διαχωρισμός μεταξύ κεφαλαίων και πεζών και τα ονόματά τους υπακούουν σε κανόνες ονοματολογίας.

Τέλος, τα στοιχεία πρέπει να είναι τοποθετημένα σωστά αντίθετα με την HTML:

- ✓ HTML : <b><i>This text is bold and italic</b></i>
- ✓ XML : <b><i>This text is bold and italic</i></b>
- ✓ Τα έγγραφα της XML πρέπει να έχουν ακριβώς ένα αρχικό στοιχείο (root element).

### **Ιδιότητες (Attributes)**

Οι ιδιότητες (attributes) δίνουν περισσότερο νόημα και βοηθούν στην περιγραφή των στοιχείων πιο αποτελεσματικά και με σαφήνεια. Στο προηγούμενο παράδειγμα, το στοιχείο <shift> έχει μία ιδιότητα “id” με τιμές “counter” και “helpdesk”. Με τη χρήση τέτοιων ιδιοτήτων, γίνεται διαχωρισμός αν ένας υπάλληλος εργάζεται στο ταμείο ή στο γραφείο βοήθειας. Αυτό βοηθάει στο να γίνονται τα δεδομένα σε ένα έγγραφο XML αυτοπεριγραφικά. Ο κύριος σκοπός των ιδιοτήτων είναι να παρέχουν περισσότερη πληροφορία σχετική με ένα στοιχείο και δεν πρέπει να χρησιμοποιούνται για να περιέχουν τα ίδια τα δεδομένα.

Όπως και στα στοιχεία έτσι και στις ιδιότητες υπάρχουν κανόνες :

- ✓ Οι τιμές των ιδιοτήτων πρέπει να είναι εσωκλείονται σε “” ή σε ‘’.
- ✓ Τα ονόματα των ιδιοτήτων ακολουθούν τους ίδιους κανόνες με αυτά των ετικετών.

### **Κανόνες ονομασίας**

Τα στοιχεία και οι ιδιότητες στην XML πρέπει να ακολουθούν στους παρακάτω κανόνες :

- ✓ Τα ονόματα μπορούν να περιέχουν γράμματα, αριθμούς και άλλους χαρακτήρες.
- ✓ Τα ονόματα δεν πρέπει να ξεκινούν με αριθμό ή χαρακτήρα στίξης.
- ✓ Τα ονόματα δεν πρέπει να ξεκινούν με τα γράμματα xml (ή XML, ή Xml κλπ.).
- ✓ Τα ονόματα δεν μπορούν να περιέχουν κενά.

### **Διαμορφωμένα έγγραφα (well formed documents)**

Ένα «καλά διαμορφωμένο» έγγραφο XML είναι ένα έγγραφο που υπακούει στους κανόνες σύνταξης της XML :

- ✓ Τα έγγραφα XML πρέπει να περιέχουν ένα αρχικό στοιχείο.
- ✓ Τα στοιχεία XML πρέπει να έχουν ετικέτες κλεισίματος.
- ✓ Στις ετικέτες XML υπάρχει διαχωρισμός κεφαλαίων και πεζών.
- ✓ Τα στοιχεία XML πρέπει να είναι σωστά τοποθετημένα.
- ✓ Οι ιδιότητες XML πρέπει να εσωκλείονται πάντα σε “” ή ‘’.

### **DTD (Document Type Definition)**

Όπως σε μία γλώσσα προγραμματισμού πρέπει Να είναι γνωστό οι προδιαγραφές της γλώσσας, με παρόμοιο τρόπο το Document Type Definition (DTD) είναι μία προδιαγραφή, η οποία πρέπει να ακολουθηθεί όταν δημιουργείται ένα έγγραφο XML. Επίσης, όπως μία από τις εργασίες του μεταγλωττιστή για κάθε γλώσσα προγραμματισμού είναι να ελέγξει αν οι προδιαγραφές ακολουθήθηκαν, με παρόμοιο τρόπο υπάρχουν XML parsers οι οποίοι χρησιμοποιούν το DTD για να ελέγξουν την εγκυρότητα ενός εγγράφου XML.

Ένα DTD, βοηθάει στον καθορισμό της δομής ενός εγγράφου XML. Παρέχει ένα αυστηρό πλαίσιο και κανόνες οι οποίοι θα ακολουθηθούν όταν δημιουργούνται έγγραφα XML. Επιπρόσθετα, το DTD μπορεί να χρησιμοποιηθεί για τον έλεγχο της εγκυρότητας και της ακεραιότητας των δεδομένων που περιέχονται σε ένα έγγραφο XML.

Μερικά χαρακτηριστικά του DTD είναι τα παρακάτω :

- ✓ Το DTD χρησιμοποιείται για να καθορίσει έγκυρα στοιχεία και ιδιότητες που μπορούν να χρησιμοποιηθούν σε ένα έγγραφο XML.
- ✓ Με ένα DTD καθορίζεται η ιεραρχική δομή στοιχείων.
- ✓ Σε ένα DTD μπορεί επίσης να καθοριστεί η διαδοχική οργάνωση μιας συλλογής στοιχείων-παιδιών τα οποία μπορούν να υπάρχουν σε ένα έγγραφο XML.

Ένα DTD μπορεί να χρησιμοποιηθεί απευθείας μέσα σε ένα έγγραφο XML ή μπορεί να υπάρχει εκτός του εγγράφου XML. Στη δεύτερη περίπτωση θα αναφέρεται με ένα δεσμό μέσα στο έγγραφο XML που δείχνει σε αυτό το DTD.

Το DTD αποτελείται από τα παρακάτω στοιχεία <sup>5</sup> :

Στοιχείο	Περιγραφή
<b>DTD Element</b>	Μεταδεδομένα για ένα στοιχείο. Καθορίζει τι είδους δεδομένα θα έχει το στοιχείο, τον αριθμό των περιστατικών κάθε στοιχείου, τις σχέσεις μεταξύ των στοιχείων και ούτω καθεξής.
<b>DTD Attributes</b>	Καθορίζει διάφορους κανόνες και ορισμούς που σχετίζονται με τα δεδομένα.
<b>DTD Entities</b>	Χρησιμοποιείται για να αναφέρει ένα εξωτερικό αρχείο ή για να παρέχει συντομεύσεις σε κοινό κείμενο.

Πίνακας 1: Τα Στοιχεία του DTD

### Παράδειγμα 1:

<!ELEMENT employee(shift+,home-address, hobbies)>

Ένα στοιχείο employee μπορεί να περιέχει ένα ή περισσότερα στοιχεία shift και πρέπει να έχει ένα στοιχείο home-address και μπορεί να έχει μηδέν ή περισσότερα στοιχεία hobbies.

### Παράδειγμα 2:

<!ATTLIST shift id CDATA #REQUIRED>

Το στοιχείο shift πρέπει να έχει μία ιδιότητα id. Ένα DTD χρησιμοποιείται για να καθορίσει μια δομή εγγράφων με τη διευκρίνιση των λεπτομερειών σχετικά με όλα τα στοιχεία και τις ιδιότητες που πρόκειται να χρησιμοποιηθούν σε ένα έγγραφο XML. Ως εκ τούτου, μπορεί να χρησιμοποιηθεί για να ελέγξει την εγκυρότητα ενός εγγράφου XML που ακολουθεί τους κανόνες που καθορίζονται από αυτό το DTD <sup>5</sup>.

### XML Schema

Το XML Schema είναι μια πιο προηγμένη έκδοση του DTD. Το DTD έχει πολλά μειονεκτήματα σε σχέση με το Schema, όπως το ότι δεν υποστηρίζει ισχυρούς τύπους δεδομένων, έχει σύνταξη διαφορετική από την XML και δεν είναι επεκτάσιμο. Το XML Schema παρουσιάστηκε για να υπερνικήσει αυτά τα μειονεκτήματα <sup>5</sup>.

Οι δύο κύριοι στόχοι του W3c XML Schema working group κατά τη διάρκεια του σχεδιασμού του προτύπου του XML Schema ήταν <sup>4</sup> :

- ✓ Να μπορέσουν να εκφράσουν μέσα στο πρότυπο αρχές αντικειμενοστραφούς σχεδιασμού οι οποίες μπορούν να βρεθούν σε όλες τις αντικειμενοστραφείς γλώσσες προγραμματισμού.
- ✓ Να παρέχουν υποστήριξη για σύνθετους τύπους δεδομένων παρόμοια με την υποστήριξη που υπάρχει στις περισσότερες σχεσιακές βάσεις δεδομένων.

Τα κυριότερα χαρακτηριστικά του XML Schema είναι τα παρακάτω :

- ✓ Η σύνταξη είναι όμοια με της XML. Αυτό σημαίνει ότι το Schema επεξεργάζεται με οποιοδήποτε επεξεργαστή XML.
- ✓ Γίνεται καθορισμός οποιοδήποτε τύπων δεδομένων πέραν των βασικών όπως: αλφαριθμητικό, ακέραιος, πραγματικός και ούτω καθεξής.

Για παράδειγμα:

```
<xs:element name="name" type="xs:string" />
```

Οι νέοι τύποι μπορεί να είναι απλοί ή σύνθετοι. Οι σύνθετοι τύποι μπορεί να περιέχουν και άλλα στοιχεία ή και ιδιότητες, ενώ οι απλοί τύποι όχι. Αντίθετα μπορούν να περιέχουν μόνο δεδομένα.

- ✓ Το XML Schema παρέχει επικύρωση βασισμένη στο περιεχόμενο (content-based validation) δηλαδή μπορεί να ορίσει την σειρά με την οποία τα στοιχεία-παιδιά εμφανίζονται. Επίσης παρέχει επικύρωση στους ίδιους τους τύπους δεδομένων.

Για παράδειγμα μπορεί να οριστεί ένας απλός τύπος "year" με τιμές μεταξύ 2000 και 2100:

```
<xsd:simpleType name="year">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="2000"/>
    <xsd:maxInclusive value="2100"/>
  </xsd:restriction>
</xsd:simpleType>
```

Παρομοίως οι σύνθετοι τύποι μπορεί να ορίσουν τη σειρά με την οποία τα στοιχεία-παιδιά θα εμφανίζονται:

```
<xsd:complexType name="Employee">
  <xsd:sequence>
    <xsd:element name="Name" type="xsd:string" />
    <xsd:element name="Address" type="xsd:string" />
    <xsd:element name="Phone" type="xsd:string" />
  </xsd:sequence>
</xsd:complexType>
```

- ✓ Το XML Schema παρέχει τη δυνατότητα επέκτασης άλλων εγγράφων το οποίο δεν είναι τίποτα άλλο παρά κληρονομικότητα. Αυτό σημαίνει ότι μπορούν να παραχθούν νέοι τύποι δεδομένων βάσει παλαιών τύπων.
- ✓ Το XML Schema παρέχει υποστήριξη για Namespaces (χρησιμοποιώντας URI). Παρέχει σε κάθε στοιχείο ένα μοναδικό αναγνωριστικό, με το οποίο αποφεύγονται συγκρούσεις ονομάτων μεταξύ των στοιχείων. Αυτό θα μπορούσε να συμβεί, για παράδειγμα, όταν δύο έγγραφα συγχωνεύονταν, και περιείχαν και τα δύο στοιχεία με όνομα "name" τα

οποία όμως είχαν διαφορετικό νόημα σε κάθε έγγραφο. Εν ολίγοις βοηθάει στο να ξεχωρίζουν στοιχεία και ιδιότητες με ίδιο όνομα και διαφορετικό νόημα. Μία απλή αναλογία στις γλώσσες προγραμματισμού είναι η χρήση καθολικών και τοπικών μεταβλητών. Μια τοπική μεταβλητή είναι μοναδική μέσα στο πεδίο ισχύος της ενώ μια καθολική μεταβλητή πρέπει να είναι μοναδική σε ολόκληρο το πρόγραμμα. Παρομοίως, με το namespace ορίζονται τύποι χωρίς να γίνεται σύγκρουση ονομάτων<sup>4</sup>.

- ✓ Τέλος, το XML Schema είναι εύκολα επεκτάσιμο για να ενσωματώσει και άλλες λειτουργίες στο μέλλον.

### Σύγκριση του XML Schema - DTD

Οι κυριότερες διαφορές συνοψίζονται ως εξής<sup>5</sup>:

- ✓ Το XML Schema είναι επέκταση του DTD.
- ✓ Το XML Schema υποστηρίζει namespaces ενώ το DTD όχι.
- ✓ Το XML Schema χρησιμοποιεί σύνταξη XML η οποία είναι εύκολα κατανοητή, ενώ το DTD χρησιμοποιεί ειδική σύνταξη.
- ✓ Το XML Schema υποστηρίζει πρότυπους τύπους δεδομένων καθώς επίσης και τύπους ορισμένους από το χρήστη (user-defined) ενώ το DTD παρέχει μόνο τύπους κειμένου.
- ✓ Το XML Schema υποστηρίζει κληρονομικότητα ενώ το DTD όχι.

### 1.5 Πρωτόκολλα των Ηλεκτρονικών Υπηρεσιών

Οι βασικές τεχνολογίες στις οποίες βασίζονται τα web services<sup>5</sup>:

XML:

- ✓ **Επίπεδο:** Ομοιόμορφος ορισμός και ανταλλαγή δεδομένων.
- ✓ **Περιγραφή:** Η Extended Markup Language (XML) είναι μια μέτα-γλώσσα (περιγραφική γλώσσα) η οποία έχει καλή καθορισμένη σύνταξη και σημασιολογία. Τα «αυτοπεριγραφικά» χαρακτηριστικά της XML την κάνουν απλό, αλλά δυνατό, μηχανισμό για τη σύλληψη και την ανταλλαγή των στοιχείων μεταξύ των διαφορετικών εφαρμογών.

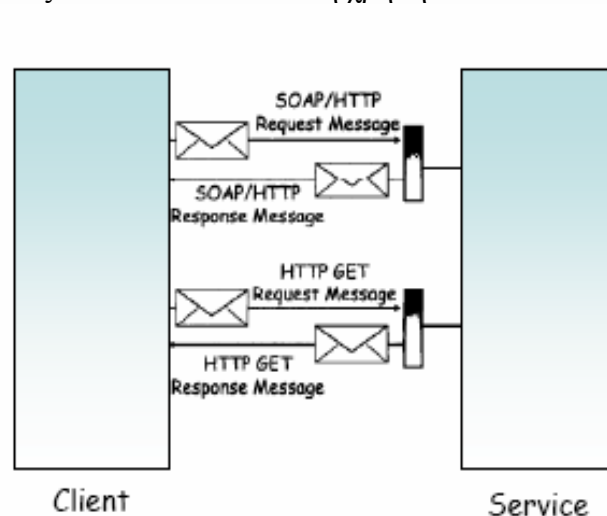
SOAP:

- ✓ **Επίπεδο:** Πρότυπο κανάλι επικοινωνίας.
- ✓ **Περιγραφή:** Το Simple Object Access Protocol (SOAP) είναι το κανάλι που χρησιμοποιείται για επικοινωνία μεταξύ μιας εφαρμογής – προμηθευτή web services και μιας εφαρμογής-πελάτη. Η απλότητα του SOAP, είναι το ότι δεν καθορίζει κανένα νέο πρωτόκολλο μεταφοράς. Αντίθετα, επαναχρησιμοποιεί μεταξύ άλλων το Hyper Text Transfer Protocol (HTTP) ή το Simple Mail Transfer Protocol (SMTP) για μεταφορά δεδομένων σαν μηνύματα. Αυτή η χρήση του HTTP ή του SMTP σαν πρωτόκολλο μεταφοράς εξασφαλίζει ότι οι εφαρμογές – προμηθευτές με τις εφαρμογές – πελάτες μπορούν να επικοινωνήσουν χρησιμοποιώντας το διαδίκτυο σαν ραχοκοκαλιά. Είναι η χρήση του SOAP που πολλαπλασιάζει τις ικανότητες των web services.

WSDL:

- ✓ **Επίπεδο:** Πρότυπη περιγραφική γλώσσα για την περιγραφή των παρεχόμενων υπηρεσιών.
- ✓ **Περιγραφή:** Οι εφαρμογές που παρέχουν web services διαφημίζουν τις διάφορες υπηρεσίες που παρέχουν χρησιμοποιώντας μια πρότυπη περιγραφική γλώσσα που ονομάζεται Web Services Description Language (WSDL). Κατά τρόπο ενδιαφέροντα, η

WSDL βασίζεται στην XML και χρησιμοποιεί ένα ειδικό σύνολο ετικετών (tags), για να περιγράψει ένα web service, τις υπηρεσίες που παρέχονται, που να εντοπιστεί και ούτω καθεξής. Οι εφαρμογές - πελάτες λαμβάνουν πληροφορίες για ένα web service, πριν από την πρόσβασή τους σε αυτό και τελικά τη χρήση του.



Εικόνα 4: Παράδειγμα Πρωτοκόλλων Επικοινωνίας WSDL

UDDI:

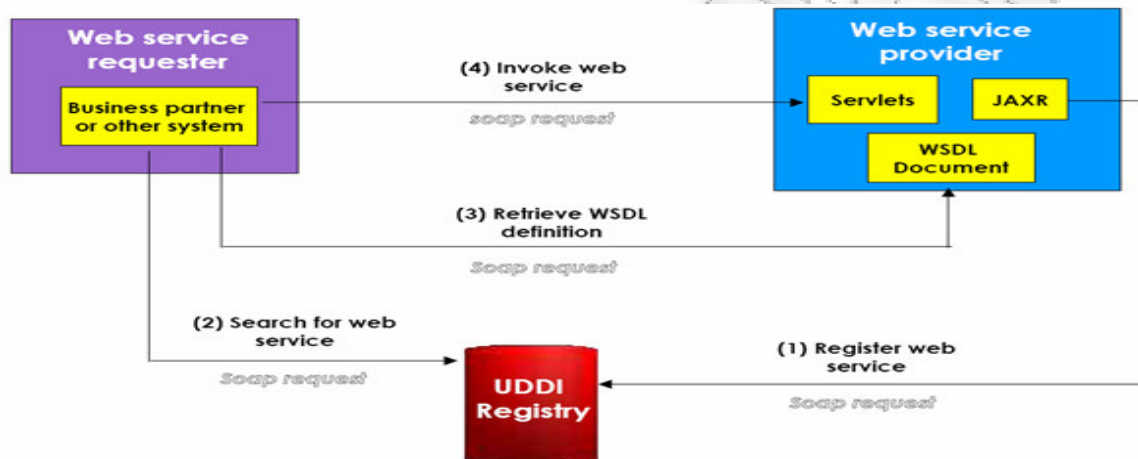
- ✓ **Επίπεδο:** Καταχώρηση και εντοπισμός των παρεχόμενων υπηρεσιών.
- ✓ **Περιγραφή:** Ο «χρυσός οδηγός» των web services είναι το Universal Description Discovery and Integration (UDDI). Οι εφαρμογές που παρέχουν web services παρατίθενται σε ένα κατάλογο από πάροχους υπηρεσιών χρησιμοποιώντας το UDDI. Παρόμοια, οι εφαρμογές-πελάτες εντοπίζουν τους πάροχους εφαρμογών web services χρησιμοποιώντας UDDI. Όπως και στην περίπτωση της WSDL, και το UDDI βασίζεται στην XML.

### 1.5.1 WSDL (Web Services Description Language)

Ο ορισμός που δίνει το W3C (World Wide Web Consortium) για την Web Services Description Language<sup>9</sup>: “Η WSDL είναι ένα σχήμα XML για την περιγραφή δικτυακών υπηρεσιών σαν ένα σύνολο από τελικά σημεία που λειτουργούν σε μηνύματα τα οποία περιέχουν πληροφορία είτε προσανατολισμένη στα έγγραφα είτε προσανατολισμένη στις διαδικασίες. Οι λειτουργίες και τα μηνύματα περιγράφονται περιληπτικά, και τότε δένονται σε ένα συγκεκριμένο πρωτόκολλο δικτύων και μορφή μηνυμάτων για να καθορίσουν ένα τελικό σημείο. Πολλά τελικά σημεία συνδυάζονται σε υπηρεσίες (services). Η WSDL είναι επεκτάσιμη στο να επιτρέπει την περιγραφή τελικών σημείων και των μηνυμάτων τους, άσχετα από τη μορφή των μηνυμάτων και των πρωτοκόλλων δικτύων που χρησιμοποιούνται για την επικοινωνία. Παρόλα αυτά, αυτή τη στιγμή στην προδιαγραφή της WSDL οι μόνες συνδέσεις που περιλαμβάνονται, περιγράφουν την χρησιμοποίηση της WSDL, σε συνδυασμό με το SOAP 1.1, το HTTP GET/POST και το MIME.” Δηλαδή, η WSDL βοηθάει στην περιγραφή αφενός ενός συνόλου από μηνύματα και αφετέρου, το πώς αυτά τα μηνύματα ανταλλάσσονται. Η WSDL καθορίζει τι πρέπει να περιέχει ένα μήνυμα και πώς πρέπει να είναι ένα μήνυμα απάντησης με σαφή σήμανση<sup>2</sup>.



Η σήμανση που χρησιμοποιείται σε ένα αρχείο WSDL, για να περιγράψει μορφές μηνυμάτων βασίζεται στο πρότυπο του XML Schema το οποίο σημαίνει ότι είναι ταυτόχρονα ανεξάρτητη από γλώσσα προγραμματισμού και βασισμένη σε πρότυπα. Αυτό το γεγονός την κάνει κατάλληλη για να περιγράψει διεπαφές web services οι οποίες είναι προσβάσιμες από μία μεγάλη ποικιλία πλατφορμών και γλωσσών προγραμματισμού. Επιπλέον, εκτός του ότι περιγράφει τα περιεχόμενα των μηνυμάτων, η WSDL ορίζει πού είναι διαθέσιμη μία υπηρεσία και ποιά πρωτόκολλα επικοινωνίας χρησιμοποιούνται για επικοινωνία, με αυτή την υπηρεσία. Αυτό σημαίνει ότι ένα αρχείο WSDL ορίζει όλα όσα χρειάζονται για να γραφεί ένα πρόγραμμα το οποίο να λειτουργεί με ένα web service .



Εικόνα 5: Οι αλληλεπιδράσεις των ρόλων στο μοντέλο Ηλεκτρονικών Υπηρεσιών.

Η WSDL παρέχει ένα τρόπο στους παροχείς υπηρεσιών να περιγράφουν τη βασική μορφή των αιτήσεων και απαντήσεων των υπηρεσιών πάνω από διαφορετικά πρωτόκολλα και κωδικοποιήσεις. Ακόμα, χρησιμοποιείται για να περιγράψει τί μπορεί να κάνει ένα web service, πού βρίσκεται και πώς να το καλέσει κανείς. Οι κατάλογοι UDDI περιγράφουν πολλές πτυχές των web services, συμπεριλαμβανομένων και των λεπτομερειών σύνδεσης μίας υπηρεσίας. Η WSDL, ταιριάζει απόλυτα σε μια τέτοια περιγραφή μιας υπηρεσίας του UDDI<sup>10</sup>. Επίσης, στην WSDL, ορίζονται υπηρεσίες σαν συλλογές από τελικά σημεία δικτύου ή αλλιώς ports. Τέλος, ο περιγραφικός ορισμός των τελικών σημείων και των μηνυμάτων διαχωρίζεται από συγκεκριμένα δικτυακά πρωτόκολλα ή μορφές δεδομένων. Αυτό επιτρέπει την επαναχρησιμοποίηση των περιγραφικών ορισμών των μηνυμάτων (messages).

Τα μηνύματα είναι αόριστες περιγραφές των δεδομένων που ανταλλάσσονται και των τύπων τελικών σημείων (port types). Οι τύποι τελικών σημείων είναι συλλογές λειτουργιών. Το συγκεκριμένο πρωτόκολλο και ο ορισμός της μορφής των δεδομένων για ένα συγκεκριμένο τύπο τελικών σημείων δημιουργεί μία επαναχρησιμοποιούμενη σύνδεση (binding). Ένα τελικό σημείο (port) ορίζεται συνδέοντας μια διεύθυνση δικτύου με μία επαναχρησιμοποιούμενη σύνδεση (binding), και μία συλλογή τελικών σημείων ορίζουν μία υπηρεσία (service). Ως εκ τούτου, ένα έγγραφο WSDL χρησιμοποιεί τα παρακάτω στοιχεία για τον ορισμό δικτυακών υπηρεσιών<sup>10</sup>:

- ✓ Types - ένα περίβλημα για ορισμούς τύπων δεδομένων χρησιμοποιώντας ένα σύστημα τύπων (όπως για παράδειγμα το XML Schema).

- ✓ Message - ένας περιγραφικός ορισμός των δεδομένων που ανταλλάσσονται.
- ✓ Operation - μία περιγραφή μίας λειτουργίας που υποστηρίζεται από μία υπηρεσία
- ✓ Port Type - ένα περιγραφικό σύνολο από λειτουργίες που υποστηρίζονται από ένα ή περισσότερα τελικά σημεία.
- ✓ Binding - ένα συγκεκριμένο πρωτόκολλο και μορφή δεδομένων για ένα συγκεκριμένο τύπο τελικών σημείων (port type).
- ✓ Port - ένα μοναδικό τελικό σημείο που ορίζεται σαν συνδυασμός μίας σύνδεσης (binding) και μιας διεύθυνσης δικτύου.
- ✓ Service - μία συλλογή από σχετικά τελικά σημεία.

### 1.5.2 UDDI (Universal Description, Discovery and Integration)

Ο σκοπός που δίνει το OASIS (Organization for the Advancement of Structured Information Standards), για το Universal Description, Discovery and Integration<sup>11</sup> : “Τα web services έχουν νόημα μόνο όταν δυνητικοί χρήστες μπορούν να βρουν πληροφορίες ικανές ώστε να επιτρέψουν την εκτέλεσή τους. Το Universal Description Discovery & Integration (UDDI) εστιάζει στον καθορισμό ενός συνόλου από υπηρεσίες που θα υποστηρίζουν την περιγραφή και την ανακάλυψη:

- ✓ Των εταιριών, των οργανισμών και άλλων παρόχων web services.
- ✓ Των web services, που είναι διαθέσιμες.
- ✓ Και των τεχνικών διεπαφών οι οποίες μπορούν να χρησιμοποιηθούν ώστε να έχει κάποιος χρήστης πρόσβαση σε αυτές τις υπηρεσίες.

Βασισμένο σε ένα κοινό σύνολο από βιομηχανικά πρότυπα, συμπεριλαμβανομένων των HTTP, XML, XML Schema και SOAP το UDDI παρέχει μία διαλειτουργική, θεμελιώδη υποδομή για ένα περιβάλλον λογισμικού προσανατολισμένο στις υπηρεσίες τόσο για δημόσια διαθέσιμες υπηρεσίες όσο και για υπηρεσίες που εκτίθενται μόνο εσωτερικά ενός οργανισμού.”

Το UDDI,<sup>21</sup> είναι ο «χρυσός οδηγός» των web services. Όπως σε ένα χρυσό οδηγό, αναζητεί κανείς, μια εταιρία που προσφέρει πληροφορίες για μια προσφερόμενη υπηρεσία και τρόπο επικοινωνίας για περισσότερες λεπτομέρειες. Φυσικά, μπορεί να δημιουργηθεί ένα web service χωρίς να καταχωρηθεί στο UDDI, όπως αν ανοίξει μία επιχείρηση στο υπόγειο ενός σπιτιού και γίνει διαφήμιση από στόμα σε στόμα. Αλλά για το ευρύ κοινό, είναι αναγκαίο το UDDI<sup>2</sup> ώστε οι δυνητικοί πελάτες να μπορέσουν να βρουν τις προσφερόμενες υπηρεσίες .

#### *Υπηρεσίες του UDDI*

Το UDDI παρέχει ένα μηχανισμό στους πελάτες να βρίσκουν δυναμικά άλλα web services. Χρησιμοποιώντας μία διεπαφή UDDI, οι επιχειρήσεις μπορούν να συνδεθούν δυναμικά με υπηρεσίες που παρέχονται από εξωτερικούς συνεργάτες. Ένας κατάλογος UDDI (UDDI registry) είναι όμοιος με ένα CORBA trader, ή με μία υπηρεσία DNS, αλλά για εφαρμογές. Ένας κατάλογος UDDI, έχει δύο ειδών πελάτες : επιχειρήσεις που θέλουν να δημοσιεύσουν μια υπηρεσία και πελάτες που θέλουν να χρησιμοποιήσουν συγκεκριμένες υπηρεσίες και συνδέονται προγραμματιστικά με αυτές<sup>10</sup> .

Ο παρακάτω πίνακας 2, περιγράφει περιληπτικά τις προσφερόμενες υπηρεσίες του UDDI<sup>10</sup>.

Πληροφορία	Λειτουργίες	Λεπτομέρειες (υποστηρίζονται από το API)
<u>White pages:</u> Πληροφορίες όπως το όνομα, η διεύθυνση, το τηλέφωνο και άλλες πληροφορίες επικοινωνίας για μία επιχείρηση.	<u>Publish:</u> Πώς ο προμηθευτής ενός web service καταχωρεί των εαυτό του.	<u>Business Information:</u> Περιλαμβάνεται σε ένα αντικείμενο, <u>BusinessEntity</u> , το οποίο με τη σειρά του περιλαμβάνει πληροφορίες για υπηρεσίες, κατηγορίες, επαφές, URLs, και άλλα αναγκαία στοιχεία για να αλληλεπιδράσουμε με μία επιχείρηση.
<u>Yellow Pages:</u> Πληροφορίες που κατηγοριοποιούν επιχειρήσεις. Βασίζονται σε υπάρχοντα πρότυπα κατηγοριοποίησης (μη ηλεκτρονικά).	<u>Find:</u> Πώς μία εφαρμογή βρίσκει ένα συγκεκριμένο web service.	<u>Service Information:</u> Περιγράφει μία ομάδα από web services. Αυτές περιλαμβάνονται σε ένα αντικείμενο <u>BusinessService</u> .
<u>Green Pages:</u> Τεχνικές πληροφορίες για τα web services που παρέχονται από μία επιχείρηση.	<u>Bind:</u> Πώς μία εφαρμογή συνδέεται, και αλληλεπιδρά με ένα web service αφού αυτό βρεθεί.	<u>Binding Information:</u> Οι απαραίτητες τεχνικές λεπτομέρειες για την κλήση ενός web service. Περιλαμβάνουν τα URLs, πληροφορίες για ονόματα μεθόδων, τύπους ορισμάτων και ούτω καθεξής. Το αντικείμενο <u>BindingTemplate</u> αναπαριστά αυτά τα δεδομένα. <u>Service Specification Detail:</u> Πρόκειται για μεταδεδομένα για διάφορες προδιαγραφές που υλοποιούνται από ένα web service. Αυτά καλούνται <u>tModels</u> .

Πίνακας 2: Υπηρεσίες UDDI

### 1.5.3 SOAP (Simple Object Access Protocol)

Το W3C από τον Ιούνιο του 2003 έχει συντάξει μία σύσταση (recommendation) η οποία είναι ότι πιο κοντινό υπάρχει στην προδιαγραφή (specification) του Simple Object Access Protocol v1.2. Μέσα στη σύσταση αυτή βρίσκεται ο παρακάτω ορισμός<sup>12</sup>: “*To SOAP στην έκδοση 1.2 είναι ένα ελαφρύ πρωτόκολλο προορισμένο για την ανταλλαγή δομημένων πληροφοριών σε ένα αποκεντρωμένο, διανεμημένο περιβάλλον. Χρησιμοποιεί τεχνολογίες XML για να καθορίσει ένα επεκτάσιμο πλαίσιο παρέχοντας μια δομή μηνυμάτων η οποία μπορεί να ανταλλαχθεί πάνω από ποικίλα δικτυακά πρωτόκολλα. Το πλαίσιο έχει σχεδιαστεί να είναι ανεξάρτητο από οποιοδήποτε προγραμματιστικό μοντέλο και σημασιολογία υλοποίησης.*”

Δύο βασικοί στόχοι του σχεδιασμού του SOAP, είναι η απλότητα και η επεκτασιμότητα. Το SOAP προσπαθεί να πετύχει αυτούς τους στόχους παραλείποντας, από το πλαίσιο μηνυμάτων, χαρακτηριστικά γνωρίσματα τα οποία συνήθως συναντούνται σε καταναμημένα συστήματα. Μερικά από αυτά τα γνωρίσματα είναι, η «αξιοπιστία» (reliability), η «ασφάλεια» (security), ο «συσχετισμός» (correlation), η «δρομολόγηση» (routing) και τα «σχέδια ανταλλαγής μηνυμάτων» (Message Exchange Patterns - MPEs).

Τα κύρια χαρακτηριστικά του είναι:

- ✓ Απλό και επεκτάσιμο
- ✓ Βασισμένο στη γλώσσα XML
- ✓ Ανεξάρτητο πρωτοκόλλου, λειτουργικού συστήματος και γλώσσας προγραμματισμού
- ✓ Το SOAP με το HTTP είναι το πιο συχνά χρησιμοποιούμενο
- ✓ Απομακρυσμένη κλήση μεθόδων (Remote Procedure Call - RPC) ή ασύγχρονη αποστολή μηνυμάτων (asynchronous message style).

Το SOAP είναι ένα πρωτόκολλο βασισμένο στην XML το οποίο επιτρέπει στις εφαρμογές να ανταλλάσσουν πληροφορία πάνω από κοινώς χρησιμοποιούμενα πρωτόκολλα του διαδικτύου.

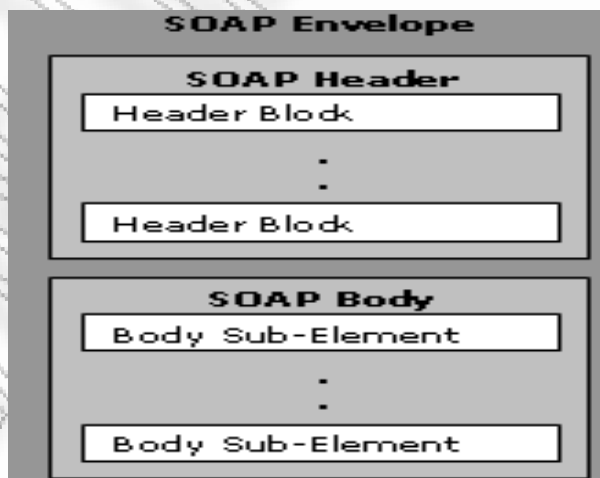
### Δομή ενός μηνύματος SOAP

Ένα μήνυμα SOAP είναι ένα συνηθισμένο έγγραφο XML το οποίο περιέχει τα παρακάτω στοιχεία (elements)<sup>14</sup>:

- ✓ Ένα απαιτούμενο στοιχείο **Envelope** από το οποίο αναγνωρίζεται το έγγραφο XML ως μήνυμα SOAP.
- ✓ Ένα προαιρετικό στοιχείο **Header** που περιλαμβάνει βοηθητικές πληροφορίες.
- ✓ Ένα απαιτούμενο στοιχείο **Body** το οποίο περιλαμβάνει την κύρια πληροφορία του μηνύματος.
- ✓ Ένα προαιρετικό στοιχείο **Fault** το οποίο παρέχει πληροφορίες για σφάλματα που προκλήθηκαν κατά την επεξεργασία ενός μηνύματος.

Όλα τα παραπάνω στοιχεία δηλώνονται στο προεπιλεγμένο namespace για το SOAP envelope : <http://www.w3.org/2003/05/soap-envelope>. Το προεπιλεγμένο namespace για την κωδικοποίηση του SOAP και τους τύπους δεδομένων είναι ο: <http://www.w3.org/2001/12/soap-encoding>.<sup>14</sup> Μερικοί σημαντικοί κανόνες σύνταξης είναι οι παρακάτω :

- ✓ Ένα μήνυμα SOAP ΠΡΕΠΕΙ να είναι κωδικοποιημένο χρησιμοποιώντας XML.
- ✓ Ένα μήνυμα SOAP ΠΡΕΠΕΙ να χρησιμοποιεί το SOAP Envelope namespace.
- ✓ Ένα μήνυμα SOAP ΠΡΕΠΕΙ να χρησιμοποιεί το SOAP Encoding namespace.
- ✓ Ένα μήνυμα SOAP ΔΕΝ ΠΡΕΠΕΙ να περιέχει αναφορά σε DTD.
- ✓ Ένα μήνυμα SOAP ΔΕΝ ΠΡΕΠΕΙ να περιέχει XML Processing Instructions.



Εικόνα 6: Δομή Μηνύματος SOAP

## SOAP Envelope<sup>12</sup>

Το SOAP Envelope είναι το στοιχείο που περικλείει όλα τα υπόλοιπα στοιχεία σε ένα μήνυμα SOAP. Η ύπαρξη του ως αρχικού στοιχείου (root element) ενός εγγράφου XML σηματοδοτεί ότι πρόκειται για μήνυμα SOAP.

Για το SOAP Envelope είναι απαραίτητα τα εξής:

- ✓ Το όνομα του στοιχείου πρέπει να είναι Envelope.
- ✓ Το όνομα του namespace του να είναι: <http://www.w3.org/2003/05/soap-envelope>
- ✓ Να περιέχει μηδέν ή περισσότερες ιδιότητες ορισμένες με namespace.
- ✓ Να περιέχει ένα ή δύο στοιχεία-παιδιά με την εξής σειρά:
  - Ένα προαιρετικό στοιχείο Header
  - Ένα απαραίτητο στοιχείο Body

## SOAP Encoding Rules

Σε ένα SOAP message μπορούν να χρησιμοποιηθούν οι κοινοί τύποι δεδομένων XSD types: int, String, date. π.χ. `<age xsi:type="xsd:int">66</age>`

Πιο πολύπλοκες δομές δεδομένων περιγράφονται σε ένα σχήμα XML. Η διαδικασία της μετάφρασης των δεδομένων σε XML καλείται κωδικοποίηση (encoding). `encodingStyle=http://schemas.xmlsoap.org/soap/encoding/`

Το χαρακτηριστικό `encodingStyle`, δείχνει πως τα δεδομένα αναπαρίστανται στο μήνυμα. Αυτό το χαρακτηριστικό, μπορεί να εμφανιστεί οπουδήποτε μέσα στο μήνυμα, αλλά συνήθως εμφανίζεται στο φάκελο (Envelope).

## SOAP Messages<sup>19</sup>

```
<soap:Envelope
xmlns:soap=http://schemas.xmlsoap.org/soap/envelope/
soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
```

Το πρόθεμα του namespace «soap» χρησιμοποιείται στα περισσότερα πεδία ενός SOAP μηνύματος. Σε αυτό το παράδειγμα αυτό το πρόθεμα σχετίζεται με το namespace URL: <http://schemas.xmlsoap.org/soap/envelope/>, και αναγνωρίζει τα πεδία που είναι μέρος ενός τυπικού SOAP μηνύματος. Όπως όλα τα προθέματα namespace, η επιλογή του soap είναι τυχαία. Έτσι για παράδειγμα, αντί για «soap» οτιδήποτε άλλο μπορεί να χρησιμοποιηθεί για πρόθεμα όπως για παράδειγμα:

```
<blah:Envelope xmlns:blah="http://schemas.xmlsoap.org/soap/envelope/"
blah:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
```

Το namespace του εγγράφου SOAP, μπορεί να παραληφθεί εντελώς όταν αυτό που χρησιμοποιείται είναι το τυπικό για το έγγραφο. Αυτό δηλώνεται με τη χρήση του χαρακτηριστικού `xmlns`.

<sup>27</sup>  
Παράδειγμα :

---

```
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
```

---

Ένα Namespace για το Envelope, είναι το URL "http://schemas.xmlsoap.org/soap/envelope/". Μηνύματα που δε χρησιμοποιούν αυτό το namespace, είναι άκυρα και οπότε αυτοί που τα λαμβάνουν επιστρέφουν λάθος. Η επικεφαλίδα δεν είναι υποχρεωτική σε ένα SOAP μήνυμα. Εάν υπάρχει, τότε αυτή είναι το πρώτο παιδί μετά το χαρακτηριστικό Envelope. Το κυρίως σώμα, όταν υπάρχει επικεφαλίδα ακολουθεί την επικεφαλίδα, αλλιώς είναι το πρώτο παιδί μετά το χαρακτηριστικό Envelope.

---

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
```

```
<soap:Header>.....</soap:Header>      <soap:Body>.....</soap:Body>
</soap:Envelope>
```

---

### ***SOAP και άλλα πρωτόκολλα ανταλλαγής μηνυμάτων***

Πριν ανακαλυφθεί το SOAP υπήρχανε και άλλες κατανεμημένες τεχνολογίες, τόσο για ανταλλαγή μηνυμάτων όσο και για απομακρυσμένη κλήση διαδικασιών (remote procedure call).

Για την καλύτερη ανάδειξη των πλεονεκτημάτων του SOAP, εξετάζονται και οι άλλες τεχνολογίες (επιφανειακά) φανερώνοντας τα πλεονεκτήματα και τα μειονεκτήματα της κάθε μιας και τα οποία οδήγησαν στη δημιουργία αυτού του πρωτοκόλλου<sup>13</sup>.

### ***Χρήσεις του SOAP***

Το πρωτόκολλο SOAP χρησιμοποιείται συχνά ως πρωτόκολλο για απομακρυσμένες κλήσεις (Remote Procedure Calls - RPC), πάνω από το πρωτόκολλο Hypertext Transfer Protocol (HTTP). Η χρήση του SOAP, με το πρωτόκολλο HTTP δεν είναι υποχρεωτική και επιπλέον το SOAP υποστηρίζει και άλλα μοντέλα πλην του μοντέλου αίτηση / απάντηση.

Το SOAP, μπορεί να χρησιμοποιηθεί με κάθε πρωτόκολλο που υποστηρίζει τη μεταφορά XML δεδομένων από τον αποστολέα στο παραλήπτη. Η Microsoft και η IBM έχουν υλοποιήσει μηνύματα SOAP, πάνω από το πρωτόκολλο SMTP, που σημαίνει ότι τα μηνύματα SOAP, μπορούν να δρομολογηθούν μέσω e-mail servers.

Το κατώτερο επίπεδο του SOAP, είναι ένα ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων που μπορεί να χρησιμοποιηθεί για την αποστολή μηνυμάτων μεταξύ δύο ή περισσότερων σημείων.

Κύριος στόχος του SOAP είναι, η παροχή ενός κοινού τρόπου για το πακετάρισμα των δεδομένων των μηνυμάτων και ο καθορισμός κανόνων για τη κωδικοποίηση και αποκωδικοποίηση των δεδομένων κατά τη μεταφορά.

### ***Λειτουργικότητα του SOAP***

Εξετάζοντας τις παραπάνω τεχνολογίες, υπάρχουν σε κάθε περίπτωση κάποια από τα παρακάτω μειονεκτήματα:

- ✓ Κόστος υποδομής (EDI, CORBA)

- ✓ Κόστος και πολυπλοκότητα υλοποίησης (EDI, CORBA)
- ✓ Χρήση μόνο σε ιδιωτικά δίκτυα (EDI, CORBA, DCOM, RMI)
- ✓ Χρήση μόνο σε εφαρμογές που εκτελούνται στην ίδια πλατφόρμα (DCOM)
- ✓ Χρήση μόνο σε εφαρμογές γραμμένες στην ίδια γλώσσα προγραμματισμού (RMI)
- ✓ Μειωμένες λειτουργίες (XML-RPC)
- ✓ Έλλειψη ευελιξίας (EDI, CORBA, DCOM, RMI)

Στην προσπάθεια δημιουργίας του SOAP, λήφθηκαν υπόψη όλα τα παραπάνω και δημιουργήθηκε ένα πρωτόκολλο με τα εξής χαρακτηριστικά:

- ✓ Το SOAP είναι απλό. Άρα το κόστος και η πολυπλοκότητα υλοποίησης μειώνονται αισθητά.
- ✓ Το SOAP είναι ανεξάρτητο από πλατφόρμα και γλώσσα προγραμματισμού, οπότε μπορεί να χρησιμοποιηθεί για επικοινωνία μεταξύ εφαρμογών γραμμένων για διαφορετικές πλατφόρμες και σε διαφορετικές γλώσσες προγραμματισμού.
- ✓ Το SOAP είναι ευέλικτο. Χρησιμοποιεί πρότυπα πρωτόκολλα, όπως το HTTP και το SMTP ως μέσα μεταφοράς, οπότε μπορεί να χρησιμοποιηθεί στο διαδίκτυο και να διαπερνά τύχη προστασίας (firewalls) χωρίς συμβιβασμούς στην ασφάλεια της υποδομής μιας επιχείρησης. Αυτό αυτομάτως, μειώνει και σε ορισμένες περιπτώσεις εξαλείφει το κόστος υποδομής, αφού οι περισσότερες επιχειρήσεις σήμερα έχουν και τον εξοπλισμό και την τεχνογνωσία για τη χρήση του διαδικτύου.
- ✓ Το SOAP είναι επεκτάσιμο. Αν και δεν προσφέρει τόσες πολλές λειτουργίες όσο άλλες τεχνολογίες, όπως το CORBA και το DCOM επιτρέπει σε άλλα πρότυπα να το επεκτείνουν παρέχοντας υπηρεσίες που λείπουν από αυτό. Αυτό το χαρακτηριστικό αποδείχθηκε ίσως το σημαντικότερο, γιατί επάνω του βασίζονται πολλές αναπτυσσόμενες τεχνολογίες των web services που προσφέρουν υπηρεσίες όπως «αξιοπιστία» (reliability), «δρομολόγηση» (routing) και «ασφάλεια» (security).

## 1.6 Εφαρμογές των Ηλεκτρονικών Υπηρεσιών και Παραδείγματα <sup>18</sup>

Αρχικά τα web services, ήταν πηγές πληροφορίας τις οποίες μπορεί κανείς πολύ εύκολα να ενσωματώσει στις εφαρμογές του, όπως για παράδειγμα, τιμές μετοχών, προβλέψεις καιρού, αποτελέσματα αθλητικών παιχνιδιών. Είναι εύκολο να φανταστεί κανείς, μια ολόκληρη κατηγορία εφαρμογών που μπορεί να κατασκευάσει, ώστε να αναλύει και να συνδυάζει πληροφορία που τον ενδιαφέρει και να την παρουσιάζει με ποικίλους τρόπους. Για παράδειγμα, λογιστικό φύλλο, το οποίο συνοψίζει όλη την οικονομική εικόνα: μετοχές, τραπεζικούς λογαριασμούς, δάνεια και άλλα. Αν αυτή η πληροφορία, ήταν διαθέσιμη μέσω web services, το λογιστικό φύλλο, θα μπορούσε να ενημερώνεται συνεχώς. Οι περισσότερες από αυτές τις πληροφορίες, είναι ήδη διαθέσιμες στον παγκόσμιο ιστό, αλλά τα web services υλοποιούν την προγραμματιστική πρόσβαση σε αυτές πιο εύκολα και πιο αξιόπιστα <sup>2</sup>.

Μια άλλη εφαρμογή, θα μπορούσε να είναι μία εφαρμογή προμηθειών, η οποία να παίρνει αυτόματα τιμές από προμηθευτές, να επιστρέφει στο χρήστη να επιλέξει προμηθευτή, να υποβάλει την παραγγελία και να παρακολουθεί την αποστολή, έως ότου να γίνει η παραλαβή της. Η εφαρμογή του προμηθευτή, εκτός από το να εκθέτει τις υπηρεσίες της στον ιστό, θα μπορούσε να χρησιμοποιήσει άλλα web services, για να ελέγξει την πιστοληπτική ικανότητα του πελάτη, να χρεώσει τον τραπεζικό λογαριασμό του πελάτη και να καθορίσει την αποστολή με μια εταιρία μεταφορών <sup>2</sup>.

Στο άμεσο μέλλον, μερικά από τα πιο ενδιαφέροντα web services θα υποστηρίζουν εφαρμογές που χρησιμοποιούν τον ιστό για να πραγματοποιήσουν διεργασίες που δεν μπορούν να γίνουν σήμερα. Για παράδειγμα, μία από τις υπηρεσίες που τα web services εμφανίζονται υλοποιήσιμα, είναι η υπηρεσία ημερολογίου. Αν ένας οδοντίατρος ή ένας μηχανικός εξέθεταν τα ημερολόγιά τους μέσω μιας τέτοιας web service, θα μπορούσαν οι πελάτες τους να προγραμματίσουν τα ραντεβού τους ή θα μπορούσαν να προγραμματίσουν αυτοί τα ραντεβού κατευθείαν στο δικό τους ημερολόγιο. Έτσι, μπορούν να σχεδιαστούν εκατοντάδες εφαρμογές οι οποίες μπορούν να κατασκευαστούν, όταν θα δοθεί η δυνατότητα να προγραμματισμού τον ιστό<sup>2</sup>. Υπάρχει μία μεγάλη λίστα από έτοιμα web services, που θα μπορούσε να χρησιμοποιήσει κανείς, ακόμα και εντελώς δωρεάν.<sup>17</sup> Ψάχνοντας για παράδειγμα στη διεύθυνση <http://www.webservicelist.com> υπάρχει, μία πληθώρα από web services συνοδευόμενα από το wsdl file καθώς και με on-line demo της λειτουργίας τους. Στον πίνακα 3 που ακολουθεί, αναγράφονται κάποια ενδεικτικά από την παραπάνω διεύθυνση:

Web Service	Λειτουργία	URL
<b>BN Quote Service</b>	Δέχεται το ISBN ενός βιβλίου και επιστρέφει την τιμή του	<a href="http://www.xmethods.com/help/addspecs.html">http://www.xmethods.com/help/addspecs.html</a>
<b>Rich Credit Card Validator</b>	Ελέγχει τα στοιχεία μίας πιστωτικής κάρτας αν αντιστοιχούν σε υπάρχουσα πιστωτική.	<a href="http://www.richsolutions.com">http://www.richsolutions.com</a>
<b>SOAP SMS</b>	Στέλνει κείμενα των χρηστών ως sms σε κινητά.	<a href="http://www.redcoal.com">http://www.redcoal.com</a>
<b>Google Web Service</b>	Απαντά σε ερωτήσεις εύρεσης σελίδων και επιστρέφει τα αποτελέσματα σε μορφή επεξεργάσιμη.	<a href="http://www.google.com/apis">http://www.google.com/apis</a>
<b>FreshScore</b>	Δίνει τα αποτελέσματα των αγώνων σε πραγματικό χρόνο.	<a href="http://www.freshscore.com">http://www.freshscore.com</a>

22, 23, 24, 25, 26

Πίνακας 3: Εφαρμογές Ηλεκτρονικών Υπηρεσιών αξιόπιστη

### **RSS - Really Simple Syndication**

Η τεχνολογία RSS (Really Simple Syndication) αποτελεί έναν απλό τρόπο για την αποστολή πληροφοριών από μια ιστοσελίδα, χωρίς να χρειάζεται ο χρήστης να μπαίνει στη διαδικασία συχνών επισκέψεων και αναζήτησης των πληροφοριών αυτών από την ιστοσελίδα. 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 στον



υπολογιστή του. Συγκεκριμένα, το RSS είναι ένα format ανταλλαγής περιεχομένου βασισμένο στη γλώσσα XML. Κάθε κανάλι RSS αποτελείται από μία λίστα στοιχείων που περιέχουν έναν τίτλο καθώς και το σύνδεσμο προς την αντίστοιχη ιστοσελίδα. Οι πιο συνηθισμένοι τρόποι χρήσης του είναι:

- ✓ **Χρησιμοποιώντας ένα πρόγραμμα ανάγνωσης ειδήσεων (News Aggregator):** Τα προγράμματα ανάγνωσης ειδήσεων, είναι αυτόνομες εφαρμογές, οι οποίες ανακτούν και εμφανίζουν τα περιεχόμενα των καναλιών τροφοδοσίας RSS (RSS feeds) που ο χρήστης έχει επιλέξει. Προκειμένου ο χρήστης να προσθέσει κάποια κατηγορία στο πρόγραμμα ανάγνωσης ειδήσεων που χρησιμοποιεί, με δεξί κλικ σε κάποια από τις κατηγορίες που υπάρχουν στο γκρι πλαίσιο και επιλέγοντας "Αντιγραφή συντόμευσης" (Copy shortcut), και Επικόλληση (Paste) της συντόμευσης στο πεδίο διευθύνσεων του προγράμματος.
- ✓ **Ενσωματώνοντας το RSS feed σε προσωπικό weblog:** Ένας άλλος τρόπος χρήσης της υπηρεσίας, είναι να ενσωματώσει ο χρήστης το περιεχόμενο του feed στο προσωπικό του web log (ή blog). Τα web logs, είναι προσωπικές σελίδες που δημιουργούν οι χρήστες και εμφανίζουν περιεχόμενο που ανανεώνεται συχνά. Εξάλλου, η συγκεκριμένη τεχνολογία έκανε για πρώτη φορά την εμφάνισή της στα web logs, ως ένας τρόπος για τους χρήστες να παρακολουθούν τις εξελίξεις στα blogs της προτίμησής τους, χωρίς να χρειάζεται να ερευνούν για ανανεώσεις. Σύντομα όμως επεκτάθηκε και πέραν των blogs, συμπεριλαμβανομένων και ορισμένων από τους μεγαλύτερους οργανισμούς μέσω μαζικής ενημέρωσης στην Ευρώπη, που πλέον κωδικοποιούν το περιεχόμενό τους σε format, που επιτρέπει την ανάγνωσή του από το λογισμικό των προγραμμάτων Atom και RSS.
- ✓ **Το απαραίτητο λογισμικό:** Για να ενημερώνεται κανείς συνεχώς για την αλλαγή του περιεχομένου, χρειάζεται ειδικό λογισμικό - aggregator ή news reader. Μπορεί κανείς να κατεβάσει ένα πρόγραμμα aggregator από το Διαδίκτυο. Στη συνέχεια, ο χρήστης έχει τη δυνατότητα να ζητήσει από τον aggregator να συγκεντρώνει όλες τις ανανεώσεις σχετικά με ένα συγκεκριμένο θέμα από μία ιστοσελίδα ή λίστα ιστοσελίδων, προβαίνοντας σε αναζήτηση στο Διαδίκτυο ανά τακτά χρονικά διαστήματα.

Παρ' όλα αυτά, οι aggregators δεν έχουν τη δυνατότητα να συγκεντρώνουν πληροφορίες από κάθε ιστοσελίδα με τον τρόπο που συγκεντρώνει τις πληροφορίες το Google ή οποιαδήποτε άλλη μηχανή αναζήτησης όταν εισάγει κανείς μια λέξη - κλειδί. Οι aggregators μπορούν να "σκανάρουν" τις ιστοσελίδες που έχουν κωδικοποιήσει το περιεχόμενό τους, βάσει της τεχνολογίας XML (extensible markup language). Τα προγράμματα aggregator είναι παρόμοια με το λογισμικό ηλεκτρονικού ταχυδρομείου. Οι χρήστες μπορούν να δημιουργήσουν φακέλους διαφορετικών κατηγοριών - ειδήσεις, επιχειρήσεις, τεχνολογία - που θα τροφοδοτούνται με πληροφορίες ανά τακτά χρονικά διαστήματα.

Για τους προσωπικούς υπολογιστές (PCs) υπάρχουν πολλά τέτοιου είδους προγράμματα, όπως το FeedDemon της Bradbury Software ή το NewzCrawler της ρωσικής εταιρίας ADC Software. Και τα δύο προγράμματα, προορίζονται για προσωπικούς υπολογιστές με λειτουργικό σύστημα Windows. Για το σύστημα Macintosh της Apple Computers, μεταξύ των διαθέσιμων προγραμμάτων, συγκαταλέγονται το NetNewsWire της αμερικανικής Ranchero Software και το Shrook 2, της βρετανικής Shrook.

Η βοήθεια του RSS μπορεί να αποδειχθεί πολύτιμη. Πρόκειται για ένα format, που επιτρέπει στο χρήστη να τροφοδοτήσει άλλους με πληροφορίες - ενημερωτικό περιεχόμενο ιστοσελίδων, μια online εφημερίδα, ειδήσεις. Η "τροφοδοσία" εμφανίζεται σε προγράμματα που αποκαλούνται news readers και μοιάζουν αρκετά με προγράμματα ηλεκτρονικού ταχυδρομείου.

Τα "δυνατά σημεία" του RSS, είναι η απλότητα και η πολυχρηστικότητα του. Μπορεί να ενταχθεί ως επιπρόσθετο σε άλλα προγράμματα - browsers, Microsoft Outlook ή κάποιο άλλο πρόγραμμα e-mail - ή μπορεί να αποσταλεί σε κινητό τηλέφωνο, υπολογιστή παλάμης ή ακόμη και σε MP3 player. Είναι πολύ πιο ισχυρό από το e-mail και - με λίγη τύχη - εγγυάται πως ο χρήστης θα παραμείνει ανενόχλητος από τα spams.

### **Παραδείγματα RSS feeds**

- ✓ Go-Online.gr: Ο κόμβος του Δικτυωθείτε προσφέρει ήδη το περιεχόμενο των Αφιερωμάτων η-επιχειρείν και των Ειδήσεων του μέσω RSS για κάθε ενδιαφερόμενο. Το κανάλι RSS του κόμβου είναι διαθέσιμο στην ηλεκτρονική διεύθυνση: <http://www.go-online.gr/rss.xml><sup>35</sup>. Η υπηρεσία παρέχεται δωρεάν.
- ✓ Ναυτεμπορική: Οι ειδήσεις της εφημερίδας - Η Ναυτεμπορική - είναι από τις αρχές του 2004 διαθέσιμες μέσω της υπηρεσίας "RSS feeds". Συγκεκριμένα, το πλήρες περιεχόμενο ενός άρθρου είναι διαθέσιμο στην ιστοσελίδα της εφημερίδας (<http://www.naftemporiki.gr/news/rss.asp>)<sup>36</sup> και είναι προσβάσιμο μέσω της υπηρεσίας "RSS feeds". Μέσω αυτής της υπηρεσίας, μπορεί να λαμβάνει ο χρήστης τους τίτλους των ειδήσεων της εφημερίδας δωρεάν και να τους ενσωματώνει στο πρόγραμμα ανάγνωσης ειδήσεων που χρησιμοποιεί ή στο προσωπικό του weblog.
- ✓ Διαθέσιμα κανάλια από τη Ναυτεμπορική: Newsroom, Οικονομία, Πολιτικά, Ελλάδα, Κόσμος, Επιχειρήσεις, Αγορές, Ναυτιλία, The Wall Street Journal, Απόψεις, Κόσμος, Αθλητικά, Πολιτιστικά, Media.

### **BBC News**

Το ειδησεογραφικό δίκτυο του BBC προσφέρει μέσω του δικτυακού του τόπου υπηρεσία τροφοδοσίας ειδήσεων στην αγγλική γλώσσα μέσω RSS, και συγκεκριμένα τις κατηγορίες:

News Front Page, World, UK, England, Northern Ireland, Scotland, Wales, Business, Politics, Health, Education, Science/Nature, Technology, Entertainment, Have Your Say, Magazine, Week At a Glance, Programmes.

### **1.7 Βιβλιογραφία 1<sup>ο</sup> Κεφαλαίου**

1. <http://www-128.ibm.com/developerworks/webservices/newto/websvc.html> IBM (2007), "New to SOA and Web services"
2. <http://msdn2.microsoft.com/en-us/library/ms996507.aspx> MSDN (2001), "XML Web Services Basics"
3. <http://www.roseindia.net/webservices/webservices.shtml> Roseindia.net (2007), "Web Services"
4. Developer.com (2003), "Web Services Tutorial: Understanding XML and XML Schema" "Part 1" <http://www.developer.com/services/print.php/2195981> "Part 2" [http://www.developer.com/services/print.php/10928\\_2195981\\_2](http://www.developer.com/services/print.php/10928_2195981_2)
5. Developer.com (2002), "Introduction to Web Services" "Part 1" <http://www.developer.com/services/article.php/1485821> "Part..2Architecture" <http://www.developer.com/services/article.php/1495091>

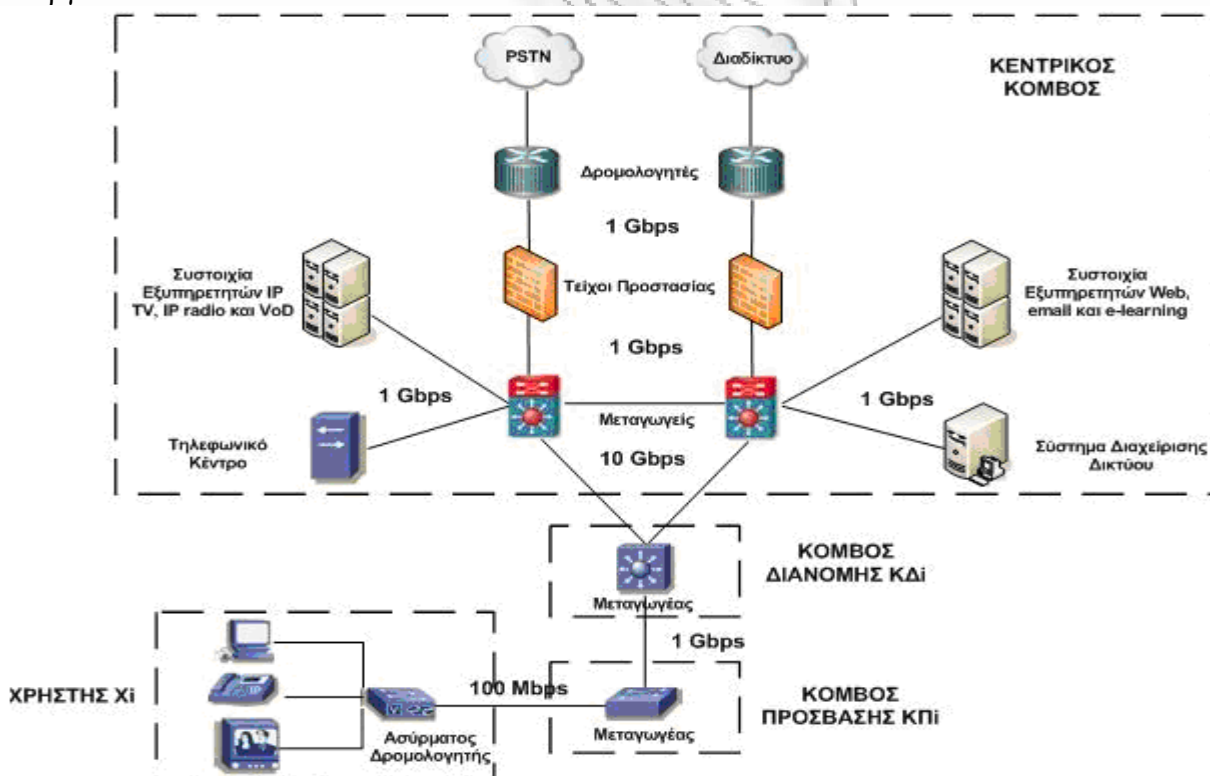
- “Part 3: Understanding XML” <http://www.developer.com/services/article.php/1557871>
6. <http://www.onjava.com/lpt/a/1025> ONJava.com (2001), “Java and Web Services Primer”
  7. Horton I. (2003) “Beginning Java 2” : Wrox
  8. <http://www.w3schools.com/xml/default.asp> W3schools.com (2007), “XML Tutorial”
  9. <http://www.w3.org/TR/wsdl> W3C (2001), “Web Service Definition Language (WSDL)”
  10. <http://onjava.com/pub/a/onjava/2001/08/07/webservices.html> XML.com (by Al Saganich 08/07/2001), “A Web Services Primer”
  11. [http://uddi.org/pubs/uddi\\_v3.htm](http://uddi.org/pubs/uddi_v3.htm) UDDI.org (2004), “UDDI Version 3.0.2”
  12. W3C (2006), “SOAP Version 1.2”  
“Part 0: Primer” <http://www.w3.org/TR/2006/PER-soap12-part0-20061219/>  
Part 1: Messaging Framework” <http://www.w3.org/TR/soap12-part1/>  
Part 2: Adjuncts” <http://www.w3.org/TR/2003/REC-soap12-part2-20030624/>
  13. Borgen B. (2001) “SOAP Programming with Java” : Sybex Inc
  14. <http://www.w3schools.com/soap/default.asp> W3schools.com (2007), “SOAP Tutorial”
  15. Newcomer E., Lomow G (2005) “Understanding SOA with Web Services” : Addison-Wesley Professional
  16. Fremantle, P., Weerawarana, S., and Khalaf, R. Enterprise Services, Communications of the ACM, October 2002/Vol.45.No 10, pp.77-82.
  17. <http://www.webserviceslist.com/> Εφαρμογές ηλεκτρονικών υπηρεσιών
  18. [http://myweb.fsu.edu/chofacker/pubs/Hofacker\\_Goldsmith\\_Bridges\\_Swilley\\_2007.pdf](http://myweb.fsu.edu/chofacker/pubs/Hofacker_Goldsmith_Bridges_Swilley_2007.pdf) , C, Hofacker etc, Journal of Value Chain Management, 2007, e-services.
  19. <http://www.disi.unige.it> ,  
<http://www.disi.unige.it/person/ReggioG/ISII04WWW/WebServices.ppt> , C, Peraire and D Coleman, HP
  20. An Overview of Standards and related technology in Web Services, A. Tsalgatidou, Th. Pilioura, Distributed and Parallel Databases, 2002
  21. Understanding SOA with Web Services, Eric Newcomer, Greg Lomow, Addison Wesley Professional, 2004.
  22. <http://www.xmethods.com/help/addspecs.html>
  23. <http://www.richsolutions.com>
  24. <http://www.redcoal.com>
  25. <http://www.google.com/apis>
  26. <http://www.freshscore.com/>
  27. <http://schemas.xmlsoap.org/soap/encoding/>
  28. <http://javascript.internet.com/>
  29. <http://www.microsoft.com/net/>
  30. <http://www.acunetix.com/websitesecurity/xss.htm>
  31. <http://msdn.microsoft.com/en-us/library/ms161953.aspx>
  32. [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci549024,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html)
  33. <http://www.ibm.com/developerworks/xml/library/x-transws/>
  34. <http://www.go-online.gr/rss.xml>
  35. <http://www.naftemporiki.gr/news/rss.asp>

## ΚΕΦΑΛΑΙΟ 2

### ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

Η τεράστια ανάπτυξη του διαδικτύου οδηγεί καθημερινά στην μετατροπή των δεδομένων του φυσικού κόσμου σε ψηφιακή - ηλεκτρονική μορφή. Καθώς σχεδόν οποιαδήποτε υπηρεσία ή οργανισμός, ιδρύματα, εταιρείες και ιδιώτες, χρησιμοποιούν υπολογιστές με πρόσβαση στο διαδίκτυο τις περισσότερες φορές για την διαχείριση των δεδομένων τους, η αξία της πληροφορίας που συγκεντρώνεται στο διαδίκτυο αποκτά τεράστιες διαστάσεις και γίνεται ένα θέμα που ολοένα και περισσότερο συζητιέται. Σε πολλές περιπτώσεις μάλιστα, ολόκληρη η πληροφορία είναι αποθηκευμένη σε ψηφιακά μέσα, χωρίς να υπάρχει σε έντυπη ή αναλογική μορφή.

Η εξάρτηση από τα συστήματα αυτά, και το γεγονός ότι η λειτουργικότητα και η φιλικότητα των υπολογιστικών συστημάτων έχουν αυξηθεί σημαντικά, οδηγούν σε μια ενισχυμένη πολυπλοκότητα των συστημάτων αυτών. Η πολυπλοκότητα αυτή οδηγεί σε μια πληθώρα αδυναμιών και προβλημάτων στην ασφάλεια των συστημάτων και των δεδομένων, είτε από προγραμματιστικά λάθη, είτε από κακές ρυθμίσεις, είτε από τις σχέσεις εμπιστοσύνης που δημιουργούνται.



Εικόνα 7: Γενική Τοπολογία Δικτύου

Στην παραπάνω εικόνα 7, απεικονίζεται μία γενική τοπολογία ενός δικτύου και παρατηρούνται κάποια απαραίτητα στοιχεία που πρέπει να υπάρχουν σε ένα δίκτυο, καθώς και την θέση όπου θα πρέπει να τοποθετούνται, ώστε να έχουν ως κύριο σκοπό τους την ασφάλεια.

Μερικά από αυτά είναι ο δρομολογητής, το τείχος προστασίας, ο μεταγωγέας, οι κεντρικοί υπολογιστές καθώς και οι υπολογιστές των χρηστών του δικτύου.

Ο πληθυσμός του Διαδικτύου, αν και έχει ακουστά πολλές περιπτώσεις παραβίασης της ασφάλειας συστημάτων και κλοπής δεδομένων, δεν έχει δεχτεί μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν την δικτυακή ασφάλεια. Οι περισσότεροι χρήστες, βρίσκονται σε σύγχυση όσον αφορά την ασφάλεια των δεδομένων τους, μην γνωρίζοντας τους κινδύνους και τις απειλές που αντιμετωπίζουν.

Οι επιθέσεις στο Διαδίκτυο, αυξάνονται συνεχώς και η προσπάθεια για τον περιορισμό τους οδήγησε στην ανάγκη απόκτησης εξειδικευμένης γνώσης για τα γεγονότα που διαδραματίζονται σε ένα δίκτυο. Αν και οι μέθοδοι και τα εργαλεία για την προστασία των συστημάτων βελτιώνονται συνεχώς, ο αριθμός των επιτυχημένων επιθέσεων συνεχώς αυξάνει. Σε αυτό, μεγάλο ρόλο παίζει η πολυπλοκότητα των συστημάτων, αλλά και ο αυξανόμενος αριθμός των διαθέσιμων από το διαδίκτυο πόρων.

Όλες αυτές οι απειλές, είναι σημαντικοί λόγοι για να αυξηθεί η ασφάλεια στο Διαδίκτυο και μεταξύ των χρηστών του. Αυτό περιλαμβάνει, τη βελτίωση της ασφάλειας των συστημάτων που συνδέονται με το Διαδίκτυο και την ενημέρωση και εκπαίδευση των χρηστών για τις απειλές.

## 2.1 Βασικά Χαρακτηριστικά

### *Απειλή(Threat)*

Μια απειλή (threat) είναι: Ένα πρόσωπο, πράγμα, γεγονός ή ιδέα το οποίο αποτελεί κίνδυνο για κάποιο αγαθό(asset) σε σχέση με την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή/και τη νόμιμη χρήση (legitimate use) του συγκεκριμένου αγαθού.

Οι απειλές εκφράζονται ως ηλεκτρονικό έγκλημα, ως εξής:

- ✓ μη εξουσιοδοτημένη πρόσβαση στα υπολογιστικά συστήματα
- ✓ κακόβουλα προγράμματα
- ✓ ιοί, δούρειοι ίπποι, παγίδες
- ✓ πειρατεία λογισμικού
- ✓ παράνομη χρήση ηλεκτρονικών ή δικτυακών πόρων
- ✓ απάτη στις ηλεκτρονικές συναλλαγές

### *Μηχανισμοί προστασίας*

Αποτελούν την τεχνική υλοποίηση των υπηρεσιών ασφαλείας και διαιρούνται σε δύο κατηγορίες:

α) Συγκεκριμένοι μηχανισμοί ασφαλείας.

- ✓ Μηχανισμοί κρυπτογράφησης (encryption)
- ✓ Μηχανισμοί ψηφιακών υπογραφών (digital signatures)
- ✓ Μηχανισμοί ελέγχου πρόσβασης (access control)
- ✓ Μηχανισμοί ανταλλαγής για πιστοποίηση ταυτότητας (Authentication Exchanges)
- ✓ Μηχανισμοί ελέγχου δρομολόγησης (routing)

(β) Γενικοί μηχανισμοί ασφαλείας:

- ✓ Έμπιστη λειτουργικότητα (trusted functionality)
- ✓ Ετικέτες ασφαλείας (security labels)

- ✓ Ανακάλυψη γεγονότων (event detection)
- ✓ Ακολουθία αρχείων καταγραφής περιστατικών ασφάλειας (security audit trail)
- ✓ Ανάκαμψη ασφάλειας (security recovery)

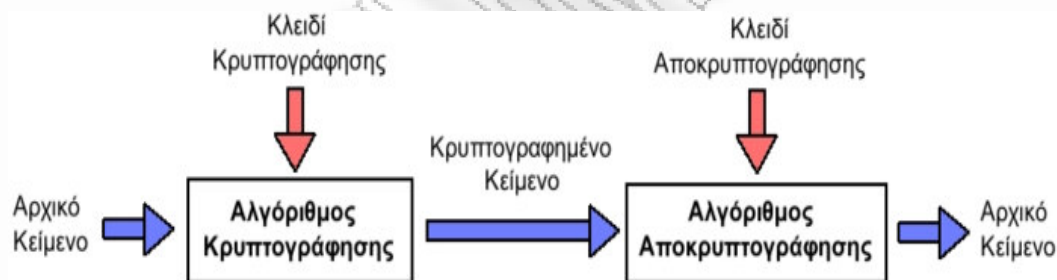
### Μηχανισμοί κρυπτογράφησης

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.

Το κρυπτογραφικό σύστημα, μετατρέπει τις εμπιστευτικές πληροφορίες σε μια μορφή η οποία δεν θα παρέχει κανένα νόημα σε κάποιο μη εξουσιοδοτημένο πρόσωπο. Στόχοι είναι: α) η ασφαλής αποθήκευση δεδομένων σε έναν υπολογιστή και β) η ασφαλής μετάδοση μέσα από ένα ανασφαλές κανάλι σαν το Internet.

Βασικοί ορισμοί κρυπτογραφίας<sup>36</sup>:

- α) Το κρυπτογραφημένο κείμενο ονομάζεται κρυπτόγραμμα (ciphertext)
- β) Το σύνολο των κανόνων που χρησιμοποιούμε για να κρυπτογραφήσουμε ονομάζεται αλγόριθμος κρυπτογράφησης (encryption algorithm)
- γ) Η λειτουργία του αλγορίθμου κρυπτογράφησης βασίζεται σε ένα κλειδί (encryption key)
- δ) Ο παραλήπτης χρησιμοποιεί τον αλγόριθμο αποκρυπτογράφησης (decryption algorithm)
- ε) Το αντίστοιχο κλειδί αποκρυπτογράφησης (decryption key)



Εικόνα 8: Τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης

Στην διάκριση κρυπτοσυστημάτων έχουμε δύο κατηγορίες:

- α) Συμβατικό (conventional) ή συμμετρικό (symmetric): Όταν είναι εύκολο να βρεθεί το κλειδί αποκρυπτογράφησης από το αντίστοιχο κλειδί κρυπτογράφησης.
- β) Ασύμμετρο (asymmetric) ή δημοσίου κλειδιού (public key): Όταν πρακτικά είναι αδύνατο να βρεθεί το κλειδί αποκρυπτογράφησης, ακόμα και αν είναι γνωστό το αντίστοιχο κλειδί κρυπτογράφησης. Επισημαίνεται η ανάγκη προστασίας του κλειδιού κρυπτογράφησης.

### Ιστορικοί κρυπτογραφικοί αλγόριθμοι<sup>37</sup>

- α. Αλγόριθμος ΚΑΙΣΑΡΑ: Κάθε γράμμα του αλφαβήτου αντικαθίσταται με εκείνο που βρίσκεται στην 3η επόμενη θέση στην αλφάβητο.
- β. Αλγόριθμος, ΑΠΛΗΣ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ: Σ' αυτούς το κάθε γράμμα του κώδικα αντικαθιστά τυχαία κάποιο γράμμα της αλφαβήτου.

- γ. Αλγόριθμος. PLAYFAIR: Στο συγκεκριμένο αλγόριθμο χρησιμοποιούνται δύο γράμματα (bigrams) σαν μια μονάδα τα οποία και κρυπτογραφεί.
- δ. Αλγόριθμος ΟΜΟΦΩΝΟΙ ΚΩΔΙΚΕΣ: Κάθε γράμμα αντιστοιχεί με έναν αριθμό, με τα πιο δημοφιλή από αυτά να αντιστοιχίζονται σε παραπάνω από έναν αριθμούς.
- ε. Αλγόριθμος ΚΩΔΙΚΕΣ VIGENERE: Χρησιμοποιεί ταυτόχρονα πολλούς κώδικες απλής αντικατάστασης σε αυστηρή όμως διάταξη. Οι πιο πάνω αλγόριθμοι είναι απλοί και μπορούν εύκολα να αποκρυπτογραφηθούν. Ο αλγόριθμος Vigenere έμεινε άσπαστος για περισσότερο από δύο αιώνες.

### **Μοντέρνοι κρυπτογραφικοί αλγόριθμοι<sup>37</sup>**

Οι μοντέρνοι αλγόριθμοι δεν χρησιμοποιούν αντικαταστάσεις γραμμάτων και χαρακτήρων, αλλά βασίζονται στο δυαδικό σύστημα και στις μετατροπές της δυαδικής αναπαράστασης αριθμών και χαρακτήρων. Οι μοντέρνοι αλγόριθμοι κατατάσσονται σε δύο κατηγορίες:

- α) Stream αλγόριθμοι, όπου η ακολουθία κρυπτογραφείται bit-προς-bit και
- β) Block αλγόριθμοι, όπου η ακολουθία διαχωρίζεται σε blocks προκαθορισμένου μήκους και κρυπτογραφείται ανά block.

### **Επίθεση(Attack)**

Επίθεση (attack), είναι οποιαδήποτε προσπάθεια για παραβίαση της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας ενός συστήματος ή δικτύου. Επίσης, είναι οποιαδήποτε μη εξουσιοδοτημένη ενέργεια που έχει σκοπό να εμποδίσει, να παρακάμψει ή να αχρηστεύσει τους μηχανισμούς ασφάλειας και ελέγχου πρόσβασης ενός συστήματος ή δικτύου. Τα αποτελέσματα μίας επίθεσης είναι:

- ✓ Εμπιστευτικότητα (Confidentiality): Μία επίθεση προκαλεί την παραβίαση της εμπιστευτικότητας, όταν ο επιτιθέμενος αποκτά πρόσβαση σε πληροφορίες για τις οποίες δεν είναι εξουσιοδοτημένος από τον κάτοχό τους.
- ✓ Ακεραιότητα (Integrity): Μία επίθεση προκαλεί παραβίαση της ακεραιότητας, όταν επιτρέπει στον (μη εξουσιοδοτημένο) επιτιθέμενο να αλλάξει την κατάσταση του συστήματος ή οποιασδήποτε πληροφορίας βρίσκεται σε αυτό.
- ✓ Διαθεσιμότητα (Availability): Μια επίθεση προκαλεί την παραβίαση της διαθεσιμότητας, όταν μέσω αυτής δεν επιτρέπεται στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε συγκεκριμένους πόρους του συστήματος όταν, όποτε και με τον τρόπο που έχουν εξουσιοδοτηθεί.

## **2.2 Ασφάλεια Δικτύων<sup>38, 40</sup>**

Αρχικά, αναφέρονται τα είδη επιθέσεων που μπορεί να δεχθεί μια εταιρεία η οποία έχει συνδεθεί με το Διαδίκτυο.

### **Denial of Service<sup>39, 53</sup>**

Η απλούστερη μορφή επιθέσεως ονομάζεται denial of service (παλιά την αποκαλούσαν ping of death) και συνίσταται στην αποστολή πάρα πολλών "νόμιμων" αιτημάτων προς το δίκτυο του θύματος. Για παράδειγμα, αν ο δεχόμενος την επίθεση έχει ένα web site, ο επιτιθέμενος του

αποστέλλει διαρκώς αιτήματα λήψης web σελίδων από πλαστές διευθύνσεις. Για να ικανοποιήσει αυτά τα αιτήματα ο web server, είτε προσπαθεί να στείλει web σελίδες σε παραλήπτες που δεν τις ζήτησαν, είτε τις στέλνει σε διευθύνσεις που δεν υπάρχουν.

Και στις δύο περιπτώσεις οι σελίδες δεν παραδίδονται ποτέ (ο web server καταλαβαίνει το λάθος του και σταματά την αποστολή). Το σύστημα όμως καταναλώνει μεγάλα ποσά υπολογιστικής ισχύος και bandwidth στην προσπάθειά του να παραδώσει τις σελίδες και να καταλάβει τι συμβαίνει. Αν λοιπόν τα ψεύτικα αιτήματα που λαμβάνει, είναι πάρα πολλά, τότε το σύστημα υπερφορτώνεται και παύει πλέον να λειτουργεί ή καθυστερεί πάρα πολύ να εξυπηρετήσει ένα "νόμιμο" αίτημα, διότι είναι απασχολημένο με την διαχείριση όλων των πλαστών αιτημάτων τα οποία λαμβάνει συνεχώς.

Όπως φαίνεται από την παραπάνω περιγραφή, οι επιθέσεις αυτής της μορφής δεν κλέβουν δεδομένα, ούτε επιτρέπουν στον επιτιθέμενο να αποκτήσει τον έλεγχο του εξοπλισμού μιας επιχείρησης. Απλώς, δεν επιτρέπουν στο θύμα να εξυπηρετήσει τους πελάτες και τους συνδρομητές του (γι' αυτό και ονομάζονται denial of service).

Αυτή η ιδιαιτερότητα όμως, καθιστά τις επιθέσεις λιγότερο επίφοβες. Το πρόβλημα με τις επιθέσεις denial of service, είναι πως δεν υπάρχει ακόμη κάποιος απλός και αποτελεσματικός τρόπος προστασίας από αυτές. Συνήθως, ο επιτιθέμενος αποστέλλει τα αιτήματά του από πολλά μηχανήματα μέσα στο δίκτυο (distributed denial-of-service ή DDS), κρύβοντας έτσι τα ίχνη του και κάνοντας πολύ δύσκολη την αναγνώριση μιας επίθεσης denial of service, μέχρι να είναι αργά (επειδή είναι πολύ δύσκολο να καταλάβει κανείς ότι τα αιτήματα που λαμβάνει είναι πλαστά, ο συναγερμός δεν δίνεται παρά μόνο όταν το δίκτυο δέχεται πλέον τόσο μεγάλο όγκο αιτημάτων που σχεδόν παύει να λειτουργεί)<sup>51</sup>.

Δυστυχώς, το πρωτόκολλο IP version 4 που χρησιμοποιείται αυτή τη στιγμή, δεν επιτρέπει την εύκολη αποκάλυψη του πραγματικού αποστολέα κάθε πακέτου δεδομένων. Το πρόβλημα αυτό θα λυθεί πλήρως, μόνο με την υιοθέτηση του νεότερου πρωτοκόλλου IP version 6 (IPv6) το οποίο όμως αργεί ακόμη να εφαρμοστεί.

Το IPv6, διαθέτει εξαιρετικά μεγάλο αριθμό IP διευθύνσεων (πολλές εκατοντάδες για κάθε κάτοικο της γης) και όταν υλοποιηθεί, κάθε συσκευή και κάθε χρήστης θα έχουν μια αποκλειστικά δική τους διεύθυνση, καθιστώντας εξαιρετικά δύσκολη οποιαδήποτε πλαστοπροσωπία.

### **Μορφές επίθεσης ενός δικτύου<sup>41</sup>**

Η συνηθέστερη μορφή επίθεσης συνίσταται στην "κατάληψη" των υπολογιστών ενός τοπικού δικτύου από τρίτους. Το κύριο χαρακτηριστικό μιας διείσδυσης αυτής της μορφής, είναι πως ο επιτιθέμενος έχει τη δυνατότητα να αντιγράψει, να τροποποιήσει ή να διαγράψει δεδομένα, να αλλάξει τις ρυθμίσεις των εγκατεστημένων προγραμμάτων και το χειρότερο απ' όλα, να εγκαταστήσει δικά του προγράμματα στο μηχάνημα ή το δίκτυο ενός τρίτου.

Μερικές φορές η επίθεση γίνεται διότι ο εισβολέας ενδιαφέρεται για την ίδια την επιχείρηση (για παράδειγμα, θέλει να της κάνει ζημιά ή να κλέψει κάποια στοιχεία). Συχνά όμως ο επιτιθέμενος εισβάλλει σε ένα δίκτυο αποκλειστικά και μόνο για να το χρησιμοποιήσει ως εφελτήριο για την επόμενη επίθεσή του.

Για παράδειγμα, μπορεί να θέλει να επιτεθεί στο δίκτυο ενός συνεταιίρου ή συνεργάτη της επιχείρησης και εκτιμά πως οι επιθέσεις του θα γίνουν πιο δύσκολα αντιληπτές αν πραγματοποιηθούν από μια αξιόπιστη τοποθεσία όπως το δίκτυο και τα μηχανήματα μιας εταιρείας την οποία εμπιστεύεται ο επιτιθέμενος, διότι έχει συχνά (δικτυακές) επαφές μαζί της.



Επίσης, οι επιθέσεις denial of service γίνονται συνήθως από μηχανήματα τρίτων, διότι η αποστολή των πλαστών αιτημάτων, απαιτεί μεγάλο bandwidth (δυνατότητα μεταφοράς δεδομένων) που είναι δύσκολο να βρεθεί σε ένα μόνο μηχανήμα. Ένας άλλος λόγος για τη χρήση πολλών μηχανημάτων για μια επίθεση denial of service, είναι πως η κατανομή της αποστολής των πλαστών αιτημάτων σε πολλά μηχανήματα, καθιστά πιο δύσκολη την αναγνώριση και την αντιμετώπισή της (στην αρχή το θύμα νομίζει απλώς πως αυξήθηκε το ενδιαφέρον για τις υπηρεσίες του δικτύου του).

Το πρόβλημα για κάθε επιχείρηση η οποία θέλει να προστατεύσει το δίκτυό της από τις επιβουλές τρίτων, είναι πως οι επιταγές της ασφάλειας απαιτούν την όσο το δυνατόν μικρότερη σύνδεσή της με το Internet, ενώ οι επιταγές της κερδοφορίας (αύξηση της παραγωγικότητάς της και καλύτερη εξυπηρέτηση των πελατών της) απαιτούν το όσο το δυνατόν μεγαλύτερο άνοιγμά της στον εξωτερικό δικτυακό κόσμο.

Ακολουθώντας το μοντέλο e-business, η επιχείρηση πρέπει να δίνει στον πελάτη τη δυνατότητα να παρακολουθεί online το υπόλοιπο του λογαριασμού του, να στέλνει παραγγελίες, να μαθαίνει για τη διαθεσιμότητα κάθε προϊόντος και γενικά να προβαίνει σε μια σειρά από εργασίες, οι οποίες απαιτούν πρόσβαση στο πληροφοριακό σύστημα της εταιρείας, δηλαδή στο εσωτερικό τοπικό δίκτυο που αυτή διατηρεί και στα μηχανήματα που το απαρτίζουν.

Τέλος, η εταιρεία πρέπει να παρέχει στο προσωπικό της τη δυνατότητα να συνδέεται με το Internet, ενώ σε πολλές περιπτώσεις πρέπει να επιτρέπει στους εξωτερικούς συνεργάτες της ή στο εκτός γραφείου προσωπικό της, να συνδέεται με το εσωτερικό της δίκτυο και να εκτελεί μια σειρά από "ευαίσθητες εργασίες", όπως η αλλαγή του ποσοστού έκπτωσης ή του πιστωτικού ορίου ενός πελάτη και η τροποποίηση του τύπου παράδοσης μιας παραγγελίας.

### ***Κατανομή δικαιωμάτων πρόσβασης<sup>41</sup>***

Από την παραπάνω περιγραφή, γίνεται φανερό πως κάθε επιχείρηση ή οργανισμός χρειάζεται ένα δίκτυο, όπου κάποια από τα τμήματα του οποίου θα είναι απόλυτα ανοικτά σε όλους (για παράδειγμα, ο τιμοκατάλογος ή οι περιγραφές των προϊόντων), κάποια θα είναι διαθέσιμα μόνο σε ορισμένους (για παράδειγμα, πωλητές οι οποίοι συνδέονται από το γραφείο του πελάτη για να οριστικοποιήσουν μια παραγγελία), ενώ κάποια άλλα θα παραμένουν εντελώς κλειστά στον υπόλοιπο κόσμο (για παράδειγμα, λογιστήριο).

Το πρώτο βήμα για να επιτευχθεί αυτός ο διαχωρισμός, είναι η λεπτομερής καταγραφή όλων όσων έχουν πρόσβαση στο σύστημα, καθώς και των εργασιών που επιτρέπεται να εκτελέσει ο καθένας. Ο παλαιός τρόπος δικτύωσης (κληρονομιά της εποχής του ανοιχτού σε όλους Internet) ορίζει πως συγκεκριμενοποιούνται οι απαγορεύσεις (ποια πράγματα δεν μπορεί να κάνει κάθε χρήστης) και στη συνέχεια δηλώνεται στο σύστημα ασφαλείας του δικτύου τι απαγορεύεται. Έτσι, ότι δεν απαγορεύεται είναι επιτρεπτό.

Δυστυχώς, η εποχή αυτή ανήκει πια στο παρελθόν και σήμερα ακολουθείται η ακριβώς αντίθετη στρατηγική: Ορίζεται τι επιτρέπεται και απαγορεύονται, όλα τα υπόλοιπα. Αυτό είναι το πρώτο και πιο ουσιαστικό βήμα για την εγκαθίδρυση μηχανισμών ασφαλείας μέσα σε ένα δίκτυο το οποίο είναι συνδεδεμένο με το Internet.

Ας σημειωθεί, πως παρά τη μεγάλη δημοτικότητα που αποκτούν οι επιθέσεις τρίτων σε επιχειρήσεις, η εμπειρία έχει δείξει πως η πλειοψηφία των παραβιάσεων ασφαλείας δικτύων, γίνεται από το ίδιο το προσωπικό της εταιρείας, είτε από κακοήθεια (για παράδειγμα, από δυσαρεστημένους εργαζόμενους), είτε από υπολογισμό (για παράδειγμα, δωροδοκία από ανταγωνιστές). Για τον λόγο αυτό, κάθε μηχανισμός ασφαλείας δεν πρέπει να περιορίζεται στον

απλουστευτικό διαχωρισμό του "ξένοι" και "δικοί μας", αλλά να ορίζει με λεπτομέρεια τα δικαιώματα πρόσβασης που δίδονται σε κάθε εργαζόμενο ή κάθε ομάδα του προσωπικού.

### 2.3 Φιλτράρισμα Πακέτων (Packet Filtering)<sup>44</sup>

Το επόμενο βήμα, μετά τον καθορισμό των δικαιωμάτων κάθε ομάδας χρηστών, είναι η επιλογή του καταλληλότερου μηχανισμού ασφαλείας, η αξιοπιστία και η αποτελεσματικότητα του οποίου συναρτώνται άμεσα με τις οικονομικές δυνατότητες της επιχείρησης, καθώς και με τις τεχνικές γνώσεις του δικτυακού προσωπικού της.

Η απλούστερη μέθοδος προστασίας ενός δικτύου, είναι η χρήση της τεχνικής του Packet Filtering. Όπως είναι γνωστό, όλα τα δεδομένα, τα μηνύματα και οι εντολές, διακινούνται μέσα στο Διαδίκτυο, με τη μορφή πακέτων δεδομένων τα οποία διαβιβάζονται από τον ένα δρομολογητή (router) στον άλλον, μέχρι να παραδοθούν στον τελικό προορισμό τους (συνήθως στον Η/Υ όπου τρέχει η εφαρμογή η οποία θα τα διαχειριστεί).

Στην πραγματικότητα, ο router είναι και αυτός ένας Η/Υ, με τη διαφορά πως έχει εξειδικευθεί αποκλειστικά στη διακίνηση των στοιχείων που χρησιμοποιούν τα άλλα μηχανήματα του δικτύου. Λόγω αυτής της ιδιαιτερότητας, ο router είναι ο πρώτος ο οποίος θα λάβει και θα διαβιβάσει οποιοδήποτε "παράνομο" αίτημα πρόσβασης ή οποιαδήποτε εντολή δοκιμάζει να δώσει σε κάποιον Η/Υ του τοπικού δικτύου, όποιος προσπαθεί να διεισδύσει αδικαιολόγητα σε αυτό.

Για τον λόγο αυτό, πολλοί διαχειριστές συστημάτων χρησιμοποιούν τον router μέσω του οποίου συνδέονται με το Internet ως την πρώτη γραμμή άμυνας τους, ορίζοντας στους πίνακες δρομολόγησής του (routing tables) πώς πρέπει να αντιδρά σε κάθε αίτημα (για παράδειγμα, αν ζητηθούν να σταλούν δεδομένα αυτής της μορφής στο μηχάνημα X, απάντησε πως αυτή η δυνατότητα ή αυτό το μηχάνημα δεν υπάρχει).

Η τεχνική του Packet Filtering, είναι συνήθως απλή στην εφαρμογή της και σχετικά φθηνή (απαιτείται μόνο η ρύθμιση του router ο οποίος υπάρχει ήδη στις εγκαταστάσεις της εταιρείας). Για τον λόγο αυτό υπάρχουν συστήματα Firewall (Τείχη Προστασίας), τα οποία βασίζονται αποκλειστικά και μόνο στο Packet Filtering, για την προστασία ενός ή περισσότερων δικτύων.

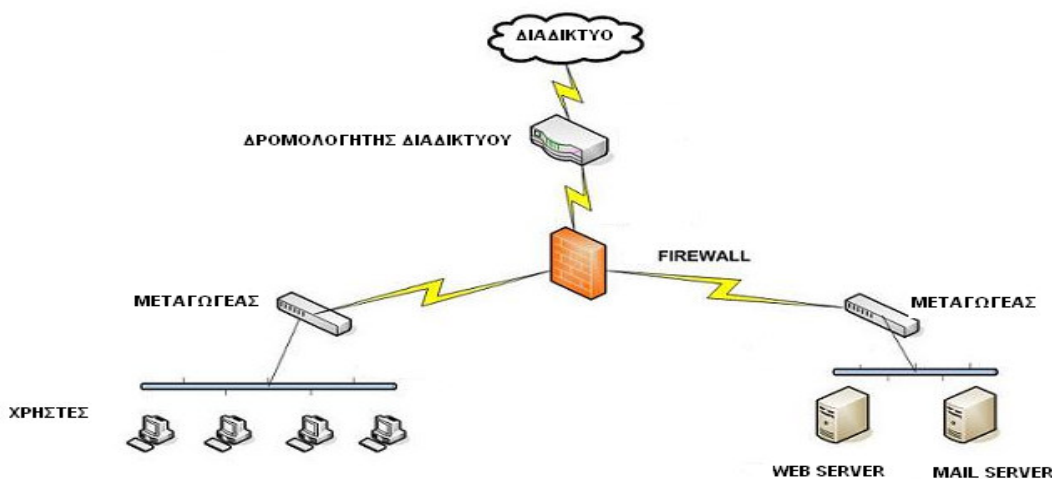
Ένα σοβαρό μειονέκτημα του Packet Filtering, είναι πως λειτουργεί αποτελεσματικά μόνο αν ο router πρέπει να διαχειριστεί χαμηλό όγκο κίνησης ή αν ο αριθμός των φίλτρων είναι μικρός. Όσο αυξάνει η κίνηση, τόσο περισσότερα πακέτα πρέπει να ελέγξει ο router, ενώ όσο αυξάνουν τα φίλτρα τόσο περισσότεροι έλεγχοι πρέπει να γίνουν, πριν επιτραπεί σε ένα πακέτο να μπει στο τοπικό δίκτυο ή να βγει από αυτό. Έτσι όμως, επιβαρύνεται υπερβολικά ο επεξεργαστής του router και περιορίζεται η απόδοσή του.

Τέλος, το Packet Filtering είναι εξαιρετικά δύσκολο να εφαρμοστεί σε περίπλοκα τοπικά δίκτυα τα οποία έχουν μεγάλη ποικιλία επαφών με το Διαδίκτυο. Όσο περισσότερες υπηρεσίες (telnet, ftp, smtp, pop, http και άλλα) πρέπει να ελεγχθούν από τον router, τόσο δυσκολότερη γίνεται η καλή ρύθμισή του, για εφαρμογές Packet Filtering. Το πρόβλημα βρίσκεται στο γεγονός, ότι όποια παράμετρος δεν έχει προβλεφθεί να φιλτράρεται, είναι ελεύθερη να διακινηθεί από και προς το τοπικό δίκτυο.

Έτσι, ακόμη και το παραμικρό λάθος ή αβλεψία μπορεί να αποβεί μοιραίο (για παράδειγμα, πολλοί crackers χρησιμοποιούν ειδικά προγράμματα που δοκιμάζουν μία - μία όλες τις δυνατές τεχνικές παράκαμψης των φίλτρων μέχρι να βρουν εκείνη τη δίοδο που από άγνοια, λάθος ή αδιαφορία έχει μείνει ανεξέλεγκτη).

## 2.4 Τείχος Προστασίας (Firewall)<sup>42</sup>

Το επόμενο, και ανώτερο, επίπεδο προστασίας είναι η εγκατάσταση και καλή αξιοποίηση ενός Τείχους Προστασίας - Firewall. Τα πρώτα Firewalls, ήταν απλώς Packet Filtering Routers, οι οποίοι τοποθετούνταν σε στρατηγικά σημεία του δικτύου, έτσι ώστε ακόμη και αν κάποιος εξωτερικός εχθρός διείσδυε σε ένα μέρος του δικτύου να μην αποκτά αμέσως ελεύθερη πρόσβαση στο σύνολο των μηχανημάτων που το απαρτίζουν. Λειτουργούσαν δηλαδή, ως αντιπυρικές πόρτες (Firewalls), οι οποίες εμποδίζουν τη φωτιά η οποία έχει ανάψει σε κάποιο δωμάτιο να εξαπλωθεί στο υπόλοιπο κτίριο. Ένα Firewall, αποτελείται συνήθως από έναν Η/Υ, γνωστό με το όνομα Bastion host (κόμβος προμαχώνας) και μια σειρά από εφαρμογές ανταπόκρισης (proxy services). Ο Bastion host, έχει εγκατεστημένη μια ασφαλή έκδοση ενός λειτουργικού συστήματος. Η έκδοση αυτή είναι ουσιαστικά η ίδια με εκείνη, που χρησιμοποιείται από την πλειοψηφία των χρηστών (για παράδειγμα, UNIX, NT και άλλα) με τη διαφορά πως έχουν απενεργοποιηθεί όλα τα χαρακτηριστικά της, πλην των απολύτως απαραίτητων (το σκεπτικό εδώ είναι πως όσο λιγότερες εφαρμογές περιλαμβάνει το λειτουργικό, τόσο μειώνονται οι πιθανότητες να ανακαλυφθεί κάποιο τρωτό σημείο σε μια από αυτές).



Εικόνα 9: Firewall - Η χρήση ενός firewall προστατεύει το εσωτερικό δίκτυο από το Internet, αλλά γίνεται και υλοποίησή του για εσωτερικό διαχωρισμό τμημάτων του δικτύου από το υπόλοιπο εσωτερικό δίκτυο.

Μερικές φορές, πάνω στον Bastion host, εγκαθίσταται μια σειρά από Circuit Level Gateways (προγράμματα τα οποία παρακολουθούν, ποιος συνδέεται με το εσωτερικό δίκτυο και καθορίζουν ποιες εργασίες μπορεί να κάνει μέσα σε αυτό). Συνήθως όμως, ο Bastion host, έχει εγκατεστημένα διάφορα Application-Level Gateways, τα οποία λειτουργούν ως proxy services, μεταφράζοντας τα αιτήματα από και προς τους Η/Υ του τοπικού δικτύου. Έτσι, οποιοσδήποτε μέσα στο Διαδίκτυο επικοινωνεί με ένα μηχάνημα του εσωτερικού δικτύου, δεν έχει ποτέ απευθείας επαφή με αυτό. Το αίτημά του διατυπώνεται στο αντίστοιχο Application-Level Gateway, το οποίο το διαβιβάζει στο μηχάνημα και επιστρέφει την απάντηση.

Χάρη στα Application-Level Gateways, απαγορεύεται οποιαδήποτε μορφή επικοινωνίας μεταξύ του εσωτερικού δικτύου και του Διαδικτύου, εκτός από εκείνες για τις οποίες έχει εγκατασταθεί το ανάλογο λογισμικό (το Application-Level Gateway που επιτρέπει τη χρήση της

συγκεκριμένης υπηρεσίας). Ο διαχειριστής του συστήματος, εγκαθιστά ένα Application-Level Gateway για κάθε εφαρμογή και φροντίζει να το ρυθμίσει κατάλληλα. Με τον τρόπο αυτό, η επικοινωνία μεταξύ τοπικού δικτύου και του Διαδικτύου, μπορεί να επιτευχθεί μόνο για όσες υπηρεσίες έχουν εγκατεστημένο το αντίστοιχο Application-Level Gateway στον Bastion host και μόνο αν το Application-Level Gateway έχει ρυθμιστεί με τέτοιο τρόπο, ώστε να επιτρέπεται η μορφή επικοινωνίας που ζητάει ο χρήστης. Η τεχνική αυτή ονομάζεται και protocol filtering, διότι απ' όλα τα πρωτόκολλα του Διαδικτύου, επιτρέπεται η διέλευση μόνο σε όσα ορίζει το Application-Level Gateway.

Τα χαρακτηριστικά ενός firewall, περιλαμβάνουν<sup>43</sup>:

- α) εξασφάλιση της πρόσβασης στο δίκτυο
- β) έλεγχος, όλων των συνδέσεων από και προς το δίκτυο
- γ) φιλτράρισμα των δεδομένων, βάσει προκαθορισμένων κανόνων
- δ) πιστοποίηση, χρηστών και εφαρμογών
- ε) καταγραφή δραστηριοτήτων
- ς) δυναμική ειδοποίηση των κατάλληλων ατόμων, όταν συμβεί κάποια ύποπτη δραστηριότητα

Αξίζει να σημειωθεί, πως τα Firewalls δεν ελέγχουν μόνο ότι εισέρχεται στο εσωτερικό δίκτυο, αλλά και ότι εξέρχεται από αυτό. Έτσι, μερικές φορές, οι χρήστες του εσωτερικού δικτύου μπορούν να δουν ιστοσελίδες στο Διαδίκτυο, αλλά δεν μπορούν να επικοινωνήσουν με αυτά, πράγμα που φυσικά προκαλεί δυσφορία και έντονες διαμάχες μεταξύ των διαχειριστών του εσωτερικού δικτύου (οι οποίοι θέλουν να το κρατήσουν όσο πιο "κλειστό" γίνεται) και των χρηστών του (οι οποίοι θέλουν να έχουν πρόσβαση σε όσο το δυνατόν περισσότερες υπηρεσίες).

Η παραπάνω δομή, επιτυγχάνει υψηλά επίπεδα ασφαλείας, καθώς το Firewall λειτουργεί πάντοτε ως ενδιάμεσος, ελέγχοντας και μεταφράζοντας όλες τις επαφές του τοπικού δικτύου με το Διαδίκτυο. Δυστυχώς, αυτή η μετάφραση αποτελεί και το μεγαλύτερο μειονέκτημα των Firewalls, καθώς πολλές φορές απαιτείται η χρήση ειδικών εφαρμογών από τον χρήστη του Διαδικτύου, ο οποίος θέλει να επικοινωνήσει με κάποιο μηχάνημα του εσωτερικού δικτύου.

Άλλα μειονεκτήματα των Firewalls, είναι το μεγάλο κόστος προμήθειας εξοπλισμού και εκπαίδευσης προσωπικού και η μειωμένη ταχύτητα επικοινωνίας του εσωτερικού δικτύου με το Διαδίκτυο. Γενικά, η λειτουργία των Firewalls, απαιτεί ισχυρά μηχανήματα με μεγάλη υπολογιστική ισχύ, καθώς το Firewall είναι υποχρεωμένο όχι μόνο να μεταφράζει κάθε μεταφορά δεδομένων από και προς το εσωτερικό δίκτυο, αλλά και να επιβεβαιώνει πως κάθε αίτημα σύνδεσης έρχεται από "έμπιστη" IP διεύθυνση. Πολύ συχνά οι crackers ακολουθούν μια τεχνική, με το όνομα IP spoofing, χάρη στην οποία ένα μηχάνημα μπορεί να ιδιοποιηθεί την IP διεύθυνση ενός άλλου. Έτσι, ένας "απλός" router μπορεί να εξαπατηθεί και να επιτρέψει τη χρήση του εσωτερικού δικτύου σε έναν H/Y ο οποίος κανονικά δεν δικαιούται πρόσβαση σε αυτό.

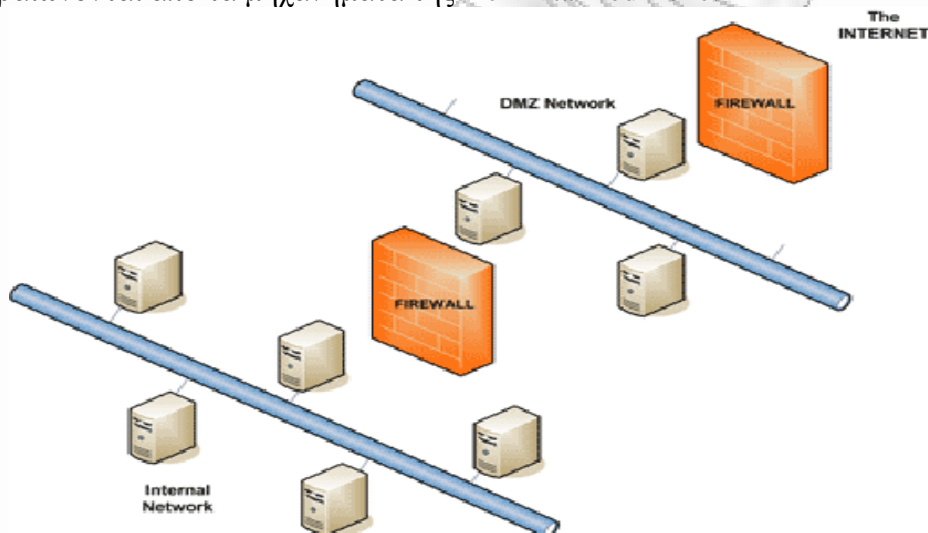
Παρόλα αυτά, η λύση των Firewalls αποτελεί σήμερα τον πιο δημοφιλή τρόπο προστασίας ενός δικτύου. Πολλές επιχειρήσεις μάλιστα συνδυάζουν τη χρήση των Firewalls, με Packet Filtering για να αυξήσουν ακόμη περισσότερο τη δυσκολία διείσδυσης ανεπιθύμητων, μέσα στο εσωτερικό δίκτυό τους. Η τεχνική του συνδυασμού Packet Filtering με Circuit Level και Application-Level Gateways ονομάζεται Stateful Multilayer Inspection Firewall. Τα μοντέρνα συστήματα firewalls, είναι -ουσιαστικά- «υβρίδια» όλων των κατηγοριών και υλοποιούνται με συνδυασμό κατάλληλου υλικού και λογισμικού. Η συγκεκριμένη τεχνολογία δεν μετρά περισσότερα από 10 χρόνια ζωής, η εκτεταμένη όμως χρήση τους, δείχνει πως στο μέλλον θα αποτελέσουν βασικό και αναπόσπαστο κομμάτι κάθε δικτυακής αρχιτεκτονικής. Η τάση είναι ο

συνδυασμός, της χρήσης της ισχύος του υλικού (hardware) και της ευφυΐας του λογισμικού (software).

## 2.5 Αποστρατικοποιημένη Περιοχή (DMZ - Demilitarized Zone)<sup>45</sup>

Το υψηλότερο επίπεδο ασφαλείας δικτύων επιτυγχάνεται με μια άλλη μέθοδο γνωστή με το όνομα, Demilitarized Zone (DMZ) ή Screened-Subnet Firewall. Η τεχνική αυτή, χρησιμοποιεί ένα Firewall και ένα Packet Filtering router μέσω των οποίων εξασφαλίζεται η επικοινωνία ενός τμήματος του εσωτερικού δικτύου, γνωστού με το όνομα Demilitarized Zone (αποστρατικοποιημένη περιοχή), με το Διαδίκτυο. Αυτή η περιοχή, περιέχει μόνο τις πολύ βασικές υπηρεσίες (για παράδειγμα, web) και τα μηχανήματά της, είναι προσβάσιμα από το Διαδίκτυο, μέσω του Firewall και του Packet Filtering router.

Στην αρχιτεκτονική αυτή όμως, υπάρχει και ένας δεύτερος Packet Filtering router ο οποίος συνδέει την Demilitarized Zone με το υπόλοιπο εσωτερικό δίκτυο της εταιρείας και καθιστά το τμήμα αυτό του δικτύου, αόρατο από τον έξω κόσμο. Με τον τρόπο αυτό, επιτυγχάνεται το υψηλότερο δυνατό επίπεδο προστασίας, αφού ουσιαστικά κρύβεται από τους πιθανούς εισβολείς ακόμη και την ύπαρξη των πιο ευαίσθητων μηχανημάτων, ενώ απαγορεύεται σε οποιαδήποτε δεδομένα από το Διαδίκτυο, να φθάσουν μέχρι το αόρατο δίκτυο, αφού όλα τα αιτήματα διεκπεραιώνονται από τα μηχανήματα της Demilitarized Zone.



Εικόνα 10: Απεικόνιση DMZ<sup>45</sup>

## 2.6 IDS - Intrusion Detection Systems (Αυτοματοποιημένη Ανίχνευση Επιθέσεων)<sup>49</sup>

Με δεδομένη την αύξηση των κακόβουλων ενεργειών και επιθέσεων στο Διαδίκτυο, τα κλασικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που περιέχουν αυτά και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.

Μία σχετικά νέα και συνεχώς αναπτυσσόμενη μέθοδος προστασίας, είναι η αυτοματοποιημένη Ανίχνευση Επιθέσεων (Intrusion Detection). Δίνονται οι παρακάτω δύο ορισμοί, για το IDS<sup>48, 49, 50</sup>:

- ✓ *Ο όρος Intrusion Detection, σημαίνει ανίχνευση επιθέσεων και έχει να κάνει με την παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο και την ανάλυσή τους για σημάδια επιθέσεων.*
- ✓ *Ο όρος Intrusion Detection Systems (IDSs) σημαίνει συστήματα ανίχνευσης επιθέσεων και έχει να κάνει με software ή hardware προϊόντα, που αυτοματοποιούν την παραπάνω διαδικασία παρακολούθησης και ανάλυσης.*

Για ένα IDS, ύποπτοι θεωρούνται τόσο οι εξωτερικοί χρήστες που συνδέονται στο εσωτερικό δίκτυο μέσω του Internet, όσο και οι εσωτερικοί χρήστες του δικτύου (όσοι έχουν πρόσβαση από τοπικά συνδεδεμένα μηχανήματα). Τα IDSs, παρακολουθούν το δίκτυο όλο το 24ωρο, δίνοντας συνεχώς αναφορές τόσο για επικίνδυνα περιστατικά (για παράδειγμα, ένας χρήστης προσπάθησε να διαγράψει ή να αντιγράψει αρχεία στα οποία δεν έχει δικαίωμα πρόσβασης), όσο και για ύποπτες ανωμαλίες οι οποίες μπορεί να υποδηλώνουν την αρχή μιας επίθεσης (για παράδειγμα, η εφαρμογή X, έχει πολύ περισσότερη κίνηση απ' ό τι συνήθως και οι περισσότερες εντολές που λαμβάνει είναι λανθασμένες. Αυτό μπορεί να σημαίνει πως κάποιος δοκιμάζει να της στείλει διάφορες "τρελές" εντολές, ελπίζοντας πως θα την μπερδέψει, ώστε να του δώσει πρόσβαση στο σύστημα).

Ένα καλό IDS, θα πρέπει να είναι αρκετά ευαίσθητο για να αναγνωρίζει όλες τις ύποπτες καταστάσεις, αλλά αρκετά έξυπνο, ώστε να μην κρούει συχνά τον κώδωνα του κινδύνου χωρίς λόγο. Είναι αναπόφευκτο πως μερικές φορές το IDS θα κάνει λάθη, σημαίνοντας συναγερμό για ασυνήθιστες, αλλά όχι επικίνδυνες, καταστάσεις. Αν όμως αυτό γίνεται συχνά, τότε οι χειριστές του θα συνηθίσουν να θεωρούν ως λανθασμένες όλες τις προειδοποιήσεις του και πιθανόν να μην το πιστέψουν ακόμη κι αν γίνεται πραγματικά επίθεση.

Το IDS, θα πρέπει να ελέγχει συχνά τον εαυτό του για να εξασφαλίσει ότι λειτουργεί σε άριστη κατάσταση και ότι δεν έχει αποκτήσει πρόσβαση σε αυτό κάποιος τρίτος δίνοντάς του παραπλανητικά στοιχεία. Το IDS, θα πρέπει επίσης να ελέγχει σε τακτά χρονικά διαστήματα τα δεδομένα που είναι αποθηκευμένα στο εσωτερικό δίκτυο (για παράδειγμα, συγκρίνοντάς τα με κάποια δικά του εφεδρικά αρχεία) για να εξασφαλίσει πως δεν έχουν τροποποιηθεί.

Τέλος, το IDS θα πρέπει να έχει καλή μνήμη και να μην ξεγελιέται από μεμονωμένες, φαινομενικά αθώες, ενέργειες. Συχνά, μια επίθεση κατανέμεται σε πολλές μικρές ήσσονος σημασίας και φαινομενικά άσχετες μεταξύ τους εργασίες οι οποίες περνούν απαρατήρητες, αλλά τελικά καταφέρνουν να παρακάμψουν τα συστήματα ασφαλείας και να επιτρέψουν την είσοδο του εισβολέα στο σύστημα.

### **Alerts (Επισήμανση Ανίχνευσης)**<sup>49, 52</sup>

Μία επισήμανση για την ανίχνευση κάποιας επίθεσης, συνήθως ονομάζεται alert. Τα περισσότερα IDSs, δίνουν την δυνατότητα στον χρήστη να καθορίσει με σχετική ευχέρεια, την στιγμή και την μορφή που θα παράγονται τα alerts και σε ποιους χρήστες θα παρουσιάζονται. Ένα IDS, είναι δυνατόν να ρυθμιστεί ώστε τα alerts να εμφανίζονται σε πραγματικό χρόνο, την ώρα που εντοπίζεται μία επίθεση, όπως για παράδειγμα, με αναδυόμενα παράθυρα στην οθόνη ή μπορεί να ρυθμιστεί ώστε να καταγράφει τα alerts σε κάποιο αρχείο για μετέπειτα εξέταση, ή ακόμα και να τα στέλνει με email στον διαχειριστή του δικτύου.

Η μορφή που θα παράγεται ένα alert από το IDS, μπορεί να είναι από μία απλή αναφορά στο είδος της επίθεσης με έναν τίτλο, στον επιτιθέμενο και στο θύμα αυτής, μέχρι και αναλυτική αναφορά που θα περιέχει και πληροφορίες για το πακέτο που οδήγησε στον εντοπισμό της επίθεσης, κάνοντας λεπτομερή περιγραφή του ή αναφορά στο εργαλείο που χρησιμοποιήθηκε για την υλοποίησή της.

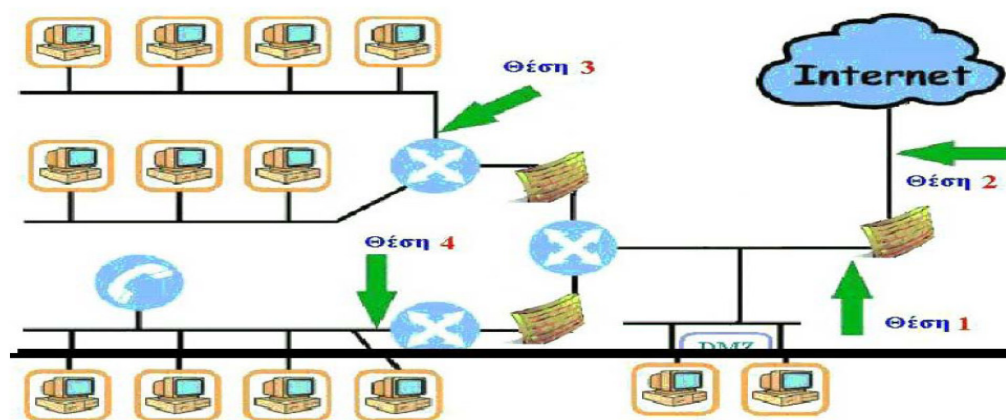
### Τοποθέτηση του IDS<sup>48, 49</sup>

Η επιλογή του σημείου στο δίκτυο που θα τοποθετηθεί το IDS, πρέπει να γίνει αφού ληφθούν υπόψη διάφορα κριτήρια, αφού θα καθορίσει τη φύση των αποτελεσμάτων που θα παίρνονται από το IDS. Έχει διαφορά για παράδειγμα, αν το IDS τοποθετηθεί πίσω από το firewall ή μπροστά, ή αν θα παρακολουθεί μόνο ένα συγκεκριμένο υποδίκτυο.

Ανάλογα με την υπάρχουσα τοπολογία ενός δικτύου, μπορεί να χρειαστεί να τοποθετηθούν συστήματα ανίχνευσης επιθέσεων σε ένα ή περισσότερα σημεία ενός δικτύου. Εξαρτάται ακόμη, τι είδους επιθέσεις θέλει κανείς να ανιχνεύσει. Δηλαδή: Εξωτερικές, Εσωτερικές, ή και τις δύο περιπτώσεις μαζί.

Αν για παράδειγμα θέλει κανείς να ανιχνεύσει μόνο τις εξωτερικές επιθέσεις και έχει μόνο έναν δρομολογητή (router) για την σύνδεσή του στο Διαδίκτυο, το καλύτερο σημείο για την τοποθέτηση ενός τέτοιου συστήματος ανίχνευσης επιθέσεων, μπορεί να είναι μέσα στον router ή το firewall. Αν διαθέτει κανείς περισσότερα από ένα σημεία σύνδεσης στο Διαδίκτυο, το καλύτερο σημείο για να τοποθετηθεί ένα IDS, είναι σε κάθε ένα από τα σημεία εισόδου. Αν κανείς παρόλα αυτά, θέλει να εντοπίσει και εσωτερικές απειλές, επίσης μπορεί να τοποθετήσει ένα τέτοιο σύστημα σε κάθε σημείο χρήσης του δικτύου. Σε πολλές περιπτώσεις, δεν χρειάζεται να τοποθετηθούν τόσο πολλά IDS σε κάθε σημείο χρήσης, αλλά στα σημεία εκείνα που παρουσιάζουν ιδιαίτερη ευαισθησία.

Άλλωστε, θα πρέπει να δώσει κανείς ιδιαίτερη σημασία σε αυτό, η εγκατάσταση πολλών τέτοιων συστημάτων σε πολλά σημεία του δικτύου συνεπάγεται αυξημένα επίπεδα εργασίας για την εγκατάστασή τους και επίσης αυξημένα κόστη συντήρησης. Η απόφαση, βασίζεται αποκλειστικά στις πολιτικές ασφαλείας, οι οποίες τελικά καθορίζουν το πως και με ποιόν τρόπο θέλει κανείς να προστατευτεί. Το παρακάτω διάγραμμα, περιγράφει την πιθανή τοπολογία ενός συστήματος Ανίχνευσης Επιθέσεων σε ένα δίκτυο. Στην επόμενη εικόνα 11, είναι οι πιθανές θέσεις που μπορεί να τοποθετηθεί το IDS<sup>48, 49</sup>.



Εικόνα 11: Θέσεις Τοποθέτησης ενός IDS<sup>49, 42</sup>

- ✓ **Θέση 1:** Με την τοποθέτηση του IDS σε αυτήν την θέση, είναι δυνατόν να επισημανθούν πιθανά λάθη στις ρυθμίσεις του firewall. Είναι δυνατόν να ανιχνευτούν επιθέσεις που στοχεύουν τον web server ή τον ftp server και άλλα συστήματα που πέφτουν συχνά στόχοι μίας επίθεσης και συνήθως βρίσκονται στην DMZ ενός δικτύου. Ακόμα και αν δεν ανιχνευτεί η επίθεση, όπως αυτή κατευθύνεται προς το εσωτερικό του δικτύου, είναι δυνατό με το IDS σε αυτή τη θέση, να εντοπιστεί το εξερχόμενο traffic, που δημιουργείται από τα συστήματα που ήταν στόχοι και μέσω αυτού να γίνει αντιληπτή η επίθεση.
- ✓ **Θέση 2:** Μπροστά από κάθε συνοριακό firewall. Σε αυτό το σημείο το IDS, είναι δυνατό να εντοπίσει όλες τις επιθέσεις που στοχεύουν το δίκτυο, ακόμα και αυτές που θα αποτραπούν από το firewall. Με αυτόν τον τρόπο υπάρχει η δυνατότητα να καταγραφεί, το πλήθος και το είδος των επιθέσεων που στοχεύουν το δίκτυο καθημερινά.
- ✓ **Θέση 3:** Στο δίκτυο κορμού (backbone) του δικτύου. Σε αυτή την θέση το IDS, παρακολουθεί ένα μεγάλο μέρος του traffic του δικτύου, που έχει σχέση με τα υποδίκτυα που συνδέονται πάνω στο backbone και έχει την δυνατότητα να εντοπίσει επιθέσεις που σχετίζονται με αυτά. Είναι δυνατό, να ανιχνευτούν επιθέσεις που προέρχονται από συστήματα, που ανήκουν μέσα στην ζώνη ασφαλείας του δικτύου.
- ✓ **Θέση 4:** Σε σημαντικά υποδίκτυα του δικτύου. Το IDS μπορεί να εντοπίσει επιθέσεις που στοχεύουν σημαντικά συστήματα του δικτύου, που περιέχουν κρίσιμες πληροφορίες. Επιτρέπει την εστίαση της προσοχής σε πόρους του δικτύου που έχουν μεγάλη αξία.

### **IDS Policy**<sup>49</sup>

Προτού να εγκατασταθεί το IDS σύστημα στο δίκτυο, πρέπει να υπάρχει μια πολιτική για να ανιχνευθούν οι εισβολείς και να ληφθούν μέτρα, όταν βρεθεί μία τέτοια δραστηριότητα. Μια πολιτική πρέπει να υπαγορεύσει τους κανόνες IDS και πώς θα εφαρμοστούν. Η πολιτική IDS πρέπει να περιέχει τα ακόλουθα συστατικά και μπορούν να προστεθούν περισσότερα ανάλογα με τις απαιτήσεις ενός οργανισμού.

- ✓ **Έλεγχος IDS:** Ανάλογα με το IDS, υπάρχουν προειδοποιητικοί μηχανισμοί που παρέχουν τις πληροφορίες για τη δραστηριότητα εισβολέων. Αυτά τα προειδοποιητικά συστήματα μπορούν να είναι υπό μορφή απλών αρχείων κειμένων, ή σε μία MySQL βάση δεδομένων. Η πολιτική πρέπει να καθορίζει το αρμόδιο πρόσωπο που απαιτείται για να ελέγξει τη δραστηριότητα εισβολέων. Η δραστηριότητα εισβολέων, μπορεί επίσης να ελεγχθεί σε πραγματικό χρόνο χρησιμοποιώντας τα pop-up windows. Σε αυτήν την περίπτωση οι υπεύθυνοι πρέπει να έχουν γνώση των alerts και της σημασία τους σε επίπεδο ασφάλειας.
- ✓ **Υπεύθυνος IDS:** Όπως σε όλα τα συστήματα πρέπει να υπάρχει ένα συγκεκριμένο άτομο - administrator, υπεύθυνο να χειριστεί, να ελέγχει και να παρατηρεί το IDS σύστημα.
- ✓ **Υποβολή έκθεσης:** Οι εκθέσεις μπορούν να παραχθούν παρουσιάζοντας τι συνέβη κατά τη διάρκεια της τελευταίας ημέρας, εβδομάδας, μήνα.
- ✓ **Updates:** Όπως σε κάθε σύστημα, έτσι και εδώ χρειάζεται αναβαθμίσεις. Οι εισβολείς δημιουργούν συνεχώς τους νέους τύπους επιθέσεων. Αυτές οι επιθέσεις ανιχνεύονται από το IDS σύστημα, εάν ξέρει για την επίθεση υπό μορφή υπογραφών. Οι υπογραφές



επίθεσης χρησιμοποιούνται στους Snort κανόνες, για να ανιχνεύσει τις επιθέσεις. Λόγω της συνεχώς μεταβαλλόμενης φύσης των επιθέσεων, πρέπει να ενημερώνονται οι υπογραφές και οι κανόνες για IDS σύστημα.

- ✓ **Documentation:** Η τεκμηρίωση απαιτείται για κάθε πρόγραμμα. Η πολιτική IDS, πρέπει να περιγράψει ποιος τύπος τεκμηρίωσης θα γίνει όταν ανιχνεύονται οι επιθέσεις. Η τεκμηρίωση, μπορεί να περιλάβει ένα απλό log αρχείο που περιγράφει την πλήρη δραστηριότητα των εισβολέων.

### **Συστήματα Προστασίας - Secure Sockets Layer (SSL)**

Το πρωτόκολλο αυτό, χρησιμοποιείται σαν ένας μηχανισμός ασφάλειας στο επίπεδο εφαρμογής, το ανώτερο επίπεδο τόσο στην αρχιτεκτονική OSI όσο και την αρχιτεκτονική TCP/IP. Το SSL, σχεδιάστηκε για να κάνει χρήση του πρωτοκόλλου TCP, προσφέροντας μια αξιόπιστη από-άκρη-σε-άκρη υπηρεσία και χρησιμοποιείται κυρίως σε Web Browsers και Servers. Σχεδόν πάντα, ο εξυπηρετητής πετυχαίνει να πιστοποιήσει την ταυτότητα του, κυρίως μέσω (RSA) ψηφιακών υπογραφών.

Τα πρωτόκολλα αυτά, χρησιμοποιούνται στη διαχείριση της ανταλλαγής των μηνυμάτων του πρωτοκόλλου HTTP (Hyper Text Transfer Protocol). Οι παράμετροι που περιέχονται σε μια σύνδεση HTTP είναι οι ακόλουθοι:

- ✓ Τυχαίοι αριθμοί μεταξύ πελάτη (client) και εξυπηρετητή (server), οι οποίοι είναι διαφορετικοί για κάθε σύνδεση
- ✓ Μυστικό MAC (Message Authentication Code), για εγγραφή δεδομένων στον εξυπηρετητή
- ✓ Μυστικό MAC, για εγγραφή δεδομένων στον πελάτη
- ✓ Κλειδί, για εγγραφή δεδομένων στον εξυπηρετητή
- ✓ Κλειδί, για εγγραφή δεδομένων στον πελάτη
- ✓ Διανύσματα αρχικοποίησης της σύνδεσης
- ✓ Αριθμοί ακολουθίας (μεταξύ εξυπηρετητή και του πελάτη)
- ✓ Υλοποίηση Λύσης Ασφαλείας

Η διαδικασία υλοποίησης μιας λύσης ασφαλείας, πρέπει να λάβει χώρα με μεγάλη προσοχή ώστε να διασφαλισθεί η προστασία και η αδιάλειπτη λειτουργία της εγκατάστασης και να περιλαμβάνει τα ακόλουθα στάδια:

1. Καθορισμός προδιαγραφών συστημάτων ασφαλείας
2. Επιλογή των συστημάτων-προϊόντων ασφαλείας
3. Εγκατάσταση και χρήση των συστημάτων σε περιβάλλον δοκιμών
4. Ρύθμιση των συστημάτων ασφαλείας, βάση των επιμέρους πολιτικών ασφαλείας και έλεγχός τους σε περιβάλλον δοκιμών
5. Δημιουργία πλάνου εγκατάστασης των συστημάτων, στο περιβάλλον παραγωγής
6. Εγκατάσταση των συστημάτων ασφαλείας, στο περιβάλλον παραγωγής
7. Έλεγχος σωστής λειτουργίας των συστημάτων, σε πραγματικές συνθήκες

### **Ο ανθρώπινος παράγοντας<sup>49, 54</sup>**

Τα Intrusion Detection Systems (IDS), αποτελούν την προτελευταία γραμμή αμύνης ενός δικτύου απέναντι στους εσωτερικούς και εξωτερικούς εισβολείς. Υπάρχει ένα ακόμη επίπεδο ασφαλείας το οποίο, αν και δύσκολο στην εφαρμογή του, είναι απαραίτητο για την εξασφάλιση

της μακροπρόθεσμης ασφάλειας κάθε δικτύου. Η αναφορά αφορά φυσικά, στο προσωπικό που χρησιμοποιεί το δίκτυο.

Πρέπει να γίνει κατανοητό, πως η ασφάλεια δικτύων αποτελεί μια συνεχώς μεταβαλλόμενη διαδικασία και όχι ένα οχυρό η κατασκευή του οποίου αρκεί για να κρατήσει μακριά τους ανεπιθύμητους. Οι διαχειριστές των δικτύων κάθε επιχείρησης, πρέπει να έχουν άριστη γνώση της δομής του δικτύου που επιβλέπουν και να παρακολουθούν στενά τις εξελίξεις στο χώρο της ασφάλειας δεδομένων, για να εξασφαλίζουν πως οι άμυνές τους παραμένουν πάντοτε ισχυρές.

Κάθε μέρα αποκαλύπτονται νέα τρωτά σημεία στα ήδη υπάρχοντα συστήματα ασφαλείας, καθώς και της εμφάνισης νέων ισχυρότερων προγραμμάτων αυτόματης "σάρωσης" ενός δικτύου, για την ανακάλυψη και εκμετάλλευση ευάλωτων σημείων (τα αυτόματα προγράμματα αξιοποίησης αυτών των αδυναμιών ονομάζονται exploits).

Κάθε διαχειριστής δικτύου λοιπόν, πρέπει να σκέφτεται και να ενεργεί ως cracker του δικού του δικτύου, δοκιμάζοντας κάθε νέο εργαλείο εύρεσης αδυναμιών όπως το SATAN (Security Administrator Tool for Analyzing Networks) και κλείνοντας ο ίδιος τις τρύπες που ανακαλύπτει, ή που ανακαλύπτουν άλλοι, σε άλλα παρόμοια δίκτυα, πριν αυτές γίνουν αντιληπτές από τρίτους και χρησιμοποιηθούν εναντίον του δικτύου.

Οι διαδικασίες ασφαλείας όμως, δεν περιορίζονται μόνο στους διαχειριστές του εσωτερικού δικτύου. Πρέπει να γίνουν συνείδηση για όλους τους εργαζομένους, καθώς ακόμη και το υψηλότερο επίπεδο ασφαλείας είναι άχρηστο αν η γραμματέας κολλήσει το password της επάνω στην οθόνη για να το έχει πρόχειρο, αν ο πωλητής χάσει το notebook μέσα στο οποίο είναι γραμμένα τα στοιχεία πρόσβασης στο δίκτυο ή αν το υψηλόβαθμο στέλεχος επιλέξει ως συνθηματικό το 123456 "για να το θυμάται εύκολα" (πράγμα συχνά κατανοητό αφού πολλές φορές για λόγους ασφαλείας η μηχανογράφηση έχει την παράλογο απαίτηση από το προσωπικό να θυμάται 27 διαφορετικά passwords τα οποία φυσικά δεν επιτρέπεται να γράψει πουθενά).

Τέλος, πολλά αξιόλογα συστήματα ασφαλείας παραβιάζονται καθημερινά, επειδή κάποιιοι από τους χρήστες του εσωτερικού δικτύου συνδέονται μέσω dialup σύνδεσης με το Διαδίκτυο, παρακάμπτοντας το εταιρικό Firewall για "να κάνουν πιο εύκολα τη δουλειά τους" (για παράδειγμα, να χρησιμοποιήσουν εκείνο το πρόγραμμα χρηματιστηρίου που δεν μπορεί να λειτουργήσει για όσους χρήστες συνδέονται μέσω Firewall). Δυστυχώς, δεν υπάρχουν εύκολες απαντήσεις στον τομέα της ασφάλειας δικτύων. Με προσοχή και μεθοδικότητα μπορεί να αυξηθεί η δυσκολία προσβολής, αλλά ο κίνδυνος παραβίασης κάθε εταιρικού δικτύου θα παραμείνει πάντοτε μια λιγότερο ή περισσότερο πιθανή εξέλιξη.

## 2.7 Ασφάλεια Διαδικτυακών Υπηρεσιών

Για την επίτευξη ασφαλούς ανταλλαγής πληροφοριών, μεταξύ πελάτη – διακομιστή, σε μια σύνοδο Διαδικτυακών Υπηρεσιών (Web Services Session) διακρίνονται οι εξής περιπτώσεις:

- ✓ Σύνδεση με HTTP
- ✓ Σύνδεση με HTTPS
- ✓ Σύνδεση με SOAP Security Extensions. Τα extensions αυτά είναι:
  1. Security Assertion Markup Language (SAML)
  2. Extensible Access Control Markup Language (XACML)
  3. XML Key Management Specification (XKMS)
  4. XML Encryptions
  5. XML Signature
  6. WS-Security

### **Βασική πιστοποίηση για συνδέσεις πάνω από HTTP 1.1**

Χρησιμοποιείται όνομα χρήστη και κωδικός για την είσοδο σε προστατευμένους πόρους του διακομιστή. Τα στοιχεία αυτά, στέλνονται συνήθως με κάποια κωδικοποίηση (όπως για παράδειγμα, με χρήση του αλγορίθμου MD5), για προστασία από υποκλοπή που θα συνέβαινε στην περίπτωση μετάδοσης απλού κειμένου. Το πρόβλημα εδώ, είναι ότι το σώμα του αποστέλλομένου μηνύματος, δεν κρυπτογραφείται. Για περισσότερη ασφάλεια στην πράξη, χρησιμοποιούνται κατά την μετάδοση σύνδεσμοι, από τις τεχνολογίες δημοσίου κλειδιού και Kerberos.

### **Πιστοποίηση χρήστη για συνδέσεις πάνω από HTTPS**

Στην περίπτωση αυτή γίνεται χρήση ψηφιακών πιστοποιητικών και του SSL για ασφαλή μετάδοση. Συνήθως η σύνδεση γίνεται στην θύρα 443, αντί για τη θύρα 80 στην οποία γίνονται οι συνδέσεις HTTP. Το πρόβλημα με τις Διαδικτυακές Υπηρεσίες είναι ότι κατά την εκτέλεση τους μερικές φορές χρειάζεται η πληροφορία να περάσει και από κάποιον τρίτο ενδιάμεσο κόμβο και έτσι το HTTPS δεν μπορεί να εξασφαλίσει ότι η πληροφορία δεν αλλοιώθηκε κατά την μετάβαση στον ενδιάμεσο αυτό κόμβο.

### **Άλλες μέθοδοι πιστοποίησης χρήστη**

Γενικά οι εφαρμογές που κάνουν χρήση εγγράφων XML, μέσω SOAP, έχουν πολύ υψηλές απαιτήσεις σε ασφάλεια, μιας και τα έγγραφα XML, είναι σε απλό κείμενο και όχι σε δυαδική μορφή. Έτσι, είναι πάρα πολύ εύκολη η αλλοίωση τους. Για την επίτευξη της ασφάλειας εφαρμόζονται, οι παρακάτω τεχνολογίες:

- ✓ **XML Signature:** Το World Web Consortium, μαζί με την επιτροπή Internet Engineering Task Force, έχει ορίσει το πρότυπο της υπογραφής XML (XML Signature), δηλαδή ενός αρχείου XML, που αποτελεί ψηφιακή υπογραφή για κάποιο περιεχόμενο. Το πρότυπο κάνει χρήση των αλγορίθμων DSS και SHA-1. Με τη χρήση της υπογραφής XML μπορούν να υπογραφούν αρχεία οποιουδήποτε τύπου. Το περιεχόμενο που υπογράφεται, μπορεί να βρίσκεται εντός ή και εκτός του αρχείου XML της υπογραφής. Στην δεύτερη περίπτωση απλά υπάρχει μια αναφορά με URL, στο περιεχόμενο που υπογράφεται. Αυτό επειδή, η τιμή σωρού, που προκύπτει με την εφαρμογή της συνάρτησης σωρού, θα είναι διαφορετική για αρχεία XML να λαμβάνουν μια 'κανονική μορφή', πριν δημιουργηθεί η XML υπογραφή τους. Παράλληλα με τα παραπάνω, εφαρμόζεται και το πρότυπο της κρυπτογράφησης XML (XML Encryption), με το οποίο μπορούν να κρυπτογραφηθούν ανεξάρτητα τα διάφορα στοιχεία ενός εγγράφου XML.
- ✓ **Πρότυπο XKMS:** Γίνεται η διαχείριση των δημοσίων και ιδιωτικών κλειδιών στις Διαδικτυακές Υπηρεσίες. Αποτελείται από τα βασικά συστατικά XML Key Information Service Specification (X-KISS) και XML Key Information Service Specification (X-KRSS).
- ✓ **Γλώσσα SAML:** Υλοποιείται το πρότυπο PMI (Permissions Management Infrastructure). Το πρότυπο PMI, διαμέσου ενός συνόλου κανόνων και πολιτικών ελέγχει την ταυτοποίηση χρηστών σε ένα σύστημα. Η υλοποίηση του PMI με την SAML αφορά σε B2C (εμπορικές ιστοσελίδες) και B2B εφαρμογές. Με την SAML γίνεται εφαρμογή συγκεκριμένων πολιτικών ασφαλείας (security policies). Η περιγραφή των

πολιτικών αυτών και η πιστοποίηση χρηστών και διεργασιών βάσει κριτηρίων γίνεται με πολλούς τρόπους. Ένας από αυτούς, είναι με την μορφή Extensible Access Control Markup Language (XACML), που υλοποιείται από την εταιρεία Oasis Group. Η XACML είναι μια γλώσσα που περιγράφει αναλυτικά τα κριτήρια πρόσβασης σε υπολογιστικούς πόρους και σε πληροφορίες διαθέσιμες στο Διαδίκτυο.

## 2.8 Ηλεκτρονικές Υπηρεσίες και Ασφάλεια <sup>56</sup>

Τα web services παρέχουν πολλά πλεονεκτήματα στις εφαρμογές, αλλά επίσης εκθέτουν σημαντικούς νέους κινδύνους στην ασφάλεια. Η δημιουργία και η διατήρηση ενός ασφαλούς περιβάλλοντος web services περιλαμβάνει και τη διαχείριση διαφόρων μηχανισμών για το διαδίκτυο, την XML και τα ίδια τα web services.

Η γενική αντιμετώπιση αφορά τα παρακάτω <sup>15</sup>:

- ✓ Ασφάλεια σε επίπεδο μεταφοράς, όπως τα τύχη προστασίας (firewalls), τα ιδεατά ιδιωτικά δίκτυα (VPNs), η επικύρωση (authentication), η μη αποκήρυξη ευθύνης (non-repudiation), και η κρυπτογράφηση (encryption).
- ✓ Ασφάλεια σε επίπεδο μηνύματος, όπως τα στοιχεία επικύρωσης (authentication tokens) για να επικυρώσουν την ταυτότητα του αιτούντα και οι δηλώσεις έγκρισης (authorization assertions) για να ελέγξουν την πρόσβαση στις υπηρεσίες του πάροχου.
- ✓ Ασφάλεια σε επίπεδο δεδομένων, όπως είναι η κρυπτογράφηση (encryption) και η ηλεκτρονική υπογραφή (digital signature), για την προστασία ενάντια στις αθέμιτες αλλαγές των δεδομένων.
- ✓ Ασφάλεια σε επίπεδο περιβάλλοντος, όπως είναι η διαχείριση (management), η αναγραφή (logging) και ο έλεγχος (auditing) για την αναγνώριση των προβλημάτων που πρέπει να διορθωθούν.

Για την αντιμετώπιση όλων των παραπάνω δημιουργήθηκε μια ομάδα από προδιαγραφές που είναι ακόμη υπό ανάπτυξη. Οι κυριότερες από αυτές είναι οι παρακάτω <sup>15, 55</sup>:

- ✓ **WS-Security:** καθορίζει μια αρχιτεκτονική για ασφαλή επικοινωνία.
- ✓ **WS-Policy:** οι σχετικές με αυτήν προδιαγραφές, καθορίζουν μια πολιτική από κανόνες για το πώς οι υπηρεσίες θα αλληλεπιδρούν μεταξύ τους.
- ✓ **WS-Trust:** καθορίζει το μοντέλο εμπιστοσύνης, για ασφαλείς συναλλαγές.
- ✓ **WS-Privacy:** καθορίζει, πώς τηρείται η ιδιαιτερότητα στις πληροφορίες.
- ✓ **WS-Secure Conversation:** καθορίζει, πώς θα επιτευχθεί μια ασφαλή συνεδρία μεταξύ υπηρεσιών που ανταλλάσσουν δεδομένα με κανόνες ορισμένους στα WS-Policy, WS-Trust, WS-Privacy.
- ✓ **WS-Federation:** καθορίζει τους κανόνες, σχετικά με την ταυτότητα σε καταναμημένο περιβάλλον.
- ✓ **WS-Authorization:** χειρίζεται την επεξεργασία, για την επικύρωση που αφορά στην πρόσβαση και την ανταλλαγή δεδομένων.

Όλα τα παραπάνω χρησιμοποιούν το SOAP Header και έτσι εκμεταλλεύονται στο έπακρο την επεκτασιμότητα του πρωτοκόλλου SOAP.

### Web services και μηνυματοδότηση (messaging)

Υπάρχει μία ομάδα προδιαγραφών, που πραγματεύεται ζητήματα που έχουν να κάνουν με την αξιόπιστη αποστολή μηνυμάτων (reliable messaging) και τις ειδοποιήσεις (notification) <sup>15</sup>:

- ✓ **WS-ReliableMessaging** και **WS-Reliability**: καθορίζουν μηχανισμούς για την εξασφάλιση της παράδοσης των μηνυμάτων, με τη σωστή σειρά, και την εξάλειψη των διπλότυπων.
- ✓ **WS-Eventing** και **WS-Notification**: παρέχουν ένα μηχανισμό σχετικά με τα γεγονότα (events), ώστε οι συνδρομητές να ειδοποιούνται ανεξάρτητα από τη σχέση μεταξύ του παρόχου και του αιτούντα.

Και οι παραπάνω τεχνολογίες, χρησιμοποιούν το SOAP Header.

### Αλληλεπίδραση Ηλεκτρονικών Υπηρεσιών (transactions)

Οι συναλλαγές, αποτελούν ένα πολύ σημαντικό χαρακτηριστικό, το οποίο έχει αποδειχθεί πολύ χρήσιμο στο πέρασμα των χρόνων. Οι συναλλαγές στο περιβάλλον των web services, εξασφαλίζουν ότι μία ομάδα από web services, πετυχαίνει ένα κοινό αποτέλεσμα. Τα web services συχνά, εξαρτώνται το ένα από το άλλο για να ολοκληρώσουν πολύπλοκες αιτήσεις σε μία εφαρμογή, όπως η ενημέρωση μιας εγγραφής πελάτη (η οποία μπορεί να ενημερώνει πολλαπλές βάσεις δεδομένων με στοιχεία πελάτη) ή η επεξεργασία μίας παραγγελίας (η οποία μπορεί να ενημερώνει πολλαπλές βάσεις δεδομένων αποθηκών) <sup>15</sup>. Οι πιο σημαντικές προσπάθειες που σχετίζονται με τις συναλλαγές στο περιβάλλον των web services, είναι οι παρακάτω <sup>15</sup>:

- ✓ **WS-Transaction**: μία οικογένεια προδιαγραφών που περιλαμβάνει:
  1. **WS-AtomicTransactions (WS-AT)**: Ένα πρωτόκολλο two-phase commit, για διαλειτουργικότητα των web services.
  2. **WS-BusinessActivity (WS-BA)**: Ένα ανοικτό ενσωματωμένο πρωτόκολλο, για μακροπρόθεσμες επιχειρησιακές διαδικασίες.
  3. **WS-Coordination (WS-C)**: Ένα πλαίσιο συντονισμού, που υποστηρίζει τα WS-AT και WS-C.
- ✓ **WS-Composite Application Framework**: μία οικογένεια προδιαγραφών που περιλαμβάνει:
  1. **WS-Context (WS-CTX)**: Ένας γενικός μηχανισμός διαχείρισης πλαισίου.
  2. **WS-CoordinationFramework (WS-CF)**: Ένα πλαίσιο συντονισμού, που υποστηρίζει τα WS-AT, WS-BA, και τα τρία πρωτόκολλα στο WS-TXM.
  3. **WS-TransactionManagement (WS-TXM)**: Ένα πρωτόκολλο για two-phase commit, για διαλειτουργικότητα των Web Services (ACID), ένα πρωτόκολλο βασισμένο στη διόρθωση (compensation), για μακροπρόθεσμες διαδικασίες (LRA) και ένα πρωτόκολλο διαχείρισης επιχειρησιακών διαδικασιών (BP).

Παρακάτω, στον πίνακα 4, παραθέτονται επίσης, τα μέτρα ασφαλείας ενός πληροφοριακού συστήματος και τα οποία μπορούν να αναλυθούν στις παρακάτω βασικές κατηγορίες:

<b>Βασικές κατηγορίες μέτρων ασφαλείας του Πληροφοριακού Συστήματος (ΠΣ)</b>	<b>Επιμέρους κατηγορίες των βασικών μέτρων ασφαλείας του Πληροφοριακού Συστήματος (ΠΣ)</b>
<b>Οργάνωση και διαχείριση της ασφαλείας του πληροφοριακού συστήματος</b>	<ol style="list-style-type: none"> <li>1. Σχεδιασμός της ασφαλείας του ΠΣ</li> <li>2. Κώδικας δεοντολογίας</li> <li>3. Έλεγχος, επιθεώρηση και εποπτεία της ασφαλείας του ΠΣ</li> <li>4. Ρόλοι και αρμοδιότητες υλοποίησης και διαχείρισης της ασφαλείας του ΠΣ</li> <li>5. Τεκμηρίωση και εγχειρίδια χρήσης των διαδικασιών και λειτουργιών σχετικά με την ασφάλεια του ΠΣ</li> <li>6. Εκπαίδευση, ευαισθητοποίηση, ενημέρωση χρηστών</li> </ol>
<b>Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος</b>	<ol style="list-style-type: none"> <li>1. Ανάπτυξη και συντήρηση εφαρμογών (Application development and maintenance)</li> <li>2. Διαχείρισης της υποστήριξης και απόκτησης υλικού και λογισμικού από προμηθευτές (Vendor support – contracts and reliability)</li> <li>3. Απογραφή του υλικού και λογισμικού και διαχείριση των αλλαγών (Hardware and software inventory)</li> </ol>
<b>Φυσική ασφάλεια</b>	<ol style="list-style-type: none"> <li>1. Ασφάλεια κτιριακών εγκαταστάσεων</li> <li>2. Ασφάλεια εξοπλισμού πληροφορικής και τηλεπικοινωνιακής υποδομής</li> <li>3. Προστασία από φυσικές καταστροφές (Environmental controls)</li> </ol>
<b>Ασφάλεια δεδομένων</b>	<ol style="list-style-type: none"> <li>1. Μηχανισμοί εξασφάλισης ακεραιότητας και εμπιστευτικότητας των δεδομένων</li> <li>2. Κατηγοριοποίηση, ταξινόμηση των δεδομένων (Classification of data/ information)</li> </ol>
<b>Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής</b>	<ol style="list-style-type: none"> <li>1. Διαδικασίες διαχείρισης εφεδρικών αντιγράφων ασφαλείας</li> <li>2. Διαδικασίες αντιμετώπισης ιομορφών</li> <li>3. Διαδικασίες διαχείρισης συνθηματικών</li> <li>4. Ασφάλεια εφαρμογών-λογισμικού</li> <li>5. Ασφάλεια βάσεων δεδομένων</li> <li>6. Ασφάλεια δικτύων και τηλεπικοινωνιών και ασφάλεια κατά τη σύνδεση στο Internet</li> <li>7. Έλεγχος προσπέλασης του ΠΣ</li> <li>8. Μηχανισμοί καταγραφής συμβάντων και περιστατικών ή προσπαθειών παραβίασης της ασφαλείας του ΠΣ</li> </ol>
<b>Ανάκαμψη από καταστροφές</b>	<ol style="list-style-type: none"> <li>1. Σχέδιο έκτακτης ανάγκης</li> </ol>

Πίνακας 4: Μέτρα Ασφαλείας ενός Πληροφοριακού Συστήματος.

## 2.9 Αδυναμίες και Απειλές <sup>57</sup>

Το σύνολο των γνωστών αδυναμιών που είναι δυνατό να εμφανισθούν σε μία Ιστοσελίδα και που σχετίζονται με ανάλογες απειλές, αναφέρονται στις παρακάτω κατηγορίες. Οι κατηγορίες Αδυναμιών και Απειλών αναφέρονται σε:

- ✓ Διαχείριση Διαμόρφωσης της Υποδομής (Infrastructure Configuration Management) <sup>58</sup> : κακή διαμόρφωση των web-servers, application-servers και firewalls.

- ✓ Διαχείριση Διαμόρφωσης των Εφαρμογών (Application Configuration Management): κακή διαμόρφωση των εφαρμογών και της ανάπτυξης των διαφόρων επιπέδων τους.
- ✓ Επικύρωση Εγκυρότητας των δεδομένων Εισόδου/Εξόδου (Boundary Validation Vulnerabilities)<sup>59</sup> : μη επαρκής έλεγχος των δεδομένων I/O.
- ✓ Αυθεντικοποίηση και Έλεγχο Πρόσβασης (Authentication and Access Control): αυθεντικοποίηση χρήστη καθώς και ελεγχόμενη πρόσβαση στους πόρους του συστήματος.
- ✓ Προστασία Δεδομένων (Data Protection): προστασία από μη εξουσιοδοτημένους χρήστες.
- ✓ Υπερχείλιση Buffer (Buffer Overflows): φτωχή κωδικοποίηση που μπορεί να εκθέσει σε κίνδυνο το σύστημα.
- ✓ Λάθη στη Λογική των Εφαρμογών (Application Logic Flaws): επιχειρησιακής λογικής αποφάσεις, που δεν εκτελούνται όπως έχει σχεδιαστεί το σύστημα.
- ✓ Ζητήματα Διαχείρισης Συνόδων (Session Management Issues): λήξη χρόνου συνόδου, πειρατεία ή δέσμευση συνόδου.
- ✓ Παραβίαση Ιδιωτικότητας Χρηστών (User Privacy Violations): ζητήματα, που μπορούν να αποκαλύψουν προσωπικές πληροφορίες χρηστών.
- ✓ Χειρισμό Λαθών και Εξαιρέσεων (Error and Exception Handling): λάθη του συστήματος, που μπορούν να δώσουν πληροφορίες για την κατάστασή του.

## 2.10 Μέθοδοι Ασφαλείας<sup>60</sup>

Οι βασικές μέθοδοι της ασφάλειας των web εφαρμογών είναι:

**Επιθεώρηση ασφαλείας (security audit)<sup>62</sup>** : Ένα σύστημα ελέγχεται, με βάση ένα σύνολο από πίνακες ελέγχου (checklists), οι οποίοι διαμορφώνονται με βάση διεθνή πρότυπα σχετικά με την ασφάλεια και τις κατάλληλες πολιτικές ασφαλείας ενός οργανισμού. Οι ελεγκτές εκτελούν την εργασία τους μέσα από προσωπικές συνεντεύξεις, ανιχνεύσεις αδυναμιών, εξετάσεις των ρυθμίσεων, αναλύσεις των διαμοιρασμένων πόρων δικτύου και μελέτες των ιστορικών στοιχείων (log files).

**Αυτο-αξιολόγηση ασφαλείας (security self-assessment)<sup>61</sup>** : Δεν υπάρχουν συγκεκριμένα πρότυπα - standards, ως προς τα οποία θα μετρηθεί το σύστημα, αλλά ο στόχος προσδιορίζεται από την περιοχή που χρειάζεται διερεύνηση και βελτίωση στη θωράκισή της. Η μέθοδος αυτή, ξεπερνά τους πίνακες ελέγχου (checklists) και επεκτείνεται, σε ένα πιο λεπτομερή έλεγχο για εντοπισμό αδυναμιών, αλλά και σε συστάσεις για επιδιορθώσεις και βελτιώσεις. Πλεονέκτημα της είναι, η δυνατότητα να οριστούν επίπεδα προτεραιότητας σε κάθε συστατικό που αξιολογείται, έτσι ώστε με την ολοκλήρωσή της, να δοθεί μια σειρά προτεραιότητας στην επιδιόρθωση των αδυναμιών.

**Δοκιμή διείσδυσης (penetration testing ή "ethical hacking")<sup>63</sup>** : Είναι η ελεγχόμενη προσομοίωση μιας επίθεσης, προκειμένου να επιτευχθεί ένας προκαθορισμένος στόχος. Σκοπός της είναι, να εντοπιστούν συγκεκριμένες πληροφορίες (σχετικές με την ύπαρξη γνωστών αδυναμιών) και να διερευνηθεί κατά πόσο είναι δυνατόν ένας ξένος, κάνοντας χρήση αυτών των πληροφοριών, να μπορέσει να δημιουργήσει προβλήματα. Δεν έχει σκοπό να εντοπίσει όλες τις αδυναμίες, αλλά να αποδείξει ότι η ασφάλεια του συστήματος μπορεί να διακυβευτεί. Η δοκιμή μπορεί να πραγματοποιηθεί, με βάση μηδενική γνώση (zero knowledge), ή με πλήρη γνώση (full knowledge) του συστήματος που δοκιμάζεται. Χρησιμοποιείται, για να καθορίσει την αξιοπιστία

και τη δύναμη των μέτρων ασφαλείας που παίρνονται (Οι “ethical hackers” προσπαθούν να υιοθετήσουν τις επιθέσεις και τις τεχνικές των hackers, για να μετρήσουν το επίπεδο ασφαλείας).

### Σύγκριση των Μεθόδων Μέτρησης Ασφάλειας

Για τον έλεγχο της ασφαλείας μιας web εφαρμογής με τις μεθόδους της επιθεώρησης ασφαλείας και της αυτο-αξιολόγησης, απαιτείται η μετακίνηση μιας μεγάλης ομάδας ειδικών ασφαλείας, στον τόπο που λειτουργεί ο οργανισμός, του οποίου η ασφάλεια της εφαρμογής ελέγχεται. Η ομάδα αυτή, πρέπει να έχει στη διάθεση της, τις κατάλληλες λίστες, να έχει υψηλή τεχνογνωσία και να είναι άρτια συντονισμένη. Για την ενέργεια των ελέγχων, απαιτείται πολύς χρόνος, ώστε να ολοκληρωθούν οι συνεντεύξεις, οι επιθεωρήσεις, οι αξιολογήσεις και οι έρευνες, στη διάρκεια των οποίων αποκαλύπτεται και διαταράσσεται η λειτουργία του οργανισμού.

Όλα τα παραπάνω, σε συνάρτηση με την ανάγκη για συνεχείς και επαναλαμβανόμενους ελέγχους, καθιστούν τη δοκιμή διείσδυσης, μονόδρομο και η οποία έχει τα εξής πλεονεκτήματα:

Απαιτείται ελάχιστο προσωπικό και δεν είναι αναγκαία η μετακίνηση του, παρέχει δυνατότητα πλήρους αυτοματοποίησης, διαρκεί ελάχιστο χρόνο και είναι εύκολα επαναλαμβανόμενη. Δεν απαιτεί, την σε βάθος γνώση της εφαρμογής που ελέγχεται, δεν διαταράσσει τη λειτουργία της και είναι πολύ οικονομική.

#### 2.10.1 Τεχνικές Δοκιμής Διείσδυσης

Υπάρχουν δύο κύριες προσεγγίσεις τεχνικών ελέγχου ασφαλείας των web εφαρμογών, με τη μέθοδο της δοκιμής διείσδυσης. Η Χειροκίνητη (manual), όπου όλη η διαδικασία ελέγχου γίνεται βήμα-βήμα, χωρίς την ύπαρξη αυτοματισμών επανάληψης παρόμοιων βημάτων και η Αυτοματοποιημένη (automated), όπου με τη χρήση εργαλείων, αυτοματοποιούνται μερικοί ή όλοι οι έλεγχοι και οι διαδικασίες ελέγχου. Η δεύτερη διακρίνεται σε δύο τεχνικές:

- ✓ **Black Box:** είναι η εφαρμογή δοκιμαστικών δεδομένων που έχουν προέλθει από καθορισμένες λειτουργικές απαιτήσεις, χωρίς να λαμβάνουν υπόψη τη δομή της εφαρμογής στην οποία εφαρμόζονται. Η εφαρμογή εξετάζεται χρησιμοποιώντας την εξωτερική της διεπαφή, αυτή που χρησιμοποιούν οι απλοί χρήστες. Μιμούνται την ακολουθία αλληλεπιδράσεων χρήστη-εφαρμογής και κάθε αποτυχία δείχνει ότι ο χρήστης έλαβε ανεπαρκή υπηρεσία.
- ✓ **White Box:** εξετάζεται η δομή της εφαρμογής και βάση αυτής καθορίζονται τα δεδομένα της δοκιμής. Εξετάζεται η εσωτερική δομή της εφαρμογής, χρησιμοποιώντας τη διεπαφή προγραμματισμού εφαρμογών (Application Programmatic Interface – που αποτελεί το μέσο επικοινωνίας των εφαρμογών, με τον πυρήνα του Λειτουργικού Συστήματος ή με βιβλιοθήκες τρίτων κατασκευαστών).

64, 65

#### 2.11 Εργαλεία Ελέγχου Ασφαλείας

Τα εργαλεία διακρίνονται, ως προς το σύνολο των ελέγχων που πραγματοποιούν, σε:

**Επιχειρησιακού επιπέδου (Enterprise level):** διεξάγουν ελέγχους για το σύνολο των γνωστών αδυναμιών, βάση ενημερωμένων βιβλιοθηκών. Αποτελούνται, από μια συλλογή εργαλείων και ανιχνεύουν τις εφαρμογές με την τεχνική, Black box δοκιμής διείσδυσης που



προαναφέρθηκε. Επιτρέπουν την αυτόματη ανίχνευση, αλλά και με ειδικά σενάρια, είτε ως προς τα σημεία ανίχνευσης, είτε ως προς τα είδη των αδυναμιών. Επίσης, επιτρέπουν και χειροκίνητους ελέγχους. (για παράδειγμα, Sanctum AppScan, KaVaDo ScanDo, SPI Dynamics WebInspect και OWASP WebScarab).

**Εστιασμένα (Focused):** εκτελούν συγκεκριμένες λειτουργίες ή αυτοματοποιούν ένα ή περισσότερα τεστ ελέγχου. Αποτελούν, στοιχειώδεις δομικές μονάδες, που βοηθούν στην οικοδόμηση μιας ακολουθίας δοκιμών ασφαλείας, αλλά για να πραγματοποιηθεί μια δοκιμή από τη βάση με αυτά, απαιτεί πολύ χρόνο. (για παράδειγμα, WebSphinx, AtStake WebProxy, Nikto, SPIKE Proxy, WebserverFP και Mielielkoek.pl).

Ακόμα, τα εργαλεία διακρίνονται ως προς τον κώδικα τους σε:

**Κλειστού κώδικα (Close - proprietary source):** δηλαδή, τα εμπορικά εργαλεία διαφόρων εταιριών, ανήκουν όλα τα Επιχειρησιακού επιπέδου (Enterprise level), εκτός από το WebScarab, το οποίο είναι ένα εργαλείο ανοικτού κώδικα, του οργανισμού OWASP (Open Web Application Security Project), ο οποίος είναι ένας μη κερδοσκοπικός οργανισμός για την ασφάλεια των Web εφαρμογών.

**Ανοικτού κώδικα (Open source):** περιλαμβάνονται και τα ελεύθερας χρήσεως εργαλεία (δηλαδή εργαλεία για μη εμπορική χρήση). Σε αυτή την κατηγορία, ανήκουν όλα τα Focused εργαλεία.

Τα Κλειστού κώδικα εργαλεία είναι ολοκληρωμένα προϊόντα, που δίνουν μεγάλη προσοχή στην ευκολία χρήσης από προσωπικό, μη ειδικό σε θέματα ασφαλείας.

Στο σύνολο τους τα εμπορικά εργαλεία, έχουν λίγο πολύ, τα ίδια βασικά λειτουργικά χαρακτηριστικά γνωρίσματα. Στοχεύουν στην παροχή μιας σαφούς ροής εργασιών ή μιας ολοκληρωμένης διαδικασίας, για την αξιολόγηση της ασφάλειας μιας web εφαρμογής. Προσφέρουν επίσης, πολύ περισσότερα χαρακτηριστικά γνωρίσματα από οποιοδήποτε από τα Ανοικτού κώδικα εργαλεία. Το πρόβλημα με τα Κλειστού κώδικα εργαλεία είναι, ότι χρησιμοποιούν ιδιωτικές βάσεις δεδομένων αδυναμιών και είναι δύσκολο να αξιολογηθεί πόσο περιεκτικές είναι αυτές και συνεπώς πόσο αποτελεσματικοί είναι οι έλεγχοι τους. Έχουν το πλεονέκτημα της υποστήριξης των χρηστών, έναντι αμοιβής βέβαια. Ένα άλλο πρόβλημα των Κλειστού κώδικα εργαλείων, είναι η δυσκολία επέκτασής τους, που βασίζεται στη διακριτική ευχέρεια των εταιριών που τα παρέχουν. Σε αντίθεση, τα Ανοικτού κώδικα είναι πολύ πιο εύκολα επεκτάσιμα, πράγμα που ενισχύει την εντύπωση ότι έχουν πιο ενημερωμένες βάσεις δεδομένων αδυναμιών, κάτι που τα κάνει πολύ δημοφιλή.

Συμπερασματικά, τα εστιασμένα εργαλεία είναι απαραίτητα σε έναν ελεγκτή ασφαλείας, με κατάλληλο θεωρητικό υπόβαθρο και εξειδίκευση. Μπορούν να γίνουν όμως επικίνδυνα, για κάποιον χωρίς γνώσεις που πειραματίζεται με αυτά, καθιστώντας τον επικίνδυνο για τις εφαρμογές πάνω στις οποίες τα δοκιμάζει. Τα Επιχειρησιακού επιπέδου εργαλεία, είναι κατάλληλα για κάθε επιχείρηση που θέλει να διεξάγει δικούς της ελέγχους ασφαλείας, χωρίς να έχει την ανάγκη εξωτερικών παραγόντων. Τέλος, τα Ανοικτού κώδικα, Επιχειρησιακού επιπέδου εργαλεία, είναι κατάλληλα για την εκπαίδευση και την έρευνα πάνω στον τομέα του ελέγχου ασφαλείας των web εφαρμογών, παρόλο που δεν είναι πολύ φιλικά προς τους χρήστες και απαιτούν θεωρητικό υπόβαθρο γνώσεων.

## 2.12 Βιβλιογραφία 2<sup>ου</sup> Κεφαλαίου

36. [http://www.mycrypto.net/encryption/crypto\\_algorithms.html](http://www.mycrypto.net/encryption/crypto_algorithms.html), Encryption Algorithms

37. Σύγχρονη Κρυπτογραφία, Δρ. Ε. Μάγκος Κέρκυρα, 2009

38. Tanenbaum A., Δίκτυα Υπολογιστών, Εκδόσεις Κλειδάριθμος, 2003
39. <http://www.us-cert.gov/cas/tips/ST04-015.html>
40. Forouzan B., Introduction to Data Communications and Networking, McGraw-Hill, 2003.
41. <http://www.eeci.gr>
42. <http://www.faqs.org/faqs/firewalls-faq/>
43. Article: Security, privacy, and confidentiality issues on the Internet, Grant Kelly, Bruce McKenzie at <http://www.jmir.org/>
44. <http://technet.microsoft.com/en-us/library/bb727017.aspx>
45. [http://articles.techrepublic.com.com/5100-22\\_11-5756029.html](http://articles.techrepublic.com.com/5100-22_11-5756029.html)
46. Animesh Patcha, Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061, USA, 8 June, 2006.
47. Διπλωματικές Εργασίες: “Μελέτη των επιθέσεων που στηρίζονται σε πακέτα με ψευδή IP διεύθυνση αποστολέα (IP spoofing)” του Ιωάννου Παπαπάνου και “ISLAB HACK: Βασικές Έννοιες & Προγραμματισμός του SNORT 2.0” του Δημήτρη Πρίτσου. (<http://www.islab.demokritos.gr>)
48. Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, Rafeeq Ur Rehman ([www.phptr.com](http://www.phptr.com)) - To open source and free software developers, 2003 Pearson Education, Inc.
49. Εργασία IDS – Intrusion Detection Systems στο μάθημα «Ασφάλεια Δικτυοκεντρικών Συστημάτων» του Τμήματος: Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς. Υπεύθυνος Καθηγητής: Σωκράτης Κάτσικας, Παρουσίαση: Πλακογιάννης Φωτίου Πέτρος, Λέων Χρήστος, Μενδρινός Ιωάννης.
50. S. Kumar, E.H. Spafford, An application of pattern matching in intrusion detection, The COAST Project, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA, Technical Report CSD-TR-94-013, June 17, 1994.
51. A. Patcha, J.-M. Park, Detecting denial-of-service attacks with incomplete audit data, in: Proceedings of the 14th International Conference on Computer Communications and Networks, San Diego, CA, USA, 2005.
52. D. Newman, J. Snyder, R. Thayer, Crying wolf: False alarms hide attacks, in: Network World: Network World, 2002.
53. T. Ptacek, T. Newsham, Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, Secure Networks Inc, 1998.
54. A. Liu, C. Martin, T. Hetherington, S. Matzner, A comparison of system call feature representations for insider threat detection, in: Proceedings of the 6th Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, West Point, NY, 2005.
55. [http://www.iso.org/iso/support/faqs/faqs\\_widely\\_used\\_standards/widely\\_used\\_standards\\_oth\\_er/information\\_security.htm](http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_oth_er/information_security.htm)
56. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities - By Mark Dowd, John McDonald, Justin Schuh
57. <http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=103>
58. <http://www.ca.com/us/configuration-management.aspx>
59. <http://www.crhc.illinois.edu/DEPEND/>
60. <http://www.oas.org/legal/english/admmem/admmem90.htm>
61. <http://www.itl.nist.gov/lab/bulletns/bltnsep01.htm>

62. <http://www.itsecurity.com/features/it-security-audit-010407/>
63. [http://www.infosecinstitute.com/blog/ethical\\_hacking\\_computer\\_forensics.html](http://www.infosecinstitute.com/blog/ethical_hacking_computer_forensics.html)
64. <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16696&TEMPLATE=/ContentManagement/ContentDisplay.cfm>
65. <http://e-articles.info/t/i/1627/i/gr/>

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΡΠΑΣ

## ΚΕΦΑΛΑΙΟ 3

### ΠΟΙΟΤΗΤΑ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

#### 3.1 Βασικά Χαρακτηριστικά Ποιότητας

1. Το πρότυπο ISO8402-1986<sup>69</sup>, ορίζει την ποιότητα ως το σύνολο των χαρακτηριστικών μιας οντότητας, που της αποδίδουν την ικανότητα να ικανοποιεί εκφρασμένες και συνεπαγόμενες ανάγκες. Σε πολλές περιπτώσεις οι ανάγκες μπορούν να μεταβάλλονται με την πάροδο του χρόνου, πράγμα που συνεπάγεται την αναγκαιότητα περιοδικής ανασκόπησης των απαιτήσεων για την ποιότητα. Αποτελεί, δηλαδή, έναν ορισμό, που βασίζεται σε δύο κλασσικές διαστάσεις της ποιότητας: την καταλληλότητα, ως προς τον σκοπό και την συμμόρφωση, ως προς τις απαιτήσεις
2. CARVIN(1988)<sup>78</sup>: ‘‘Η ποιότητα είναι μια απλή, μια αναλύσιμη ιδιότητα που μαθαίνουμε να την αναγνωρίζουμε μόνο με την πείρα μας.’’
3. JOSEPH .M. JURAN<sup>66</sup>: Προτείνει την χρήση μιας κυκλικής διαδικασίας του management ποιότητας, που συνδέει τον σχεδιασμό ποιότητας (δηλαδή, τον προσδιορισμό των χρηστών πελατών-πελατών και των αναγκών τους), τον έλεγχο ποιότητας (δηλαδή, την ανατροφοδότηση των υπαλλήλων με στοιχεία απόδοσης) και την βελτίωση ποιότητας (δηλαδή, βελτίωση της ικανοποίησης των υπαλλήλων και πρόληψη –όχι διόρθωση- των προβλημάτων). Η ιδέα της ευθύνης του management και όχι οι τεχνικές ελέγχου ποιότητας, αποτελούν το επίκεντρο της θεωρίας του JURAN. Επίσης, κατά τον JURAN, ποιότητα είναι η καταλληλότητα για σκοπό και χρήση και δεν είναι ποτέ τυχαία, αλλά αποτέλεσμα κατάλληλου σχεδιασμού.
4. W. EDWARDS DEMING<sup>68</sup>: Ο DEMING, προτείνει δεκατέσσερα σημεία για την διαχείριση της ποιότητας και υποστηρίζει πως για να υπάρξει αποτέλεσμα στην βελτίωση των υπηρεσιών ενός οργανισμού, πρέπει να επιτευχθούν τα ακόλουθα:
  - ✓ Προσανατολισμός της διοίκησης σε στόχους διαρκούς βελτίωσης της ποιότητας
  - ✓ Συνεχής εκπαίδευση του προσωπικού
  - ✓ Κατάργηση των διαχωριστικών γραμμών μεταξύ τμημάτων και ανθρώπων
5. PHILIP .J. CROSBY : Ο CROSBY<sup>67</sup>, στηρίζει την άποψη περί διαχείρισης ποιότητας σε πέντε απόλυτα σημεία. Αυτά είναι:
  - ✓ Η ποιότητα λειτουργεί σύμφωνα με τις απαιτήσεις
  - ✓ Δεν υπάρχουν προβλήματα ποιότητας
  - ✓ Κάνε το σωστό με την πρώτη φορά
  - ✓ Το κόστος της ποιότητας, είναι ο μόνος δείκτης απόδοσης
  - ✓ Το μηδενικό ελλάτωμα, είναι το μοναδικό standard απόδοσης
6. Η θεωρία του Crosby για το management ποιότητας, είναι πιο ολιστική. Ισοροπεί δηλαδή, την συμμετοχή και του management και των υπαλλήλων στην επίλυση θεμάτων ποιότητας:
  - ✓ Κοινά στοιχεία όλων των θεωριών
  - ✓ Ο χρήστης είναι το επίκεντρο του οργανισμού
  - ✓ Συστηματική βελτίωση λειτουργιών
  - ✓ Ανάπτυξη έμφυτου δυναμικού
  - ✓ Μακρόχρονη σκέψη και προγραμματισμός
  - ✓ Δέσμευση για την ποιότητα

### 3.2 Το Μοντέλο SERVQUAL (Service Quality)

Η θεωρία και η πρακτική του Μάρκετινγκ, αρχικά αναπτύχθηκε βασιζόμενη στα φυσικά αγαθά, όπως για παράδειγμα τα αυτοκίνητα, τα τρόφιμα, τα ποτά, τα καλλυντικά, τα ηλεκτρονικά και άλλα πάρα πολλά καταναλωτικά προϊόντα της αγοράς.

Όμως, μία από τις μεγαλύτερες τάσεις τις τελευταίες δεκαετίες ήταν η μεγάλη και ραγδαία ανάπτυξη των υπηρεσιών. Στις Η.Π.Α, από στοιχεία των τελευταίων χρόνων, οι υπηρεσίες αποτελούν το 79% των θέσεων εργασίας και το 74% του Α.Ε.Π. Τα τελευταία τουλάχιστον 20 χρόνια, η ανάπτυξη των υπηρεσιών και η σταδιακή αύξηση των ποσοστών απασχόλησης με αυτούς τους τομείς, οδήγησαν στην ανάπτυξη του ενδιαφέροντος αντιμετώπισης των ειδικών προβλημάτων, στον τομέα Μάρκετινγκ των Υπηρεσιών.

Στην συνέχεια, δίνεται ο ορισμός, η φύση, τα χαρακτηριστικά και οι στρατηγικές Μάρκετινγκ των Υπηρεσιών και γίνεται εστίαση, σε μία από αυτές τις στρατηγικές, που είναι η Διαχείριση της Ποιότητας των Υπηρεσιών.

Αναλύεται το μοντέλο 'SERVQUAL'<sup>71</sup>, που αποτελεί εργαλείο ανάλυσης, ανάπτυξης και μέτρησης της ποιότητας των υπηρεσιών, που μπορεί να προσφέρει σήμερα ένας οργανισμός προς τους πελάτες του, προκειμένου αυτοί να είναι ευχαριστημένοι και πιστοί τόσο στα προϊόντα και τις υπηρεσίες που διέπουν αυτά, πριν και μετά την πώληση τους, όσο και στις καθαρές μορφές υπηρεσιών χωρίς την πώληση απτών αγαθών.

#### Υπηρεσίες

Η Υπηρεσία σαν ορισμός, αποτελεί μια οποιαδήποτε πράξη, έργο ή παράσταση που στην ουσία είναι κυρίως, σε μία μη απτή μορφή και την οποία κάποιο συμβαλλόμενο μέρος παρέχει σε κάποιο άλλο και δεν καταλήγει στην απόκτηση ιδιοκτησίας της. Η υλοποίησή της, μπορεί να συνδέεται αλλά μπορεί και όχι με κάποιο φυσικό προϊόν.

Οι τομείς στους οποίους παρέχονται υπηρεσίες σήμερα είναι πάρα πολλοί, μερικά παραδείγματα εκ των οποίων είναι:

- ✓ **Δημόσιος Τομέας:** με υπηρεσίες όπως δικαστικές, εργασιακές, νοσοκομειακές, εκπαιδευτικές, στρατιωτικές, ταχυδρομικές, προστασίας των πολιτών (αστυνομία, πυροσβεστική).
- ✓ **Ιδιωτικός μη κερδοσκοπικός τομέας:** με υπηρεσίες όπως είναι τα μουσεία, φιλανθρωπικά ιδρύματα, εκκλησίες, διάφορα ιδρύματα.
- ✓ **Επιχειρησιακός Τομέας:** με υπηρεσίες στις αεροπορικές γραμμές και γενικότερα στις μεταφορές, στις τράπεζες, στα ξενοδοχεία, σε ασφαλιστικές εταιρίες, σε εταιρίες συμβούλων και πληροφορικής, σε λογιστικά γραφεία, σε μεσιτικές εταιρίες, σε δικηγορικά γραφεία, στις τηλεπικοινωνίες.

Οι μορφές των Υπηρεσιών που συνήθως συναντώνται, κατατάσσονται σε 4 μεγάλες κατηγορίες που είναι:

- ✓ **Φυσικά προϊόντα:** που συνοδεύονται από υπηρεσίες, μία ή περισσότερες, όπως είναι η μεταφορά και η παράδοση, η συντήρηση, η υποστήριξη, η κάλυψη εγγύησης, η επισκευή και άλλα αυτών των αγαθών πριν αλλά κυρίως μετά την πώληση τους.
- ✓ **Υβριδικές Υπηρεσίες:** που αντιστοιχούν εξίσου με την παροχή φυσικών αγαθών όπως για παράδειγμα, είναι η παροχή φαγητού και υπηρεσιών σε εστιατόρια.
- ✓ **Υπηρεσίες που συνοδεύουν φυσικά προϊόντα ή άλλες υπηρεσίες:** στις οποίες κυριαρχεί η πρωταρχική υπηρεσία η οποία συνοδεύεται από

πρόσθετες/συμπληρωματικές υπηρεσίες ή/και φυσικά προϊόντα. Παράδειγμα, αποτελούν οι αεροπορικές εταιρίες που η βασική υπηρεσία που προσφέρουν, είναι η αερομεταφορά των επιβατών αλλά που όμως επιπρόσθετα, παρέχουν φαγητό, ποτά, πώληση αφορολόγητων ειδών καθώς και υπηρεσίες εξυπηρέτησης των επιβατών μέσω του προσωπικού τους.

- ✓ **Καθαρόαιμες Υπηρεσίες:** που δεν συνοδεύονται με φυσικά αγαθά ή άλλες υπηρεσίες όπως για παράδειγμα, είναι η φυσιοθεραπεία, το baby-sitting, η επίσκεψη σε γιατρό, δικηγόρο, συμβολαιογράφο και άλλα.

Τα χαρακτηριστικά των Υπηρεσιών σε αντίθεση με τα φυσικά αγαθά είναι τέσσερα<sup>70</sup>:

- ✓ **Η έλλειψη απτότητας (Intangibility):** Σε αντίθεση με τα φυσικά προϊόντα οι Υπηρεσίες δεν είναι συνήθως απτές, που σημαίνει ότι πριν αγοραστούν δεν μπορεί κανείς να τις δει, να τις γευθεί, να τις ακούσει, να τις αισθανθεί. Το αποτέλεσμα για παράδειγμα μιας θεραπείας ενός ασθενή, που παρέχεται σαν υπηρεσία από τον γιατρό του, δεν είναι εκ των προτέρων γνωστή. Για να μειωθεί αυτή η αβεβαιότητα, οι αγοραστές των υπηρεσιών, ψάχνουν για στοιχεία και ενδείξεις που αφορούν την ποιότητα των υπηρεσιών. Τα στοιχεία από τα οποία αντλούνται οι επιρροές είναι ο τόπος, οι άνθρωποι, ο εξοπλισμός, το υλικό επικοινωνίας, τα σύμβολα και η τιμή στην οποία προσφέρεται κάθε υπηρεσία.
- ✓ **Η έλλειψη διαιρετότητας (Inseparability):** Οι υπηρεσίες συνήθως παράγονται και καταναλώνονται ταυτόχρονα, σε αντίθεση με τα φυσικά προϊόντα που παράγονται και στη συνέχεια αποθηκεύονται, διανέμονται μέσω διαφόρων πιθανώς μεσαζόντων και καταναλώνονται αργότερα, από τους αγοραστές. Ο παραγωγός και ο αποδέκτης της υπηρεσίας συμμετέχουν συνήθως για το τελικό αποτέλεσμα της υπηρεσίας και αμφότεροι μπορεί με τη συμμετοχή τους να το επηρεάσουν.
- ✓ **Μεταβλητότητα (Variability):** Λόγω του ότι οι υπηρεσίες εξαρτώνται από πού (τόπος), από ποιόν (άνθρωποι), από το πώς (μέσα και εξοπλισμός), από το πόσο(τιμή) και πότε παρέχονται, για τον λόγο αυτό είναι και μεταβλητές. Οι αγοραστές, είναι γνώστες της ύπαρξης αυτής της μεταβλητότητας και γιαυτό συχνά ομιλούν σε άλλους για τις υπηρεσίες που έλαβαν, είτε συστήνοντας είτε αποθαρρύνοντας αυτούς να γίνουν και αυτοί αποδέκτες. Αυτή είναι και η λεγόμενη “word of mouth”, έννοια στο μάρκετινγκ.
- ✓ **Φθαρτότητα (Perishability):** Οι υπηρεσίες δεν μπορούν να αποθηκευτούν, όπως τα φυσικά προϊόντα. Κατά συνέπεια δεν υπάρχει μεν το χαρακτηριστικό της φθοράς που προκύπτει από την αποθήκευση, όπως συμβαίνει με τα φυσικά προϊόντα, αλλά όμως υπάρχει το χαρακτηριστικό της φθοράς της υπηρεσίας που προκύπτει, από την κάλυψη της με το σωστό τρόπο και τη σωστή χρονική στιγμή που υπάρχει η ζήτηση εξυπηρέτησης. (προσφορά έναντι ζήτησης). Όταν η ζήτηση είναι σταθερή, δεν υπάρχουν προβλήματα φθαρτότητας. Τα προβλήματα δημιουργούνται όταν υπάρχουν διακυμάνσεις στη ζήτηση όπως για παράδειγμα σε χρονικές περιόδους αιχμής (όπως είναι οι υπηρεσίες μέσω μεταφοράς επιβατών σε ώρες αιχμής της ημέρας ή περιόδους όπως Πάσχα, Γιορτές, Τριήμερα).

Οι Στρατηγικές Μάρκετινγκ των Υπηρεσιών, αναπτύχθηκαν πολύ αργότερα από τις στρατηγικές εκείνες που αφορούσαν τα φυσικά αγαθά. Στις γνωστές τέσσερις προσεγγίσεις του Μάρκετινγκ για τα φυσικά προϊόντα, γνωστές σαν 4P (Place, Product, Promotion, Price)<sup>72</sup>, προστέθηκαν τρεις ακόμη P, για την κάλυψη και των υπηρεσιών και αυτές είναι *People* (άνθρωποι), *Physical Evidence* (Φυσική παρουσία) και *Process* (Διαδικασία).



Εικόνα 12: Οι τέσσερις προσεγγίσεις του Μάρκετινγκ, για τα φυσικά προϊόντα, γνωστές σαν 4P (Place, Product, Promotion, Price)<sup>72</sup>

Οι στρατηγικές που έχει να διαχειριστεί ένας οργανισμός παροχής υπηρεσιών σήμερα, είναι τρείς:

- ✓ **Διαφοροποίηση:** Συχνά αντιμετωπίζεται το πρόβλημα, για το πώς θα υπάρξει διαφοροποίηση στην κάθε υπηρεσία. Οι πιο γνωστοί τρόποι διαφοροποίησης, είναι η τιμή, η προσφορά καινοτομικών χαρακτηριστικών και συμπληρωματικών υπηρεσιών και αγαθών, η παράδοση με ελκυστικούς και ειδικά εκπαιδευμένους τρόπους και τέλος η εικόνα / παρουσία, μέσω συμβόλων, φίρμας και ειδικής προβολής του παρόχου και της κάθε υπηρεσίας.
- ✓ **Παραγωγικότητα:** Υπάρχουν 7 προσεγγίσεις για την αύξηση παραγωγικότητας των υπηρεσιών: Ανάπτυξη δεξιότητας εργαζομένων, Αύξηση του αριθμού υπηρεσιών έναντι μερικής μείωσης της ποιότητας (για παράδειγμα, ποιο πολλούς ασθενείς με λιγότερο χρόνο διάθεσης στον κάθε έναν), Βιομηχανοποίηση της υπηρεσίας με αυτοματοποίηση και τυποποίηση μέσω εξοπλισμού και σύγχρονων μεθόδων, Μείωση ή απαρχαίωση της υπηρεσίας με την αντικατάσταση της από προιοντική λύση, Σχεδίαση αποτελεσματικής υπηρεσίας, η προβολή κινήτρων στους πελάτες για αντικατάσταση του εργατικού δυναμικού τους, η ανάπτυξη και η διάθεση της τεχνολογίας και της διαχείρισης της πληροφορίας απευθείας στους πελάτες.
- ✓ **Ποιότητα υπηρεσιών:** Μια επιχείρηση παροχής υπηρεσιών μπορεί να πετύχει και να κερδίσει όταν και μόνον όταν, παρέχει υψηλότερης ποιότητας υπηρεσίες από τους ανταγωνιστές της και όταν υπερκαλύπτει τις προσδοκίες των πελατών, στην αγορά και στον κλάδο των υπηρεσιών που δραστηριοποιείται. Οι προσδοκίες των πελατών, σχηματίζονται από την προηγούμενη τους εμπειρία, από την επιρροή των άλλων (word of mouth) και από τις προσωπικές ανάγκες. Μετά την λήψη κάθε υπηρεσίας, οι πελάτες συγκρίνουν συνήθως την προσδοκώμενη έναντι της παρεχόμενης υπηρεσίας. Εάν αυτές συμφωνούν ή η παρεχόμενη είναι μεγαλύτερη της αναμενόμενης, τότε οι πελάτες θα ξαναχρησιμοποιήσουν τον ίδιο πάροχο.

### **Ικανοποίηση Πελατών**

Η έννοια της ικανοποίησης του πελάτη έχει αλλάξει στο πέρασμα των χρόνων. Αρχικά, η ικανοποίηση του πελάτη πιστευόταν ότι είχε σχέση με την αξιολόγηση της υπηρεσίας των πελατών. Τώρα πλέον, οι υπαιτιγμοί της ικανοποίησης των πελατών, είναι πιο πολύπλοκοι για τον κόσμο των επιχειρήσεων. Προς το παρόν, και με πολλούς τρόπους, η ικανοποίηση των πελατών στον κόσμο των επιχειρήσεων εξισώνεται με το κέρδος.

Γενικά, η ικανοποίηση του πελάτη μπορεί να εξεταστεί με πολλούς διαφορετικούς τρόπους και με πολλές διαφορετικές προσεγγίσεις. Πολλοί σχετίζουν την εξυπηρέτηση πελατών με οικονομικές εξισώσεις. Άλλοι, βλέπουν την ικανοποίηση του πελάτη σαν απλή τριάδα αξίας, εξυπηρέτησης και ποιότητας. Η ικανοποίηση του πελάτη εξετάζεται λοιπόν, είτε από πρακτική είτε από ακαδημαϊκή σκοπιά. Η ακαδημαϊκή σκοπιά αφήνει απέξω τις προσδοκίες συμπεριφοράς του πελάτη, η πρακτική σκοπιά έχει πάρα πολλές μεταβλητές. Άλλες είναι σημαντικές, άλλες όχι. Το υπόβαθρο των πελατών δεν λαμβάνεται υπόψη.

Αυτοί που ασχολούνται με το θέμα από πρακτική σκοπιά θέλουν να κάνουν την κατάσταση της ικανοποίησης των πελατών όσο πιο εύκολη και κατανοητή γίνεται. Δεν χρειάζεται να ξοδεύουν τον χρόνο και το χρήμα και συχνά δεν κατέχουν τα ποσά για να τα διαθέσουν σε έρευνες για την ικανοποίηση των πελατών. Σύντομες και γρήγορες μετρήσεις της ικανοποίησης των πελατών, μπορεί να δημιουργήσουν δεδομένα που θα οδηγήσουν την εταιρία σε λάθος εκτίμηση και κατεύθυνση που μακροπρόθεσμα μπορεί να προκαλέσει καταστροφικά αποτελέσματα.

Έχουν γίνει ανάλογες έρευνες όσον αφορά την στρέβλωση των αποτελεσμάτων στην μέτρηση της ικανοποίησης των πελατών. Ο Peterson, εξέτασε διάφορα χαρακτηριστικά στην μέτρηση της ικανοποίησης των πελατών, που στρέβλωσαν σημαντικά τα αποτελέσματα.

### **Η έννοια και το εργαλείο στρατηγικής “servqual”<sup>73</sup>**

Μια από τις τρεις στρατηγικές Μάρκετινγκ των Υπηρεσιών, είναι η Διαχείριση της Ποιότητας των Υπηρεσιών και αυτή καλύπτεται, από το μοντέλο-εργαλείο “SERVQUAL”.

Η ονομασία “SERVQUAL” σημαίνει Service Quality, δηλαδή ποιότητα υπηρεσιών. Η Ποιότητα υπηρεσιών, είναι μια γενική μέθοδος για την μέτρηση της ποιότητας υπηρεσιών ως διαφορά μεταξύ της απόδοσης που αναμένεται από τους πελάτες και της απόδοσης που δίνεται πραγματικά. Από αυτήν την διαφορά μετράται η ικανοποίηση των πελατών.

Το μοντέλο SERVQUAL αναπτύχθηκε από τους Zeithaml, Parasuraman και Berry. Η μεθοδολογία SERVQUAL, είναι ένα ανεκτίμητο εργαλείο των οργανισμών, για να κατανοήσουν καλύτερα τι εκτιμούν οι πελάτες και πόσο καλά οι ήδη υπάρχουσες επιχειρήσεις καλύπτουν τις ανάγκες και τις προσδοκίες των πελατών.

Η SERVQUAL, παρέχει ένα σχέδιο που βασίζεται στις απόψεις των πελατών για μια επιχείρηση (αξιόλογη επιχείρηση, για την ακρίβεια), στην σπουδαιότητα της αξιολόγησης των βασικών πόρων και στην σύγκριση μεταξύ του τι πιστεύουν οι εργαζόμενοι και τι νιώθουν οι πελάτες. Παρέχει επίσης αναλυτικές πληροφορίες σχετικά:

- ✓ Με τις προοπτικές για υπηρεσία που έχουν οι πελάτες
- ✓ Με τα επίπεδα απόδοσης της επιχείρησης, όπως τα αντιλαμβάνονται οι πελάτες
- ✓ Με τα σχόλια και τις προτάσεις πελατών
- ✓ Με τις εντυπώσεις υπαλλήλων, με σεβασμό στις προσδοκίες των πελατών και την ικανοποίησή τους



Η Ποιότητα Υπηρεσιών, έχει αποδειχθεί ότι είναι ένα απλό, αλλά αποτελεσματικό εργαλείο για πολλούς οργανισμούς. Το εργαλείο επιτρέπει στους οργανισμούς:

- ✓ Να αναγνωρίσουν και να κατανοήσουν που υπάρχουν κενά υπηρεσιών μέσα στον οργανισμό και μεταξύ του οργανισμού και των πελατών του
- ✓ Να θέσουν προτεραιότητες στα κενά αυτά, σε σχέση με την επίπτωση τους στην ποιότητα των υπηρεσιών
- ✓ Να αναγνωρίσουν τους λόγους για την ύπαρξη των κενών
- ✓ Να συμπληρώσουν μια σειρά από διαδικασίες, για την συνεχόμενη επιθεώρηση και καθορισμό της ποιότητας υπηρεσιών των πελατών.

### Διαστάσεις Ποιότητας Υπηρεσιών

Η SERVQUAL, είναι μεθοδολογία που καθορίζει τις διαστάσεις της ποιότητας των υπηρεσιών. Οι διαστάσεις ποιότητας, με παραδείγματα ερωτήσεων που αναφέρονται σε αυτές προκειμένου να απαντήσουν στην παροχή της ποιότητας των υπηρεσιών, ακολουθούν στον παρακάτω πίνακα 5:

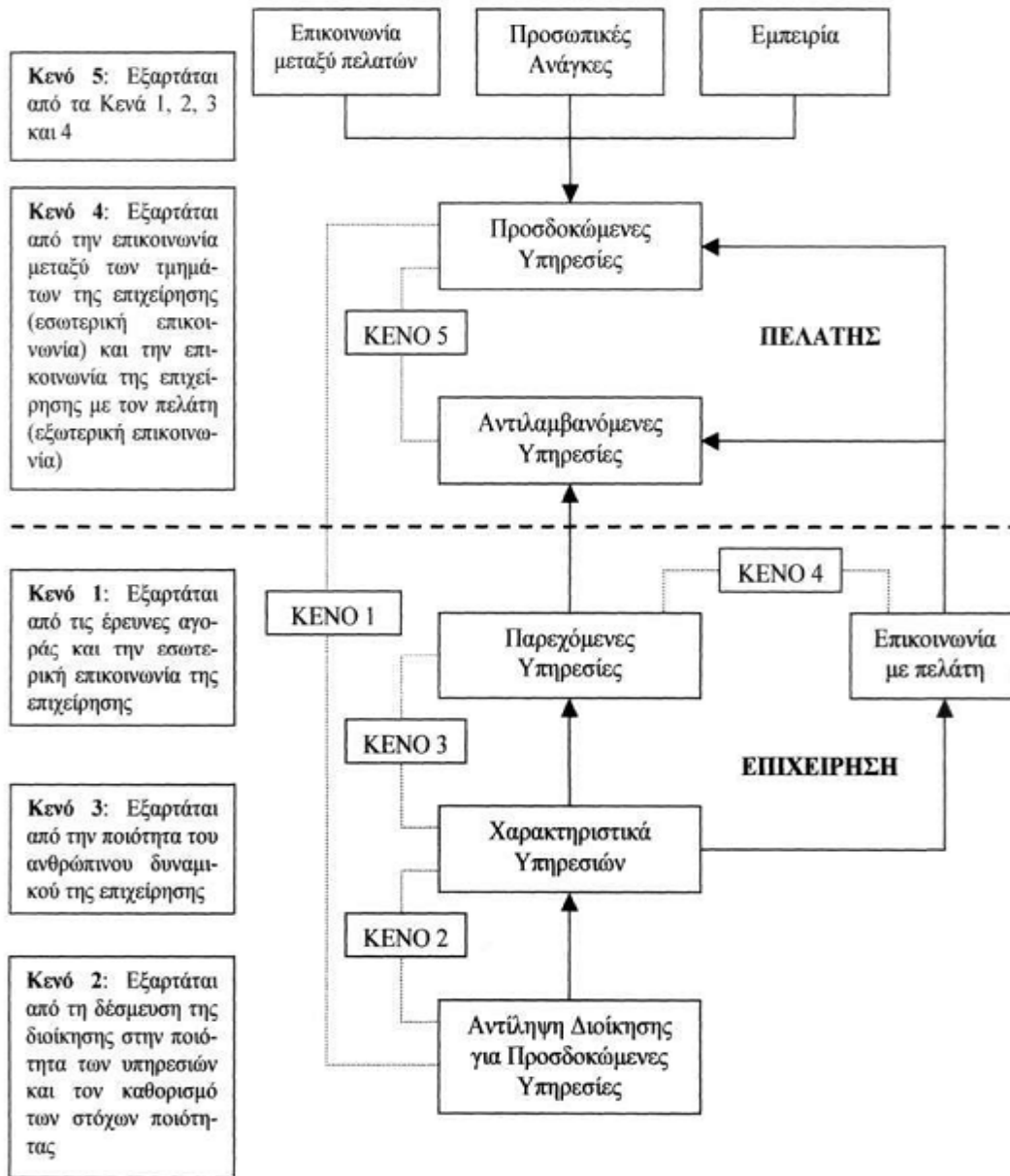
Διαστάσεις Ποιότητας	Ερμηνεία	Παραδείγματα ερωτήσεων
<b>Απτή Διάσταση</b>	Εμφάνιση φυσικών εγκαταστάσεων, εξοπλισμού, προσωπικού κλπ	<ul style="list-style-type: none"> <li>✓ Είναι οι εγκαταστάσεις ελκυστικές?</li> <li>✓ Είναι το προσωπικό ντυμένο κατάλληλα?</li> <li>✓ Η τεχνολογία είναι μοντέρνα?</li> </ul>
<b>Αξιοπιστία</b>	Η ικανότητα να παρέχεται η υπηρεσία αξιόπιστα και εύστοχα.	<ul style="list-style-type: none"> <li>✓ Η υπηρεσία παρέχεται σωστά την πρώτη φορά?</li> <li>✓ Το επίπεδο υπηρεσιών είναι ίδιο όλες τις ώρες τις ημέρας και για όλα τα μέλη του προσωπικού?</li> </ul>
<b>Ανταπόκριση</b>	Η θέληση για βοήθεια των πελατών προκειμένου να τους παρασχεθεί η υπηρεσία.	<ul style="list-style-type: none"> <li>✓ Όταν υπάρχει πρόβλημα, η επιχείρηση ανταποκρίνεται σε αυτό γρήγορα?</li> <li>✓ Το προσωπικό είναι διατεθειμένο να απαντήσει σε απορίες των πελατών?</li> <li>✓ Οι δημόσιες καταστάσεις αντιμετωπίζονται με φροντίδα και σοβαρότητα?</li> </ul>
<b>Ικανότητα</b>	Η κατοχή των απαραίτητων δεξιοτήτων και γνώσης για την παροχή της υπηρεσίας.	<ul style="list-style-type: none"> <li>✓ Μπορεί το προσωπικό να παρέχει υπηρεσία χωρίς να χρονοτριβεί?</li> <li>✓ Τα υλικά που χρησιμοποιούνται είναι τα κατάλληλα και τα πιο μοντέρνα?</li> <li>✓ Μπορεί το προσωπικό να χρησιμοποιεί την τεχνολογία γρήγορα και ικανότατα?</li> </ul>
<b>Ευγένεια</b>	Ευγένεια, σεβασμός, φιλικότητα του προσωπικού που έρχεται σε επαφή με τον πελάτη.	<ul style="list-style-type: none"> <li>✓ Το προσωπικό γνωρίζει τι κάνει?</li> <li>✓ Είναι οι εγκαταστάσεις ελκυστικές?</li> <li>✓ Το μέλος του προσωπικού είναι ευχάριστο απέναντι στον πελάτη?</li> <li>✓ Το μέλος του προσωπικού δέχεται τις τυχόν ερωτήσεις του πελάτη χωρίς να γίνεται αγενής?</li> <li>✓ Τα άτομα που απαντούν στο τηλέφωνο θεωρούνται ευγενή?</li> </ul>
<b>Εμπιστοσύνη</b>	Εμπιστοσύνη, ειλικρίνεια του παροχέα των υπηρεσιών.	<ul style="list-style-type: none"> <li>✓ Ο Οργανισμός που παρέχει τις υπηρεσίες έχει καλή φήμη?</li> <li>✓ Ο Οργανισμός εγγυείται για την ποιότητα των υπηρεσιών του?</li> </ul>
<b>Ασφάλεια</b>	Ελευθερία από	<ul style="list-style-type: none"> <li>✓ Είναι ασφαλής η χρήση του εξοπλισμού?</li> </ul>

	κίνδυνο, ρίσκο, αμφιβολία	<ul style="list-style-type: none"> <li>✓ Είναι τα έγγραφα και οι πληροφορίες που παρέχονται στον πελάτη ασφαλείς?</li> <li>✓ Είναι τα αρχεία των πελατών ασφαλή από παράνομη χρήση?</li> <li>✓ Μπορεί ο πελάτης να είναι σίγουρος ότι η υπηρεσία που παρασχέθηκε, έγινε σωστά?</li> </ul>
<b>Προσέγγιση</b>	Ευκολία στην επαφή.	<ul style="list-style-type: none"> <li>✓ Πόσο εύκολο είναι να μιλήσει κανείς σε κάποιο μέλος του προσωπικού όταν έχει κάποιο πρόβλημα?</li> <li>✓ Είναι εύκολο να προσεγγίσει κανείς το κατάλληλο μέλος του προσωπικού. <ul style="list-style-type: none"> <li>○ Ιδιαίτερος?</li> <li>○ Τηλεφωνικά?</li> <li>○ Μέσω email?</li> </ul> </li> </ul>
<b>Επικοινωνία:</b>	Το να κρατά κανείς τους πελάτες πληροφορημένους σε μια γλώσσα που καταλαβαίνουν.	<ul style="list-style-type: none"> <li>✓ Μπορεί το μέλος του προσωπικού να ακούσει το πρόβλημα του πελάτη και να επιδείξει κατανόηση και ενδιαφέρον?</li> <li>✓ Το προσωπικό αποφεύγει να χρησιμοποιεί τεχνικούς όρους όταν μιλά με τους πελάτες?</li> <li>✓ Το μέλος του προσωπικού θα ενημερώσει αν κάποιο ραντεβού ακυρωθεί?</li> </ul>
<b>Κατανοώντας τον πελάτη</b>	Η προσπάθεια να μάθουν τους πελάτες και τις ανάγκες τους.	<ul style="list-style-type: none"> <li>✓ Υπάρχει περίπτωση κάποιος από το προσωπικό να αναγνωρίζει κάθε τακτικό πελάτη και χρησιμοποιεί το μικρό του όνομα?</li> <li>✓ Το προσωπικό προσπαθεί να κατανοήσει ποιό είναι οι συγκεκριμένοι στόχοι του πελάτη?</li> <li>✓ Το επίπεδο της υπηρεσίας και του κόστους της υπηρεσίας συμβαδίζει με το τι απαιτεί και τι έχει να δώσει ο πελάτης?</li> </ul>

Πίνακας 5: Διαστάσεις ποιότητας με παραδείγματα ερωτήσεων για την καλύτερη ποιότητα υπηρεσιών

Οι 5 πιο αντιπροσωπευτικές από τις παραπάνω διαστάσεις του παραπάνω πίνακα, για το εργαλείο μέτρησης της ποιότητας υπηρεσιών SERVQUAL, είναι κατά σειρά σημαντικότητας<sup>76</sup>:

- ✓ Η Αξιοπιστία (Reliability) - το να κάνουν αυτό που λένε ότι θα κάνουν, στην ώρα τους και συγκεκριμένα
- ✓ Η Ανταπόκριση (Responsiveness) - η θέληση για παροχή βοήθειας και η ανταπόκριση σε συγκεκριμένες απαιτήσεις
- ✓ Η Εγγύηση (Assurance) - η κατοχή των απαιτούμενων ικανοτήτων, για την παροχή της υπηρεσίας καθώς και μετάδοση της εμπιστοσύνης
- ✓ Κατανόηση (Empathy) - δείχνει την κατανόηση των αναγκών των πελατών και την παροχή της συγκεκριμένης υπηρεσίας
- ✓ Απτή διάσταση (Tangibility) - περιλαμβάνει φυσική εμφάνιση των ατόμων και των εγκαταστάσεων



Εικόνα 13: Μοντέλο SERVQUAL (Θεωρία των Κενών)<sup>74, 75,77</sup>

Οι πελάτες, όπως παρατηρείται στο παραπάνω σχήμα που αντιπροσωπεύει το μοντέλο του Servqual έχουν κάποιες προσδοκίες από την επιχείρηση, οι οποίες σχετίζονται με 4 παράγοντες. Αυτοί είναι:

- ✓ Επικοινωνία και πληροφορίες που παρέχονται από φίλους και γνωστούς
- ✓ Προσωπικές ανάγκες
- ✓ Εμπειρία
- ✓ Επικοινωνία από την ίδια την εταιρία που παρέχει τις υπηρεσίες

Χρησιμοποιώντας την μεθοδολογία SERVQUAL, η ποιότητα υπηρεσιών καθορίζεται από το γενικό κενό μεταξύ αυτού που προσδοκώταν και αυτού που παραδόθηκε. Αυτό σημαίνει ότι:

- ✓ Η ποιότητα υπηρεσιών είναι σχετική, όχι απόλυτη
- ✓ Διαφορετικοί πελάτες, μπορεί να εκλάβουν διαφορετικά το επίπεδο ποιότητας υπηρεσιών
- ✓ Η ποιότητα, καθορίζεται από τον πελάτη που έχει «όλες τις ψήφους», όχι τον παροχέα των υπηρεσιών.
- ✓ Η ποιότητα των υπηρεσιών, μπορεί να επιτευχθεί είτε από την κάλυψη ή την υπερκάλυψη των προσδοκιών, είτε από την αλλαγή των προσδοκιών

### 3.3 Το Μοντέλο SERVPERFORM

Το μοντέλο SERVQUAL, εξαιτίας των βασικών παραδοχών του, υπέστη την κριτική αρκετών. Οι Hemmasi, Strong και Taylor, εξέτασαν την πλευρά των προσδοκιών του Servqual και ανακάλυψαν ότι έπασχε όσον αφορά την σχετικότητα των προσδοκιών, και δήλωσαν ότι οι περισσότεροι άνθρωποι θα βαθμολογούσαν με μεγάλο βαθμό τις προσδοκίες τους. Άλλαξαν λοιπόν το εργαλείο Servqual, εξαλείφοντας τις προσδοκίες στην μισή έρευνα και εξετάζοντας μόνο την πλευρά της απόδοσης. Επιπλέον, πρόσθεσαν ένα “τμήμα σημαντικότητας” για να δώσουν στο εργαλείο ερωτήσεις που να έχουν βαρύτητα. Αυτό, θα επέτρεπε μια έρευνα για το πού θα ήταν καλύτερο να δοθεί έμφαση για την βελτίωση της ικανοποίησης των πελατών και την παροχή στρατηγικών ευκαιριών.

Αυτή η νέα έκδοση του μοντέλου, ονομάζεται “SERVPERF” και προκύπτει από τα αρχικά λεκτικά των λέξεων “SERVice PERFormance”, δηλαδή της “Απόδοσης των Υπηρεσιών”. Καθώς οι προϋπολογισμοί γίνονται όλο και πιο σφικτοί, οι επιχειρήσεις δεν χρειάζεται να γνωρίζουν μόνο το τι αρέσει και τι δεν αρέσει στους πελάτες τους, αλλά πρέπει και να γνωρίζουν τι αρέσει και τι δεν αρέσει περισσότερο στους πελάτες τους, για να γίνουν και πιο αποδοτικοί.

Αυτό βοηθά, στην βέλτιστη κατανομή και αξιοποίηση των διάφορων πολύτιμων πόρων, όπως για παράδειγμα είναι, το χρήμα, ο χρόνος, ο εξοπλισμός και άλλα. Με λίγα λόγια, οι πόροι μιας επιχείρησης μπορούν να διατεθούν εκεί που πραγματικά προσδιορίζονται οι ανάγκες και οι απαιτήσεις των πελατών μιας επιχείρησης.

### 3.4 International Organization for Standardization (ISO)

Πριν την αξιολόγηση των ηλεκτρονικών υπηρεσιών, περιγράφεται το πρότυπο ISO (International Organization for Standardization), που αποτελεί τεκμηριωμένες έγγραφες συμφωνίες, που περιχέουν τεχνικές προδιαγραφές ή ακριβή κριτήρια για να χρησιμοποιηθούν ως κανόνες, οδηγίες ή ορισμοί χαρακτηριστικών. Γενικότερα, τα standards αυξάνουν την αξιοπιστία και την αποτελεσματικότητα των αγαθών και των υπηρεσιών που χρησιμοποιούνται.

Η Διεθνής οργάνωση τυποποίησης ISO, είναι μια παγκόσμια ομοσπονδία εθνικών επιτροπών standards, από περισσότερες από 140 χώρες, που ιδρύθηκε το 1947. Αποστολή της είναι, η ανάπτυξη της τυποποίησης και σχετικών δραστηριοτήτων, με σκοπό την διευκόλυνση της διεθνούς ανταλλαγής αγαθών και υπηρεσιών καθώς επίσης η ανάπτυξη της συνεργασίας στους τομείς της πνευματικής, επιστημονικής τεχνολογικής και οικονομικής δραστηριότητας.

Η ISO, αποτελείται από μέλη που χωρίζονται σε 3 κατηγορίες:

1. Η επιτροπή - μέλος, είναι η εθνική επιτροπή αντιπρόσωπος της τυποποίησης στη χώρα της.
2. Ένα μέλος - ανταποκριτής, είναι συνήθως μια οργάνωση, σε μια χώρα η οποία ακόμα δεν έχει πλήρης ανεπτυγμένη δραστηριότητα εθνικών Standards.

3. Η ISO, έχει επίσης καθιερώσει μια τρίτη κατηγορία, τα συνδρομητικά μέλη για χώρες με πολύ μικρές οικονομίες.

Στην τυποποίηση υπάρχουν 3 κύριες φάσεις:

**1<sup>η</sup> Φάση:** Η ανάγκη για ένα Standard, εκφράζεται συνήθως από έναν βιομηχανικό τομέα, ο οποίος μεταφέρει την ανάγκη αυτή, σε μια εθνική επιτροπή μέλος. Η επιτροπή, προτείνει το θέμα στην οργάνωση ISO και μόλις η ανάγκη για ένα διεθνές Standard αναγνωριστεί και συμφωνηθεί επίσημα, η πρώτη φάση περιλαμβάνει καθορισμό της τεχνικής θεώρησης του μελλοντικού Standard.

**2<sup>η</sup> Φάση:** Η φάση αυτή, συνήθως διεξάγεται σε ομάδες εργασίας, τις οποίες συνθέτουν ειδικοί τεχνικοί από χώρες που ενδιαφέρονται για το συγκεκριμένο θέμα. Μόλις φτάσουν σε συμφωνία για το ποιές τεχνικές πλευρές πρέπει να καλυφθούν στο Standard, ξεκινά η δεύτερη φάση κατά τη διάρκεια της οποίας, χώρες διαπραγματεύονται τις λεπτομερείς προδιαγραφές του Standard. Αυτή είναι η φάση της κοινής συναίνεσης.

**3<sup>η</sup> Φάση:** Η τρίτη φάση, περιλαμβάνει την επίσημη έγκριση του τελικού προσχεδίου του Διεθνούς Standard, όπου τα κριτήρια αποδοχής θέτουν ως όρο την έγκριση από τα 2/3 των μελών της ISO, τα οποία έχουν συμμετάσχει ενεργά στην διαδικασία ανάπτυξης των Standards καθώς και στην έγκριση από το 75% όλων των μελών που ψηφίζουν.

Τέλος, το συμφωνημένο κείμενο εκδίδεται ως ένα Διεθνές Standard ISO και τα περισσότερα Standards χρειάζονται περιοδική επανεξέταση. Μέχρι σήμερα, έχουν προκύψει 12.000 Διεθνή Standards, που παρουσιάζονται σε περισσότερα από 300.000 σελίδες.

### 3.4.1 ISO 27001: Το Πρότυπο για την Διαχείριση Ασφάλειας Πληροφοριών<sup>85, 86</sup>

Το ISO 27001, αποτελεί προδιαγραφή για την διαχείριση της ασφάλειας των πληροφοριών. Έχει εφαρμογή σε όλους τους τομείς της βιομηχανίας, εμπορίου και υπηρεσιών και η εφαρμογή του δεν περιορίζεται μόνο στις πληροφορίες που αποθηκεύονται σε ηλεκτρονικούς υπολογιστές. Απευθύνεται στην ασφάλεια των πληροφοριών, με όποιον τρόπο και αν αυτές τηρούνται. Οι πληροφορίες μπορεί να είναι καταγεγραμμένες ή εκτυπωμένες σε χαρτί, μπορεί να είναι αποθηκευμένες ηλεκτρονικά, μπορεί να αποστέλλονται με κανονικό ή με ηλεκτρονικό ταχυδρομείο, μπορεί να παρουσιάζονται σε φιλμ ή να διατυπώνονται προφορικά σε συζητήσεις. Οποιαδήποτε μορφή και εάν έχουν οι πληροφορίες, με οποιοδήποτε τρόπο και αν αυτές διαμοιράζονται ή αποθηκεύονται, το ISO 27001 βοηθάει έναν οργανισμό να τις προστατεύει επαρκώς. Όσον αφορά την ασφάλεια της πληροφορίας χαρακτηρίζεται από:

- ✓ **Εμπιστευτικότητα** - Η εξασφάλιση, ώστε η πρόσβαση στην πληροφορία να είναι κατάλληλα εξουσιοδοτημένη.
- ✓ **Ακεραιότητα** - Διαφύλαξη της ακρίβειας και πληρότητας της πληροφορίας καθώς και των μεθόδων επεξεργασίας της.
- ✓ **Διαθεσιμότητα** - Η εξασφάλιση του ότι οι εξουσιοδοτημένοι χρήστες της πληροφορίας, έχουν πρόσβαση σε αυτήν όταν την χρειάζονται.

Το ISO 27001, εμπεριέχει αριθμό ελεγκτικών επιδιώξεων, σκοπών, σημείων και ελέγχους. Δηλαδή, περιλαμβάνει: πολιτική ασφαλείας, ασφάλεια οργανισμού, κατάταξη και έλεγχος των περιουσιακών στοιχείων, ασφάλεια προσωπικού, φυσική και περιβαλλοντική ασφάλεια, διαχείριση επικοινωνίας και λειτουργιών, έλεγχο πρόσβασης καθώς και ανάπτυξη και συντήρηση συστημάτων.

### 3.4.2 ISO Πρότυπα Ηλεκτρονικών Υπηρεσιών<sup>87, 88</sup>

Από τον Ιούλιο του 2008, τρία προφίλ του WS-I (Web Services Interoperability Organization), υιοθετήθηκαν ως ISO πρότυπα από τον Οργανισμό, με σκοπό την πιστοποίηση περισσότερων επιχειρήσεων που προσφέρουν ηλεκτρονικές υπηρεσίες σε πλατφόρμες, γλώσσες προγραμματισμού και λειτουργικά συστήματα.

Πιο αναλυτικά, ο WS-I είναι ένας μη κερδοσκοπικός Οργανισμός, που στοχεύει στο να ενισχύει στις καλύτερες πρακτικές και στο να προωθεί ασφαλείς και διαδραστικές ηλεκτρονικές υπηρεσίες. Ακόμα, ο WS-I, συνίσταται από μία διαφοροποιημένη κοινότητα από ηγετικές επιχειρήσεις στον κόσμο των ηλεκτρονικών υπηρεσιών καθώς και από Οργανισμούς Ανάπτυξης Προτύπων (SDO – Standards Development Organizations). Οι επιτροπές και οι ομάδες εργασίας του WS-I, προωθούν προφίλ και εργαλεία ελέγχου, τα οποία είναι διαθέσιμα για χρήση από την κοινότητα των επιχειρήσεων.

Τα προφίλ που υιοθετούσε μέχρι τα μέσα του 2008 ο Οργανισμός, αναλύθηκαν, εξετάστηκαν, συμπληρώθηκαν και εξελίχθηκαν από τον ISO, ως διεθνή πρότυπα, τα οποία μπορούν να αναπτυχθούν περαιτέρω από επιχειρήσεις και να εγκριθούν από τον Οργανισμό ISO, ως διεθνή πρότυπα παροχής ηλεκτρονικών υπηρεσιών. Τα πρότυπα είναι τα εξής:

- ✓ ISO/IEC 29361:2008 (Information technology -- Web Services Interoperability -- WS-I Basic Profile Version 1.1)
- ✓ ISO/IEC 29362:2008 (Information technology -- Web Services Interoperability -- WS-I Attachments Profile Version 1.0)
- ✓ ISO/IEC 29363:2008 (Information technology -- Web Services Interoperability -- WS-I Simple SOAP Binding Profile Version 1.0)

Τα παραπάνω πρότυπα, προσφέρουν διαδραστική λειτουργία, σε μία βασική ομάδα προδιαγραφών για τις ηλεκτρονικές υπηρεσίες, όπως είναι τα Πρωτόκολλα SOAP, WSDL και UDDI καθώς και διορθώσεις ή συμπληρώσεις στις προδιαγραφές αυτές.

### 3.5 Αξιολόγηση Ηλεκτρονικών Υπηρεσιών<sup>79,80</sup>

Ο όρος της αξιολόγησης των ηλεκτρονικών υπηρεσιών, είναι μια πολύ γενική έννοια και εσωκλείει ζητήματα, όπως απόψεις της απόδοσης των μετρήσεων και εκτιμήσεων των ανθρώπων που χρησιμοποιούν το σύστημα, δηλαδή τόσο προσωπικού όσο και των χρηστών μιας ηλεκτρονικής υπηρεσίας. Επιπρόσθετα, μπορεί να συναντάται με ποικίλες μορφές και περιεχόμενα, όπως στην επιστήμη των υπολογιστών που η αξιολόγηση περιλαμβάνει την εκτίμηση της ποιότητας, την επαλήθευση και την εγκυρότητα. Η αξιολόγηση ηλεκτρονικών υπηρεσιών είναι σημαντική, διότι εξετάζονται θέματα που έχουν σχέση με τη χρηστικότητα, τη λειτουργικότητα και τα προβλήματα των ηλεκτρονικών υπηρεσιών. Ακόμα, εξετάζονται οι τεχνολογίες που χρησιμοποιούνται, όπως: software, hardware, networks, interfaces καθώς επίσης και θέματα ικανοποίησης των χρηστών, όπως οι αντιλήψεις, οι ανάγκες, και οι προσδοκίες τους.

#### 3.5.1 Τρόποι Αξιολόγησης

Αυτά που συνήθως αξιολογούνται σε μία Ηλεκτρονική Υπηρεσία, είναι τα συστατικά στοιχεία του συστήματος, όπως εξοπλισμός και προγράμματα, οι πληροφοριακές διεργασίες, όπως διατύπωση ερωτημάτων, τρόπος παρουσίασης και ανάκτησης των αποτελεσμάτων, τους

πληροφοριακούς πόρους (Information Resources), δηλαδή την βασική μονάδα αξιολόγησης τα βιβλία, τα περιοδικά, τις συλλογές, τις βιβλιογραφικές βάσεις δεδομένων.

Επίσης, τα προϊόντα και τις υπηρεσίες, τις πληροφοριακές λειτουργίες, όπως αναζήτηση και ανάκτηση πληροφοριών καθώς και ολόκληρο το πληροφοριακό σύστημα.

Το περιβάλλον του πληροφοριακού συστήματος, είναι ένα βασικό μέρος που αξιολογείται και που μπορεί να είναι ο οργανισμός που το ανέπτυξε ή ο πληθυσμός που εξυπηρετείται από το πληροφοριακό σύστημα.

Τέλος αξιολογείται, η τεχνολογία και το λογισμικό που χρησιμοποιείται από την Ηλεκτρονική Υπηρεσία, δηλαδή το σύστημα που παρέχει οργάνωση και κατ' επέκταση πρόσβαση στις πληροφορίες, όπως επίσης και η πληροφοριακή υπηρεσία, που είναι το σύνολο των πόρων και των συστημάτων.

### **Τρόποι αξιολόγησης**

Υπάρχουν αρκετοί τρόποι όπου μπορεί να γίνει μία αξιολόγηση.

Αρχικά μέσω ερωτηματολογίων, όπου δημιουργείται ένα ερωτηματολόγιο με συγκεκριμένες ερωτήσεις που σκοπό έχουν ο ερευνητής να αποκτήσει μία πιο ολοκληρωμένη εικόνα για το έργο του.

Ανάλογα με το θέμα της αξιολόγησης, τα εργαστηριακά πειράματα δίνουν πολύ καλά συμπεράσματα για την εξέλιξη και την ανίχνευση όποιων προβληματισμών υπάρχουν.

Οι συνεντεύξεις και οι έρευνες σε τοπικό, εθνικό αλλά και διεθνές επίπεδο, είναι ένας από τους τρόπους αξιολόγησης, αλλά απαιτούν μεγάλη διάθεση και χρόνο.

Οι αναλύσεις και οι μετρήσεις της Ηλεκτρονικής Υπηρεσίας μέσω εργαλείων, είναι ένας ακόμη τρόπος και ο οποίος δίνει πολύ καλά συμπεράσματα, αλλά εξαρτάται και από άλλους παράγοντες, όπως είναι για παράδειγμα τα ερωτηματολόγια. Να είναι δηλαδή, όσο το δυνατόν περισσότερα και ακριβή στην πληροφορία που περιέχουν.

Τέλος, η παρακολούθηση και η καταγραφή του περιβάλλοντος διεπαφής χρήστη-συστήματος καθώς και οι παρατηρήσεις και τα σχόλια χρηστών πάνω σε διαδικαστικά και πρακτικά θέματα θα μπορούσαμε να πούμε ότι είναι ένας άλλος πολύ καλός τρόπος αξιολόγησης.

### **3.5.2 Παράμετροι Αξιολόγησης**

Οι συνιστώσες της αξιολόγησης στις Ηλεκτρονικές Υπηρεσίες είναι οι παρακάτω τέσσερις:

- ✓ Η συλλογή μιας Ηλεκτρονικής Υπηρεσίας, η οποία αποτελεί και τα δεδομένα του συστήματος.
- ✓ Το "κοινό" των Ηλεκτρονικών Υπηρεσιών, δηλαδή τα άτομα που χρησιμοποιούν το όλο σύστημα. Αυτά μπορεί να είναι οι διαχειριστές του συστήματος, το προσωπικό, οι πάσης φύσεως χρήστες.
- ✓ Οι τεχνολογίες που υποστηρίζει το σύστημα αλλά και τα επιμέρους υπολογιστικά συστήματα που μπορεί να εμπεριέχει η εκάστοτε Ηλεκτρονική Υπηρεσία.
- ✓ Το γενικότερο περιβάλλον χρήσης μιας Ηλεκτρονικής Υπηρεσίας.

### **Παράμετροι αξιολόγησης**

Η αξιολόγηση έχει τις παρακάτω παραμέτρους:

- ✓ Το επίπεδο αλληλεπίδρασης χρήστη – πληροφοριακού συστήματος, το οποίο εμπεριέχει ζητήματα χρηστικότητας των πληροφοριακών συστημάτων.
- ✓ Η ύπαρξη όρων πρόσβασης και χρήσης.
- ✓ Η υποστήριξη συγκεκριμένων εργασιών, όπως η αναζήτηση και ανάκτηση πληροφοριών.
- ✓ Το σύνολο του συστήματος και οι συνιστώσες του, δηλαδή η αξιολόγηση (ποσοτική και ποιοτική) μεθόδων, τεχνικών αναζήτησης και ανάκτησης πληροφοριών και γενικότερα το θέμα λειτουργικότητας του συστήματος.
- ✓ Τα θέματα οργάνωσης, συντήρησης, διαχείρισης και διατήρησης του εκάστοτε πληροφοριακού συστήματος.

### 3.6 Μέθοδοι αξιολόγησης<sup>81,82</sup>

Οι μέθοδοι και τα συστήματα για την αξιολόγηση της χρησιμοποίησιμότητας χωρίζονται σε 4 διαφορετικές κατηγορίες:

**Αυτόματη Αξιολόγηση:** Στην περίπτωση αυτή, υπάρχει ένα σύστημα αξιολόγησης εφαρμογών, το οποίο εξάγει συμπεράσματα για την υπό εξέταση εφαρμογή. Το σύστημα αυτό, μπορεί να είναι εντελώς αυτοματοποιημένο ή ημιαυτοποιημένο. Δεν υπάρχουν τέτοια γενικά συστήματα, που να μπορούν να βγάλουν αξιόπιστα αποτελέσματα.

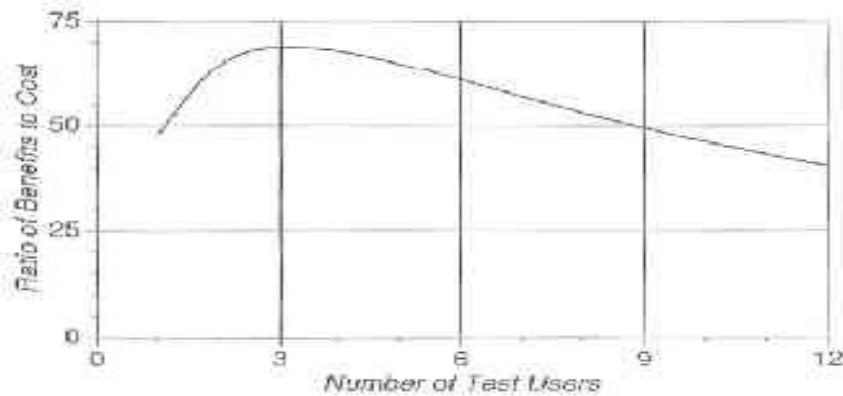
**Εμπειρική Αξιολόγηση:** Στην περίπτωση αυτή, ένας προκαθορισμένος αριθμός χρηστών χρησιμοποιεί το σύστημα διεκπεραιώνοντας συγκεκριμένες λειτουργίες. Κατά τη διάρκεια του πειράματος, λαμβάνονται μετρήσεις και γίνονται παρατηρήσεις από ειδικούς και στη συνέχεια συντάσσονται αναφορές που καταγράφονται τα συμπεράσματα. Αυτές οι τεχνικές είναι ευρέως διαδεδομένες.

**Αναλυτική Αξιολόγηση:** Χρησιμοποιούνται αναλυτικά ιδεατά μοντέλα της εφαρμογής και των χρηστών, από τα οποία υπολογίζονται μετρικές που βοηθούν στην αξιολόγηση του συστήματος. Τα σύγχρονα αλληλεπιδραστικά συστήματα, λόγω της πολυπλοκότητας τους, είναι σχεδόν αδύνατο να περιγραφούν από αναλυτικά μοντέλα, για αυτό το λόγο αυτές οι τεχνικές και δεν έχουν μεγάλη εφαρμογή.

**Ευριστική Αξιολόγηση:** Βασίζεται, στη χρησιμοποίηση γενικών ευριστικών κανόνων, γενικών οδηγιών, αλλά κυρίως στην ικανότητα, τη γνώση και την εμπειρία ειδικών, οι οποίοι διενεργούν τον έλεγχο. Χρησιμοποιούνται ευρύτατα, εντοπίζουν λάθη που δεν εντοπίζονται από απλούς χρήστες και μειώνουν τον αριθμό των χρηστών που εμπλέκονται στην διαδικασία ελέγχου. Η επιτυχία αυτών των τεχνικών εξαρτάται σε μεγάλο βαθμό από την εμπειρία των ειδικών.

**“Πειράματα” με Χρήστες:** Ο τίτλος “πειράματα χρηστών” προέρχεται από τη μετάφραση του “User Testing”. Ακόμα και στην αγγλική του έκδοση, η ονομασία μπορεί να παρερμηνευτεί διότι βεβαίως δε γίνεται κάποιου είδους έλεγχος του χρήστη, αλλά εκτελείται μία διαδικασία με χρήστες. Από πολλές απόψεις τα πειράματα χρηστών, είναι θεμελιώδη στην αξιολόγηση χρησιμοποίησιμότητας. Προσφέρει άμεση πληροφορία για το πως ο κόσμος χρησιμοποιεί υπολογιστές και για τα ακριβή προβλήματα που συναντούν σε μία συγκεκριμένη εφαρμογή. Η μέθοδος των πειραμάτων χρηστών, περιλαμβάνει την ανεξάρτητη χρήση μιας εφαρμογής από ομάδα χρηστών. Οι χρήστες, καλούνται να διεκπεραιώσουν ένα σύνολο προκαθορισμένων εργασιών. Κατά τη διάρκεια της χρήσης του συστήματος, παρακολουθούνται διακριτικά από ειδικούς, οι οποίοι κρατούν σημειώσεις ή κάνουν μετρήσεις. Τα αποτελέσματα των μετρήσεων ή παρατηρήσεων, αναλύονται και εξάγονται συμπεράσματα.





Εικόνα 14: Σχέση αναλογίας κερδών/κόστους, με αριθμό χρηστών σε πειράματα χρηστών

Παραλλαγές, υπάρχουν πολλές, όπως το “thinking aloud”, όπου ο χρήστης κατά τη διάρκεια της χρήσης “σκέφτεται δυνατά” με αποτέλεσμα, οι παρατηρητές να αποκτούν μία άποψη για τον τρόπο σκέψης των χρηστών. Επίσης, μπορεί να συνδυαστεί η χρήση του συστήματος με την συμπλήρωση ερωτηματολογίου (για παράδειγμα, εκτίμηση της υποκειμενικής ικανοποίησης του χρήστη απέναντι στην εφαρμογή). Τέλος, μπορεί να γίνει καταγραφή του χρήστη σε βίντεο με σκοπό την περαιτέρω ανάλυση.

### Ευριστικοί Κανόνες και Αξιολόγηση<sup>83</sup>

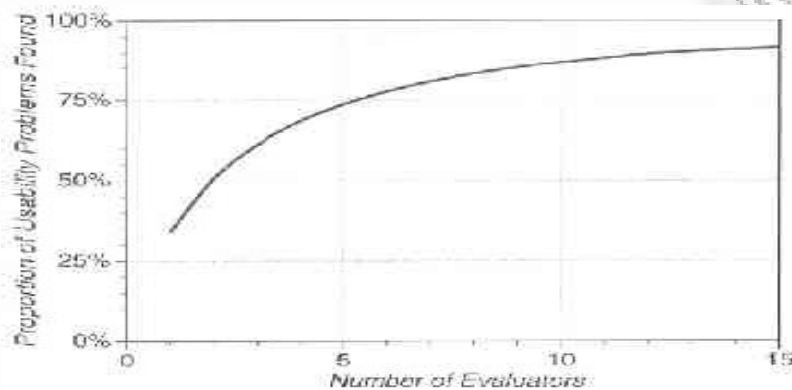
Οι ευριστικοί κανόνες στηρίζονται σε πραγματική και εμπειριστατωμένη έρευνα, αλλά η εφαρμογή τους είναι περισσότερο θέμα εμπειρίας και συστηματικής ενασχόλησης με το αντικείμενο της χρησιμοποίησιμότητας. Παρόλα αυτά, ακόμα και σχετικά άπειροι προγραμματιστές είναι σε θέση, ακολουθώντας βασικούς κανόνες, να αναπτύξουν “καλά” επίπεδα αλληλεπίδρασης των εφαρμογών.

Υπάρχουν επίσης, κανόνες και συλλογές κανόνων, που σχετίζονται με τα εκάστοτε λειτουργικά συστήματα (style guides) και έχουν ως σκοπό να παρουσιάσουν στο χρήστη όμοιες όψεις και λειτουργικότητες για τις εφαρμογές, του ίδιου λειτουργικού συστήματος. Ένας τέτοιος κανόνας για παράδειγμα, είναι ότι τα παράθυρα των εφαρμογών για το λειτουργικό σύστημα της Microsoft, έχουν στην επάνω δεξιά γωνία ένα κουμπί ορισμένου σχήματος με το οποίο “κλείνει” το παράθυρο ή η εφαρμογή.

Άλλοι κανόνες, έχουν σχέση με τις φυσικές ικανότητες του ανθρώπου και αναφέρονται για παράδειγμα, στους συνδυασμούς χρωμάτων που είναι ή δεν είναι ενδεδειγμένοι για την εμφάνιση της πληροφορίας, στις οθόνες των υπολογιστών. Η ευριστική αξιολόγηση, ακολουθεί μία πιο συστηματική και αυστηρή μέθοδο. Σκοπός είναι, να εντοπιστούν προβλήματα χρησιμοποίησιμότητας και να αντιμετωπιστούν σε μία επαναληπτική διαδικασία ανάπτυξης της εφαρμογής. Στη μέθοδο αυτή, μία σχετικά μικρή ομάδα αξιολογητών χρησιμοποιούν ανεξάρτητα μεταξύ τους την εφαρμογή και κρίνουν εάν είναι συμβατή με γνωστές σε αυτούς αρχές χρησιμοποίησιμότητας (τους ευριστικούς κανόνες). Προσπερνούν περισσότερο της μίας φοράς, όλο το επίπεδο διεπικοινωνίας της εφαρμογής.

Στην παρακάτω εικόνα 15, φαίνεται το ποσοστό των προβλημάτων που συνήθως ανακαλύπτονται, ανάλογα με το πλήθος των αξιολογητών. Από το διάγραμμα αυτό,

συμπεραίνεται ότι 5 αξιολογητές είναι ικανός αριθμός για να εντοπιστούν τα πιο σημαντικά προβλήματα.



Εικόνα 15: Σχέση, ανάμεσα σε αριθμό αξιολογητών και ποσοστού προβλημάτων χρησιμοποίησιμότητας που εντοπίζονται

Η συλλογή των αποτελεσμάτων, μπορεί να γίνει είτε με αναφορές από τους αξιολογητές, είτε έχοντας κάποιον παρατηρητή την ώρα της αξιολόγησης. Οι αξιολογητές μπορεί μετά το πέρας της χρήσης της εφαρμογής, να βρεθούν και να ανταλλάξουν τα συμπεράσματα στα οποία κατέληξαν.

Στην περίπτωση που υπάρχει παρατηρητής, η συμπεριφορά του πρέπει να είναι σαφώς πιο ανοιχτή σε προβλήματα των αξιολογητών, σε αντίθεση με τα “πειράματα χρηστών” όπου ο παρατηρητής μένει αμέτοχος. Σε αντίθεση επίσης με τα “πειράματα χρηστών”, ο παρατηρητής δεν έχει σκοπό να αξιολογήσει τη συμπεριφορά και τις ενέργειες των αξιολογητών, διότι αυτή η αξιολόγηση έρχεται ήδη από τους ίδιους τους χρήστες. Το είδος των αξιολογητών έχει βρεθεί να επηρεάζει σε μεγάλο βαθμό την ποιότητα και την ποσότητα των προβλημάτων που εντοπίζονται. Ειδικό σε θέματα χρησιμοποίησιμότητας (Usability), θα εντοπίσουν πολλά περισσότερα προβλήματα από αρχάριους χρήστες, οπότε είναι προτιμότερο για τέτοιου είδους μεθόδους, να επιλεγούν έμπειροι χρήστες.

### ***Καταγραφή Πραγματικής Χρήσης***

Σε αυτή τη μέθοδο, καταγράφεται η πραγματική χρήση μιας εφαρμογής. Για παράδειγμα, καταγράφονται στατιστικά στοιχεία με συχνότητες χρήσης των λειτουργιών της εφαρμογής ή λαθών που γίνονται. Βλέποντας για παράδειγμα, ότι κάποια λειτουργία χρησιμοποιείται πολύ σπάνια, μπορεί να αναζητηθούν οι αιτίες στις οποίες οφείλεται αυτό (μπορεί να μην χρειάζεται η λειτουργία ή να μην είναι αρκετά εμφανής ο τρόπος ενεργοποίησής της). Η καταγραφή μπορεί να γίνει είτε από τα μηνύματα χαμηλού επιπέδου του λειτουργικού συστήματος, είτε άμεσα από την ίδια την εφαρμογή. Η δεύτερη περίπτωση, έχει το πλεονέκτημα ότι τα δεδομένα που καταγράφονται μπορεί να είναι υψηλού επιπέδου έννοιες που είναι πιο εύχρηστες στην ανάλυση.

### ***Προσέγγιση Web Usage Analysis<sup>84</sup>***

Στην προηγούμενη ενότητα, για τις μεθόδους ανάλυσης χρησιμοποίησιμότητας αναφέρθηκε, ότι μία μέθοδος, βασίζεται στην καταγραφή της πραγματικής χρήσης μίας εφαρμογής και την

ανάλυση των δεδομένων που προκύπτουν από αυτήν. Στα πλαίσια της ανάλυσης χρησιμοποιησιμότητας ιστοχώρων, αυτή η μέθοδος, αποκτάει νέα διάσταση επειδή προσφέρει μοναδικά πλεονεκτήματα που την ξεχωρίζουν από τις υπόλοιπες μεθόδους. Τα πλεονεκτήματα έχουν σχέση με τη φύση των ιστοχώρων, που εισάγουν αρκετές αβεβαιότητες για τις άλλες μεθόδους.

Επισημάνθηκε ήδη, ότι ένα χαρακτηριστικό των εφαρμογών στον παγκόσμιο ιστό, είναι ότι δεν υπάρχει σαφής άποψη για τα χαρακτηριστικά των χρηστών που τις χρησιμοποιούν. Ο παγκόσμιος ιστός, προσφέρει απεριόριστη ευκολία για την επίσκεψη ενός ιστοχώρου, που καθιστά αμφίβολη την ομοιογένεια, τις κατηγορίες των χρηστών και τους στόχους που αυτοί έχουν επισκεπτόμενοι έναν ιστοχώρο.

Ο παγκόσμιος ιστός, είναι επίσης ευμετάβλητος στο χρόνο, από πολλές απόψεις. Νέες εκδόσεις εφαρμογών πλοήγησης κάνουν εφικτή, τη χρήση τεχνολογιών για την αλληλεπίδραση με το χρήστη, που πριν φάνταζαν απίθανες ή πολύ δύσκολα υλοποιήσιμες. Οι αλλαγές στον ιστοχώρο με χρήση διαφορετικών τεχνικών στην αλληλεπίδραση, μπορεί να είναι πολύ συχνές και χαρακτηρίζονται από στοιχεία πειραματισμού, που καθιστά αναγκαία τη συνεχή παρακολούθηση της ανταπόκρισης των χρηστών, στα νέα δεδομένα.

Επίσης, οι σελίδες συχνά δημιουργούνται με δυναμικό τρόπο από βάσεις δεδομένων ή άλλα μέσα, με πληροφορία, που μπορεί να αλλάζει συχνά. Ακριβώς επειδή υπάρχει η δυνατότητα σχετικά εύκολης αλλαγής του περιεχομένου αλλά και του τρόπου εμφάνισης ενός ιστοχώρου, θα ήταν επιθυμητό να ελεγχθούν πολλές εκδόσεις του ιστοχώρου ως προς την χρησιμοποιησιμότητα. Επιπρόσθετα, μπορούν μικρές αλλαγές να επιφέρουν ασύγκριτα διαφορετικά αποτελέσματα στους χρήστες ενός ιστοχώρου. Για παράδειγμα, μπορεί ένας απλός σύνδεσμος από έναν ιστοχώρο, με μεγάλο αριθμό επισκέψεων, σε έναν άλλο ιστοχώρο να βγάλει το δεύτερο από την αφάνεια και να εκτοξεύσει τις επισκέψεις και τη χρήση του σε πολύ υψηλά επίπεδα. Αυτή η αλλαγή, μπορεί να συνδυάζεται με εντελώς διαφορετικά χαρακτηριστικά των χρηστών, σε όρους πληροφορίας για την οποία ενδιαφέρονται.

Άλλο χαρακτηριστικό ορισμένων ιστοχώρων είναι ότι ο ίδιος ιστοχώρος μπορεί να είναι επισκέψιμος περιοδικά, από διαφορετικούς χρήστες στη διάρκεια του χρόνου. Για παράδειγμα, διαφορετικούς επισκέπτες έχει ένας ιστοχώρος τουριστικού προορισμού για την Κρήτη πριν τους καλοκαιρινούς μήνες σε σχέση με την περίοδο του χειμώνα.

Τέλος, όπως αναφέρθηκε και σε προηγούμενη ενότητα, οι ιστοχώροι έχουν τη δυνατότητα να προσφέρουν στους χρήστες προσωποποιημένη όψη και υπηρεσίες, ανάλογα με τις προτιμήσεις του κάθε χρήστη.

Όλα τα παραπάνω χαρακτηριστικά, καταστούν αναγκαία τη χρήση μίας μεθόδου για την αξιολόγηση χρησιμοποιησιμότητας η οποία θα είναι αρκετά ευέλικτη, ώστε να μπορεί συνεχώς να εφαρμόζεται στον υπό μελέτη ιστοχώρο και να μπορεί να ανταποκρίνεται στην ποικιλομορφία που αυτός παρουσιάζει. Σε αυτό το σημείο, η ανάλυση με την καταγραφή της συμπεριφοράς των χρηστών, μπορεί να καλύψει τις απαιτήσεις που υπάρχουν. Σε συνδυασμό με επιπλέον στοιχεία που είναι διαθέσιμα όταν η καταγραφή γίνεται σε ιστοχώρους, αποκτάει ιδιαίτερο ενδιαφέρον για περαιτέρω μελέτη. Για παράδειγμα, μπορεί να εξαχθούν στοιχεία για την προέλευση των χρηστών (χώρα, περιοχή) ή για το είδος της πληροφορίας που αναζητούν (από φράσεις αναζήτησης, σε μηχανές αναζήτησης που οδήγησαν στον ιστοχώρο). Η ονομασία που χρησιμοποιείται, για αναλύσεις στον παγκόσμιο ιστό είναι Web Analysis ή Web Mining και ειδικά για τη συμπεριφορά των χρηστών Web Usage Analysis ή Web Usage Mining.

### 3.7 Βιβλιογραφία 3<sup>ο</sup> Κεφαλαίου

66. <http://www.bluewavemag.com/blueart37.htm>  
Joseph M. Juran.
67. [http://en.wikipedia.org/wiki/Philip\\_B.\\_Crosby](http://en.wikipedia.org/wiki/Philip_B._Crosby)  
Philip\_B.\_Crosby.
68. [http://en.wikipedia.org/wiki/W.\\_Edwards\\_Deming](http://en.wikipedia.org/wiki/W._Edwards_Deming)  
W. Edwards Deming.
69. <http://www.iso.org/iso/home.htm>  
Το πρότυπο ISO8402-1986.
70. <http://dis.shef.ac.uk/sheila/marketing/services.htm>
71. Zeithaml, Parasuraman & Berry, "Delivering Quality Service; Balancing Customer Perceptions and Expectations," Free Press, 1990.
72. <http://www.netmba.com/marketing/mix/>
73. Francis Buttle, 1996, "SERVQUAL: review, critique, research agenda," European Journal of Marketing, Vol.30, Issue 1, pp.8-31.
74. <http://www.scribd.com/doc/25356471/Servqual-Model>
75. <http://www.proserv.nu/Docs/Servqual.pdf>
76. <http://en.wikipedia.org/wiki/SERVQUAL>
77. Assessing Call Centre Quality using the SERVQUAL Model Warren J S Staples & Prof. John F Dalrymple Centre for Management Quality Research, RMIT University, Australia.
78. Garvin D.A., (1998), «Managing Quality».
79. Information System Architecture Metrics: An Enterprise Engineering Evaluation Approach André Vasconcelos, Pedro Sousa, José Tribolet CEO - Centro de Engenharia Organizacional, INESC – Instituto de Engenharia de Sistemas e Computadores and Department of Information Systems and Computer Engineering, Instituto Superior Técnico, Technical University of Lisbon, Portugal.
80. “Strategies for Information Technology Governance”, Wim Van Grembergen (Ed), Idea.Group Publishing, ISBN 1-59140-140-2, Chapter IX, pp. 216-244, 2003. Technical Issues Related to IT Governance Tactics: Product Metrics, Measurements and Process Control.
81. Web Metrics October 26, 2006 Steven Schwartz President, PowerWebResults.com Southeastern Massachusetts E-Commerce Network University of Massachusetts – Dartmouth.
82. Web Content Managers Forum, 2005.
83. Using Web Analytics for Website Optimization Presented to the Webmaster’s Guild by Adrienne Buskard, President Mercury Web Solutions October 6, 2006.
84. Issue Paper for Bundaberg Hospital Commission of Inquiry Safety and Quality, July 2005.
85. <http://www.iso.org>
86. <http://www.iec.ch>
87. <http://www.ws-i.org>
88. <http://xml.coverpages.org/WS-I-Profiles-ISO.html>

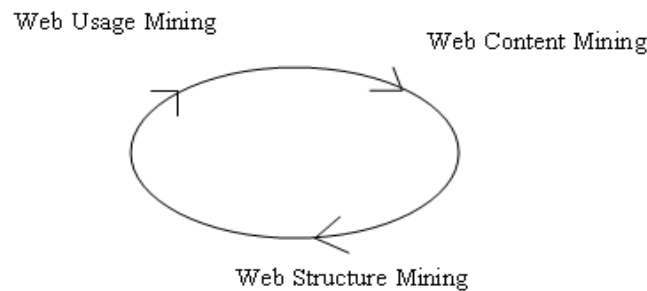
## ΚΕΦΑΛΑΙΟ 4

### ΕΡΓΑΛΕΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

#### 4.1 Εισαγωγή

Η δυνατότητα ανάλυσης των ιστοχώρων παραμένει μια ανοικτή προβληματική για τους σχεδιαστές των ιστοχώρων, που αποβλέπουν στην αποδοτικότερη ικανοποίηση των χρηστών. Η σχεδίαση ενός ιστοχώρου, επικεντρώνεται στην οργάνωση της πληροφορίας σε κάθε σελίδα και τους υπερσυνδέσμους μεταξύ των σελίδων, με σκοπό την εξυπηρέτηση των αναγκών των χρηστών.

Το Web Usage Analysis<sup>91</sup> ή Web Usage Mining<sup>91</sup>, είναι μία από τις εφαρμογές τεχνικών εξόρυξης δεδομένων (data mining) σε μεγάλες αποθήκες δεδομένων για τον παγκόσμιο ιστό (Web data repositories). Προσφέρει τεχνικές, για την ανάλυση της συμπεριφοράς των χρηστών σε ιστοχώρους για την ανακάλυψη συχνά εμφανιζόμενων διαγραμμάτων, κανόνων συσχετισμού (association rules), συνόλων ομοειδών σελίδων και χρηστών (page and user clusters) και για την ανάλυση μονοπατιών (path analysis).



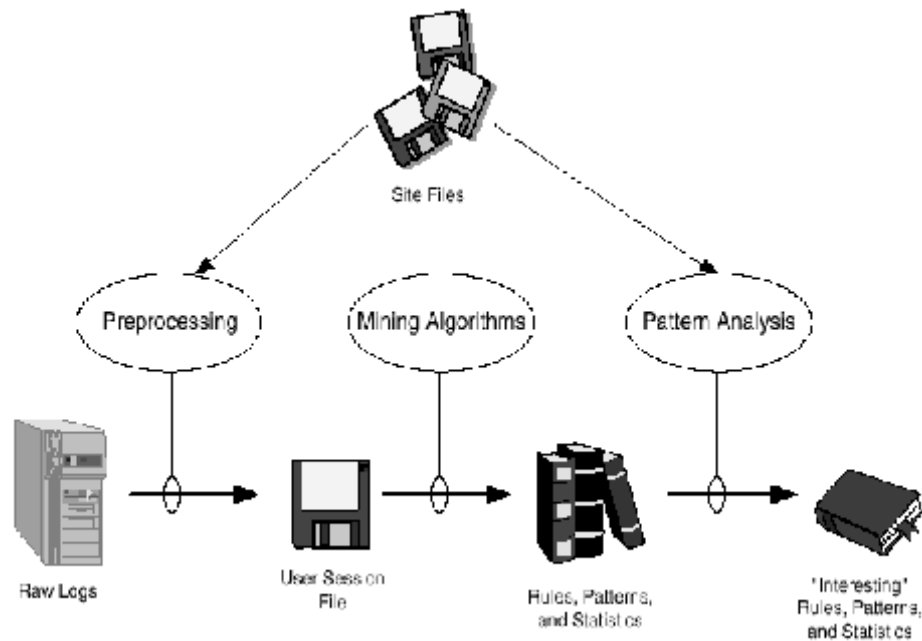
Εικόνα 16: Σχηματική παράσταση των ειδών του Web Usage Analysis

Το Web Usage Mining (Εξόρυξη Χρήσης Ιστού), ξεχωρίζει από το Web Content Mining (Εξόρυξη Περιεχομένου Ιστού), στο ότι το δεύτερο ασχολείται με την πληροφορία, δηλαδή το περιεχόμενο που παρέχεται στον παγκόσμιο ιστό και ξεχωρίζει από το Web Structure Mining (Εξόρυξη Δομής Ιστού), στο ότι αυτό ασχολείται με τη δομή του παγκόσμιου ιστού. Η έρευνα σε θέματα Web Mining, είναι ένα συγκλίνον επιστημονικό πεδίο από διάφορες επιστημονικές κοινότητες, όπως Βάσεις Δεδομένων, Ανάκτησης πληροφοριών, Τεχνητής Νοημοσύνης και Εκμάθησης Μηχανών.

#### 4.2 Ανάλυση και Αξιολόγηση Επισκεψιμότητας

Η ανάλυση επισκεψιμότητας δεν είναι μία μονοσήμαντη ή στερεότυπη διαδικασία. Παρόλο που τα αρχικά βήματα ακολουθούν συνήθως μία κοινή δομή, στη συνέχεια χρησιμοποιούνται διαφορετικές αναλύσεις, ανάλογα με τους τομείς στους οποίους κάθε φορά επικεντρώνεται η ανάλυση. Πέραν των αρχικών δεδομένων από τις προσβάσεις στον εξυπηρετητή παγκόσμιου ιστού, η εκάστοτε μέθοδος μπορεί να εμπλουτιστεί και με άλλα δεδομένα, που προέρχονται είτε

άμεσα από τον ιστοχώρο (για παράδειγμα, πληροφορίες για τη συσχέτιση των διαφορετικών σελίδων), είτε από τρίτες πηγές όπως, δημογραφικές πληροφορίες για τους επισκέπτες. Συνήθως όμως, υπάρχει μία ανάδραση από την αποκτούμενη γνώση, η οποία μετασχηματίζει την παρακάτω σειριακή διαδικασία σε μορφή κυκλική.



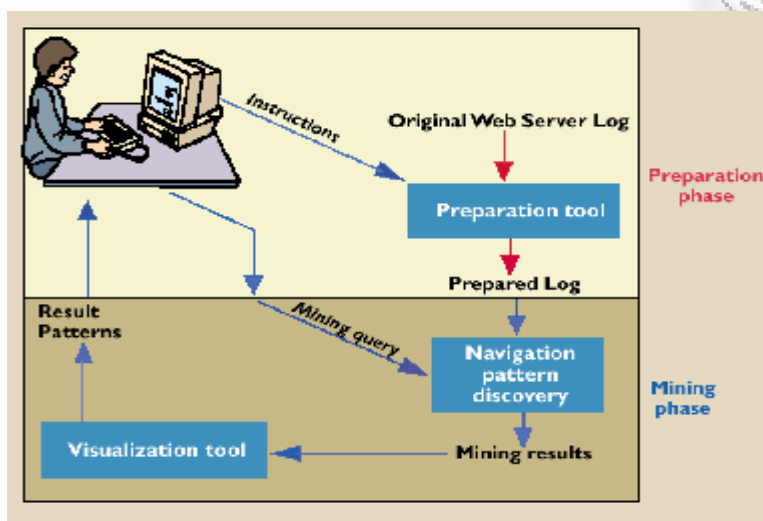
Εικόνα 17: Διαδικασία Ανάλυσης Επισκεψιμότητας

Στην παραπάνω εικόνα 17, αναλύεται η πλοήγηση στον ιστοχώρο (Navigation Pattern Discovery) και συγκρίνεται το αποτέλεσμα, με την σχεδίαση που προέβλεψαν οι σχεδιαστές κατά την ανάπτυξη του ιστοχώρου, ώστε να διαπιστωθεί εάν συμπίπτουν. Στην περίπτωση που δε συμπίπτουν, επαναλαμβάνεται η ανάλυση αφού έχει γίνει η κατάλληλη επέμβαση στο σχεδιασμό του ιστοχώρου.

Έτσι, υπάρχει μία φάση προεπεξεργασίας των πρωτογενών δεδομένων, η οποία ακολουθείται από τη φάση εξαγωγής γνώσης. Σε αυτό το στάδιο, προετοιμάζονται τα δεδομένα που αποκτήθηκαν από την κίνηση των εξυπηρετητών HTTP για την περαιτέρω ανάλυση. Συνηθισμένες εργασίες που εκτελούνται είναι:

- ✓ Καθαρισμός από μη επιθυμητή πληροφορία, όπως αιτήσεις για πόρους που δεν υπάρχουν στον εξυπηρετητή.
- ✓ Φίλτρο που αφαιρεί αιτήσεις για πόρους που δεν παρουσιάζουν ενδιαφέρον (εικόνες και άλλα μέσα). Συνήθως διατηρούνται μόνο οι αιτήσεις για σελίδες HTML.
- ✓ Συμπληρώνονται προσβάσεις που λογικά θα πρέπει να έχουν γίνει, χωρίς αυτές να εμφανίζονται στα δεδομένα καταγραφής (path completion). Τέτοιες προσβάσεις προκύπτουν από μηχανισμούς caching, στην αλυσίδα επικοινωνίας HTTP.
- ✓ Οι αιτήσεις ομαδοποιούνται ανά χρήστη και ανά επίσκεψη και υπολογίζονται έτσι τα μονοπάτια της επίσκεψης. Η ομαδοποίηση, μπορεί να επεκταθεί και σε λογικούς συσχετισμούς ανά σελίδα (visit sessions, concept hierarchies, page taxonomies).

Τα δεδομένα που προκύπτουν από αυτό το στάδιο, φυλάσσονται συνήθως σε δομημένη μορφή σε σχεσιακές βάσεις δεδομένων ώστε να είναι εύκολη και ταχεία η πρόσβαση σε αυτά.



Εικόνα 18: Διαδικασία Ανάλυσης Επισκεψιμότητας

Στην παραπάνω εικόνα 18, διακρίνεται πάλι η φάση της προεπεξεργασίας των πρωτογενών δεδομένων (Preparation phase), όπως και το στάδιο της ανακάλυψης γνώσης (Knowledge Discovery), που είναι ίσως από τα πιο ενδιαφέροντα τμήματα στην ανάλυση επισκεψιμότητας. Σε αυτό το στάδιο, πρέπει να είναι ήδη γνωστό το σημείο στο οποίο πρέπει να επικεντρωθεί η ανάλυση, διότι πρέπει να επιλεγεί η μέθοδος που θα χρησιμοποιηθεί. Ανάλογα με τη μέθοδο, πιθανώς να χρειαστεί αναμόρφωση των δεδομένων σε μορφή που να ταιριάζουν στη συγκεκριμένη μέθοδο.

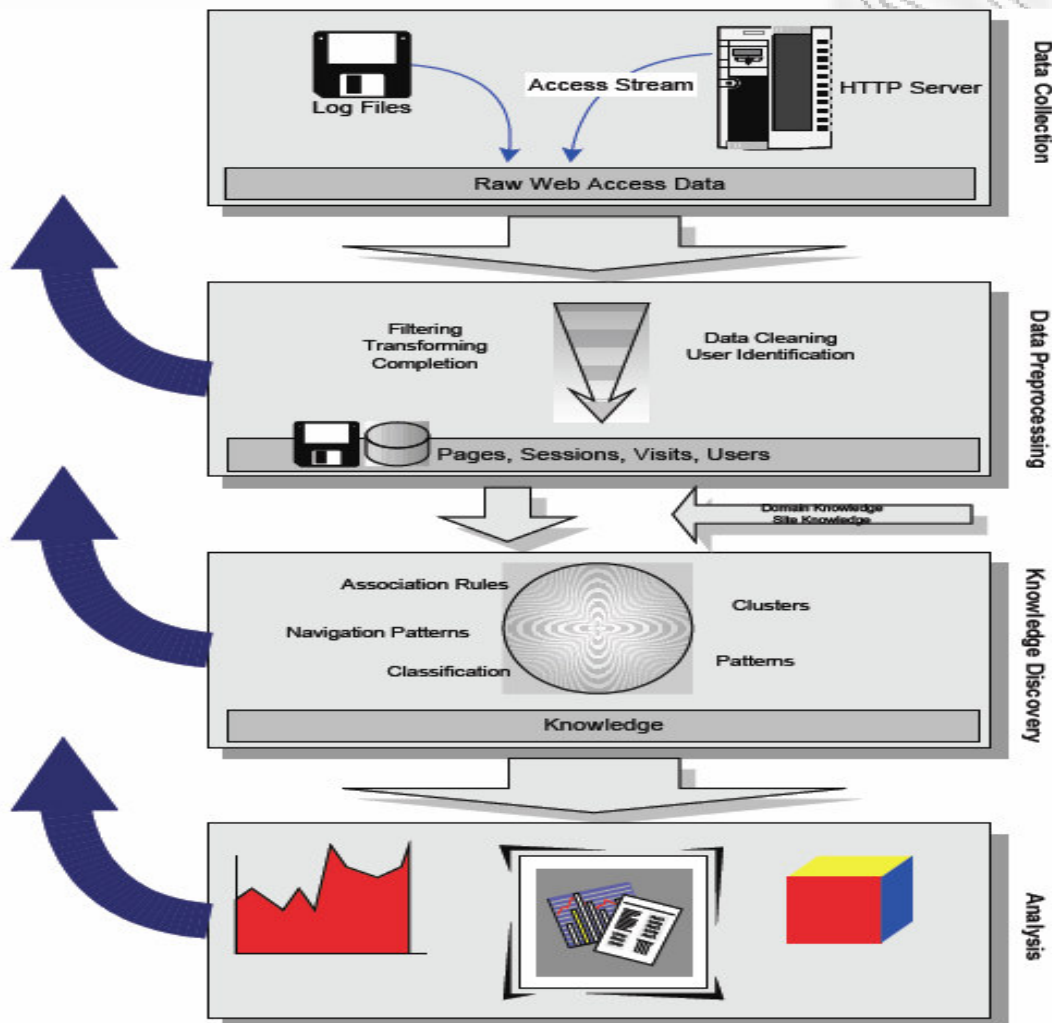
Σε αυτή τη φάση, τα δεδομένα μπορούν να εμπλουτιστούν με στοιχεία από τρίτες πηγές (ανεξάρτητα εάν αποκτήθηκαν από τον ίδιο ιστοχώρο ή από αλλού). Τέτοια στοιχεία μπορεί να είναι δημογραφικά δεδομένα για τους επισκέπτες του ιστοχώρου (για παράδειγμα, περιοχή διαμονής). Η πληροφορία που θα αποκτηθεί, μπορεί να περιορίζεται σε απλά στατιστικά στοιχεία κίνησης του ιστοχώρου (αριθμός σελιδοπροβολών ανά επίσκεψη, ώρες αιχμής, σελίδες εισόδου και εξόδου), αλλά η πραγματικά ενδιαφέρουσα πληροφορία προέρχεται από τη χρήση τεχνολογίας Εξόρυξης Δεδομένων (Data Mining), η οποία ανακαλύπτει συσχετισμούς, που δεν είναι εμφανή με την πρώτη ματιά.

Οι κύριοι τομείς έρευνας, είναι οι ακόλουθοι και προέρχονται από την κλασική εφαρμογή τεχνολογιών Data Mining:

- ✓ ανακάλυψη σχημάτων πλοήγησης (Navigation Pattern Discovery)
- ✓ κανόνες συσχετισμού (Association Rules)
- ✓ ακολουθιακά σχήματα (Sequential Patterns)
- ✓ ανακάλυψη ομοειδών (Clustering)
- ✓ κατάταξη (Classification)

Σε κάθε περίπτωση, η ακριβής διαδικασία που θα ακολουθηθεί εξαρτάται πάντα από τον τελικό στόχο που πρέπει να έχει τεθεί πριν την έναρξη της διαδικασίας. Ακόμα και για την περίπτωση όπου δεν έχουν οριοθετηθεί τα επιδιωκόμενα αποτελέσματα, μετά από μία αρχική

ανάλυση θα πρέπει αυτά να προσδιοριστούν, ώστε να προσαρμοστεί η διαδικασία για βέλτιστη απόδοση σε όρους ταχύτητας και ακρίβειας αποτελεσμάτων.



Εικόνα 19: Γενικό περίγραμμα της διαδικασίας ανάλυσης επισκεψιμότητας. Διακρίνονται τα στάδια της συλλογής δεδομένων, προεπεξεργασίας δεδομένων, ανακάλυψη γνώσεως και ανάλυσης αποτελεσμάτων. Αρχικά υπάρχει το στάδιο της συλλογής δεδομένων (data collection). Ακολουθεί το στάδιο της προεπεξεργασίας των δεδομένων (data preprocessing) και της ανακάλυψης γνώσεως (knowledge discovery). Η διαδικασία τελειώνει με την ανάλυση των δεδομένων που έχουν προκύψει.

Ανακεφαλαιώνοντας και μοντελοποιώντας τη διαδικασία ανάλυσης επισκεψιμότητας, μπορεί να καταλήξει κανείς, σε ένα γενικό διαχωρισμό της, όπως φαίνεται στη παραπάνω εικόνα 19. Στο πρώτο επίπεδο, είναι η συλλογή των δεδομένων (Data Collection) από την πλοήγηση των χρηστών του ιστοχώρου. Στον κεντρικό υπολογιστή του δικτύου, έχει οριστεί ο φάκελος που αποθηκεύονται τα αρχεία στα οποία γράφεται και αποθηκεύεται η προς επεξεργασία πληροφορία. Τα αρχεία αυτά, ονομάζονται αρχεία καταγραφής (Log Files) και κάποιες φορές, ανάλογα από την εφαρμογή, μπορεί να είναι και ένα αρχείο. Το μειονέκτημα είναι, ότι όταν δημιουργείται ένα μόνο αρχείο καταγραφής, με την πάροδο του χρόνου αποκτά μεγάλο όγκο



δεδομένων και είναι δύσκολη η επεξεργασία του. Στο δεύτερο επίπεδο του εικονοδιαγράμματος, είναι η φάση της προεπεξεργασίας των πρωτογενών δεδομένων (Data Preprocessing). Εδώ, φιλτράρονται τα δεδομένα από τα αρχεία καταγραφής και γίνεται η αναγνώριση και ο διαχωρισμός των σελίδων του ιστοχώρου, των επισκέψεων, των χρηστών και όποιων άλλων στοιχείων εξάγονται στατιστικά αποτελέσματα από τα δεδομένα. Στο τρίτο επίπεδο, είναι η Ανακάλυψη Γνώσης (Knowledge Discovery), δηλαδή την πληροφορία που αναλύεται σε στατιστικά στοιχεία κίνησης του ιστοχώρου, όπως ο αριθμός σελιδοπροβολών ανά επίσκεψη, οι ώρες αιχμής, οι σελίδες εισόδου και εξόδου, καθώς και συσχετισμούς αυτών των στατιστικών αποτελεσμάτων. Τέλος στο τέταρτο επίπεδο, είναι τα αποτελέσματα της ανάλυσης σε μορφή πινάκων και διαγραμμάτων. Η πληροφορία που αποκτήθηκε αναλύεται με εργαλεία γραφικής απεικόνισης δεδομένων και εξειδικευμένων προγραμμάτων.

### 4.3 Εφαρμογή σε Ιστοσελίδες

#### 4.3.1 Μεθοδολογία Ανάλυσης

Η εφαρμογή που ακολουθεί, υποστηρίχθηκε με την μέθοδο του ερωτηματολογίου. Οι ιστοσελίδες που χρησιμοποιήθηκαν στην ανάλυση, είναι οι επίσημοι ιστοχώροι των Περιφερειακών Επιχειρησιακών Προγραμμάτων (Π.Ε.Π) και είναι μαζί με την ηλεκτρονική τους διεύθυνση, τα παρακάτω:

- ✓ της Στερεάς Ελλάδας (<http://www.stereaellada.gr/3kps/pep.htm>),
- ✓ του Νοτίου Αιγαίου (<http://www.notioaigaio.gr/site.asp>),
- ✓ της Θεσσαλίας (<http://www.thessalia.gr/pep/default.el.asp>),
- ✓ του Βορείου Αιγαίου (<http://www.pepba.gr/>),
- ✓ της Ηπείρου ([http://www.peproe.gr/index\\_pep.html](http://www.peproe.gr/index_pep.html)),
- ✓ της Δυτικής Μακεδονίας (<http://www.pepdym.gr>),
- ✓ των Ιονίων Νήσων (<http://www.pepionia.gr/>) και
- ✓ της Δυτικής Ελλάδας ([http://www.dytikiellada.gr/per\\_perifereia.htm](http://www.dytikiellada.gr/per_perifereia.htm)).

Τα Π.Ε.Π συμβάλουν στην κάλυψη των εθνικών στρατηγικών στόχων με έμφαση στα ιδιαίτερα χαρακτηριστικά και στις ανάγκες κάθε Περιφέρειας. Σε κάθε περίπτωση, τα Π.Ε.Π καλύπτουν τις κοινωνικές υποδομές, την υγεία και την κοινωνική αλληλεγγύη (υποδομές νοσοκομείων και δομών κοινωνικής φροντίδας, ειδικών μονάδων, κέντρων υγείας και ανοιχτής φροντίδας, εξειδικευμένος εξοπλισμός, μέτρα ανάπτυξης και προστασίας της Δημόσιας Υγείας), τον πολιτισμό (ενίσχυση των βασικών πολιτιστικών υποδομών, προστασία και ανάδειξη της πολιτιστικής κληρονομιάς), τα έργα προσπελασιμότητας και περιβάλλοντος τοπικής κλίμακας καθώς και την ενίσχυση ορεινών, μειονεκτικών, νησιωτικών περιοχών. Οι ιστοχώροι αυτοί, περιέχουν πολυποίκιλα μενού, επιτρέπουν την πρόσβαση σε πληθώρα πληροφοριών διαφορετικών θεμάτων και έχουν επισκεψιμότητα σε ημερήσια βάση.

Οι χρήστες περιηγήθηκαν και απαντήσανε στο ερωτηματολόγιο και για τις οχτώ (8) αυτές ιστοσελίδες. Παρακάτω, γίνεται ανάλυση των αποτελεσμάτων του ερωτηματολογίου για την ιστοσελίδα του Π.Ε.Π της Στερεάς Ελλάδας (<http://www.stereaellada.gr/3kps/pep.htm>), με την βοήθεια της στατιστικής και του προγράμματος SPSS, όπου διαπιστώνεται η σημασία του μοντέλου SERVQUAL. Ακόμα, παρουσιάζεται το εργαλείο WebTrends Analysis Series 7.0 που αναλύει την επισκεψιμότητα, εξάγοντας γενικά και αναλυτικά αποτελέσματα για όλο τον ιστοχώρο. Επίσης, δίνονται κάποια γενικά αποτελέσματα μέσω διαγραμμάτων και πινάκων για το Π.Ε.Π της Στερεάς Ελλάδας. Τέλος, παρουσιάζεται ένας συγκεντρωτικός πίνακας όλων των

οχτώ (8) ιστοσελίδων με κάποια γενικά στοιχεία που εξήχθησαν μέσω του εργαλείου WebTrends.

Στο ερωτηματολόγιο, έγινε μία προσπάθεια να περιέχει ερωτήματα που καλύπτουν στοχευμένη πληροφόρηση σχετικά με την ασφάλεια, την ποιότητα και την αξιολόγηση των ιστοχώρων αυτών. Το ερωτηματολόγιο αποτελείται από δεκαεννέα (19) ερωτήσεις. Οι απαντήσεις δίνονται σε μία κλίμακα από μηδέν έως τέσσερα, κατ' αύξουσα βέλτιστη σειρά.

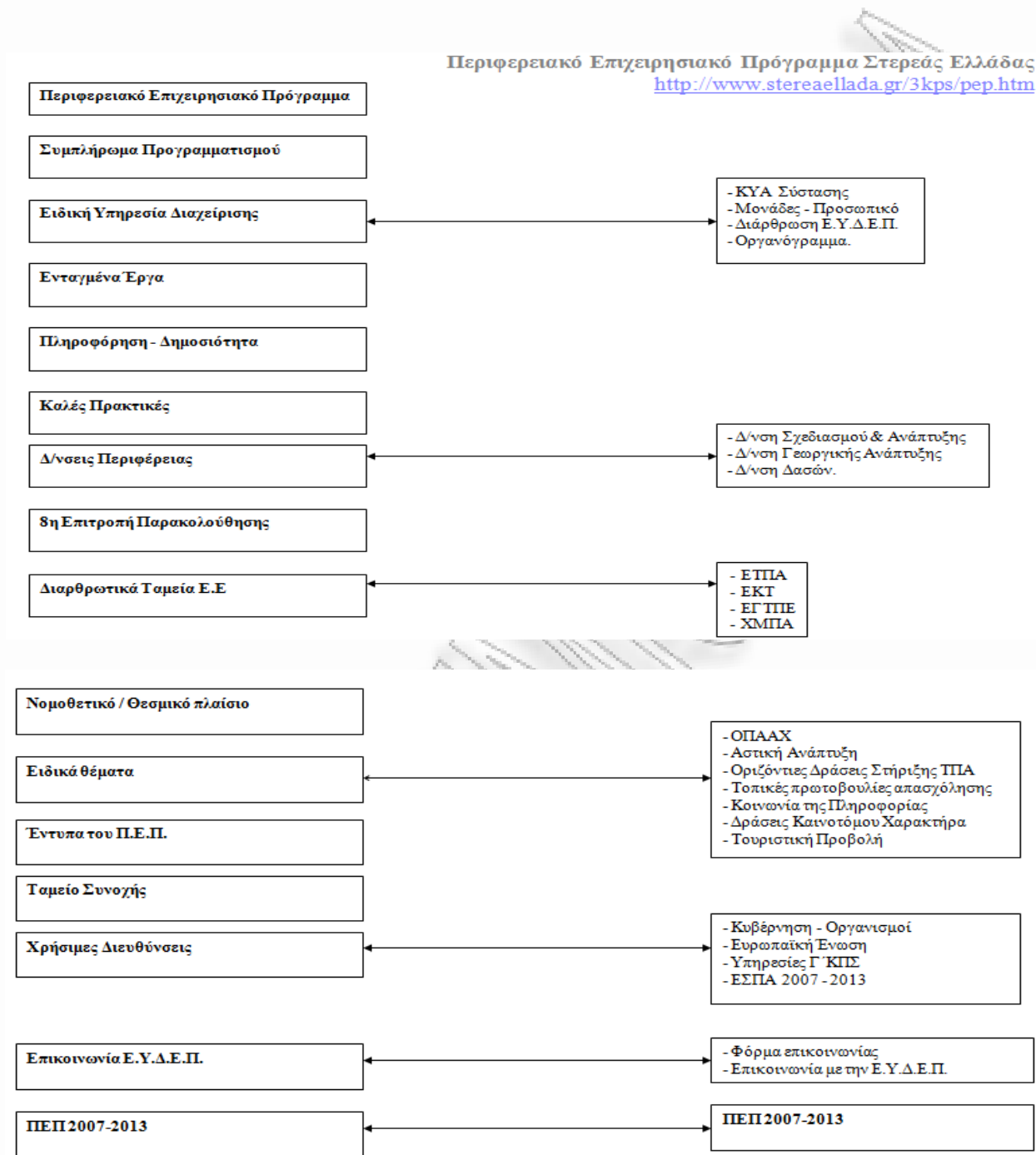
Το δείγμα του ερωτηματολογίου, αποτελείται από σαράντα πέντε (45) άτομα εκ των οποίων τα είκοσι επτά (27) είναι άντρες σε ποσοστό 60% και τα δεκαοκτώ (18) γυναίκες σε ποσοστό 40%. Επίσης, τα άτομα χωρίζονται σε τέσσερις κατηγορίες βάσει εργασιακής εμπειρίας σε ανάπτυξη και διαχείριση ιστοσελίδων, υποδομές και δίκτυα ηλεκτρονικών υπολογιστών, ανάπτυξη βάσεων δεδομένων και η τέταρτη κατηγορία αφορά άτομα που έχουν επάγγελμα διαφορετικό της Πληροφορικής. Παρακάτω παρατίθεται το ερωτηματολόγιο.

### **Ερωτηματολόγιο Αξιολόγησης**

1. Πόσο εύκολο είναι να βρείτε την επιθυμητή ιστοσελίδα;
2. Πόσο εύκολο είναι να βρείτε την επιθυμητή σύνδεση στην συγκεκριμένη ιστοσελίδα;
3. Πόσο εύκολο είναι να βρείτε τις πληροφορίες που αναζητάτε;
4. Είναι γρήγορη η πρόσβαση στις πληροφορίες της ιστοσελίδας;
5. Είναι ικανοποιητικός ο τρόπος σχεδίασης της αναζήτησης πληροφοριών;
6. Υπάρχει δυνατότητα επίσκεψης συναφών ιστοσελίδων;
7. Ελαχιστοποιείται ο χρόνος ανίχνευσης κειμένου;
8. Πληρούνται οι κανόνες προσωπικών δεδομένων;
9. Η εγγραφή στην ιστοσελίδα είναι εύκολη;
10. Ανίχνευση του κειμένου γίνεται με μικρότερο κόστος (χρήση ποντικιού);
11. Υπάρχουν εύκολοι τρόποι αναζήτησης;
12. Είναι εύκολη η χρήση της πλατφόρμας;
13. Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;
14. Οι απαντήσεις που δύνονται περιέχουν συνδέσεις που εξυπηρετούν τον χρήστη;
15. Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;
16. Σκοπεύετε να επισκεφτείτε ξανά την ιστοσελίδα;
17. Θα την προτείνετε σε γνωστούς και φίλους;
18. Θα μιλούσατε θετικά για την ιστοσελίδα;
19. Υπάρχει άμεση πρόσβαση στο υλικό της ιστοσελίδας;

### **4.3.2 Περιγραφή Ιστοσελίδας**

Στην παράγραφο αυτή, δίνεται μία αναλυτική περιγραφή της αρχικής σελίδας του ιστοχώρου του Π.Ε.Π Στερεάς Ελλάδας - <http://www.stereaellada.gr/3kps/pep.htm> με σχεδιάγραμμα και εικόνα από την ίδια την ιστοσελίδα.



Εικόνα 20: Διάγραμμα παρουσίασης της αρχικής σελίδας της ιστοσελίδας του Π.Ε.Π Στερεάς Ελλάδας - <http://www.stereaellada.gr/3kps/pep.htm>.

Στην παραπάνω εικόνα 20, παρουσιάζεται το διάγραμμα που αποτελεί το βασικό κορμό της ιστοσελίδας του Π.Ε.Π Στερεάς Ελλάδας (<http://www.stereaellada.gr/3kps/pep.htm>).

Οι κεντρικές επιλογές (menu) βρίσκονται στα αριστερά της ιστοσελίδας. Οι βασικές επιλογές της ιστοσελίδας φτάνουν μέχρι και δύο επίπεδα. Έχει αυτή την εικόνα και όπου υπάρχει βέλος δείχνει πως ξεδιπλώνουν οι επιλογές που έχει ο χρήστης. Στο διάγραμμα, όπου δεν υπάρχει

βέλος, απλά πατώντας επάνω, πηγαίνει στην ανάλογη σελίδα του ιστοχώρου και από εκεί και πέρα υπάρχει κουμπί επιστροφής στην προηγούμενη σελίδα, στο επάνω δεξί μέρος της ιστοσελίδας μαζί με την ημερομηνία.

Δεξιά και κάτω από τις κεντρικές επιλογές που αναφέρθηκαν, μπορεί ο χρήστης, να ανατρέξει σε Ευρετήριο Όρων του Γ' Κοινοτικού Πλαισίου Στήριξης (Κ.Π.Σ), να αλλάξει την γλώσσα στην ιστοσελίδα και να κάνει κάποια Αναζήτηση (Απλή ή Σύνθετη).

Στο κέντρο της αρχικής σελίδας υπάρχει μία περιγραφή του Προγράμματος και κάτω από αυτή την περιγραφή δύο σύνδεσμοι:

- Άξονες προτεραιότητας Π.Ε.Π Στερεάς Ελλάδας
- Αναθεωρημένο Π.Ε.Π Στερεάς Ελλάδας 2000-2006

Δεξιά από αυτή την περιγραφή, είναι τα ΤΕΛΕΥΤΑΙΑ ΝΕΑ, όπου αν ο επισκέπτης πατήσει πάνω στο τίτλο του νέου, του ανοίγει το νέο. Επίσης, έχει επιλογή να ανατρέξει στο Αρχείο Νέων καθώς και στις Τρέχουσες Προσκλήσεις του προγράμματος

Τέλος, η σελίδα στο κάτω μέρος έχει κάποια εικονίδια, όπου πατώντας επάνω, οδηγούν τον χρήστη σε σελίδες εκτός του ιστοχώρου, αλλά που έχουν σχέση με το Γ'Κ.Π.Σ.

Εικόνα 21: Αρχική σελίδα του Περιφερειακού Επιχειρησιακού Προγράμματος Στερεάς Ελλάδας - <http://www.stereaellada.gr/3kps/pep.htm>.

#### 4.4 Στατιστική <sup>100, 101, 102, 103, 104</sup>

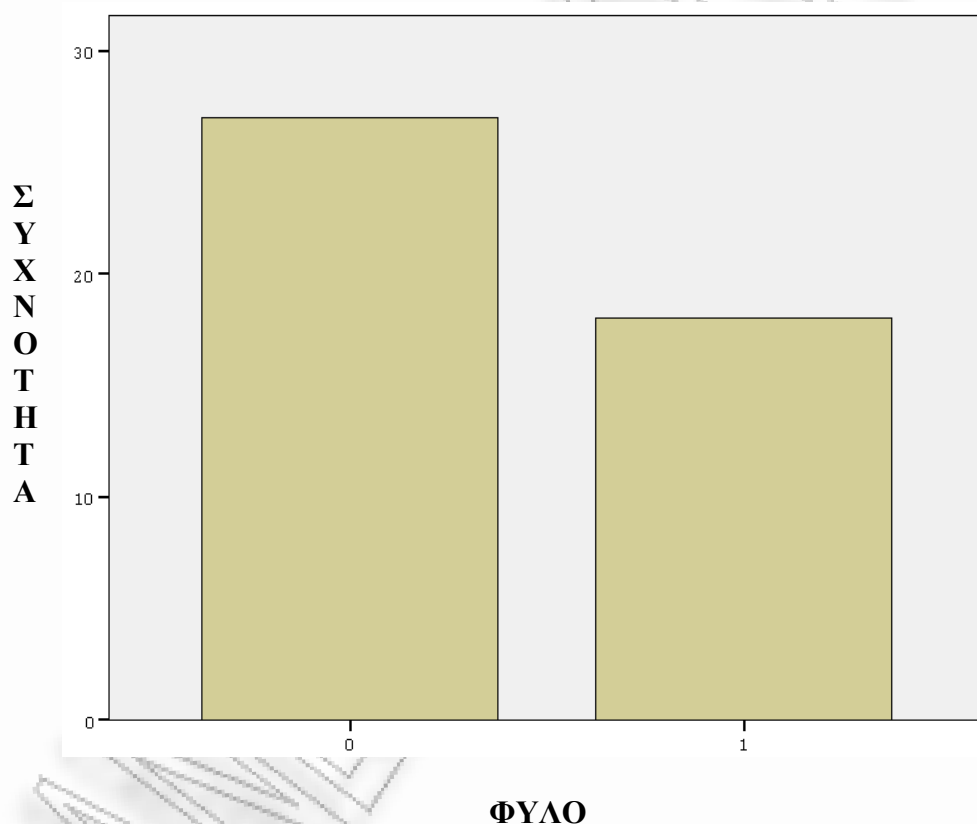
Η στατιστική είναι η επιστήμη που ασχολείται με τη συλλογή δεδομένων, την περιγραφή τους και την εξαγωγή τεκμηριωμένων συμπερασμάτων με σκοπό την αποδοτικότερη λήψη αποφάσεων.

Στατιστική είναι ένα σύνολο αρχών και μεθοδολογιών για:

- ✓ Το σχεδιασμό της διαδικασίας συλλογής δεδομένων.
- ✓ Τη συνοπτική και αποτελεσματική παρουσίαση τους.
- ✓ Την ανάλυση δεδομένων και εξαγωγή αντίστοιχων συμπερασμάτων.

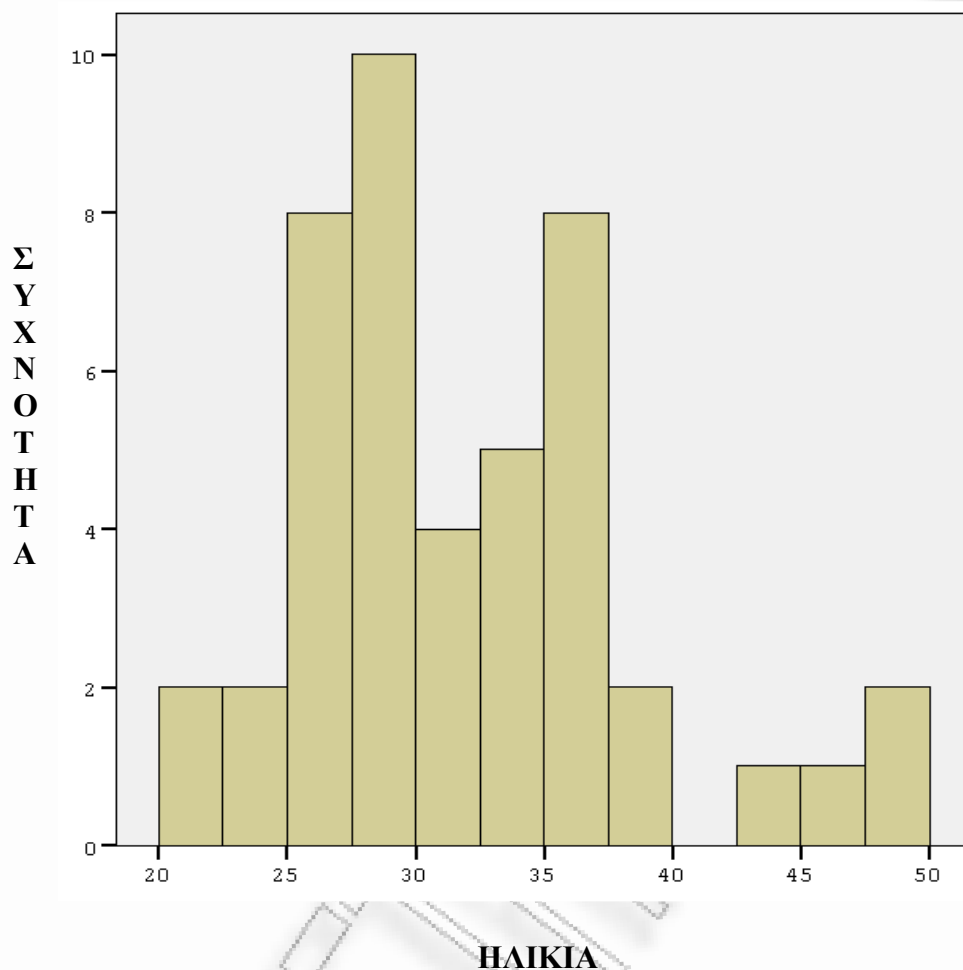
Στην συγκεκριμένη εργασία δίνεται ιδιαίτερη βάση στις δύο βασικές κατηγορίες της στατιστικής: Την Περιγραφική Στατιστική και την Στατιστική Συμπερασματολογία. Με αυτές τις δύο κατηγορίες ελέγχεται η σημαντικότητα της πληροφορίας και η συσχέτιση των πληροφοριών, με απώτερο σκοπό την ποσοτικοποίηση της ικανοποίησης των χρηστών των ιστοσελίδων, χρησιμοποιώντας το SPSS πρόγραμμα.

Το SPSS, έχει χρησιμοποιηθεί σε πολλές έρευνες διαφορετικών κλάδων και επιστημών, δίνοντας αξιόπιστες αναλύσεις. Εδώ, χρησιμοποιείται σε επίπεδο ανάλυσης ικανό να δώσει συμπεράσματα στην έρευνα που διεξήχθη με την χρήση ερωτηματολογίου και ακόμα πιο συγκεκριμένα στις απαντήσεις του ερωτηματολογίου που αφορούν την ιστοσελίδα του Π.Ε.Π. ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ - [http://www.stereaellada.gr/per\\_perifereia.htm](http://www.stereaellada.gr/per_perifereia.htm).



Εικόνα 22: Κατανομή πληθυσμού ερωτηματολογίου βάσει φύλου.

Από την εικόνα 22, παρατηρείται ότι επί συνόλου σαράντα πέντε (45) ατόμων που λάβανε μέρος στη μελέτη, το ποσοστό των αντρών είναι 60% και των γυναικών 40%.



Εικόνα 23: Κατανομή πληθυσμού ερωτηματολογίου βάσει ηλικίας.

Από την εικόνα 23, παρατηρείται ότι ο πληθυσμός παρουσιάζει μεγαλύτερη συγκέντρωση ατόμων στις ηλικίες από 26 έως 30 ετών. Το διάγραμμα επεξηγείται και από τον παρακάτω πίνακα 6.

ΗΛΙΚΙΑ	ΣΥΧΝΟΤΗΤΑ	ΠΟΣΟΣΤΟ %	ΑΘΡΟΙΣΤΙΚΟ ΠΟΣΟΣΤΟ
22	2	4,4	4,4
23	1	2,2	6,7
24	1	2,2	8,9
26	6	13,3	22,2
27	2	4,4	26,7
28	7	15,6	42,2
29	3	6,7	48,9
30	2	4,4	53,3
31	1	2,2	55,6
32	1	2,2	57,8

33	3	6,7	64,4
34	2	4,4	68,9
35	3	6,7	75,6
36	2	4,4	80
37	3	6,7	86,7
38	1	2,2	88,9
39	1	2,2	91,1
44	1	2,2	93,3
46	1	2,2	95,6
48	1	2,2	97,8
50	1	2,2	100
<b>ΣΥΝΟΛΟ</b>	45	100,0	

Πίνακας 6: Κατανομή Συχνοτήτων Ηλικιών

Στον παραπάνω πίνακα 6, η μέση ηλικία που έλαβαν μέρος είναι 31,71 έτη με 95% διάστημα εμπιστοσύνης για την εκτίμηση του πληθυσμιακού μέσου δηλαδή,  $31,71 \pm 0,998$ . Η Διάμεσος έχει τιμή τα 30 έτη και η Επικρατούσα Τιμή είναι τα 28 έτη.

Για την συγκεκριμένη ανάλυση των δεδομένων, μετατράπηκε η ποσοτική μεταβλητή ηλικία, σε ηλικιακές κλάσεις (κατηγορίες): (1.) [20 - 30], (2.) [30 - 40], και (3.) [40 – 50].

		ΗΛΙΚΙΑ			Σύνολο	
		[20-30]	[30-40]	[40-50]		
Φύλο	Αντρας	Συχνότητα	12	11	4	27
		% Φύλο	44,4%	40,7%	14,8%	100,0%
		% ΗΛΙΚΙΑ	54,5%	57,9%	100,0%	60,0%
		% Συνόλου	26,7%	24,4%	8,9%	60,0%
	Γυναίκα	Συχνότητα	10	8	0	18
		% Φύλο	55,6%	44,4%	,0%	100,0%
		% ΗΛΙΚΙΑ	45,6%	42,1%	,0%	40,0%
		% Συνόλου	22,2%	17,8%	,0%	40,0%
Σύνολο		Συχνότητα	22	19	4	45
		% Φύλο	48,9%	42,2%	8,9%	100,0%
		% ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%
		% Συνόλου	48,9%	42,2%	8,9%	100,0%

Πίνακας 7: Σχέση Φύλου με την Ηλικία.

Ο παραπάνω πίνακας 7, απεικονίζει την σχέση φύλου με την μεταβλητή ΗΛΙΚΙΑ. Παρατηρείται, ότι το μεγαλύτερο ποσοστό, 48,9%, αποτελείται από άτομα που ανήκουν στην κλάση από 20 έως 30 ετών και το 42,2% ανήκουν στην ηλικία από 30 έως 40 ετών. Ειδικότερα, επί συνολικού αριθμού ατόμων που βρίσκονται μεταξύ της ηλικιακής κλάσης 20 έως 30 ετών, παρατηρούμε ότι το 54,5% είναι άντρες, ενώ επί συνόλου ατόμων που ανήκουν στην ηλικιακή κλάση από 30 έως 40 ετών το 57,9% είναι άντρες. Τέλος, ιδιαίτερο χαρακτηριστικό είναι το ποσοστό των ατόμων που ανήκει στην ηλικιακή κλάση από 40 έως 50 ετών που ανέρχεται στο 100% και είναι 4 άντρες.

Στην συνέχεια, ο παρακάτω πίνακας 8, δείχνει την συμπεριφορά της μεταβλητής Ηλικία σε σχέση με το επάγγελμα. Η κατηγοριοποίηση των κλάσεων των ηλικιών είναι αυτή που έχει προαναφερθεί, δηλαδή: 1. Ανάπτυξη και Διαχείριση Ιστοσελίδων, 2. Υποδομές και Δίκτυα Ηλεκτρονικών Υπολογιστών, 3. Βάσεις Δεδομένων – Ανάπτυξη και 4. Διαφορετικό της Πληροφορικής.

Έτσι, επί συνολικού αριθμού ατόμων που έλαβαν μέρος στην μελέτη, το 37,8% ασχολείται με επάγγελμα διαφορετικό της Πληροφορικής, το 20% με τα επαγγέλματα Υποδομές και Δίκτυα Ηλεκτρονικών Υπολογιστών (2) και Βάσεις Δεδομένων – Ανάπτυξη (3). Ακόμα, επί του συνόλου των ατόμων που ασχολούνται με το επαγγέλματα, Ανάπτυξη και Διαχείριση Ιστοσελίδων (1) και Υποδομές και Δίκτυα Ηλεκτρονικών Υπολογιστών (2), το 50% και το 55,6% αντίστοιχα είναι από 20 έως 30 ετών. Επίσης, για αυτούς που ασχολούνται με επάγγελμα διαφορετικό της Πληροφορικής (4), το μεγαλύτερο ποσοστό 66,7 % των ατόμων, είναι 30 έως 40 ετών. στα άτομα που ασχολούνται με το επάγγελμα 4, το μεγαλύτερο ποσοστό 58,8 % των ατόμων είναι 20 έως 29 ετών. Τέλος, επί συνόλου ατόμων που έλαβαν μέρος στην μελέτη το ποσοστό που ανήκει στην ηλικιακή κλάση από 40 έως 50 ετών, το 50% ασχολείται με Υποδομές και Δίκτυα Ηλεκτρονικών Υπολογιστών και επι της ουσίας είναι 2 άτομα και το υπόλοιπο 50% μοιράζεται στα επαγγέλματα Ανάπτυξη και Διαχείριση Ιστοσελίδων (1), και Βάσεις Δεδομένων – Ανάπτυξη (3).

		ΗΛΙΚΙΑ			Σύνολο
		[20-30]	[30-40]	[40-50]	
<b>Επάγγελμα 1</b>	Συχνότητα	5	4	1	10
	% σε σχέση Επάγγελμα	50,0%	40,0%	10,0%	100,0%
	% σε σχέση ΗΛΙΚΙΑ	22,7%	21,1%	25,0%	22,2%
	% επί Συνόλου	11,1%	8,9%	2,2%	22,2%
<b>2</b>	Συχνότητα	5	2	2	9
	% σε σχέση Επάγγελμα	55,6%	22,2%	22,2%	100,0%
	% σε σχέση ΗΛΙΚΙΑ	22,7%	10,5%	50,0%	20,0%
	% επί Συνόλου	11,1%	4,4%	4,4%	20,0%
<b>3</b>	Συχνότητα	2	6	1	9
	% σε σχέση Επάγγελμα	22,2%	66,7%	11,1%	100,0%
	% σε σχέση ΗΛΙΚΙΑ	9,1%	31,6%	25,0%	20,0%
	% επί Συνόλου	4,4%	13,3%	2,2%	20,0%
<b>4</b>	Συχνότητα	10	7	0	17
	% σε σχέση Επάγγελμα	58,8%	41,2%	,0%	100,0%
	% σε σχέση ΗΛΙΚΙΑ	45,5%	36,8%	,0%	37,8%
	% επί Συνόλου	22,2%	15,6%	,0%	37,8%
<b>ΣΥΝΟΛΟ</b>	Συχνότητα	22	19	4	45
	% σε σχέση Επάγγελμα	48,9%	42,2%	8,9%	100,0%
	% σε σχέση ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%
	% επί Συνόλου	48,9%	42,2%	8,9%	100,0%

Πίνακας 8: Σχέση Επαγγέλματος με την Ηλικία. Επάγγελμα: 1. Ανάπτυξη και Διαχείριση Ιστοσελίδων, 2. Υποδομές και Δίκτυα Ηλεκτρονικών Υπολογιστών, 3. Βάσεις Δεδομένων – Ανάπτυξη, 4. Διαφορετικό της Πληροφορικής.

Στην συνέχεια δίνεται ο ορισμό της συσχέτισης (Correlation - r), η οποία βοηθήσει για την εξαγωγή συμπερασμάτων στην μελέτη. Έτσι, συσχέτιση (Correlation - r), είναι μία παραμετρική στατιστική διαδικασία που ελέγχει κατά πόσο δύο ή περισσότερα χαρακτηριστικά



μεταβάλλονται ταυτοχρόνως. Συμβολίζεται με τον συντελεστή  $r$  (Pearsonian  $r$  / Pearson product-moment correlation). Χρησιμοποιείται, όταν υπάρχει μόνο ένα δείγμα που δεν διαιρείται σε υποσύνολα και παίρνονται μετρήσεις για δύο χαρακτηριστικά του δείγματος. Στην περίπτωση που οι δύο μετρήσεις μεταβάλλονται ταυτοχρόνως, όταν είναι προς την ίδια κατεύθυνση τότε υπάρχει θετική συσχέτιση, ενώ όταν είναι σε αντίθετες κατευθύνσεις υπάρχει αρνητική συσχέτιση. Τέλος, οι τιμές που παίρνει ο συντελεστής είναι από -1 έως 1.

Έπειτα από τις πρώτες ενδεικτικές μετρήσεις με την βοήθεια της μεταβλητής ηλικία, γίνεται μία προσπάθεια να συσχετιστούν οι μεταβλητές (correlation) των ερωτήσεων για να δούμε την συσχέτιση των ερωτήσεων. Ο παρακάτω πίνακας 9, παρουσιάζει την συσχέτιση μεταξύ των ερωτήσεων. Σε κάθε περίπτωση, για να συσχετίζονται δύο ερωτήσεις θα πρέπει ο συντελεστής συσχέτισης να έχει θετικό πρόσημο.

Οπότε, εάν ο συντελεστής συσχέτισης είναι από 0 έως 0,3 η συσχέτιση χαρακτηρίζεται ασθενής, από 0,31 έως 0,5 αρκετά καλή, από 0,51 έως 0,7 είναι μέτρια και από 0,71 έως 1 χαρακτηρίζεται πολύ καλή. Καταλήγοντας, μία θετική μέτρια συσχέτιση ή μία πολύ καλή συσχέτιση εξυπηρετούν τις μετρήσεις. Έτσι, εξάγεται ο παρακάτω πίνακας 9, που παραθέτονται οι συσχετίσεις μεταξύ των 19 ερωτήσεων που έλαβαν μέρος στην μελέτη. Παρατηρείται, ότι οι υψηλότερες θετικές συσχετίσεις είναι η  $Q_5$  με την  $Q_7$  με συντελεστή 0,816, η  $Q_6$  με την  $Q_7$  με συντελεστή 0,710 και η  $Q_{10}$  με την  $Q_{15}$  με συντελεστή 0,891.

ΣΥΣΧΕΤΙΣΜΟΣ ΕΡΩΤΗΣΕΩΝ		ΣΥΝΤΕΛΕΣΤΗΣ ΣΥΣΧΕΤΗΣΗΣ
$Q_1$	$Q_2$	0,536
$Q_2$	$Q_3$	0,584
$Q_3$	$Q_4$	0,525
$Q_5$	$Q_6$   $Q_7$	0,609   <b>0,816</b>
$Q_6$	$Q_7$	<b>0,710</b>
$Q_7$	-	-
$Q_8$	$Q_9$   $Q_{19}$	0,624   0,570
$Q_9$	$Q_{15}$   $Q_{16}$   $Q_{17}$	0,496   0,563   0,532
$Q_{10}$	$Q_{13}$   $Q_{15}$	0,491   <b>0,891</b>
$Q_{11}$	$Q_{13}$	0,645
$Q_{12}$	-	-
$Q_{13}$	$Q_{14}$	0,622
$Q_{14}$	-	-
$Q_{15}$	$Q_{17}$	0,589
$Q_{16}$	$Q_{17}$	0,667
$Q_{17}$	$Q_{18}$	0,528
$Q_{18}$	$Q_{19}$	0,499
$Q_{19}$	-	-

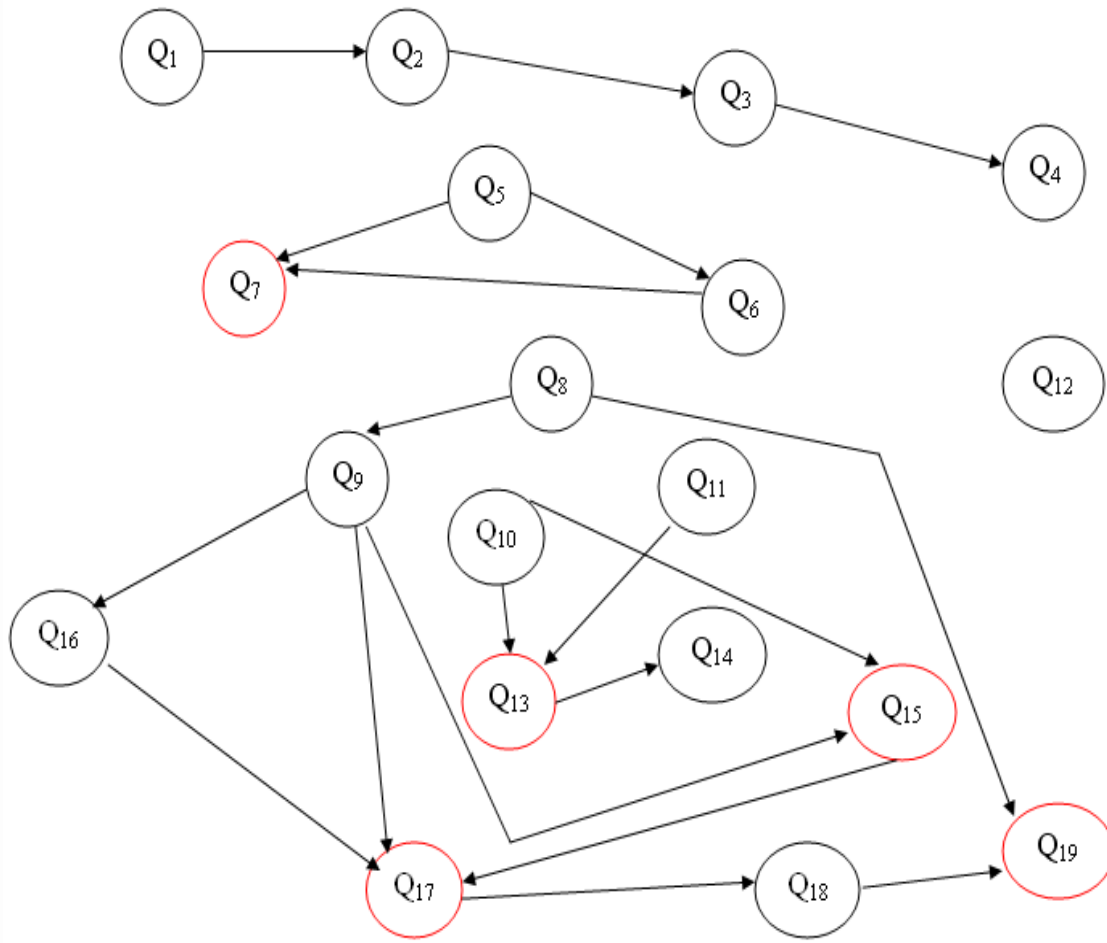
Πίνακας 9: Συσχετισμός των ερωτήσεων

Παρακάτω αναφέρονται πιο αναλυτικά, ο συσχετισμός των ερωτήσεων του πίνακα 9, με τον συντελεστή συσχέτισής τους.

- ✓ Η Q<sub>1</sub> (Πόσο εύκολο είναι να βρείτε την επιθυμητή ιστοσελίδα;) με την Q<sub>2</sub> (Πόσο εύκολο είναι να βρείτε την επιθυμητή σύνδεση στην συγκεκριμένη ιστοσελίδα;) έχει συντελεστή 0,536.
- ✓ Η Q<sub>2</sub> (Πόσο εύκολο είναι να βρείτε την επιθυμητή σύνδεση στην συγκεκριμένη ιστοσελίδα;) με την Q<sub>3</sub> (Πόσο εύκολο είναι να βρείτε τις πληροφορίες που αναζητάτε;) έχει συντελεστή 0,584.
- ✓ Η Q<sub>3</sub> (Πόσο εύκολο είναι να βρείτε τις πληροφορίες που αναζητάτε;) με την Q<sub>4</sub> (Είναι γρήγορη η πρόσβαση στις πληροφορίες της ιστοσελίδας;) έχει συντελεστή 0,525.
- ✓ Η Q<sub>5</sub> (Είναι ικανοποιητικός ο τρόπος σχεδίασης της αναζήτησης πληροφοριών;) με την Q<sub>6</sub> (Υπάρχει δυνατότητα επίσκεψης συναφών ιστοσελίδων;) έχει συντελεστή 0,609 και με την Q<sub>7</sub> (Ελαχιστοποιείται ο χρόνος ανίχνευσης κειμένου;) έχει συντελεστή 0,816.
- ✓ Η Q<sub>6</sub> (Υπάρχει δυνατότητα επίσκεψης συναφών ιστοσελίδων;) με την Q<sub>7</sub> (Ελαχιστοποιείται ο χρόνος ανίχνευσης κειμένου;) έχει συντελεστή 0,710.
- ✓ Η Q<sub>8</sub> (Πληρούνται οι κανόνες προσωπικών δεδομένων;) με την Q<sub>9</sub> (Η εγγραφή στην ιστοσελίδα είναι εύκολη;) έχει συντελεστή 0,624 και με την Q<sub>19</sub> (Υπάρχει άμεση πρόσβαση στο υλικό της ιστοσελίδας;) έχει συντελεστή 0,570.
- ✓ Η Q<sub>9</sub> (Η εγγραφή στην ιστοσελίδα είναι εύκολη;) με την Q<sub>15</sub> (Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;) έχει συντελεστή 0,496 και με την Q<sub>16</sub> (Σκοπεύετε να επισκεφτείτε ξανά την ιστοσελίδα;) έχει συντελεστή 0,563 και με την Q<sub>17</sub> (Θα την προτείνετε σε γνωστούς και φίλους;) έχει συντελεστή 0,532.
- ✓ Η Q<sub>10</sub> (Ανίχνευση του κειμένου γίνεται με μικρότερο κόστος δηλαδή χρήση ποντικιού;) με την Q<sub>13</sub> (Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;) έχει συντελεστή 0,491 και με την Q<sub>15</sub> (Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;) έχει συντελεστή 0,891.
- ✓ Η Q<sub>11</sub> (Υπάρχουν εύκολοι τρόποι αναζήτησης;) με την Q<sub>13</sub> (Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;) έχει συντελεστή 0,645.
- ✓ Η Q<sub>13</sub> (Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;) με την Q<sub>14</sub> (Οι απαντήσεις που δύνονται περιέχουν συνδέσεις που εξυπηρετούν τον χρήστη;) έχει συντελεστή 0,622.
- ✓ Η Q<sub>15</sub> (Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;) με την Q<sub>17</sub> (Θα την προτείνετε σε γνωστούς και φίλους;) έχει συντελεστή 0,589.
- ✓ Η Q<sub>16</sub> (Σκοπεύετε να επισκεφτείτε ξανά την ιστοσελίδα;) με την Q<sub>17</sub> (Θα την προτείνετε σε γνωστούς και φίλους;) έχει συντελεστή 0,667.
- ✓ Η Q<sub>17</sub> (Θα την προτείνετε σε γνωστούς και φίλους;) με την Q<sub>18</sub> (Θα μιλούσατε θετικά για την ιστοσελίδα;) έχει συντελεστή 0,528.
- ✓ Η Q<sub>18</sub> (Θα μιλούσατε θετικά για την ιστοσελίδα;) με την Q<sub>19</sub> (Υπάρχει άμεση πρόσβαση στο υλικό της ιστοσελίδας;) έχει συντελεστή 0,499.

Με βάση τον παραπάνω πίνακα 9, που παραθέτει τις υψηλές θετικές ισχυρές συσχετίσεις, δημιουργήθηκε το αντίστοιχο διάγραμμα ροής των συσχετιζόμενων ερωτήσεων, με σκοπό την διερεύνηση των σημαντικότερων ερωτήσεων, στις οποίες αποτυπώνονται ποσοτικά χαρακτηριστικά της ποιότητας της αξιολόγησης των ερωτήσεων.

Στην παρακάτω εικόνα 24, παρατίθεται, το διάγραμμα ροής των ερωτήσεων από το οποίο διαπιστώνεται, ότι οι ερωτήσεις Q<sub>7</sub>, Q<sub>13</sub>, Q<sub>15</sub>, Q<sub>17</sub>, και Q<sub>19</sub> είναι οι σημαντικότερες λόγω του γεγονότος ότι είναι αποδέκτες των περισσότερων ροών (βέλη).



Εικόνα 24: Διάγραμμα Ροής των ερωτήσεων.

Οι σημαντικές ερωτήσεις: Q7, Q13, Q15, Q17, Q19 και είναι σημειωμένες σε κόκκινο κύκλο.

Στο διάγραμμα ροής παρατηρείται, ότι οι ερωτήσεις Q7, Q13, Q15, και Q19 έχουν 2 εισροές ενώ η Q17, έχει 3 εισροές. Όλες οι υπόλοιπες ερωτήσεις έχουν από μία ή και καμία εισροή. Για αυτό το λόγο, η ερώτηση Q17, είναι η πιο σημαντική.

Στην συνέχεια, για κάθε μία από τις σημαντικές ερωτήσεις Q7, Q13, Q15, Q17, Q19 γίνεται συσχετίσή τους με το φύλο και την μεταβλητή ηλικία. Εδώ, πρέπει να σημειωθεί, ότι σε κάθε μία από τις ερωτήσεις, έχουν ληφθεί υπόψη και οι βαθμολογίες που έδωσε ο πληθυσμός για την κάθε μία από τις ερωτήσεις στο ερωτηματολόγιο, όπου η κλίμακα βαθμολογίας έχει ως εξής:

- 1: Καθόλου Ικανοποιημένος,
- 2: Ελάχιστα Ικανοποιημένος,
- 3: Μέτρια Ικανοποιημένος
- 4: Πολύ Ικανοποιημένος.

		ΦΥΛΟ		ΣΥΝΟΛΟ	
		Αντρας	Γυναίκα		
Q <sub>7</sub>	1	Συχνότητα	1	2	3
		% σε σχέση με Q <sub>7</sub>	33,3%	66,7%	100,0%
		% σε σχέση με Φύλο	3,7%	11,1%	6,7%
		% επί Συνόλου	2,2%	4,4%	6,7%
	2	Συχνότητα	7	4	11
		% σε σχέση με Q <sub>7</sub>	63,6%	36,4%	100,0%
		% σε σχέση με Φύλο	25,9%	22,2%	24,4%
		% επί Συνόλου	15,6%	8,9%	24,4%
	3	Συχνότητα	5	5	10
		% σε σχέση με Q <sub>7</sub>	50,0%	50,0%	100,0%
		% σε σχέση με Φύλο	18,5%	27,8%	22,2%
		% επί Συνόλου	11,1%	11,1%	22,2%
	4	Συχνότητα	14	7	21
		% σε σχέση με Q <sub>7</sub>	66,7%	33,3%	100,0%
		% σε σχέση με Φύλο	51,9%	38,9%	46,7%
		% επί Συνόλου	31,1%	15,6%	46,7%
<b>ΣΥΝΟΛΟ</b>		Συχνότητα	27	18	45
		% σε σχέση με Q <sub>7</sub>	60,0%	40,0%	100,0%
		% σε σχέση με Φύλο	100,0%	100,0%	100,0%
		% επί Συνόλου	60,0%	40,0%	100,0%

Πίνακας 10: Συσχέτιση ερώτησης Q<sub>7</sub> με το Φύλο

Στον παραπάνω πίνακα 10, το 46,7% του πληθυσμού βαθμολόγησε στην ερώτηση Q<sub>7</sub> (Ελαχιστοποιείται ο χρόνος ανίχνευσης κειμένου;) με την μεγαλύτερη τιμή της κλίμακας, δηλαδή 4 (πολύ ικανοποιημένο), εκ των οποίων το 31,1% είναι άντρες και το 15,6% είναι γυναίκες. Το 22,2% του πληθυσμού βαθμολόγησε με 3 (μέτρια ικανοποιημένο), ποσοστό που είναι μοιρασμένο ακριβώς στα δύο φύλα με 11,1%. Επίσης, το 24,4% βαθμολόγησε με 2 (ελάχιστα ικανοποιημένο) και το 6,7% βαθμολόγησε με 1 (καθόλου ικανοποιημένο) γεγονός που δείχνει και γιατί η ερώτηση Q<sub>7</sub> ανήκει στις σημαντικές ερωτήσεις.

		ΗΛΙΚΙΑ			ΣΥΝΟΛΟ	
		[20-30]	[30-40]	[40-50]		
Q <sub>7</sub>	1	Συχνότητα	1	2	0	3
		% σε σχέση με Q <sub>7</sub>	33,3%	66,7%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	4,5%	10,5%	0,0%	6,7%
		% επί Συνόλου	2,2%	4,4%	0,0%	6,7%
	2	Συχνότητα	3	7	1	11
		% σε σχέση με Q <sub>7</sub>	27,3%	63,6%	9,1%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	13,6%	36,8%	25,0%	24,4%
		% επί Συνόλου	6,7%	15,6%	2,2%	24,4%
	3	Συχνότητα	7	3	0	10
		% σε σχέση με Q <sub>7</sub>	70,0%	30,0%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	31,8%	15,8%	0,0%	22,2%
		% επί Συνόλου	15,6%	6,7%	0,0%	22,2%
	4	Συχνότητα	11	7	3	21
		% σε σχέση με Q <sub>7</sub>	52,4%	33,3%	14,3%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	50,0%	36,8%	75,0%	46,7%
		% επί Συνόλου	24,4%	15,6%	6,7%	46,7%

ΣΥΝΟΛΟ	Συχνότητα	22	19	4	45
	% σε σχέση με Q <sub>7</sub>	48,9%	42,2%	8,9%	100,0%
	% σε σχέση με ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%
	% επί Συνόλου	48,9%	42,2%	8,9%	100,0%

Πίνακας 11: Συσχέτιση ερώτησης Q<sub>7</sub> με την Ηλικία.

Στον παραπάνω πίνακα 11, το 46,7% του πληθυσμού βαθμολόγησε στην ερώτηση Q<sub>7</sub> (Ελαχιστοποιείται ο χρόνος ανίχνευσης κειμένου;) με την μεγαλύτερη τιμή της κλίμακας, δηλαδή 4 (πολύ ικανοποιημένο), εκ του οποίου το 24,4% ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 15,6% στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών) και το 6,7% στην τρίτη ηλικιακή κλάση (40 έως 50 ετών). Το 22,2% βαθμολόγησε με 3 (μέτρια ικανοποιημένο), εκ των οποίων το 15,6% ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), ενώ επί συνόλου το 24,4% βαθμολόγησε με 2 (ελάχιστα ικανοποιημένο) όπου, το 15,6% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών). Κάτι, που επίσης δείχνει την σημαντικότητα της ερώτησης 7 είναι ότι μόνο το 6,7% βαθμολόγησε με 1 (καθόλου ικανοποιημένο) την ερώτηση.

		ΦΥΛΟ		ΣΥΝΟΛΟ	
		Άντρας	Γυναίκα		
Q <sub>13</sub>	1	Συχνότητα	0	2	2
		% σε σχέση με Q <sub>13</sub>	0,0%	100,0%	100,0%
		% σε σχέση με Φύλο	0,0%	11,1%	4,4%
		% επί Συνόλου	0,0%	4,4%	4,4%
	2	Συχνότητα	7	6	13
		% σε σχέση με Q <sub>13</sub>	53,8%	46,2%	100,0%
		% σε σχέση με Φύλο	25,9%	33,3%	28,9%
		% επί Συνόλου	15,6%	13,3%	28,9%
	3	Συχνότητα	15	4	19
		% σε σχέση με Q <sub>13</sub>	78,9%	21,1%	100,0%
		% σε σχέση με Φύλο	55,6%	22,2%	42,2%
		% επί Συνόλου	33,3%	8,9%	42,2%
	4	Συχνότητα	5	6	11
		% σε σχέση με Q <sub>13</sub>	45,5%	54,5%	100,0%
		% σε σχέση με Φύλο	18,5%	33,3%	24,4%
		% επί Συνόλου	11,1%	13,3%	24,4%
ΣΥΝΟΛΟ	Συχνότητα	27	27	18	
	% σε σχέση με Q <sub>13</sub>	60,0%	60,0%	40,0%	
	% σε σχέση με Φύλο	100,0%	100,0%	100,0%	
	% επί Συνόλου	60,0%	40,0%	100,0%	

Πίνακας 12: Συσχέτιση ερώτησης Q<sub>13</sub> με το Φύλο

Ο παραπάνω πίνακας 12, απεικονίζει την συσχέτιση της Q<sub>13</sub> (Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;) με το φύλο, όπου το 42,2% του πληθυσμού βαθμολόγησε στην Q<sub>13</sub> με 3 (μέτρια ικανοποιημένο), εκ των οποίων το 33,3% είναι άντρες και το 8,9% είναι γυναίκες. Το 28,9% βαθμολόγησε με 2 (ελάχιστα ικανοποιημένο) και το ποσοστό αυτό είναι μοιρασμένο στα δύο φύλα. Επίσης, το 24,4% βαθμολόγησε με 4 (πολύ ικανοποιημένο) εκ των οποίων το 13,3% είναι γυναίκες και το 11,1% είναι άντρες. Από τα μεγάλα ποσοστά που

παρατηρείται στις βαθμολογίες 3 (μέτρια ικανοποιημένο) και 4 (πολύ ικανοποιημένο) αποδεικνύεται και η σημαντικότητα της Q<sub>13</sub>.

			ΗΛΙΚΙΑ			ΣΥΝΟΛΟ
			[20-30]	[30-40]	[40-50]	
Q <sub>13</sub>	1	Συχνότητα	1	1	0	2
		% σε σχέση με Q <sub>13</sub>	50,0%	50,0%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	4,5%	5,3%	0,0%	4,4%
		% επί Συνόλου	2,2%	2,2%	0,0%	4,4%
	2	Συχνότητα	5	7	1	13
		% σε σχέση με Q <sub>13</sub>	38,5%	53,8%	7,7%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	22,7%	36,8%	25,0%	28,9%
		% επί Συνόλου	11,1%	15,6%	2,2%	28,9%
	3	Συχνότητα	10	8	1	19
		% σε σχέση με Q <sub>13</sub>	52,6%	42,1%	5,3%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	45,5%	42,1%	25,0%	42,2%
		% επί Συνόλου	22,2%	17,8%	2,2%	42,2%
	4	Συχνότητα	6	3	2	11
		% σε σχέση με Q <sub>13</sub>	54,5%	27,3%	18,2%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	27,3%	15,8%	50,0%	24,4%
		% επί Συνόλου	13,3%	6,7%	4,4%	24,4%
ΣΥΝΟΛΟ		Συχνότητα	22	19	4	45
		% σε σχέση με Q <sub>13</sub>	48,9%	42,2%	8,9%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%
		% επί Συνόλου	48,9%	42,2%	8,9%	100,0%

Πίνακας 13: Συσχέτιση ερώτησης Q<sub>13</sub> με την Ηλικία

Στον παραπάνω πίνακα 13, απεικονίζεται η συσχέτιση της Q<sub>13</sub> (Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;) με την ηλικία, όπου το 42,2% του πληθυσμού βαθμολόγησε στην ερώτηση Q<sub>13</sub> με 3 (μέτρια ικανοποιημένο), εκ του οποίου το 22,2% ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 17,8% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών) και ένα πολύ μικρό ποσοστό της τάξης του 2,2% ανήκει στην τρίτη ηλικιακή κλάση (40 έως 50 ετών). Επίσης, το 28,9% βαθμολόγησε στην ερώτηση Q<sub>13</sub> με 2 (ελάχιστα ικανοποιημένο), όπου το μεγαλύτερο μέρος αυτού του ποσοστού 15,6% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών). Και σε αυτή την ερώτηση η βαθμολογία με 1 (καθόλου ικανοποιημένο) έχει πολύ μικρά ποσοστά της τάξης του 2,2% σε κάθε ηλικιακή κλάση.

			ΦΥΛΟ		ΣΥΝΟΛΟ
			Αντρας	Γυναίκα	
Q <sub>15</sub>	1	Συχνότητα	1	1	2
		% σε σχέση με Q <sub>15</sub>	50,0%	50,0%	100,0%
		% σε σχέση με Φύλο	3,7%	5,6%	4,4%
		% επί Συνόλου	2,2%	2,2%	4,4%
	2	Συχνότητα	3	3	6
		% σε σχέση με Q <sub>15</sub>	50,0%	50,0%	100,0%
		% σε σχέση με Φύλο	11,1%	16,7%	13,3%
		% επί Συνόλου	6,70%	6,7%	13,3%
	3	Συχνότητα	16	8	24
		% σε σχέση με Q <sub>15</sub>	66,7%	33,3%	100,0%

		% σε σχέση με Φύλο	59,3%	44,4%	53,3%
		% επί Συνόλου	35,6%	17,8%	53,3%
	4	Συχνότητα	7	6	13
		% σε σχέση με Q <sub>15</sub>	53,8%	46,2%	100,0%
		% σε σχέση με Φύλο	25,9%	33,3%	28,9%
		% επί Συνόλου	15,6%	13,3%	28,9%
ΣΥΝΟΛΟ	Συχνότητα	27	27	18	
	% σε σχέση με Q <sub>15</sub>	60,0%	60,0%	40,0%	
	% σε σχέση με Φύλο	100,0%	100,0%	100,0%	
	% επί Συνόλου	60,0%	60,0%	40,0%	

Πίνακας 14: Συσχέτιση ερώτησης Q<sub>15</sub> με το Φύλο

Στον παραπάνω πίνακα 14, απεικονίζεται η συσχέτιση της ερώτησης Q<sub>15</sub> (Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;) με το φύλο, όπου το 53% του πληθυσμού βαθμολόγησε στην ερώτηση Q<sub>15</sub> με 3 (μέτρια ικανοποιημένο), εκ των οποίων το 35,6% είναι άντρες και το 17,8% είναι γυναίκες. Ακόμα, το 28,9% βαθμολόγησε με 4 (πολύ ικανοποιημένο) όπου το 15,6% είναι άντρες και το 13,3% είναι γυναίκες και από τις βαθμολογίες αυτές, παρατηρείται, ότι είναι πολύ ικανοποιημένοι με το αντικείμενο της ιστοσελίδας. Τέλος, πολύ μικρά είναι τα ποσοστά στις βαθμολογίες 1 (καθόλου ικανοποιημένο) με 4,4% και 2 (ελάχιστα ικανοποιημένο) με 13,3%.

			ΗΛΙΚΙΑ			ΣΥΝΟΛΟ
			[20-30]	[30-40]	[40-50]	
Q <sub>15</sub>	1	Συχνότητα	2	0	0	2
		% σε σχέση με Q <sub>15</sub>	100,0%	0,0%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	9,1%	0,0%	0,0%	4,4%
		% επί Συνόλου	4,4%	0,0%	0,0%	4,4%
	2	Συχνότητα	1	5	0	6
		% σε σχέση με Q <sub>15</sub>	16,7%	83,3%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	4,5%	26,3%	0,0%	13,3%
		% επί Συνόλου	2,2%	11,1%	0,0%	13,3%
	3	Συχνότητα	13	10	1	24
		% σε σχέση με Q <sub>15</sub>	54,2%	41,7%	4,2%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	59,1%	52,6%	25,0%	53,3%
		% επί Συνόλου	28,9%	22,2%	2,2%	53,3%
	4	Συχνότητα	6	4	3	13
		% σε σχέση με Q <sub>15</sub>	46,2%	30,8%	23,1%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	27,3%	21,1%	75,0%	28,9%
		% επί Συνόλου	13,3%	8,9%	6,7%	28,9%
ΣΥΝΟΛΟ	Συχνότητα	22	19	4	45	
	% σε σχέση με Q <sub>15</sub>	48,9%	42,2%	8,9%	100,0%	
	% σε σχέση με ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%	
	% επί Συνόλου	48,9%	42,2%	8,9%	100,0%	

Πίνακας 15: Συσχέτιση ερώτησης Q<sub>15</sub> με την Ηλικία

Στον παραπάνω πίνακα 15, απεικονίζεται η συσχέτιση της ερώτησης Q<sub>15</sub> (Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;) με την ηλικία, όπου το 53,3% του πληθυσμού βαθμολόγησε στην Q<sub>15</sub> με 3 (μέτρια ικανοποιημένο), εκ του οποίου το 28,9% ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 22,2% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών) και

ένα πολύ μικρό ποσοστό (2,2%) στην τρίτη ηλικιακή κλάση (40 έως 50 ετών). Επίσης, το 28,9% του πληθυσμού βαθμολόγησε στην Q<sub>15</sub> με 4 (πολύ ικανοποιημένο), εκ του οποίου το 13,3% ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 8,9% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών), και το 6,7% ανήκει στην τρίτη ηλικιακή κλάση (40 έως 50 ετών). Και εδώ, όπως και στην Q<sub>13</sub> είναι μικρά τα ποσοστά στις βαθμολογίες 2 (ελάχιστα ικανοποιημένο) και ιδιαίτερα με 1 (καθόλου ικανοποιημένο) από 4,4%, γεγονός που δείχνει ότι το ενδιαφέρον της ιστοσελίδας είναι μεγάλο και στις τρεις ηλικιακές κλάσεις.

			ΦΥΛΟ		ΣΥΝΟΛΟ
			Άντρας	Γυναίκα	
Q <sub>17</sub>	1	Συχνότητα	2	1	3
		% σε σχέση με Q <sub>17</sub>	66,7%	33,3%	100,0%
		% σε σχέση με Φύλο	7,4%	5,6%	6,7%
		% επί Συνόλου	4,4%	2,2%	6,7%
	2	Συχνότητα	10	9	19
		% σε σχέση με Q <sub>17</sub>	52,6%	47,4%	100,0%
		% σε σχέση με Φύλο	37,0%	50,0%	42,2%
		% επί Συνόλου	22,2%	20,0%	42,2%
	3	Συχνότητα	10	3	13
		% σε σχέση με Q <sub>17</sub>	76,9%	23,1%	100,0%
		% σε σχέση με Φύλο	37,0%	16,7%	28,9%
		% επί Συνόλου	22,2%	6,7%	28,9%
	4	Συχνότητα	5	4	9
		% σε σχέση με Q <sub>17</sub>	55,6%	44,4%	100,0%
		% σε σχέση με Φύλο	18,5%	22,2%	20,0%
		% επί Συνόλου	11,1%	8,9%	20,0%
ΣΥΝΟΛΟ		Συχνότητα	27	18	45
		% σε σχέση με Q <sub>17</sub>	60,0%	40,0%	100,0%
		% σε σχέση με Φύλο	100,0%	100,0%	100,0%
		% επί Συνόλου	60,0%	40,0%	100,0%

Πίνακας 16: Συσχέτιση ερώτησης Q<sub>17</sub> με το Φύλο

Στον παραπάνω πίνακα 16, απεικονίζεται η συσχέτιση της ερώτησης Q<sub>17</sub> (Θα την προτείνετε σε γνωστούς και φίλους;) με το φύλο, όπου το 42,2% του πληθυσμού βαθμολόγησε στην Q<sub>17</sub> με 2 (ελάχιστα ικανοποιημένο). Ένα μοιρασμένο ποσοστό, εκ των οποίων το 22,2% είναι άντρες και το 20,0% είναι γυναίκες. Το 28,9% βαθμολόγησε με 3 (μέτρια ικανοποιημένο) και το 20% με 4 (πολύ ικανοποιημένο), όπου τα μεγαλύτερα ποσοστά ανήκουν στους άντρες. Στην ερώτηση αυτή, παρατηρείται ότι οι βαθμολογίες είναι μικρές καθώς επίσης και η σημαντικότητα της ερώτησης αυτής, γιατί παρέχει μία γενική πληροφορία για την συνολική εικόνα της ιστοσελίδας.

			ΗΛΙΚΙΑ			ΣΥΝΟΛΟ
			[20-30]	[30-40]	[40-50]	
Q <sub>17</sub>	1	Συχνότητα	3	0	0	3
		% σε σχέση με Q <sub>17</sub>	100,0%	0,0%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	13,6%	0,0%	0,0%	6,7%
		% επί Συνόλου	6,7%	0,0%	0,0%	6,7%
	2	Συχνότητα	10	8	1	19
		% σε σχέση με Q <sub>17</sub>	52,6%	42,1%	5,3%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	45,5%	42,1%	25,0%	42,2%



		% επί Συνόλου	22,2%	17,8%	2,2%	42,2%
	3	Συχνότητα	5	7	1	13
		% σε σχέση με Q <sub>17</sub>	38,5%	53,8%	7,7%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	22,7%	36,8%	25,0%	28,9%
		% επί Συνόλου	11,1%	15,6%	2,2%	28,9%
	4	Συχνότητα	4	3	2	9
		% σε σχέση με Q <sub>17</sub>	44,4%	33,3%	22,2%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	18,2%	15,8%	50,0%	20,0%
		% επί Συνόλου	8,9%	6,7%	4,4%	20,0%
ΣΥΝΟΛΟ	Συχνότητα	22	19	4	45	
	% σε σχέση με Q <sub>17</sub>	48,9%	42,2%	8,9%	100,0%	
	% σε σχέση με ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%	
	% επί Συνόλου	48,9%	42,2%	8,9%	100,0%	

Πίνακας 17: Συσχέτιση ερώτησης Q<sub>17</sub> με την Ηλικία

Στον παραπάνω πίνακα 17, απεικονίζεται η συσχέτιση της ερώτησης Q<sub>17</sub> (Θα την προτείνετε σε γνωστούς και φίλους;) με την ηλικία, όπου το 42,2% του πληθυσμού βαθμολόγησε στην ερώτηση με 2 (ελάχιστα ικανοποιημένο), εκ του οποίου το 22,2% ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 17,8% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών) και το μικρό ποσοστό 2,2% ανήκει στην τρίτη ηλικιακή κλάση (40 έως 50 ετών). Επίσης, το 28,9% βαθμολόγησε με 3 (μέτρια ικανοποιημένο), όπου το 11,1% και ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 15,6% ανήκει στην δεύτερη ηλικιακή κλάση (30 έως 40 ετών) και το 2,2% στην τρίτη. Τέλος, ένα 20% βαθμολόγησε με 4 (πολύ ικανοποιημένο) και τα επιμέρους ποσοστά είναι σχετικά μοιρασμένα στις ηλικιακές κλάσεις.

			ΦΥΛΟ		ΣΥΝΟΛΟ
			Αντρας	Γυναίκα	
Q <sub>19</sub>	1	Συχνότητα	3	1	4
		% σε σχέση με Q <sub>19</sub>	75,0%	25,0%	100,0%
		% σε σχέση με Φύλο	11,1%	5,6%	8,9%
		% επί Συνόλου	6,7%	2,2%	8,9%
	2	Συχνότητα	11	8	19
		% σε σχέση με Q <sub>19</sub>	57,9%	42,1%	100,0%
		% σε σχέση με Φύλο	40,7%	44,4%	42,2%
		% επί Συνόλου	24,4%	17,8%	42,2%
	3	Συχνότητα	6	9	15
		% σε σχέση με Q <sub>19</sub>	40,0%	60,0%	100,0%
		% σε σχέση με Φύλο	22,2%	50,0%	33,3%
		% επί Συνόλου	13,3%	20,0%	33,3%
	4	Συχνότητα	7	0	7
		% σε σχέση με Q <sub>19</sub>	100,0%	0,0%	100,0%
		% σε σχέση με Φύλο	25,9%	0,0%	15,6%
		% επί Συνόλου	15,6%	0,0%	15,6%
ΣΥΝΟΛΟ	Συχνότητα	27	18	45	
	% σε σχέση με Q <sub>19</sub>	60,0%	40,0%	100,0%	
	% σε σχέση με Φύλο	100,0%	100,0%	100,0%	
	% επί Συνόλου	60,0%	40,0%	100,0%	

Πίνακας 18: Συσχέτιση ερώτησης Q<sub>19</sub> με το Φύλο

Στον παραπάνω πίνακα 18, απεικονίζεται η συσχέτιση της ερώτησης Q<sub>19</sub> (Υπάρχει άμεση πρόσβαση στο υλικό της ιστοσελίδας;) με το φύλο, όπου το 42,2% του πληθυσμού βαθμολόγησε στην ερώτηση Q<sub>19</sub> με 2 (ελάχιστα ικανοποιημένο), εκ των οποίων το 24,4% είναι άντρες και το 17,8% είναι γυναίκες. Επίσης, το 33,3% βαθμολόγησε με 3 (μέτρια ικανοποιημένο) εκ των οποίων το 20% είναι γυναίκες και το 13,3% είναι άντρες. Ακόμα, στην ερώτηση αυτή το 15,6% βαθμολόγησε με 4 (πολύ ικανοποιημένο) και όλο το ποσοστό ήταν άντρες. Τέλος, το 8,9% βαθμολόγησε με 1 (καθόλου ικανοποιημένο), νούμερο που δείχνει ότι υπάρχει μέρος πληθυσμού που δεν βρήκε εύκολα υλικό της ιστοσελίδας και αυτό ίσως οφείλεται στο μενού της ιστοσελίδας.

		ΗΛΙΚΙΑ			ΣΥΝΟΛΟ	
		[20-30]	[30-40]	[40-50]		
Q <sub>19</sub>	1	Συχνότητα	2	2	0	4
		% σε σχέση με Q <sub>19</sub>	50,0%	50,0%	0,0%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	9,1%	10,5%	0,0%	8,9%
		% επί Συνόλου	4,4%	4,4%	0,0%	8,9%
	2	Συχνότητα	9	9	1	19
		% σε σχέση με Q <sub>19</sub>	47,4%	47,4%	5,3%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	40,9%	47,4%	25,0%	42,2%
		% επί Συνόλου	20,0%	20,0%	2,2%	42,2%
	3	Συχνότητα	8	6	1	15
		% σε σχέση με Q <sub>19</sub>	53,3%	40,0%	6,7%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	36,4%	31,6%	25,0%	33,3%
		% επί Συνόλου	17,8%	13,3%	2,2%	33,3%
	4	Συχνότητα	3	2	2	7
		% σε σχέση με Q <sub>19</sub>	42,9%	28,6%	28,6%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	13,6%	10,5%	50,0%	15,6%
		% επί Συνόλου	6,7%	4,4%	4,4%	15,6%
ΣΥΝΟΛΟ		Συχνότητα	22	19	4	45
		% σε σχέση με Q <sub>19</sub>	48,9%	42,2%	8,9%	100,0%
		% σε σχέση με ΗΛΙΚΙΑ	100,0%	100,0%	100,0%	100,0%
		% επί Συνόλου	48,9%	42,2%	8,9%	100,0%

Πίνακας 19: Συσχέτιση ερώτησης Q<sub>19</sub> με την Ηλικία

Στον παραπάνω πίνακα 19, απεικονίζεται η συσχέτιση της Q<sub>19</sub> (Υπάρχει άμεση πρόσβαση στο υλικό της ιστοσελίδας;) με την ηλικία, όπου το 42,2% του πληθυσμού βαθμολόγησε στην ερώτηση με 2 (ελάχιστα ικανοποιημένο), εκ του οποίου το 20,0% ανήκει στην πρώτη (20 έως 30 ετών) και στην δεύτερη (30 έως 40 ετών) ηλικιακή κλάση. Επίσης, το 33,3% βαθμολόγησε με 3 (μέτρια ικανοποιημένο), με το 17,7% του πληθυσμού να ανήκει στην πρώτη ηλικιακή κλάση (20 έως 30 ετών), το 13,3% στην δεύτερη (30 έως 40 ετών) και το 2,2% στην Τρίτη (40 έως 50 ετών). Τέλος, μόνο το 15,6% βαθμολόγησε με 4 (πολύ ικανοποιημένο), γεγονός που φανερώνει ότι ο κόσμος, δεν έμεινε πλήρως ικανοποιημένος από την πρόσβαση στον ιστοχώρο.

Από τους παραπάνω πίνακες συμπεραίνεται, ότι τα μεγαλύτερα ποσοστά όσον αφορά το φύλο ανήκουν στον αντρικό πληθυσμό και όσον αφορά την ηλικία τα μεγαλύτερα ποσοστά συναντιούνται στην πρώτη ηλικιακή κλάση, από 20 έως 30 ετών. Ακόμα, υπάρχει μία μέση βαθμολογία, για την συγκεκριμένη ιστοσελίδα, αφού τα μεγαλύτερα ποσοστά έχουν βαθμολογήσει τις σημαντικές ερωτήσεις με 2 (ελάχιστα ικανοποιημένο) ή με 3 (μέτρια ικανοποιημένο).

Στην συνέχεια, παρουσιάζεται ο πίνακας 20, για τις σημαντικές ερωτήσεις επί συνόλου πληθυσμού, όπου εξάγονται τα εξής περιγραφικά στατιστικά σε : Μέση βαθμολογία πληθυσμού (Mean), Διάμεσος (Median), επικρατούσα τιμή (Mode) και Τυπική Απόκλιση (Std. Deviation).

Σε γενικές γραμμές, η μέση τιμή παίρνει τιμές  $3,09 \pm 0,996$  με επικρατούσα τιμή την 4 στην ερώτηση Q<sub>7</sub>. Η διάμεσος είναι σχεδόν ίδια σε όλες τις ερωτήσεις. Οι ερωτήσεις Q<sub>7</sub> και Q<sub>15</sub> βάση μέσης βαθμολογίας και επικρατούσας τιμής (Mode) παρατηρείται, ότι ικανοποίησαν περισσότερο πληθυσμό.

	Q <sub>7</sub>	Q <sub>13</sub>	Q <sub>15</sub>	Q <sub>17</sub>	Q <sub>19</sub>
<b>Πλήθος (N)</b>	45	45	45	45	45
<b>Μέση Βαθμολογία Πληθυσμού (Mean)</b>	3,09	2,87	3,07	2,58	2,56
<b>Σφάλμα Μέσου (Std. Error of Mean)</b>	0,148	0,126	0,116	0,144	0,129
<b>Διάμεσος (Median)</b>	3,00	3,00	3,00	2,00	2,00
<b>Επικρατούσα Τιμή (Mode)</b>	4	3	3	2	2
<b>Τυπική Απόκλιση (Std. Deviation)</b>	0,996	0,842	0,780	0,965	0,867
<b>Ελάχιστο (Minimum)</b>	1	1	1	0	1

Πίνακας 20: Περιγραφικά στατιστικά στοιχεία για τις σημαντικές ερωτήσεις:  
Q<sub>7</sub>, Q<sub>13</sub>, Q<sub>15</sub>, Q<sub>17</sub>, Q<sub>19</sub>.

Στην παραπάνω εικόνα 24, μέσα από το Διάγραμμα Ροής, παρατηρήθηκε ότι η ερώτηση 17 (Θα την προτείνετε σε γνωστούς και φίλους;) είναι η σημαντικότερη, αφού σε αυτή καταλήγουν οι περισσότερες ερωτήσεις. Με βάση αυτό το Διάγραμμα Ροής, ελέγχεται και συσχετίζεται η ερώτηση 17 με τις υπόλοιπες σημαντικές ερωτήσεις.

			Q <sub>17</sub>				ΣΥΝΟΛΟ	
			0	1	2	3	4	
Q <sub>7</sub>	1	Συχνότητα	0	1	2	0	0	3
		% σε σχέση με Q <sub>7</sub>	0,0%	33,3%	66,7%	0,0%	0,0%	100,0%
		% σε σχέση με Q <sub>17</sub>	0,0%	33,3%	10,5%	0,0%	0,0%	6,7%
		% επί Συνόλου	0,0%	2,2%	4,4%	0,0%	0,0%	6,7%
	2	Συχνότητα	1	0	4	3	3	11
		% σε σχέση με Q <sub>7</sub>	9,1%	0,0%	36,4%	27,3%	27,3%	100,0%
		% σε σχέση με Q <sub>17</sub>	100,0%	0,0%	21,1%	23,1%	33,3%	24,4%
		% επί Συνόλου	2,2%	0,0%	8,9%	6,7%	6,7%	24,4%
	3	Συχνότητα	0	2	4	4	0	10
		% σε σχέση με Q <sub>7</sub>	0,0%	20,0%	40,0%	40,0%	0,0%	100,0%
		% σε σχέση με Q <sub>17</sub>	0,0%	66,7%	21,1%	30,8%	0,0%	22,2%
		% επί Συνόλου	0,0%	4,4%	8,9%	8,9%	0,0%	22,2%
	4	Συχνότητα	0	0	9	6	6	21
		% σε σχέση με Q <sub>7</sub>	0,0%	0,0%	42,9%	28,6%	28,6%	100,0%
		% σε σχέση με Q <sub>17</sub>	0,0%	0,0%	47,4%	46,2%	66,7%	46,7%
		% επί Συνόλου	0,0%	0,0%	20,0%	13,3%	13,3%	46,7%
ΣΥΝΟΛΟ	Συχνότητα	1	3	19	13	9	45	
	% σε σχέση με Q <sub>7</sub>	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%	
	% σε σχέση με Q <sub>17</sub>	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	
	% επί Συνόλου	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%	

Πίνακας 21: Συσχέτιση της Q<sub>17</sub> με την Q<sub>7</sub>

Στον παραπάνω πίνακα 21, συγκρίνεται η  $Q_7$  (Ελαχιστοποιείται ο χρόνος ανίχνευσης κειμένου;) με την  $Q_{17}$  (Θα την προτείνετε σε γνωστούς και φίλους;) και παρατηρείται ότι το μεγαλύτερο ποσοστό (66,7%) έχει βαθμολογήσει με 4 (πολύ ικανοποιημένο) και τις δύο ερωτήσεις που σημαίνει ότι ο πληθυσμός είναι πολύ ικανοποιημένο και με τις δύο ερωτήσεις.

			$Q_{17}$					ΣΥΝΟΛΟ
			0	1	2	3	4	
$Q_{13}$	1	Συχνότητα	1	1	0	0	0	2
		% σε σχέση με $Q_{13}$	50,0%	50,0%	0,0%	0,0%	0,0%	100,0%
		% σε σχέση με $Q_{17}$	100,0%	33,3%	0,0%	0,0%	0,0%	4,4%
		% επί Συνόλου	2,2%	2,2%	0,0%	0,0%	0,0%	4,4%
	2	Συχνότητα	0	1	6	3	3	13
		% σε σχέση με $Q_{13}$	0,0%	7,7%	46,2%	23,1%	23,1%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	33,3%	31,6%	23,1%	33,3%	28,9%
		% επί Συνόλου	0,0%	2,2%	13,3%	6,7%	6,7%	28,9%
	3	Συχνότητα	0	1	11	7	0	19
		% σε σχέση με $Q_{13}$	0,0%	5,3%	57,9%	36,8%	0,0%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	33,3%	57,9%	53,8%	0,0%	42,2%
		% επί Συνόλου	0,0%	2,2%	24,4%	15,6%	0,0%	42,2%
	4	Συχνότητα	0	0	2	3	6	11
		% σε σχέση με $Q_{13}$	0,0%	0,0%	18,2%	27,3%	54,5%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	0,0%	10,5%	23,1%	66,7%	24,4%
		% επί Συνόλου	0,0%	0,0%	4,4%	6,7%	13,3%	24,4%
ΣΥΝΟΛΟ	Συχνότητα	1	3	19	13	9	45	
	% σε σχέση με $Q_{13}$	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%	
	% σε σχέση με $Q_{17}$	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	
	% επί Συνόλου	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%	

Πίνακας 22: Συσχέτιση της  $Q_{17}$  με την  $Q_{13}$ 

Στον παραπάνω πίνακα 22, συγκρίνεται η  $Q_{13}$  (Οι πληροφορίες που δύνονται είναι άμεσες και κατανοητές;) με την  $Q_{17}$  (Θα την προτείνετε σε γνωστούς και φίλους;) και παρατηρείται ότι το 53,8% βαθμολόγησε με 3 (μέτρια ικανοποιημένο) και το 66,75 με 4 (πολύ ικανοποιημένο), αριθμοί που δείχνουν επίσης μία ικανοποίηση.

			$Q_{17}$					ΣΥΝΟΛΟ
			0	1	2	3	4	
$Q_{15}$	1	Συχνότητα	0	1	1	0	0	2
		% σε σχέση με $Q_{15}$	0,0%	50,0%	50,0%	0,0%	0,0%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	33,3%	5,3%	0,0%	0,0%	4,4%
		% επί Συνόλου	0,0%	2,2%	2,2%	0,0%	0,0%	4,4%
	2	Συχνότητα	1	0	4	1	0	6
		% σε σχέση με $Q_{15}$	16,7%	0,0%	66,7%	16,7%	0,0%	100,0%
		% σε σχέση με $Q_{17}$	100,0%	0,0%	21,1%	7,7%	0,0%	13,3%
		% επί Συνόλου	2,2%	0,0%	8,9%	2,2%	0,0%	13,3%
	3	Συχνότητα	0	1	13	9	1	24
		% σε σχέση με $Q_{15}$	0,0%	4,2%	54,2%	37,5%	4,2%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	33,3%	68,4%	69,2%	11,1%	53,3%
		% επί Συνόλου	0,0%	2,2%	28,9%	20,0%	2,2%	53,3%
	4	Συχνότητα	0	1	1	3	8	13
		% σε σχέση με $Q_{15}$	0,0%	7,7%	7,7%	23,1%	61,5%	100,0%

	% σε σχέση με $Q_{17}$	0,0%	33,3%	5,3%	23,1%	88,9%	28,9%
	% επί Συνόλου	0,0%	2,2%	2,2%	6,7%	17,8%	28,9%
<b>ΣΥΝΟΛΟ</b>	<b>Συχνότητα</b>	1	3	19	13	9	45
	% σε σχέση με $Q_{15}$	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%
	% σε σχέση με $Q_{17}$	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%
	% επί Συνόλου	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%

Πίνακας 23: Συσχέτιση της  $Q_{17}$  με την  $Q_{15}$ 

Στον παραπάνω πίνακα 23, συγκρίνεται η  $Q_{15}$  (Είναι ενδιαφέρον το αντικείμενο της ιστοσελίδας;) με την  $Q_{17}$  (Θα την προτείνετε σε γνωστούς και φίλους;) και παρατηρείται ότι το 88,9% βαθμολόγησε με 4 (πολύ ικανοποιημένο) που δείχνει ότι και από αυτές τις ερωτήσεις είναι ικανοποιημένος ο πληθυσμός.

		$Q_{17}$					<b>ΣΥΝΟΛΟ</b>	
		0	1	2	3	4		
$Q_{19}$	<b>1</b>	<b>Συχνότητα</b>	0	1	1	2	0	4
		% σε σχέση με $Q_{19}$	0,0%	25,0%	25,0%	50,0%	0,0%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	33,3%	5,3%	15,4%	0,0%	8,9%
		% επί Συνόλου	0,0%	2,2%	2,2%	4,4%	0,0%	8,9%
	<b>2</b>	<b>Συχνότητα</b>	0	0	14	1	4	19
		% σε σχέση με $Q_{19}$	0,0%	0,0%	73,7%	5,3%	21,1%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	0,0%	73,7%	7,7%	44,4%	42,2%
		% επί Συνόλου	0,0%	0,0%	31,1%	2,2%	8,9%	42,2%
	<b>3</b>	<b>Συχνότητα</b>	1	1	4	6	3	15
		% σε σχέση με $Q_{19}$	6,7%	6,7%	26,7%	40,0%	20,0%	100,0%
		% σε σχέση με $Q_{17}$	100,0%	33,3%	21,1%	46,2%	33,3%	33,3%
		% επί Συνόλου	2,2%	2,2%	8,9%	13,3%	6,7%	33,3%
	<b>4</b>	<b>Συχνότητα</b>	0	1	0	4	2	7
		% σε σχέση με $Q_{19}$	0,0%	14,3%	0,0%	57,1%	28,6%	100,0%
		% σε σχέση με $Q_{17}$	0,0%	33,3%	0,0%	30,8%	22,2%	15,6%
		% επί Συνόλου	0,0%	2,2%	0,0%	8,9%	4,4%	15,6%
<b>ΣΥΝΟΛΟ</b>	<b>Συχνότητα</b>	1	3	19	13	9	45	
	% σε σχέση με $Q_{19}$	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%	
	% σε σχέση με $Q_{17}$	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	
	% επί Συνόλου	2,2%	6,7%	42,2%	28,9%	20,0%	100,0%	

Πίνακας 24: Συσχέτιση της  $Q_{17}$  με την  $Q_{19}$ 

Στον παραπάνω πίνακα 24, συγκρίνεται η  $Q_{19}$  (Υπάρχει άμεση πρόσβαση στο υλικό της ιστοσελίδας;) με την  $Q_{17}$  (Θα την προτείνετε σε γνωστούς και φίλους;) και παρατηρούμε ότι το 73,7% βαθμολόγησε με 2 (ελάχιστα ικανοποιημένο), γεγονός που δείχνει ότι δεν έμεινε ικανοποιημένος ο πληθυσμός.

Τέλος, από τους παραπάνω πίνακες, παρατηρείται και ιδιαίτερα από τον τελευταίο ότι οι δύο ερωτήσεις  $Q_{17}$  και  $Q_{19}$  μοιάζουν μεταξύ τους και ότι ο πληθυσμός που απάντησε σε αυτό το ερωτηματολόγιο, δεν θα πρότεινε την ιστοσελίδα σε γνωστούς και φίλους, ούτε θα μιλούσε θετικά για την ιστοσελίδα αλλά όσον αφορά το περιεχόμενο – αντικείμενο της ιστοσελίδας, το βρήκε εύκολα και οι πληροφορίες ήταν άμεσες και κατανοητές.

#### 4.5 Εργαλείο Ανάλυσης Επισκεψιμότητας Ιστοσελίδων - WebTrends Analysis Series 7.0<sup>89, 90, 91</sup>

Η WebTrends παρέχει στατιστικά στοιχεία σχετικά με σελίδες δικτυακών τόπων, που οι χρήστες ιστοσελίδων επισκέπτονται με μεγαλύτερη συχνότητα και για περισσότερο χρονικό διάστημα. Αυτή η πληροφόρηση, βοηθάει τις εταιρίες στο να βελτιώσουν τον δικτυακό τους τόπο και τις πληροφορίες για τις υπηρεσίες και τα προϊόντα που παρέχουν μέσω αυτού.

Η WebTrends χρησιμοποιεί ένα αρχείο δεδομένων (cookie), για να ανιχνεύσει τον αριθμό χρηστών - επισκεπτών του δικτυακού τόπου. Πληροφορεί δηλαδή, για το εάν υπάρχει μικρός αριθμός τακτικών επισκεπτών ή μεγάλος αριθμός μη τακτικών επισκεπτών. Καμία πληροφορία δεν μπορεί να οδηγήσει στην ταυτότητα του επισκέπτη και φυσικά το cookie, ανιχνεύει μόνο την επισκεψιμότητα του εκάστοτε δικτυακού τόπου.

##### 4.5.1 Στατιστικά Στοιχεία Δημοτικότητας ενός Web Site<sup>91</sup>

Στο σημείο αυτό, παρουσιάζονται οι σημαντικότεροι όροι στατιστικών στοιχείων κίνησης ενός ιστοχώρου. Τα νούμερα αυτά, δεν δίνουν πάντοτε όλες τις επιθυμητές πληροφορίες. Για παράδειγμα, δεν μπορεί να γνωρίζει κανείς, τον ακριβή αριθμό των ανθρώπων που επισκέφθηκαν κάποιες σελίδες, ωστόσο ο παγκόσμιος ιστός, αποτελεί το περισσότερο μετρήσιμο μέσο, απ' όλα τα διαφημιστικά μέσα και παρέχει μεγάλη πληθώρα δεδομένων, πολλά από τα οποία μπορούν να αποδειχθούν εξαιρετικά πολύτιμα για τη σχεδίαση μιας ιστοσελίδας.

Τα σημαντικότερα από τα πληροφοριακά στοιχεία τα οποία μας παρέχονται για τη δημοτικότητα ενός ιστοχώρου τα παραθέτονται παρακάτω.

##### *Αιτήσεις (Hits)*

Ο αριθμός των αιτήσεων (hits) αναφέρεται στο σύνολο των αρχείων τα οποία ζητήθηκαν από ένα κεντρικό διαδικτυακό υπολογιστή - web server. Κάθε ιστοσελίδα, αποτελείται από ένα αρχείο HTML, καθώς και από τα αρχεία όλων των γραφικών (φωτογραφίες, ζωγραφίες, εικονίδια) που περιέχει. Έτσι, η επιτυχημένη ή μη αίτηση αποστολής μιας σελίδας με 2 φωτογραφίες και 3 γραφικά (π.χ. κουμπιά περιήγησης) στον ηλεκτρονικό υπολογιστή ενός χρήστη καταγράφεται από τον web server ως 6 hits (1 για το αρχείο HTML, 2 αρχεία για τις φωτογραφίες και 3 αρχεία για τα γραφικά). Επειδή ο αριθμός των φωτογραφιών και των γραφικών, διαφέρει από σελίδα σε σελίδα, τα hits, είναι αναξιόπιστα ως μέτρο υπολογισμού της δημοτικότητας ενός ιστοχώρου και πρέπει να χρησιμοποιούνται μόνο ως ένα προσεγγιστικό μέτρο του φόρτου που δημιουργεί ο ιστοχώρος στον web server. Δυστυχώς, είτε από άγνοια είτε από υπολογισμό, πολλές φορές εξισώνονται τα hits με σελίδες ή, ακόμη χειρότερα, με χρήστες, με αποτέλεσμα να δημιουργούνται λανθασμένες εντυπώσεις.

##### *Χρήστες ή μοναδικές IP Διευθύνσεις (Users ή Unique IP Addresses)*

Αν ο web server, δεν χρησιμοποιεί cookies, τότε ο αριθμός των επισκεπτών μιας ιστοσελίδας θεωρείται ίσος με τον αριθμό των IP διευθύνσεων από τις οποίες ζητήθηκαν σελίδες. Το νούμερο αυτό, είναι προσεγγιστικό και πολλές φορές υποεκτιμά τον αριθμό των επισκεπτών, καθώς πολλοί χρήστες που είναι συνήθως από εταιρείες, δεν έχουν IP διευθύνσεις στα μηχανήματά τους, αλλά διαθέτουν πρόσβαση στο διαδίκτυο μέσω ενός proxy. Έτσι, αν δύο ή

περισσότεροι χρήστες επισκεφθούν την ίδια ιστοσελίδα, ο web server θα καταγράψει μόνο μια IP διεύθυνση (τον proxy) και θα θεωρήσει πως υπάρχει μόνο ένας επισκέπτης. Επίσης, πολλοί υπολογιστές έχουν σταθερή IP διεύθυνση (static), αλλά χρησιμοποιούνται από πολλούς χρήστες όπως για παράδειγμα, σε ένα ίντερνετ καφέ. Και σε αυτή την περίπτωση αν δύο ή περισσότεροι χρήστες ζητήσουν σελίδες από την ίδια ιστοσελίδα θα θεωρηθούν ως ένας επισκέπτης.

Η χρήση των IP διευθύνσεων μπορεί όμως και να οδηγήσει σε υπερεκτίμηση του αριθμού των επισκεπτών, διότι οι περισσότεροι dial-up χρήστες διαθέτουν πρόσβαση dynamic PPP. Δηλαδή, κάθε φορά που συνδέονται στο δίκτυο, τους δίνεται μια IP διεύθυνση από το σύνολο όσων διαθέτει ο παροχέας, η οποία τους "ανήκει" μόνο κατά τη διάρκεια της σύνδεσής τους. Όταν αποσυνδεθούν, την "επιστρέφουν πίσω" και όταν συνδεθούν και πάλι θα ζητήσουν να τους αποδοθεί μια νέα διεύθυνση η οποία μπορεί να είναι η ίδια με πριν, αλλά μπορεί να είναι και κάποια άλλη επειδή οι διευθύνσεις μοιράζονται στην τύχη. Έτσι, ένας χρήστης μπορεί να επισκεφθεί δύο φορές την ίδια ιστοσελίδα, χρησιμοποιώντας διαφορετική κάθε φορά IP διεύθυνση, οπότε θα θεωρηθεί ως δύο ξεχωριστοί επισκέπτες. Αντίστοιχα, δύο dial-up χρήστες μπορεί να επισκεφθούν τον ιστοχώρο χρησιμοποιώντας την ίδια IP διεύθυνση (έτυχε όταν αποσυνδέθηκε ο ένας να αποδοθεί η ίδια διεύθυνση στον άλλον), οπότε θα θεωρηθούν ως ένας επισκέπτης. Προσεγγιστικά πάντως λέγεται, ότι οι επισκέπτες ενός ιστοχώρου είναι τουλάχιστον όσοι και οι χρήστες του.

### ***Επισκέψεις (Visits ή sessions)***

Κάθε φορά που ζητεί κανείς μια ιστοσελίδα, ο υπολογιστής συνδέεται με τον web server ο οποίος φιλοξενεί τη σελίδα, λαμβάνει ένα αντίγραφο της και στη συνέχεια, αφού βεβαιωθεί πως η σελίδα έφτασε χωρίς πρόβλημα, διακόπτει τη σύνδεση με τον server από τον οποίον την παρέλαβε. Αν, αμέσως μετά, ζητηθεί και δεύτερη σελίδα από τον ίδιο τον ιστοχώρο, τότε θα πραγματοποιηθεί μια νέα σύνδεση με τον ίδιο web server η οποία θα διακοπεί και πάλι όταν ολοκληρωθεί η μεταφορά της σελίδας.

Αν λοιπόν, επισκεφθεί κανείς τη σελίδα X, ενός ιστοχώρου και από αυτή κάνει κλικ, σε μια παραπομπή προς τη σελίδα Ψ, τότε ο web server θα καταγράψει δύο ξεχωριστές και ανεξάρτητες μεταξύ τους συνδέσεις (μια για τη σελίδα X και μια για την Ψ) οι οποίες όμως έγιναν όλες με την ίδια IP διεύθυνση. Αν ο χρήστης έχει στατική IP διεύθυνση και καταγράφηκε μια σειρά από επισκέψεις του από τις 12:05 έως τις 12:23 (12:05 σελίδα A, 12:08 σελίδα B και ου το καθεξής) και μια δεύτερη σειρά από τις 15:22 έως τις 15:46 της ίδιας ημέρας είναι λογικό να υποθέσουμε ότι δεν είναι δυνατόν να μελετούσε την ίδια σελίδα από τις 12:23 έως τις 15:22. Το πιο πιθανό είναι ότι μετά τη σελίδα των 12:23 είτε αποσυνδέθηκε και ξαναμπήκε στο δίκτυο στις 15:22, είτε επισκεφθηκε άλλους δικτυακούς τόπους και στις 15:22 επέστρεψε στη δική μας ιστοσελίδα (δηλαδή ζήτησε κάποια ακόμη σελίδα από αυτό). Γι' αυτό και σ' αυτή την περίπτωση λέγεται ότι υπήρχε ένας χρήστης αλλά δύο επισκέψεις (visits), δηλαδή πως από το ίδιο μηχάνημα ή από το ίδιο άτομο έγιναν δύο επισκέψεις.

Το κριτήριο με το οποίο αποφασίζεται αν δύο επισκέψεις ανήκουν στο ίδιο ή σε διαφορετικό session είναι ο χρόνος που μεσολαβεί μεταξύ τους. Τρεις ώρες, όπως στο παραπάνω παράδειγμα, σημαίνουν ότι υπάρχει ξεχωριστό session, ενώ 10 λεπτά σημαίνουν πως ο επισκέπτης θεωρείται ενεργός. Συνήθως, θεωρείται ότι πραγματοποιείται ένα καινούριο session όταν μεσολαβούν πάνω από 30 λεπτά μεταξύ δύο αιτημάτων από την ίδια IP διεύθυνση. Το νούμερο αυτό όμως, είναι αυθαίρετο και μπορεί να τροποποιηθεί αν οι επισκέψεις σε κάποιο site έχουν ορισμένες ιδιαιτερότητες. Επειδή τα visits πληροφορούν για τον αριθμό των επισκέψεων

σε μία ιστοσελίδα, ισχύει ότι οι επισκέπτες ενός ιστοχώρου μπορούν να είναι το πολύ τόσοι όσα και τα visits που έχει δεχθεί.

### ***Μέσος Όρος Αιτήσεων ανά χρήστη (Average requests per visit)***

Το νούμερο αυτό δηλώνει πόσες σελίδες είδε - ζήτησε ο μέσος επισκέπτης σε κάθε επίσκεψή του. Όσο μεγαλύτερο είναι αυτό το νούμερο, τόσο πιο χρήσιμη θεώρησε την ιστοσελίδα ο επισκέπτης και γι' αυτό θέλησε να δει περισσότερες σελίδες του.

### ***Χρόνος παραμονής σε σελίδα (Request duration)***

Το request duration δηλώνει πόσο χρόνο αφιέρωσε σε κάθε σελίδα ο επισκέπτης μέχρι να ζητήσει μια άλλη του ίδιου ιστοχώρου (δηλαδή, πόσος χρόνος μεσολάβησε μεταξύ δύο συνεχόμενων requests). Μικρός χρόνος, σημαίνει είτε ότι το περιεχόμενο της σελίδας δεν κρίθηκε αξιόλογο είτε ότι η ιστοσελίδα δεν έχει καλή σχεδίαση και ο επισκέπτης υποχρεώνεται να ψάξει σε πολλές σελίδες, μέχρι να βρει το πληροφοριακό υλικό που τον ενδιαφέρει ή μέχρι να εγκαταλείψει την προσπάθεια. Η άθροιση όλων των χρόνων παραμονής σε κάθε σελίδα (Request durations) κάθε χρήστη, δίνει το συνολικό χρόνο (visit duration) που παρέμεινε ο χρήστης στον ιστοχώρο.

### ***Σελίδες Εισόδου (Entry pages)***

Οι σελίδες τις οποίες φορτώνουν πρώτες οι επισκέπτες ενός ιστοχώρου. Η αρχική σελίδα (home page), είναι η συνηθέστερη σελίδα εισόδου (entry page). Αν όμως παρατηρηθεί πως υπάρχουν και άλλες, τότε αυτό σημαίνει ότι για κάποιο λόγο οι χρήστες θεωρούν αυτές τις σελίδες τόσο σημαντικές, που πηγαίνουν απευθείας εκεί χωρίς να έχουν επισκεφθεί την αρχική σελίδα ή κάποια άλλη σελίδα του ιστοχώρου.

### ***Σελίδες Εξόδου (Exit pages)***

Οι τελευταίες σελίδες που βλέπουν οι χρήστες πριν εγκαταλείψουν τον ιστοχώρο. Με το στοιχείο αυτό, φαίνεται ποιες σελίδες περιείχαν αυτό που ήθελαν οι χρήστες ή σε ποια σελίδα εγκαταλείπουν συνήθως την προσπάθεια να βρουν αυτό που θέλουν και φεύγουν.

### ***Σφάλματα (ή 404 Errors)***

Ποιες διευθύνσεις ζητήθηκαν και παρουσίασαν μήνυμα λάθους (ότι δεν υπήρχε η διεύθυνση). Με το στοιχείο αυτό φαίνεται ποιοι εσωτερικοί σύνδεσμοι έχουν πρόβλημα ή ποιες διευθύνσεις του ιστοχώρου οι οποίες δεν υπάρχουν πια, ζητούνται από τους χρήστες του δικτύου (για παράδειγμα, σελίδες που δεν υπάρχουν πια και προς τις οποίες υπάρχουν παραπομπές από άλλους ιστοχώρους).

### ***Λέξεις κλειδιά (Referrer Data ή Referrals)***

Ποιες λέξεις κλειδιά χρησιμοποιήθηκαν από τους χρήστες μιας μηχανής αναζήτησης και τους οδήγησαν τελικά σε αυτόν τον ιστοχώρο.



### Συμπεράσματα ανάλυσης στοιχείων επισκεψιμότητας

Τα παραπάνω στοιχεία είναι τα σημαντικότερα απ' όσα πρέπει να γνωρίζει κάθε υπεύθυνος ενός ιστοχώρου για να παρακολουθεί τη δημοτικότητά του και να ανακαλύπτει τις ενέργειες οι οποίες απαιτούνται για την αύξησή της. Υπάρχουν φυσικά και πολλοί άλλοι λιγότερο σημαντικοί όροι, όπως επίσης, μερικές από τις υπηρεσίες παροχής στατιστικών στοιχείων δημοτικότητας πιθανώς να χρησιμοποιούν ορολογία, λίγο διαφορετική από εκείνη που περιγράφηκε σε αυτήν την εργασία (για παράδειγμα Page views αντί για Requests). Ωστόσο, το περιεχόμενο των όρων είναι σχεδόν πάντοτε το ίδιο.

Όλα τα στοιχεία μέτρησης δημοτικότητας που αναφέρθηκαν παραπάνω, έχουν προσεγγιστική και όχι απόλυτη ισχύ. Είναι λοιπόν αξιόπιστα για τη συντριπτική πλειοψηφία των ιστοχώρων, αλλά σε πολύ ειδικές περιπτώσεις πιθανώς να επιβάλλεται ένας διαφορετικός τρόπος ερμηνείας τους.

Αυτό πάντως σε καμία περίπτωση δεν μειώνει τη χρησιμότητά τους. Ο παγκόσμιος ιστός αποτελεί χωρίς καμία αμφιβολία το καλύτερα μετρήσιμο απ' όλα τα διαφημιστικά μέσα. Έτσι, επιτρέπει την γρήγορη αναγνώριση των λαθών, της στρατηγικής που έχει επιλεχθεί σε ένα ιστοχώρο και άμεση προσαρμογή της πολιτικής, στις διαθέσεις των χρηστών και τις ανάγκες της στιγμής. Η μελέτη των στατιστικών αποτελεί κατά γενική ομολογία μια επένδυση η οποία αξίζει με το παραπάνω τα χρήματα και τον χρόνο που διαθέτει συνήθως κάποια εταιρία για την ιστοσελίδα της.

#### 4.5.2 Γενικά Κριτήρια Αναλυτικής Αξιολόγησης Ιστοσελίδων

Παρακάτω, παρουσιάζεται ο πίνακας 25, με τα κριτήρια αναλυτικής αξιολόγησης ιστοσελίδων.

ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ	ΑΝΑΛΥΤΙΚΑ ΑΝΑ ΚΡΙΤΗΡΙΟ
<b>ΧΡΗΣΗ</b>	Ευκολία στον εντοπισμό της ιστοσελίδας
	Ευκολία πρόσβασης σε κατάλογο προϊόντων και υπηρεσιών
	Ευκολία στην περιήγηση και επιστροφή στην αρχική σελίδα
<b>ΠΕΡΙΕΧΟΜΕΝΟ</b>	Υψηλή ποιότητα και εκτενείς πληροφορίες προϊόντων και υπηρεσιών
	Μεγάλη ποικιλία διαφημιζόμενων προϊόντων
	Πληροφορίες γενικές για το είδος και την τιμή
	Συνεχής ενημέρωση της ιστοσελίδας
	Πληροφορίες για την πολιτική της εταιρείας
	Περιεχόμενο μη-επαναλαμβανόμενο που αναφέρεται στο αντικείμενο της ιστοσελίδας
<b>ΔΟΜΗ</b>	Περιεχόμενο λογικά δομημένο, σε διαφορετικούς τομείς και επίπεδα
	Ευκολονόητα μενού.
	Χάρτης ή πίνακας των περιεχομένων
	Τα γραφικά και τα πολυμέσα να συνεισφέρουν στην διευκόλυνση κατανόησης της πλοήγησης.
	Εικονίδια εύκολα αναγνωρίσιμα
<b>ΣΥΝΔΕΣΜΟΙ</b>	Τα κείμενα να διαβάζονται εύκολα.
	Αποφυγή υπερβολικής χρήσης γραφικών ή πολυμέσων που επηρεάζουν το χρόνο ανάκτησης.
	Να παρέχονται ξένες γλώσσες
	Ηλεκτρονικές και φυσικές διευθύνσεις
	Μη χρήση σελίδων «υπό-κατασκευή» (under construction)

	Ευδιάκριτοι σύνδεσμοι και τοποθέτησή τους
<b>ΠΛΟΗΓΗΣΗ</b>	Συνεχής πλοήγηση σε όλα τα επίπεδα της ιστοσελίδας
	Εύκολη χρήση της μηχανής αναζήτησης
	Αναλυτική περιγραφή των αποτελεσμάτων εύρεσης
	Μη ύπαρξη προβλημάτων στην μηχανή αναζήτησης
	Ευκολόχρηστο πρόγραμμα βοήθειας
	Γρήγορη ανάκτηση των σελίδων
<b>ΕΜΦΑΝΙΣΗ</b>	Καλή ταχύτητα ανάκτησης της βάσης δεδομένων
	Ιστοσελίδα αισθητικά ελκυστική
	Η αρχική σελίδα να είναι περιεκτική και άμεσα αντίληπτη
	Σωστή χρήση των χρωμάτων και του φόντου
	Ευανάγνωστα κείμενα.
	Αποφυγή υπερβολικής χρήσης γραφικών / πολυμέσων
<b>ΑΣΦΑΛΕΙΑ</b>	Αξιόπιστα συστήματα ασφαλείας
	Επαρκή πρωτόκολλα ασφαλείας
	Ασφαλή συστήματα πληρωμής
	Προστασία προσωπικών δεδομένων
<b>ΕΠΙΚΟΙΝΩΝΙΑ</b>	Ευκολία στην εγγραφή και καταχώριση στην ιστοσελίδα
	Δυνατότητα πληρωμής με διάφορους τρόπους
	Απόθεμα προϊόντων
	Άμεση ενημέρωση για την πρόοδο της παραγγελίας
	Δυνατότητα εντοπισμού και επιβεβαίωσης της παραγγελίας
	Συνέπεια στην παράδοση και παραλαβή.
	Συνέχιση υπηρεσιών μετά την παραγγελία και παράδοση
	Άμεση ανταπόκριση σε προβλήματα που προέκυψαν πριν και μετά την παραγγελία
	Διατήρηση σχέσεων με τον πελάτη

Πίνακας 25: Κριτήρια Αναλυτικής Αξιολόγησης Ιστοσελίδων

#### 4.5.3 Περιγραφή του εργαλείου WebTrends Analysis Series 7.0<sup>91</sup>

Στην παράγραφο αυτή, παρουσιάζουμε το εργαλείο «WebTrends Analysis Series 7.0» με μερικές βασικές εικόνες.

Εικόνα 25: Το εργαλείο «WebTrends Analysis Series 7.0». <sup>91</sup>

Η παραπάνω εικόνα 25, εμφανίζεται, με το που ανοίγει το εργαλείο και περιέχει ένα βοηθητικό κατάλογο (help menu) καθώς και το σημείο εκκίνησης του εργαλείου.

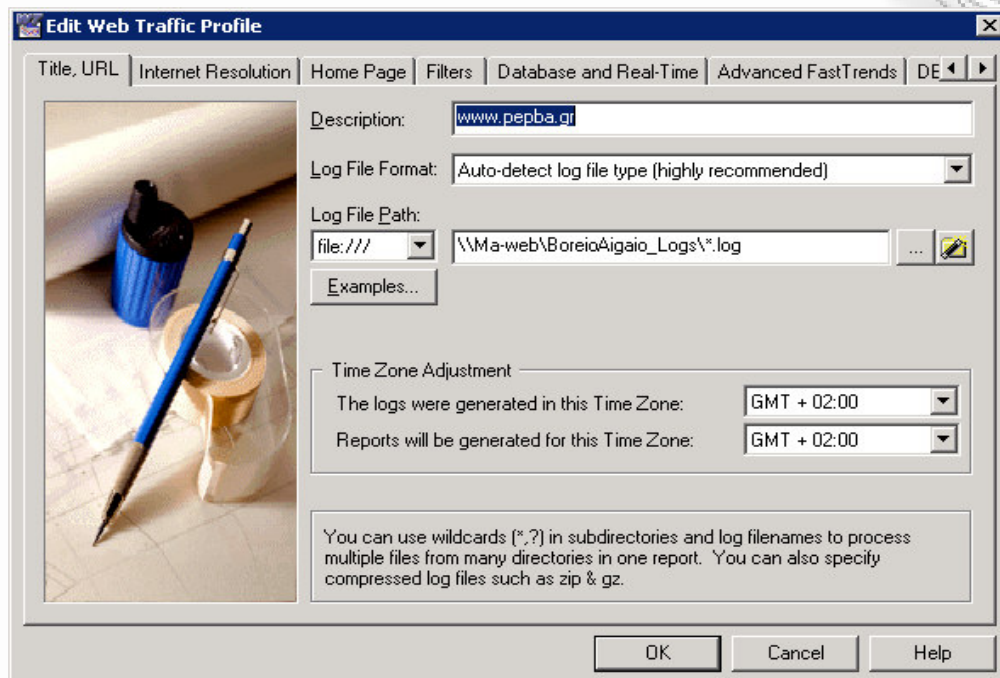
Η επόμενη εικόνα 26, απεικονίζει την κεντρική διαχείριση του εργαλείου, όπου όπως φαίνεται και στον αριστερό βοηθητικό κατάλογο μπορούν να προγραμματιστούν αναφορές επισκευμότητας (Schedule Event) στην περίπτωση που θέλει κανείς από ένα προφίλ να έχει για παράδειγμα συνεχώς μηνιαίες αναφορές.

Ακόμα, μπορεί να δημιουργήσει κανείς καινούργιο προφίλ (New Profile), όπως φαίνεται και στο κεντρικό σημείο της οθόνης (από ήδη δημιουργημένα προφίλ) ή να επεξεργαστεί ένα προφίλ (Edit Profile), να διαγράψει (Delete profile) και φυσικά να ξεκινήσει την αναφορά του προφίλ πατώντας το Reports.

The screenshot displays the 'WebTrends Analysis Series' application window. The main area shows a table of profiles under the 'Schedule Event' tab. The table has three columns: 'Profile Description', 'URL', and 'Profile Filename'. The profiles listed include various Greek domains and their corresponding log file paths and filenames.

Profile Description	URL	Profile Filename
www.agrotikianaphxi.gr (2007-2013)	file:///C:/Cronus/Vlogs_ops/agrotiknew-access_log	00000038.wlp
www.aleia.gr	file:///H:/Hydra/Logs_aleia/	0000000F.wlp
www.antagonistikotita.gr (2000-2006)	file:///M:/Ma-web/logs_EPAN/ access_log	00000011.wlp
www.antagonistikotita.gr (2007-2013)	file:///E:/LogFiles/LogFiles_Antagonistikotita/	00000010.wlp
www.dytikiellada.gr	file:///H:/Hydra/Vlogs_dytikiellada/	00000012.wlp
www.edel.gr	file:///M:/Mouwwwsvr01/W3SVC2/	00000037.wlp
www.edull.gr	file:///I:/Info/W3SVC12/	00000013.wlp
www.epeaek.gr	file:///E:/LogFiles/LogFiles_Epeaek/access_log	00000014.wlp
www.ependyseis.gr	file:///E:/LogFiles/LogFiles_www.ependyseis.gr/	00000016.wlp
www.ependyseis.gr/mis	file:///E:/LogFiles/LogFiles_www.ependyseis.gr/	00000015.wlp
www.epoalaa.gr	file:///M:/Ma-web/W3SVC4/	00000017.wlp
www.epper.gr (EPPER-2000-2006)	file:///H:/Hydra/vlogs_epper/	00000018.wlp
www.epper.gr (EPPEREA-2007-2013)	file:///C:/Cronus/W3SVC1614374215/	00000031.wlp
www.equal-greece.gr (2000-2006)	file:///M:/Ma-web/W3SVC10/	00000019.wlp
www.equal-greece.gr (2007-2013)	file:///C:/Cronus/Vlogs_ops/equalsnew-access_log	00000039.wlp
www.esthellas.gr	file:///C:/Cronus/W3SVC105129154/	00000035.wlp
www.espa.gr	file:///E:/LogFiles/LogFiles_Espa/	0000001A.wlp
www.espa.gr - 2009	file:///E:/LogFiles/LogFiles_Espa/	00000030.wlp
www.eyek.gr	file:///C:/Cronus/W3SVC90704940/	00000032.wlp
www.ggea.gr	file:///K/ps3central/W3SVC5-ggea/	0000001B.wlp
www.hellaskps.gr	file:///K/ps3central/Vlogs_hellaskps/	0000001C.wlp
www.hellaskps.gr - bestpractices	file:///K/ps3central/Vlogs_hellaskps/	0000001D.wlp
www.hellaskps.gr - bestpractices - 2009	file:///C:/Cronus/LogFiles/LogFiles_Hellaskps/bestpractices/	0000002F.wlp
www.info3kps.gr	file:///I:/Info/W3SVC9-info3kps/	0000001E.wlp
www.info3kps.gr (3mino)	file:///E:/LogFiles/LogFiles_info3kps/	0000001F.wlp
www.inferreg.gr	file:///M:/Ma-web/W3SVC12/	00000020.wlp
www.leader-plus.gr	file:///H:/Hydra/W3SVC9/	00000021.wlp
www.metro132.gr	file:///E:/LogFiles/LogFiles_www.metro132.gr/metro132-access_log	0000003A.wlp
www.mou.gr	file:///M/Mod-server1/Vlogs_mou/	00000022.wlp
www.mou.gr - 2009	file:///C:/Cronus/LogFiles/2/	0000002E.wlp
www.notoaigaio.gr	file:///H:/Hydra/NotoigaioNEW2010/	00000041.wlp
www.ops.gr	file:///C:/Cronus/Vlogs_ops/ops.gr-access_log	0000003F.wlp
www.peloponnisos.gr	file:///C:/Cronus/Vlogs_ops/peloponnisos.gr-access_log	00000040.wlp
www.pepba.gr	file:///M:/Ma-web/Bcreia/igaio_Logs/	00000024.wlp
www.pepdm.gr	file:///I:/Info/W3SVC7/	00000025.wlp
www.peponia.gr	file:///C:/Cronus/W3SVC1810703783/	00000026.wlp
www.pepkm.gr	file:///E:/LogFiles/LogFiles_www.pepkm.gr/www.pepkm.gr_access_log	0000003D.wlp
www.peproe.gr	file:///I:/Info/W3SVC5/	00000027.wlp

Εικόνα 26: Κεντρική οθόνη του εργαλείου.<sup>91</sup>



Εικόνα 27: Επεξεργασία προφίλ ιστοσελίδας.<sup>91</sup>

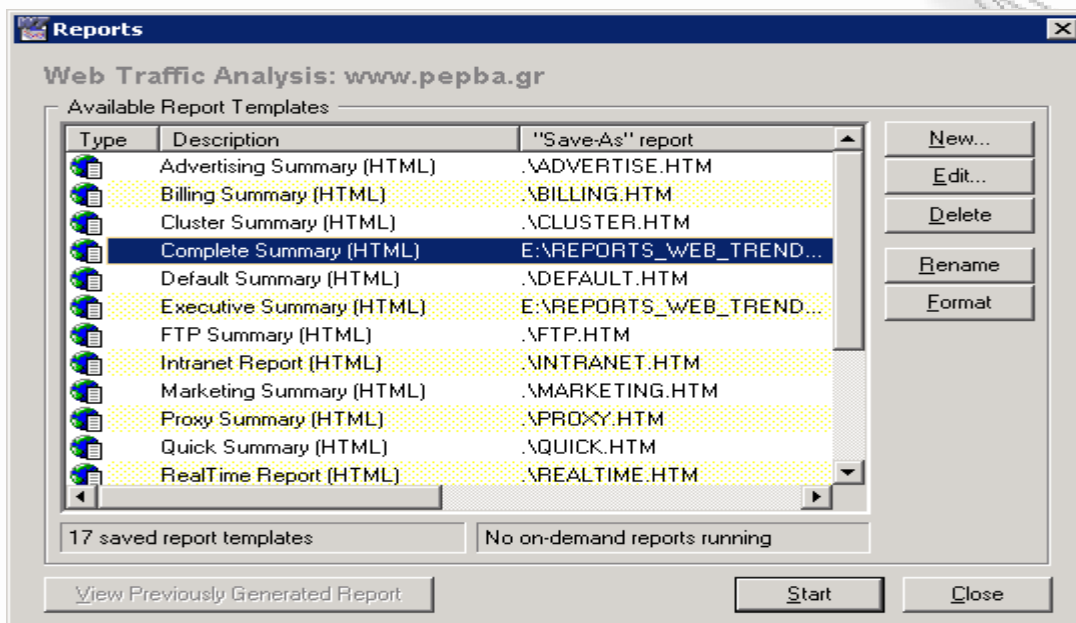
Στην παραπάνω εικόνα 27, παρουσιάζεται η επεξεργασία ενός προφίλ. Από εδώ δίνει κανείς μία περιγραφή του προφίλ (Description-για παράδειγμα, [www.pepba.gr](http://www.pepba.gr)): πως θα βρει το «format του log file» (Log File Format), που θα βρει τα «log files», που θέλει να τρέξει η αναφορά (συνήθως δίνεται κατευθείαν το path του κεντρικού υπολογιστή και τα τραβάει δικτυακά, εκτός και αν έχουν μεταφερθεί τοπικά στο μηχάνημα).

Επίσης, ρυθμίζεται και η ώρα που θα τρέξει η αναφορά επισκεψιμότητας. Στις επόμενες ετικέτες, δηλώνεται η αρχική σελίδα της ιστοσελίδας, και τα φίλτρα (για παράδειγμα, να μην διαβάσει συγκεκριμένες σελίδες του ιστοχώρου, γιατί μπορεί να είναι παλιές και να μην ενδιαφέρει αυτό στην αναφορά επισκεψιμότητας).

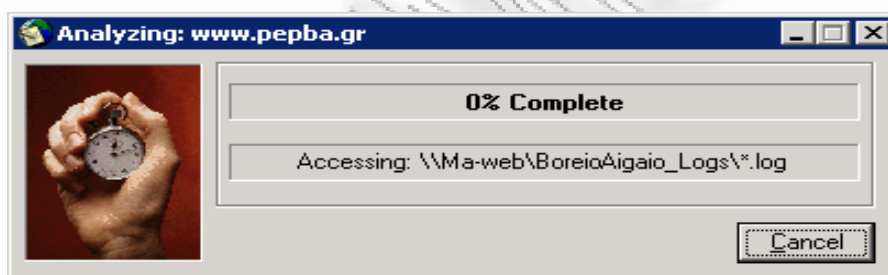
Στην συνέχεια, περιγράφεται η εικόνα 28, που αφορά την Αναφορά Επισκεψιμότητας (Report). Υπάρχουν κάποια έτοιμα πρότυπα, αλλά από το δεξί μενού, δίνεται η δυνατότητα:

- ✓ της δημιουργίας ενός νέου,
- ✓ της επεξεργασίας των ήδη έτοιμων ή του καινούργιου που έχει δημιουργηθεί,
- ✓ της διαγραφής,
- ✓ της μετονομασίας,
- ✓ της επισήμανσης των ιδιοτήτων της αναφοράς

Από το κάτω μέρος της οθόνης ξεκινάει η αναφορά επισκεψιμότητας (Report).



Εικόνα 28: Εκκίνηση Αναφοράς Επισκεψιμότητας (Report).<sup>91</sup>



Εικόνα 29: Ανάλυση αναφοράς επισκεψιμότητας.<sup>91</sup>

Τέλος, η παραπάνω εικόνα 29, παρουσιάζει την οθόνη που εμφανίζεται κατά την διάρκεια που τρέχει ένα Report μέχρι να εξάγει τα αποτελέσματα. Η διάρκειά του, εξαρτάται συνήθως, από το μέγεθος του «log file». Στην επόμενη παράγραφο παρουσιάζεται ένα αποτέλεσμα – μία αναφορά επισκεψιμότητας (Report), όσον αφορά τα γενικά της στοιχεία.

#### 4.5.4 Παράδειγμα Αναφοράς Επισκεψιμότητας μέσω του εργαλείου WebTrends Analysis Series 7.0<sup>91, 92</sup>

Μέσω του εργαλείου WebTrends Analysis Series 7.0, εκτελέστηκαν αναφορές επισκεψιμότητας για όλες τις ιστοσελίδες της μελέτης και στην παράγραφο αυτή, παρατίθεται ένα παράδειγμα αναφοράς επισκεψιμότητας της ιστοσελίδας του Π.Ε.Π Στερεάς Ελλάδας - <http://www.stereaeellada.gr/3kps/pep.htm>, που περιγράφηκε στην παράγραφο 4.3.2, αυτού του κεφαλαίου.

Το αποτέλεσμα που εξάγει το εργαλείο, είναι μία ιστοσελίδα με αρκετές σελίδες, ανάλογα με τις επιλογές που έχουν οριστεί στο εργαλείο. Εδώ, παρουσιάζεται η αρχική σελίδα της

συνολικής αναφοράς, που περιέχει το βασικό διάγραμμα των συνολικών επισκέψεων καθώς και ένα πίνακα με τα γενικά στατιστικά στοιχεία της αναφοράς επισκεψιμότητας.

Τα γενικά στατιστικά στοιχεία που δίνει ο πίνακας στην αρχική σελίδα της αναφοράς επισκεψιμότητας για την ιστοσελίδα, είναι τα παρακάτω:

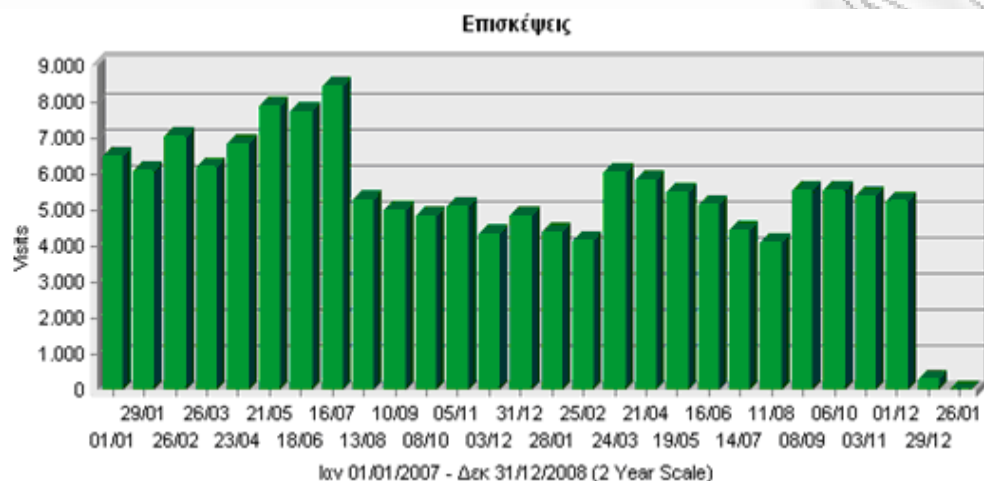
- ✓ Αιτήσεις (Hits)
  - Επιτυχημένες Αιτήσεις (Hits) σε όλο τον Ιστοχώρο
  - Μέσος Όρος Ημερησίως
  - Αρχική Σελίδα (Home Page)
- ✓ Εμφανίσεις Σελίδων
  - Εμφανίσεις Σελίδων
  - Μέσος Όρος Ημερησίως
  - Average per Unique Visitor 16
  - Εμφανίσεις Αρχείων
- ✓ Επισκέψεις
  - Μέσος Όρος Ημερησίως
  - Μέσος Χρόνος Επίσκεψης
  - Median Visit Length
  - Διεθνείς Επισκέψεις
  - Επισκέψεις από άγνωστη προέλευση
  - Visits from United States
  - Visits Referred by Search Engines
  - Visits from Spiders
- ✓ Επισκέπτες

Τα υπόλοιπα περιεχόμενα μιας αναφοράς επισκεψιμότητας είναι τα Στοιχεία Πρόσβασης, Visitors & Demographics, Στατιστικά Δραστηριοτήτων (Activity Statistics), τα Τεχνικά Στοιχεία, Λέξεις Κλειδιά (Keywords), Μηχανές Αναζήτησης και Πλατφόρμες (Browsers & Platforms), Σφάλματα σε σημεία της ιστοσελίδας (Debug Statistics) και Γλωσσάριο (Glossary), τα οποία περιέχουν και δίνουν μία πολλή καλή πληροφορία και εικόνα αντίστοιχα, της ιστοσελίδας.

Το χρονικό διάστημα που επιλέχτηκε, αφορά τα έτη 2007 και 2008, διότι για αυτά τα χρονικά διαστήματα υπήρχαν τα αρχεία καταγραφής (Log Files) που χρειάστηκαν, για την εκτέλεση της αναφορά επισκεψιμότητας, μέσω του εργαλείου.

Τέλος, στα παρακάτω αποτελέσματα, τα γραφήματα επισκέψεων εμφανίζουν το συνολικό αριθμό επισκέψεων στην ιστοσελίδα. Ο συνοπτικός πίνακας στατιστικών στοιχείων, εμφανίζει μία σύνοψη της δραστηριότητας στην ιστοσελίδα κατά το καθορισμένο χρονικό διάστημα.

Αναφορά επισκεψιμότητας Ιστοσελίδας Περιφερειακού Επιχειρησιακού Προγράμματος Στερεάς Ελλάδας ([http://www.stereaellada.gr/per\\_perifereia.htm](http://www.stereaellada.gr/per_perifereia.htm)).



Εικόνα 30: Γράφημα επισκέψεων Ιστοσελίδας Στερεάς Ελλάδας, με Χρονικό Διάστημα Αναφοράς Επισκεψιμότητας: 01/01/2007 έως 31/12/2008<sup>91, 92</sup>.

Γενικά Στοιχεία		
<b>Αιτήσεις (Hits)</b>	Επιτυχημένες Αιτήσεις (Hits) σε όλο τον ιστοχώρο	3.279.708
	Μέσος όρος ημερησίως	4.486
	Αρχική σελίδα (Home Page)	54.826
<b>Εμφανίσεις Σελίδων</b>	Εμφανίσεις σελίδων	740.115
	Μέσος όρος ημερησίως	1.012
	Average per Unique Visitor	16
	Εμφανίσεις αρχείων	720.291
<b>Επισκέψεις</b>	Επισκέψεις	148.614
	Μέσος όρος ημερησίως	203
	Μέσος χρόνος επίσκεψης	0:07:19
	Διεθνείς επισκέψεις	20.85%
	Επισκέψεις από άγνωστη προέλευση	62.35%
	Επισκέψεις από τις Ηνωμένες Πολιτείες	16.78%
	Επισκέψεις από μηχανές αναζήτησης	38
<b>Επισκέπτες</b>	Διαφορετικοί επισκέπτες	44.375
	Επισκέπτες με μία επίσκεψη	34.573
	Επισκέπτες με περισσότερες από μία επισκέψεις	9.802

Πίνακας 26: Γενικά στοιχεία επισκεψιμότητας

#### 4.5.5 Συμπεράσματα Αναφοράς Επισκεψιμότητας του εργαλείου WebTrends Analysis Series 7.0

Στον παρακάτω πίνακα 26, από την προηγούμενη παράγραφο, συγκεντρώθηκαν κάποια γενικά στοιχεία, από την αναφορά επισκεψιμότητας της κάθε ιστοσελίδας. Αυτά τα γενικά στοιχεία, είναι οι Αιτήσεις (Hits), οι Εμφανίσεις Σελίδων, οι Επισκέψεις και οι Επισκέπτες της κάθε ιστοσελίδας για τα έτη 2007 και 2008.

ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	ΣΤΕΡΕΑ ΕΛΛΑΔΑ	ΝΟΤΙΟ ΑΙΓΑΙΟ	ΘΕΣΣΑΛΙΑ	ΒΟΡΕΙΟ ΑΙΓΑΙΟ	ΔΥΤΙΚΗ ΕΛΛΑΔΑ	ΗΠΕΙΡΟΣ	ΔΥΤΙΚΗ ΜΑΚΕΔΟΝΙΑ	ΙΟΝΙΩΝ ΝΗΣΩΝ
<b>Αιτήσεις</b>								
1. Επιτυχημένες Αιτήσεις σε όλο Τον Ιστοχώρο	3.279.708	<b>4.014.186</b>	3.969.053	878.233	1.623.149	7.966.222	2.066.186	848.856
2. Μέσος Όρος Ημερησίως	4.486	5.491	5.429	1.201	2.220	<b>10.912</b>	2.830	1.161
3. Αρχική Σελίδα	54.826	N/A	117.183	36.352	49.750	<b>162.018</b>	48.331	29.290
<b>Εμφανίσεις Σελίδων</b>								
Εμφανίσεις Σελίδων	740.115	<b>997.522</b>	946.104	244.005	329.711	449.298	249.534	206.31
1. Μέσος Όρος ανά Μοναδικό Επισκέπτη	16	<b>12</b>	7	8	10	11	6	10
<b>Επισκέψεις</b>								
1. Επισκέψεις	148.614	381.337	<b>426.306</b>	229.211	129.227	176.063	185.807	114.240
2. Μέσος Όρος Ημερησίως	203	521	<b>583</b>	143	176	241	254	156
3. Από άγνωστη προέλευση	62.35%	<b>65.00%</b>	62.34%	24.63%	63.88%	33.12%	50.67%	54.48%
4. Από Μηχανές Αναζήτησης	38	84	149	1.374	10	426	806	13
<b>Επισκέπτες</b>								
1. Διαφορετικοί Επισκέπτες	44.375	77.051	<b>134.419</b>	29.287	30.477	40.057	36.788	20.072
2. Επισκέπτες με μία επίσκεψη	34.573	59.334	<b>105.706</b>	23.347	22.118	27.808	25.813	14.227
3. Επισκέπτες με περισσότερες από μία επισκέψεις	9.802	17.717	<b>28.713</b>	5.940	8.359	12.249	10.975	5.845

Πίνακας 27: Συγκεντρωτικός πίνακας Ανάλυσης Επισκεψιμότητας Ιστοσελίδων Εφαρμογής.

Στον τον παραπάνω πίνακα 27, παρατηρείται ότι, τις περισσότερες επιτυχημένες αιτήσεις σε όλο τον ιστοχώρο τις έχει η ιστοσελίδα του Νότιου Αιγαίου (<http://www.notioaigaio.gr/site.asp>). Για τον μέσο όρο των αιτήσεων ημερησίως καθώς και για τις αιτήσεις της αρχικής σελίδας τα μεγαλύτερα νούμερα συγκεντρώνονται στην ιστοσελίδα της Ηπείρου ([http://www.peproe.gr/index\\_pep.html](http://www.peproe.gr/index_pep.html)). Στην συνέχεια, για τις εμφανίσεις σελίδων, πάλι το Νότιο Αιγαίο (<http://www.notioaigaio.gr/site.asp>) έχει τα μεγαλύτερα νούμερα. Όσον αφορά τις επισκέψεις των ιστοσελίδων, που είναι ένα από τα σημαντικότερα στοιχεία, η ιστοσελίδα της Θεσσαλίας (<http://www.thessalia.gr/pep/default.el.asp/>) είναι πρώτη σε επισκέψεις ακόμα και σε διαφορετικούς επισκέπτες.



#### 4.6 Βιβλιογραφία 4ου Κεφαλαίου

89. <http://www.webtrends.com>
90. <http://www.webtrends.com/Products.aspx>
91. WEBTRENDS e-business intelligence solutions from NetIQ WeTrends Analysis Series, (WebTrends Analysis Suite are trademarks of Net IQ Corporation. WebTrends is a registered trademark of NetIQ Coorporation 2001).
92. [http://www.stereaellada.gr/per\\_perifereia.htm](http://www.stereaellada.gr/per_perifereia.htm)  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Στερεάς Ελλάδας.
93. <http://www.notioaigaio.gr/site.asp>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Νοτίου Αιγαίου.
94. <http://www.thessalia.gr/pep/default.el.asp>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Θεσσαλίας.
95. <http://www.pepba.gr>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Βορείου Αιγαίου.
96. [http://www.peproe.gr/index\\_pep.html](http://www.peproe.gr/index_pep.html)  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Ηπείρου.
97. <http://www.pepdym.gr>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Δυτικής Μακεδονίας.
98. <http://www.pepionia.gr>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Ιονίων Νήσων.
99. [http://www.dytikiellada.gr/per\\_perifereia.htm](http://www.dytikiellada.gr/per_perifereia.htm)  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Δυτικής Ελλάδας.
100. Επιχειρησιακή Στατιστική, Λευτέρης Ι. Θαλασσινός, Αθήνα – Πειραιάς 1996.
101. <http://www.spss.gr>
102. <http://www.spss.com/>
103. <http://en.wikipedia.org/wiki/SPSS>
104. <http://www.ibm.com/gr/el/>

## ΕΠΙΛΟΓΟΣ

Στην παρούσα εργασία, διερευνήθηκε η Αξιολόγηση των Ηλεκτρονικών Υπηρεσιών μέσα από διαδικασία μοντελοποίησης. Η διαρκής ενημέρωση των Ηλεκτρονικών Υπηρεσιών με ποιοτικά χαρακτηριστικά, αποτελεί πλεονέκτημα τόσο για τους χρήστες όσο και για τους πάροχους αυτών. Αυτό έχει επίδραση στα κριτήρια επιλογής της υπηρεσίας, με αποτέλεσμα να επιλέγεται η αποδοτικότερη σε ότι αφορά παράγοντες (κόστος, χρόνος απόκρισης και άλλα). Τα ποιοτικά χαρακτηριστικά μιας υπηρεσίας δίνουν ένα σημαντικό και ανταγωνιστικό προτέρημα στους πάροχους και έτσι ελκύουν περισσότερους χρήστες. Η αρχιτεκτονική των Ηλεκτρονικών Υπηρεσιών που παρουσιάστηκε, προσφέρει πλεονεκτήματα, με σημαντικότερο αυτό της διαλειτουργικότητας των εφαρμογών, μιας και μέσω της τεχνολογίας αυτής είναι εφικτή η επικοινωνία τους, ανεξάρτητα από το λειτουργικό σύστημα που χρησιμοποιείται, της γλώσσας προγραμματισμού και της αρχιτεκτονικής του υπολογιστικού συστήματος στο οποίο υλοποιήθηκαν.

Είναι γεγονός, ότι παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές πρόσθετες επιβαρύνσεις στην απόδοση και στο κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Το κόστος της ασφάλειας είναι και κόστος χρόνου και χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι, η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Απαιτείται συνεπώς, μια πολιτική ασφάλειας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται ασφαλιστικές στρατηγικές, ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης.

Η αναγκαία πολιτική ασφάλειας, καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση, με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας, ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη ασφαλιστικών μέτρων, πρέπει να εξετάζεται η πιθανότητα να εμφανιστούν προβλήματα σχετικά με την ασφάλεια. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης. Επίσης, η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η εμφάνιση κακόβουλων λογισμικών, απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφάλειας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται, όπου αυτό κρίνεται απαραίτητο.

Η έννοια της ικανοποίησης του πελάτη (Customer Satisfaction) συσχετίζεται με την ποιότητα των υπηρεσιών (SERVQUAL) και η ποιότητα των υπηρεσιών που προσφέρει ένας οργανισμός συσχετίζεται άμεσα με την κερδοφορία του (Profit). Επομένως, η επιχείρηση που μπορεί να βεβαιώσει τις ανάγκες των πελατών της καθώς και τον βαθμό ικανοποίησή τους (Customer Satisfaction), θα παρέχει καλύτερες, αποδοτικότερες και ασφαλέστερες υπηρεσίες, αυξάνοντας την Απόδοση των Υπηρεσιών της (SERVPERFORM) και μειώνοντας παράλληλα τα κόστη της αυξανόμενης κερδοφορίας της (Profit).

Η εικόνα μιας εταιρείας, των προϊόντων της και η αξιοπιστία σε αυτήν, καταγραφόμενα μέσα από την ικανοποίηση των πελατών, συνδέονται άμεσα με την αύξηση και διατήρηση του μεριδίου αγοράς τους καθώς και την κερδοφορία του οργανισμού. Συμπερασματικά, η Ποιότητα των Υπηρεσιών (SERVQUAL) και η Απόδοση των Υπηρεσιών (SERVPERFORM)

ισούται με την Ικανοποίηση του Πελάτη (CUSTOMER SATISFACTION) συν το Κέρδος (PROFIT).

Σε ένα ιστοχώρο, υπάρχουν πολλοί παράγοντες που απαιτούν παρακολούθηση και ανάλυση, οι οποίοι σε συνδυασμό με συνεχείς δοκιμαστικές παρεμβάσεις στον δικτυακό τόπο, σε πολλά επίπεδα (στο σχεδιασμό, στο περιεχόμενο και στο λογισμικό), μπορούν να φέρουν το επιθυμητό αποτέλεσμα. Μια σοβαρή και επαγγελματική ανάλυση περιλαμβάνει εξαιρετικά περίπλοκες και χρονοβόρες διαδικασίες, και λαμβάνει υπόψη πολλούς περισσότερους παράγοντες. Τα σύγχρονα συστήματα, επιτρέπουν την ανάγνωση των συνηθειών και την προέλευση των επισκεπτών ενός ιστοχώρου, με μεγάλη ακρίβεια. Έτσι, με την κατάλληλη ανάλυση, οι πιο σημαντικές διαδικασίες, είναι αυτές που αποσκοπούν στην βελτιστοποίηση ιστοσελίδων σε θέματα χρηστικότητας (usability) και στην βελτιστοποίηση περιεχομένου για τις Μηχανές Αναζήτησης (Search Engine Optimization) των ιστοσελίδων.

Μία από τις σημαντικότερες δράσεις που καλείται να αναπτύξει μια επιχείρηση, η οποία επιθυμεί να ενισχύσει τη δικτυακή της παρουσία και να αξιολογήσει τις ηλεκτρονικές υπηρεσίες που παρέχει, είναι να συγκεντρώσει στοιχεία για τους επισκέπτες του δικτυακού της τόπου. Ποιοι και από πού, πότε και για πόσο, γιατί και πώς επισκέφθηκαν την ιστοσελίδα, καθώς και αν έμειναν ικανοποιημένοι από το περιεχόμενο ή αντιμετώπισαν δυσκολίες κατά την επίσκεψή τους, είναι μερικά από τα ερωτήματα στα οποία ανταποκρίνονται με επιτυχία διάφορα εργαλεία μετρήσεων και ανάλυσης επισκεψιμότητας, όπως και το “WebTrends Analysis Series 7.0”, που αναλύθηκε στην παρούσα εργασία.

Με την βοήθεια της στατιστικής (κάνοντας χρήση του στατιστικού προγράμματος SPSS), διαπιστώθηκε, ύστερα από ανάλυση των απαντήσεων των χρηστών του ερωτηματολογίου για την Ιστοσελίδα του Π.Ε.Π. Στερεάς Ελλάδας και μέσα από διαγράμματα και πίνακες, η σημασία και η χρησιμότητα του μοντέλου SERVQUAL. Μέσα από την ανάλυση των ερωτήσεων του ερωτηματολογίου, διαπιστώθηκε το πόσο σημαντικό είναι το περιεχόμενο σε μία ιστοσελίδα, δηλαδή να έχει πολύ καλή δομή και την απαιτούμενη από τον χρήστη πληροφορία. Ακόμα, το πόσο καλά λειτουργεί η αναζήτηση του ιστοχώρου ώστε ο χρήστης να βρίσκει εύκολα και γρήγορα αυτό που αναζητεί. Επίσης, μεγάλη σημασία έχουν οι κανόνες προσωπικών δεδομένων που τηρούνται, καθώς ακόμα, αν το μενού είναι εύκολο στην χρήση και δεν ‘χάνεται’ ο χρήστης, αν υπάρχουν αρκετοί εξωτερικοί σύνδεσμοι ώστε να κατευθύνουν τον επισκέπτη σε μία επιπλέον ενημέρωση και τέλος η γενικότερη χρήση του ιστοχώρου.

Σε αυτά τα συμπεράσματα καταλήγουμε και από την μελέτη των αναφορών επισκεψιμότητας του εργαλείου WebTrends Analysis Series 7.0. και από την μελέτη των διαγραμμάτων και πινάκων μέσα από την ανάλυση των αποτελεσμάτων του SPSS. Όλα τα παραπάνω, καταστούν αναγκαία τη χρήση μίας μεθόδου για την αξιολόγηση της επισκεψιμότητας, η οποία θα είναι αρκετά ευέλικτη ώστε να μπορεί συνεχώς να εφαρμόζεται στον υπό μελέτη ιστοχώρο και να μπορεί να ανταποκρίνεται στην ποικιλομορφία που αυτός παρουσιάζει. Μέσα από την Αξιολόγηση των Ηλεκτρονικών Υπηρεσιών, εξετάζονται θέματα που έχουν σχέση με τη χρηστικότητα, τη λειτουργικότητα και τα προβλήματα των ηλεκτρονικών υπηρεσιών που μπορούν να παρουσιαστούν σε ένα ιστοχώρο.

Η αύξηση της χρήσης του διαδικτύου, έχει οδηγήσει σε πολλές έρευνες με σκοπό τη καταγραφή και την ανάλυση των συνηθειών και προτιμήσεων των χρηστών του διαδικτύου. Στις αρχές του 2009, δημοσιεύτηκε ίσως η μεγαλύτερη on-line έρευνα<sup>105</sup> που διεξάγεται για πέμπτη συνεχή χρονιά στην Ελλάδα. Η e-metrics<sup>105</sup> έρευνα, που πραγματοποιήθηκε από την AGB Nielsen Media Research και την Phaistos Networks, υπό την αιγίδα του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας και με τη συνεργασία του IAB Hellas, φιλοξενήθηκε σε 97

διαδικτυακούς τόπους και συμπληρώθηκαν 21.221 ερωτηματολόγια παρέχοντας ιδιαίτερα χρήσιμες πληροφορίες για τη χρήση του Διαδικτύου.

Η Αξιολόγηση Ηλεκτρονικών Υπηρεσιών με εφαρμογές και έρευνες, όπως της e-metrics, πρέπει να λαμβάνονται σοβαρά υπόψη από τους επιχειρηματίες που θέλουν να δράσουν στο χώρο του διαδικτύου, αλλά και από τους κοινωνικούς φορείς και τους κρατικούς μηχανισμούς, οι οποίοι είναι αναγκαίο να διαμορφώσουν και να προσφέρουν ανάλογη εκπαίδευση, πόρους και νομικά πλαίσια μέσω των οποίων θα διανθίσουν οι νέες τεχνολογίες σε κάθε επιχειρηματικό και ψυχαγωγικό τομέα.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

1. <http://www-128.ibm.com/developerworks/webservices/newto/websvc.html> IBM (2007), “New to SOA and Web services”
2. <http://msdn2.microsoft.com/en-us/library/ms996507.aspx> MSDN (2001), “XML Web Services Basics”
3. <http://www.roseindia.net/webservices/webservices.shtml> Roseindia.net (2007), “Web Services”
4. Developer.com (2003), “Web Services Tutorial: Understanding XML and XML Schema”  
“Part 1” <http://www.developer.com/services/print.php/2195981>  
“Part 2” [http://www.developer.com/services/print.php/10928\\_2195981\\_2](http://www.developer.com/services/print.php/10928_2195981_2)
5. Developer.com (2002), “Introduction to Web Services”  
“Part 1” <http://www.developer.com/services/article.php/1485821>  
“Part..2Architecture” <http://www.developer.com/services/article.php/1495091>  
“Part 3: Understanding XML” <http://www.developer.com/services/article.php/1557871>
6. <http://www.onjava.com/lpt/a/1025> ONJava.com (2001), “Java and Web Services Primer”
7. Horton I. (2003) “Beginning Java 2” : Wrox
8. <http://www.w3schools.com/xml/default.asp> W3schools.com (2007), “XML Tutorial”
9. <http://www.w3.org/TR/wSDL> W3C (2001), “Web Service Definition Language (WSDL)”
10. <http://onjava.com/pub/a/onjava/2001/08/07/webservices.html> XML.com (by Al Saganich 08/07/2001), “A Web Services Primer”
11. [http://uddi.org/pubs/uddi\\_v3.htm](http://uddi.org/pubs/uddi_v3.htm) UDDI.org (2004), “UDDI Version 3.0.2”
12. W3C (2006), “SOAP Version 1.2”  
“Part 0: Primer” <http://www.w3.org/TR/2006/PER-soap12-part0-20061219/>  
Part 1: Messaging Framework” <http://www.w3.org/TR/soap12-part1/>  
Part 2: Adjuncts” <http://www.w3.org/TR/2003/REC-soap12-part2-20030624/>
13. Borgen B. (2001) “SOAP Programming with Java” : Sybex Inc
14. <http://www.w3schools.com/soap/default.asp> W3schools.com (2007), “SOAP Tutorial”
15. Newcomer E., Lomow G (2005) “Understanding SOA with Web Services” : Addison-Wesley Professional
16. Fremantle, P., Weerawarana, S., and Khalaf, R. Enterprise Services, Communications of the ACM, October 2002/Vol.45.No 10, pp.77-82.
17. <http://www.webserviceslist.com/> Εφαρμογές ηλεκτρονικών υπηρεσιών
18. [http://myweb.fsu.edu/chofacker/pubs/Hofacker\\_Goldsmith\\_Bridges\\_Swilley\\_2007.pdf](http://myweb.fsu.edu/chofacker/pubs/Hofacker_Goldsmith_Bridges_Swilley_2007.pdf) , C, Hofacker etc, Journal of Value Chain Management, 2007, e-services.
19. <http://www.disi.unige.it> , <http://www.disi.unige.it/person/ReggioG/ISII04WWW/WebServices.ppt> , C, Peraire and D Coleman, HP
20. An Overview of Standards and related technology in Web Services, A. Tsalgaidou, Th. Pilioura, Distributed and Parallel Databases, 2002
21. Understanding SOA with Web Services, Eric Newcomer, Greg Lomow, Addison Wesley Professional, 2004.
22. <http://www.xmethods.com/help/addspecs.html>
23. <http://www.richsolutions.com>
24. <http://www.redcoal.com>
25. <http://www.google.com/apis>

26. <http://www.freshscore.com/>
27. <http://schemas.xmlsoap.org/soap/encoding/>
28. <http://javascript.internet.com/>
29. <http://www.microsoft.com/net/>
30. <http://www.acunetix.com/websitesecurity/xss.htm>
31. <http://msdn.microsoft.com/en-us/library/ms161953.aspx>
32. [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci549024,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html)
33. <http://www.ibm.com/developerworks/xml/library/x-transws/>
34. <http://www.go-online.gr/rss.xml>
35. <http://www.naftemporiki.gr/news/rss.asp>
36. [http://www.mycrypto.net/encryption/crypto\\_algorithms.html](http://www.mycrypto.net/encryption/crypto_algorithms.html), Encryption Algorithms
37. Σύγχρονη Κρυπτογραφία, Δρ. Ε. Μάγκος Κέρκυρα, 2009
38. Tanenbaum A., Δίκτυα Υπολογιστών, Εκδόσεις Κλειδάριθμος, 2003
39. <http://www.us-cert.gov/cas/tips/ST04-015.html>
40. Forouzan B., Introduction to Data Communications and Networking, McGraw-Hill, 2003.
41. <http://www.eeci.gr>
42. <http://www.faqs.org/faqs/firewalls-faq/>
43. Article: Security, privacy, and confidentiality issues on the Internet, Grant Kelly, Bruce McKenzie at <http://www.jmir.org/>
44. <http://technet.microsoft.com/en-us/library/bb727017.aspx>
45. [http://articles.techrepublic.com.com/5100-22\\_11-5756029.html](http://articles.techrepublic.com.com/5100-22_11-5756029.html)
46. Animesh Pacha, Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061, USA, 8 June, 2006.
47. Διπλωματικές Εργασίες: “Μελέτη των επιθέσεων που στηρίζονται σε πακέτα με ψευδή IP διεύθυνση αποστολέα (IP spoofing)” του Ιωάννου Παπαπάνου και “ISLAB HACK: Βασικές Έννοιες & Προγραμματισμός του SNORT 2.0” του Δημήτρη Πρίτσου. (<http://www.islab.demokritos.gr>)
48. Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, Rafeeq Ur Rehman ([www.phptr.com](http://www.phptr.com)) - To open source and free software developers, 2003 Pearson Education, Inc.
49. Εργασία IDS – Intrusion Detection Systems στο μάθημα «Ασφάλεια Δικτυοκεντρικών Συστημάτων» του Τμήματος: Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς. Υπεύθυνος Καθηγητής: Σωκράτης Κάτσικας, Παρουσίαση: Πλακογιάννης Φωτίου Πέτρος, Λέων Χρήστος, Μενδρινός Ιωάννης.
50. S. Kumar, E.H. Spafford, An application of pattern matching in intrusion detection, The COAST Project, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA, Technical Report CSD-TR-94-013, June 17, 1994.
51. A. Pacha, J.-M. Park, Detecting denial-of-service attacks with incomplete audit data, in: Proceedings of the 14th International Conference on Computer Communications and Networks, San Diego, CA, USA, 2005.
52. D. Newman, J. Snyder, R. Thayer, Crying wolf: False alarms hide attacks, in: Network World: Network World, 2002.

53. T. Ptacek, T. Newsham, Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, Secure Networks Inc, 1998.
54. A. Liu, C. Martin, T. Hetherington, S. Matzner, A comparison of system call feature representations for insider threat detection, in: Proceedings of the 6th Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, West Point, NY, 2005.
55. [http://www.iso.org/iso/support/faqs/faqs\\_widely\\_used\\_standards/widely\\_used\\_standards\\_other/information\\_security.htm](http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm)
56. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities - By Mark Dowd, John McDonald, Justin Schuh
57. <http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=103>
58. <http://www.ca.com/us/configuration-management.aspx>
59. <http://www.crhc.illinois.edu/DEPEND/>
60. <http://www.oas.org/legal/english/admmem/admmem90.htm>
61. <http://www.itl.nist.gov/lab/bulletns/bltnsep01.htm>
62. <http://www.itsecurity.com/features/it-security-audit-010407/>
63. [http://www.infosecinstitute.com/blog/ethical\\_hacking\\_computer\\_forensics.html](http://www.infosecinstitute.com/blog/ethical_hacking_computer_forensics.html)
64. <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16696&TEMPLAT E=/ContentManagement/ContentDisplay.cfm>
65. <http://e-articles.info/t/i/1627/l/gr/>
66. <http://www.bluewavemag.com/blueart37.htm>  
Joseph M. Juran.
67. [http://en.wikipedia.org/wiki/Philip\\_B.\\_Crosby](http://en.wikipedia.org/wiki/Philip_B._Crosby)  
Philip\_B.\_Crosby.
68. [http://en.wikipedia.org/wiki/W.\\_Edwards\\_Deming](http://en.wikipedia.org/wiki/W._Edwards_Deming)  
W. Edwards Deming.
69. <http://www.iso.org/iso/home.htm>  
Το πρότυπο ISO8402-1986.
70. <http://dis.shef.ac.uk/sheila/marketing/services.htm>
71. Zeithaml, Parasuraman & Berry, "Delivering Quality Service; Balancing Customer Perceptions and Expectations," Free Press, 1990.
72. <http://www.netmba.com/marketing/mix/>
73. Francis Buttle, 1996, "SERVQUAL: review, critique, research agenda," European Journal of Marketing, Vol.30, Issue 1, pp.8-31.
74. <http://www.scribd.com/doc/25356471/Servqual-Model>
75. <http://www.proserv.nu/Docs/Servqual.pdf>
76. <http://en.wikipedia.org/wiki/SERVQUAL>
77. Assessing Call Centre Quality using the SERVQUAL Model Warren J S Staples & Prof. John F Dalrymple Centre for Management Quality Research, RMIT University, Australia.
78. Garvin D.A., (1998), «Managing Quality».
79. Information System Architecture Metrics: An Enterprise Engineering Evaluation Approach André Vasconcelos, Pedro Sousa, José Tribolet CEO - Centro de Engenharia Organizacional, INESC – Instituto de Engenharia de Sistemas e Computadores and Department of Information Systems and Computer Engineering, Instituto Superior Técnico, Technical University of Lisbon, Portugal.

80. “Strategies for Information Technology Governance”, Wim Van Grembergen (Ed), Idea.Group Publishing, ISBN 1-59140-140-2, Chapter IX, pp. 216-244, 2003. Technical Issues Related to IT Governance Tactics: Product Metrics, Measurements and Process Control.
81. Web Metrics October 26, 2006 Steven Schwartz President, PowerWebResults.com Southeastern Massachusetts E-Commerce Network University of Massachusetts – Dartmouth.
82. Web Content Managers Forum, 2005.
83. Using Web Analytics for Website Optimization Presented to the Webmaster’s Guild by Adrienne Buskard, President Mercury Web Solutions October 6, 2006.
84. Issue Paper for Bundaberg Hospital Commission of Inquiry Safety and Quality, July 2005.
85. <http://www.iso.org>
86. <http://www.iec.ch>
87. <http://www.ws-i.org>
88. <http://xml.coverpages.org/WS-I-Profiles-ISO.html>
89. <http://www.webtrends.com>
90. <http://www.webtrends.com/Products.aspx>
91. WEBTRENDS e-business intelligence solutions from NetIQ WeTrends Analysis Series, (WebTrends Analysis Suite are trademarks of Net IQ Corporation. WebTrends is a registered trademark of NetIQ Corporation 2001).
92. [http://www.stereaellada.gr/per\\_perifereia.htm](http://www.stereaellada.gr/per_perifereia.htm)  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Στερεάς Ελλάδας.
93. <http://www.notioaigaio.gr/site.asp>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Νοτίου Αιγαίου.
94. <http://www.thessalia.gr/pep/default.el.asp>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Θεσσαλίας.
95. <http://www.pepba.gr>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Βορείου Αιγαίου.
96. [http://www.peproe.gr/index\\_pep.html](http://www.peproe.gr/index_pep.html)  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Ηπείρου.
97. <http://www.pepdym.gr>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Δυτικής Μακεδονίας.
98. <http://www.pepionia.gr>  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Ιονίων Νήσων.
99. [http://www.dyτικιellada.gr/per\\_perifereia.htm](http://www.dyтикиellada.gr/per_perifereia.htm)  
Ιστοσελίδα Περιφερειακού Επιχειρησιακού Προγράμματος Δυτικής Ελλάδας.
100. Επιχειρησιακή Στατιστική, Λευτέρης Ι. Θαλασσινός, Αθήνα – Πειραιάς 1996.
101. <http://www.spss.gr>
102. <http://www.spss.com/>
103. <http://en.wikipedia.org/wiki/SPSS>
104. <http://www.ibm.com/gr/el/>
105. <http://www.e-metrics.gr>