Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών : *Πληροφοριακά και Επικοινωνιακά Συστήματα*

Μεταπτυχιακή Διατριβή

Διερεύνηση ρυθμιστικών πλαισίων και απαιτήσεων των ζητημάτων ασφάλειας στο υπολογιστικό νέφος (Cloud).

Σκανδάλης Ιωάννης

Επιβλέπων Καθηγητής
Δρ. Μιχάλης Γεωργιάδης

Μάιος 2016

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών : *Πληροφοριακά και Επικοινωνιακά Συστήματα*

Μεταπτυχιακή Διατριβή

Διερεύνηση ρυθμιστικών πλαισίων και απαιτήσεων των ζητημάτων ασφάλειας στο υπολογιστικό νέφος (cloud).

Ιωάννης Σκανδάλης

Επιβλέπων Καθηγητής
Μιχάλης Γεωργιάδης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
Στα Πληροφοριακά Συστήματα
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2016

Περίληψη

Ο χώρος του cloud computing αποτελεί μία ιδιαίτερα ανερχόμενη τεχνολογία που φιλοδοξεί να κυριαρχήσει στο χώρο της πληροφορικής και να αντικαταστήσει τις παραδοσιακές μεθόδους μεταφοράς και αποθήκευσης των δεδομένων. Σε συνδυασμό με τα παραπάνω, παρέχει μία πληθώρα υπηρεσιών στο χρήστη που του προσφέρουν αφενός ευκολία και αφετέρου ταχύτητα στο χώρο του διαδικτύου. Ασφαλώς τα πλεονεκτήματα που εισάγονται από τη χρήση της τεχνολογίας αυτής είναι μοναδικά, την ίδια στιγμή όμως εισέρχεται και ένας αριθμός μειονεκτημάτων που αφορά κυρίως στην ασφάλεια των δεδομένων καθώς αυτά ταξιδεύουν στο διαδίκτυο αλλά και αποθηκεύονται σε διαφορετικές τοποθεσία ανά τον κόσμο.

Η Ευρωπαϊκή Ένωση, αλλά και μία σειρά φορέων που εδρεύουν στην Ευρώπη έχουν θεσπίσει νόμους οδηγίες και πολιτικές που αφορούν στη διασφάλιση των δεδομένων προσωπικού χαρακτήρα για το χρήστη αλλά και στην παροχή της βέλτιστης υπηρεσίας προς αυτόν.

Η παρούσα διπλωματική εργασία κάνει μία βιβλιογραφική αναφορά στο χώρο του cloud computing προσπαθώντας να εξηγήσει το χρήστη τον τρόπο λειτουργίας της τεχνολογίας αυτής. Παράλληλα, κάνει μία ενδελεχή μελέτη αλλά και μία εκτενή παρουσίαση των οδηγιών που έχουν θεσπιστεί από την Ευρωπαϊκή Ένωση, ώστε ο χρήστης να είναι σε θέσει να κατανοήσει αλλά και να αναγνωρίσει πλήρως τα δικαιώματά του σε ότι αφορά στην προστασία των προσωπικών του δεδομένων. Μετά από μία σύντομη αναφορά που γίνεται στους νόμους που έχουν θεσπιστεί από τα Ευρωπαϊκά κράτη, δίνεται ιδιαίτερη έμφαση στην ελληνική νομοθεσία ενώ προτείνονται οι τρόποι και τα μέτρα που πρέπει αυτή να υιοθετήσει ώστε να προωθηθεί η τεχνολογία αυτή στη χώρα αλλά και να αναβαθμιστεί το επίπεδο των διαδικτυακών υπηρεσιών.

Summary

The emerging technology of cloud computing aims to dominate the field of information technology and replace traditional data transfer and storage methods. The benefits introduced by this technology are unique, and most of the times include simplicity and speed in the services offered via internet.

On the other hand, there are some serious disadvantages that raise concern over the integrity and the security of the data while being transmitted over the internet or stored in various servers all over the world. Trying to face these issues, the European Union published some rules and guidelines related to the safeguarding of personal data.

This thesis makes a brief reference to the field of cloud computing, trying to explain to the reader the operation of this technology. Furthermore, it makes a comprehensive presentation of the directives adopted by the European Union, so that the reader shall be able to understand and to fully recognize his rights regarding the protection of his personal data. In addition, special emphasis is given to the Greek legislation and are proposed measures that should be adopted in order to promote this technology to the country and raise the level of web services offered.

Ευχαριστίες

Στα πλαίσια της εκπαίδευσής μου, μέσω του μεταπτυχιακού προγράμματος σπουδών στα «Πληροφοριακά και Επικοινωνιακά Συστήματα» στο ανοιχτό Πανεπιστήμιο της Κύπρου , μου ανατέθηκε να διεκπεραιώσω την παρούσα διατριβή. Κατά τη διάρκεια εκπόνησής της, καθοριστική ήταν η βοήθεια του επιβλέποντα καθηγητή μου κ. Μιχάλη Γεωργιάδη, ο οποίος συνέβαλε κατά το μέγιστο δυνατό στην ανάπτυξή της. Τον ευχαριστώ για την υποστήριξή του και την πολύτιμη βοήθειά του.

Στο τέλος άφησα την αναφορά στην πολύτιμη βοήθεια που μου προσέφεραν κάποιοι άνθρωποι που δεν ανήκουν στην ακαδημαϊκή ή εργασιακή κοινότητα, αλλά των οποίων η βοήθεια και κυρίως η συμπαράσταση ήταν πολύτιμη. Αναφέρομαι στους γονείς μου Γιώργο και Παναγιώτα, καθώς και στη γυναίκα μου Δήμητρα, οι οποίοι μου συμπαραστάθηκαν καθ' όλη τη διάρκεια όχι μόνο της εκπόνησης αυτής της διατριβής, αλλά και των προηγούμενων ετών των σπουδών μου. Η ευγνωμοσύνη που τους οφείλω δεν είναι δυνατόν να περιγραφεί με λόγια.

Περιεχόμενα

Κεφάλαιο 1
Το Νέφος (Cloud)

1.1 Η έλευση του νέφους

Ο αυξημένος βαθμός συνδεσιμότητας αλλά και ο αυξημένος όγκος των δεδομένων οδήγησε πολλούς παρόχους, ιδιαίτερα αυτούς που δραστηριοποιούνται στον τομέα της διαχείρισης των δεδομένων, στην ανάπτυξη μεγαλύτερων αρχιτεκτονικών και υποδομών με δυνατότητες δυναμικής διαχείρισης του φόρτου και ταυτόχρονης πρόσβασης στα δεδομένα για όλους τους χρήστες (1). Ο διαμοιρασμός των δεδομένων αλλά και η αναπαραγωγή αυτών σε διάφορους servers, κατόπιν ανάλογης ζήτησης, βελτίωσε σημαντικά την χρήση των διαθέσιμων πόρων καθώς μείωσε των αριθμό των δεδομένων που πρέπει αυτοί να διαχειρίζονται. Την ίδια στιγμή, οι hosts των web servers απέκτησαν τη δυνατότητα αναπαραγωγής εικόνων από πελάτες που αιτήθηκαν συγκεκριμένο βαθμό πρόσβασης σε αυτούς και δρομολογούν αιτήματα προκαλώντας φόρτο στο δίκτυο (2).

Ό όρος υπολογιστικό νέφος χρησιμοποιήθηκε για πρώτη φορά και συνδέθηκε με τις διάφορες ελαστικές δομές και με την πρόσβαση μετά από απαίτηση στις IT πηγές από τη στιγμή που η εταιρία Amazon διέθεσε τους εσωτερικούς της πόρους αλλά και τους μηχανισμούς διαχείρισης αυτών προς όφελος και χρήση των πελατών της (3). Από τότε, πολλοί από τους παρόχους μετέτρεψαν τις δομές τους σε νέφη, παρόλο που αυτό σε πρώτη φάση είχε κάποιες αρνητικές συνέπειες στον τρόπο με τον οποίο πρόσφερα τις υπηρεσίες τους.

Στο σημείο αυτό θα πρέπει να τονιστεί ότι ο όρος νέφος χρησιμοποιήθηκε για πρώτη φορά στη δεκαετία του 1990 και αναφέρεται στη δυναμική δρομολόγηση της κίνησης σε τηλεπικοινωνιακά δίκτυα ώστε να εξισορροπηθεί η χρήση των δικτύων αυτών αλλά και

να οπτικοποιηθεί η εσωτερική δομή τους χωρίς ο τελικός χρήστης να γνωρίζει τα κανάλια από τα οποία δρομολογείται η κίνηση (4).

Η εταιρία Microsoft, χρησιμοποίησε τον όρο αυτό το 2001, σε μία παρουσίασή της για το .NET framework, με στόχο να επεξηγήσει πλήρως στο κοινό την εσωτερική δομή των υπολογιστών που απαρτίζουν το διαδίκτυο. Σύμφωνα με την ηλεκτρονική εγκυκλοπαίδεια Wikipedia, η ιδέα του υπολογιστικού νέφους παρουσιάστηκε για πρώτη φορά σε μία δημόσια ομιλία του John McCarthy το 1961 όπου προέβλεψε ότι ο διαμοιρασμός του χρόνου στους υπολογιστές θα αποτελέσει τη βάση για το μελλοντικό διαμοιρασμό των πηγών και των εφαρμογών (5). Έτσι λοιπόν, τόσο η ιδέα όσο και η τεχνολογική εξέλιξη που βρίσκεται πίσω από το υπολογιστικό νέφος δε μπορεί σε καμία περίπτωση να θεωρηθεί καινοτομία, καθώς συγκεκριμένα κέντρα δεδομένων χρησιμοποιούσαν ήδη της λειτουργίες και της μεθόδους αυτές για να επιτύχουν κλιμάκωση, να προσφέρουν αξιοπιστία και να διασφαλίσουν την προσβασιμότητα στα δεδομένα τους.

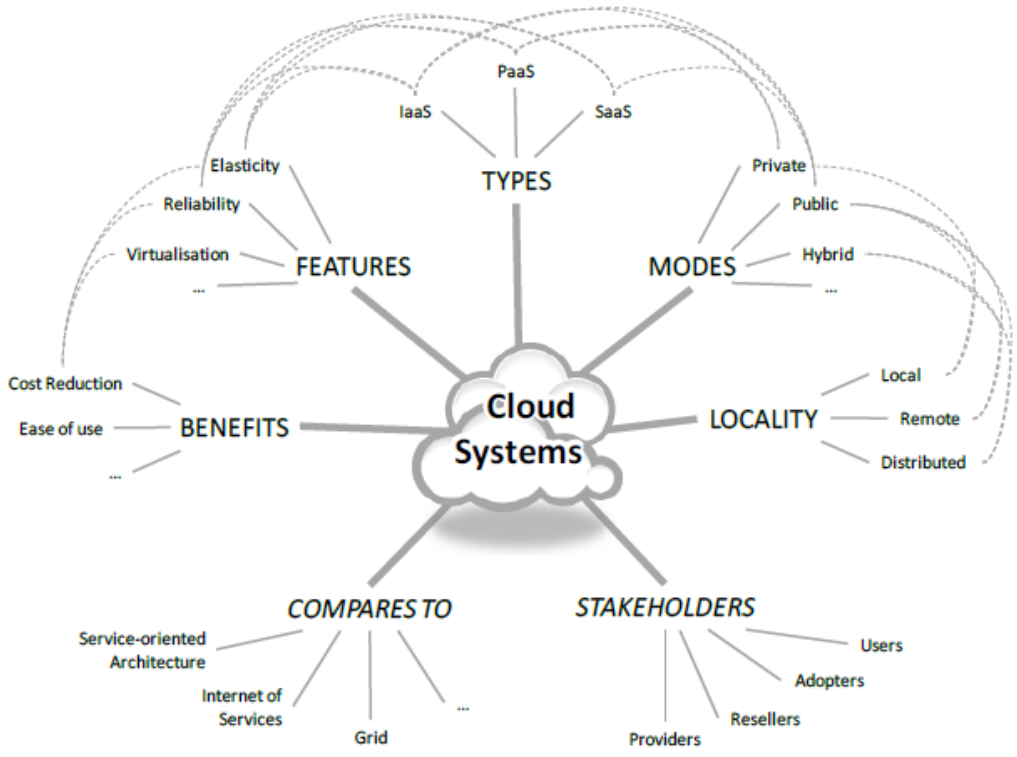

Figure 1 : Μέρη που απαρτίζουν ένα υπολογιστικό σύστημα

Το πέρασμα λοιπόν των ετών αλλά και η εξέλιξη της τεχνολογίας έφερε στο προσκήνιο πλέον πολλούς παρόχους υπολογιστικών νεφών, και όπως είναι αναμενόμενο, ο όρος

συνδέθηκε με πολλές και διαφορετικές ερμηνείες. Οι πλέον αντιπροσωπευτικοί τομείς νεφών συνοψίζονται στις παρακάτω περιοχές (2) :

1. Κέντρα δεδομένων που προσπαθούν να εξασφαλίσουν τη κλιμάκωση αλλά και να αυξήσουν τη διαθεσιμότητά τους
2. Αυτοματοποιημένοι Web Servers
3. Μηχανισμοί και αρχιτεκτονικές εντός των εταιριών που έχουν ως στόχο την εξισορρόπηση στη διάθεση των πηγών της εταιρίας ώστε να προσφέρουν επιχειρηματικές λύσεις
4. Εξωτερικές τύπου ASAP εφαρμογές

Στο σημείο αυτό θα πρέπει να καταστεί σαφές ότι όρος νέφη δεν αναφέρεται σε συγκριμένες τεχνολογίες ή σε συγκεκριμένα framework αλλά σε ένα σύνολο συνδυασμένων τεχνολογιών. Μάλιστα πολλές φορές οι αρχιτεκτονικές πλέγματος αλλά και οι SOA (Service Oriented Architectures) συγχέονται και θεωρούνται όμοιες με αυτές τις αρχιτεκτονικές των Clouds (6). Αντίστοιχα, οι πάροχοι νεφών σήμερα, λειτουργούν με βάση την υπάρχουσα εμπορική τεχνολογία αλλά και τις δικές τους προτεινόμενες λύσεις και έτσι έως και σήμερα έχει γίνει σχετικά μικρή προσπάθεια προς τη δημιουργία ενός γενικότερου framework που θα υποστηρίζει όλα εκείνα τα χαρακτηριστικά που θα συνδέονται με το cloud.

Το 2004 χρησιμοποιήθηκε για πρώτη φορά ο επεξεργαστής πολλαπλών πυρήνων όταν η εταιρία Intel αποφάσισε να αντικαταστήσει την παραγωγή των επεξεργαστών 4GHz και να στρέψει τη γραμμή παραγωγής της προς αυτή την κατεύθυνση (6). Ένας μεγάλος αριθμός προγραμματιστών αλλά και χρηστών ξεκίνησε να ερευνά τα πλεονεκτήματα αλλά και τα προβλήματα που εγείρονται από την προσέγγιση αυτή αλλά και την κλιμάκωση που μπορεί να επέλθει, τόσο οριζόντια όσο και κάθετα. Αναμένεται ότι στο μέλλον τα υπολογιστικά νέφη θα κερδίσουν ακόμη περισσότερο έδαφος καθώς θα προσφέρουν έναν ιδιαίτερα σημαντικό αριθμό δυνατοτήτων αλλά και υπηρεσιών που σε καμία περίπτωση δεν ήταν διαθέσιμες έως σήμερα.

Έως τώρα προσπάθησαν να δοθούν διάφοροι ορισμοί αλλά και υιοθετήθηκαν πολλές και διαφορετικές προσεγγίσεις σχετικά με το τι είναι τα υπολογιστικά νέφη ή απλώς νέφη. Με μία ευρύτερη έννοια, ένα υπολογιστικό νέφος θα μπορούσε να θεωρηθεί, μία πλατφόρμα η οποία επιτρέπει εκτελέσεις διαφόρων μορφών κατά μήκος διαφόρων

πηγών. Φυσικά και υπάρχουν διαφορετικοί τύποι νεφών οι οποίοι έχουν ως κοινό χαρακτηριστικό το γεγονός ότι ενισχύουν τις πηγές αλλά και τις υπηρεσίες που προκύπτουν από αυτές με δυνατότητες που σχετίζονται με τη διαχειρισιμότητα, την ελαστικότητα αλλά κα την ανεξαρτησία των διαφόρων πλατφορμών (1). Πιο συγκεκριμένα, ένα νέφος, είναι μία πλατφόρμα ή μία δομή που επιτρέπει την εκτέλεση κώδικα σε μία διαχειρίσιμη και ελαστική μορφή. Ο όρος διαχειρίσιμη αφορά κυρίως στην αξιοπιστία που οφείλει να προσφέρεται αυτοματοποιημένα ενώ ο όρος ελαστικότητα στις διαθέσιμες πηγές που πρέπει να χρησιμοποιηθούν ανάλογα με τις τρέχουσες απαιτήσεις.

Τα μελλοντικά συστήματα υπολογιστικών νεφών θα πρέπει να είναι σε θέση να διατηρούν ένα προκαθορισμένο επίπεδο ποιότητας αλλά και να επιτρέπουν την ενσωμάτωση διαφόρων πηγών εντός των οργανωτικών τους δομών. Οι διαφορετικοί τρόποι ανάπτυξης των υπολογιστικών νεφών, διαφέρουν ελάχιστα και κυρίως ως προς τον τρόπο με τον οποίο αναπτύσσονται. Από τη στιγμή που αυτά σχετίζονται άμεσα με θέματα χρήσης και όχι με τις διαφορετικές τεχνολογίες, χρησιμοποιούνται ευρέως και βρίσκουν εφαρμογή και σε πολλούς και διαφορετικούς τομείς.

Για τους παραπάνω λόγους λοιπόν, θα πρέπει να διαχωριστούν οι διαφορετικοί τύποι νεφών αλλά και τα διάφορες δυνατότητες που προκύπτουν από την κάθε κατηγορία. Ο πλέον γνωστός διαχωρισμός του υπολογιστικού νέφους γίνεται στις παρακάτω τρεις κατηγορίες (7) :

1. Λογισμικό ως Υπηρεσία (Software as a Service - SaaS)
2. Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS)
3. Υποδομή ως Υπηρεσία (Infrastructure as a Service - IaaS)

Το **SaaS** αποτελεί το μοντέλο εκείνο κατά το οποίο ο πάροχος του νέφους παρέχει πρόσβαση που έχουν ήδη αναπτυχθεί μέσα στη δική του υποδομή. Οι εφαρμογές αυτές είναι συνήθως διαθέσιμες διαμέσου των διεπαφών του διαδικτύου και καλύπτουν ένα ευρύ φάσμα συσκευών όπως οι προσωπικοί υπολογιστές, τα tablets, τα smartphones και πολλές άλλες φορητές συσκευές. Ο χρήστης ασφαλώς και δεν μπορεί σε καμία περίπτωση να επηρεάσει το διαδίκτυο, τους διακομιστές, τα λειτουργικά συστήματα ή τους αποθηκευτικούς χώρους και στις περισσότερες περιπτώσεις δεν έχει καθόλου (ή έχει περιορισμένο) έλεγχο πάνω στην ίδια την εφαρμογή (7).

Το **PaaS** αποτελεί ένα μοντέλο το οποίο βασίζεται την παροχή εκ μέρους του παρόχου προς τους χρήστες δυνατοτήτων ανάπτυξης των προσωπικών τους εφαρμογών μέσα στα πλαίσια των δομών του υπολογιστικού νέφους. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει το υφιστάμενο δίκτυο, τους διακομιστές, τα λειτουργικά συστήματα ή τους αποθηκευτικούς χώρους, αλλά μπορεί να ελέγξει τις ίδιες τις εφαρμογές και σε μερικές περιπτώσεις το περιβάλλον των εφαρμογών (7).

Τέλος, το **IaaS** είναι το μοντέλο εκείνο με βάση το οποίο ο πάροχος δίνει την δυνατότητα επεξεργασίας, αποθήκευσης, δικτύων και άλλων βασικών υπολογιστικών πόρων απευθείας στον χρήστη ο οποίος αναπτύσσει και «τρέχει» το δικό του λογισμικό που περιλαμβάνει λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει την υφιστάμενη υποδομή του νέφους αλλά ελέγχει τα λειτουργικά συστήματα, την αποθήκευση, τις εφαρμογές ανάπτυξης και πιθανώς ελέγχει σε μικρότερο βαθμό κάποια στοιχεία όπως το τείχος προστασίας και την εξισορρόπηση φόρτου (7).

Η αρχιτεκτονική πάνω στην οποία βασίζεται το υπολογιστικό νέφος είναι γενικευμένη, δεν περιγράφει κάποιο συγκεκριμένο μοντέλο υλοποίησης και έχει κυρίως ως στόχο να δείξει ποιοι παράγοντες διαδραματίζουν ρόλο στα υπολογιστικά νέφη αλλά και ποιες είναι οι δραστηριότητες που εκτελούν οι παράγοντες αυτοί.

Ξεκινώντας λοιπόν από τον πελάτη του υπολογιστικού νέφους, θα μπορούσε κανείς να υποστηρίξει ότι αυτός αποτελεί τον τελικό χρήστη των υπηρεσιών του νέφους. Επικοινωνεί, με τον πάροχο και επιλέγει τις υπηρεσίες εκείνες που θα του παρέχονται. Οι χρήστες του μοντέλου Saas, μπορούν να είναι ακόμη και οργανισμοί οι οποίοι θα προσφέρουν στα μέλη τους πρόσβαση σε διάφορες εφαρμογές, απευθείας χρήση αυτών, ή ακόμη και διαχείρισή τους (2). Στο μοντέλο PaaS, η ομάδα αυτή χρηστών θα είναι σε θέση να αναπτύξει διάφορα εργαλεία αλλά και να χρησιμοποιήσει τους πόρους του νέφους ώστε να αναπτύξει, να δοκιμάσει, να επεξεργαστεί και να διαχειριστεί τις διάφορες εφαρμογές που φιλοξενούνται σε ένα τέτοιο περιβάλλον. Οι χρήστες αυτοί μπορούν φυσικά να ανήκουν στην κατηγορία των προγραμματιστών οι οποίοι δημιουργούν εφαρμογές που τρέχουν σε τέτοια περιβάλλοντα και έχουν εξουσιοδοτημένα δικαιώματα ώστε να τις δοκιμάζουν σε ένα τέτοιο περιβάλλον. Ακόλουθα, στη μερίδα των πελατών του IaaS συγκαταλέγονται διαχειριστές πληροφοριακών συστημάτων που ενδιαφέρονται για την δημιουργία, εγκατάσταση,

διαχείριση και παρακολούθηση των υπηρεσιών για την λειτουργία της υποδομής των πληροφοριακών συστημάτων (1). Η μερίδα αυτή των χρηστών, έχει άμεση πρόσβαση στους υπολογιστικούς πόρους και χρεώνεται σύμφωνα με τον όγκο ή την διάρκεια των πόρων που κατανάλωσε.

Πέραν του παραπάνω διαχωρισμού, καθίσταται δυνατή η ανάπτυξη των υπολογιστικών νεφών σε διαφορετικές μορφές ώστε ο διαχωρισμός αυτών να γίνει με βάση τον τρόπο με τον οποίο χρησιμοποιούνται.

Η έως τώρα τάση σε ότι αφορά στα υπολογιστικά νέφη περιοριζόταν σε εσωτερικές λύσεις που καθιστούν εύκολη τη διαχείριση των υποδομών αλλά και τον αριθμό των αιτημάτων τίθενται. Το παραπάνω, προκύπτει κυρίως από το γεγονός ότι οι πρώτες εφαρμογές νεφών δημιουργήθηκαν με στόχο την εσωτερική διαχείριση των ιδιοτήτων αυτών και δεν είχαν ως στόχο την πώληση των υπηρεσιών.

Στη σημερινή εποχή, όπου οι πάροχοι πλέον παρουσιάζουν ιδιαίτερα αυξημένη εμπιστοσύνη στα χαρακτηριστικά των νεφών τα οποία προωθούν προς κατανάλωση, έχουν προκύψει ακόμη και υβριδικές λύσεις. Η «μεταφορά» όπως θα μπορούσε κανείς να χαρακτηρίσει τη μετάβαση από τον ιδιωτικό προς το δημόσιο τομέα, και η παροχή συνδυασμένων λύσεων συχνά χαρακτηρίζεται ως μία φυσική μετάβαση των συστημάτων αυτών καθώς πλέον δεν υπάρχει κανένας απολύτως λόγος που να περιορίζει τους παρόχους από το να προσφέρουν υπηρεσίες αυτού του είδους.

Έτσι λοιπόν, αναπτύχθηκαν λύσεις που ανήκουν στους παρακάτω τομείς (7) :

- Ιδιωτικά νέφη : Πρόκειται για νέφη που ανήκουν κυρίως σε εταιρίες ή μισθώνονται από αυτές. Οι λειτουργίες τους δεν είναι πλήρως εκτεθειμένες στον πελάτη παρόλο που σε κάποιες περιπτώσεις κάποιες από τις υπηρεσίες που χρησιμοποιούν μπορεί να αφορούν σε αυτούς. Χαρακτηριστικό παράδειγμα της κατηγορίας αυτής αποτελεί το πολύ γνωστό σε όλους E-Bay.
- Δημόσια νέφη : Οι εταιρίες μπορούν να χρησιμοποιήσουν τις λειτουργίες των νεφών με στόχο να προσφέρουν τις υπηρεσίες τους σε χρήστες που βρίσκονται εκτός αυτών. Η παροχή της δυνατότητας στο χρήστη να χρησιμοποιεί τα χαρακτηριστικά των νεφών για τους δικούς του προσωπικούς λόγους δίνει ταυτόχρονα τη δυνατότητα στις επιχειρήσεις να αναθέσουν τις υπηρεσίες τους στους παρόχους τον νεφών και έτσι να μειώσουν τόσο το κόστος όσο και την

προσπάθεια που απαιτείται για τη δημιουργία ίδιας υποδομής. Χαρακτηριστικό παράδειγμα της κατηγορίας αυτής αποτελούν η Amazon, τα Google Apps και το Windows Azure.

- Υβριδικά νέφη : Παρόλο που τα δημόσια νέφη δίνουν τη δυνατότητα στις επιχειρήσεις να αναθέσουν μέρος της υποδομής τους στους παρόχους νεφών, δυστυχώς την ίδια στιγμή, δημιουργούν σχετικές απώλειες σε ότι αφορά στον έλεγχο των πηγών αλλά και στην κατανομή και τη διαχείριση των δεδομένων και του κώδικα γεγονός το οποίο πολλές φορές δεν είναι επιθυμητό. Τα υβριδικά νέφη, αποτελούνται από μία μικτή αρχιτεκτονική που περιλαμβάνει δομές τόσο δημόσιων όσο και ιδιωτικών νεφών με στόχο την μέγιστη μείωση του κόστους διαμέσου του outsourcing αλλά και το βέλτιστο επίπεδο ελέγχου σε ότι αφορά τα δεδομένα που χρησιμοποιούνται από τα τοπικά νέφη. Ο αριθμός των υβριδικών νεφών που χρησιμοποιείται σήμερα είναι περιορισμένος παρόλα αυτά εταιρίες όπως η IBM και η Jupiter έχουν αρχίσει να κινούνται προς την κατεύθυνση αυτή.
- Κοινοτικά νέφη : Τις περισσότερες φορές, τα νέφη, περιορίζονται από τις τοπικές υποδομές. Έτσι παρόλο που κάποιος πάροχος μπορεί ουσιαστικά να πουλήσει την υποδομή του σε κάποιον άλλο πάροχο, τα νέφη δυστυχώς δεν έχουν τη δυνατότητα να συναθροίζονται ώστε να αναπτύξουν νέες και πιο ισχυρές υποδομής. Τα κοινοτικά νέφη, θα έχουν την δυνατότητα είτε να συναθροίζουν τα δημόσια νέφη, είτε να συναθροίζουν συγκεκριμένες υποδομές. Για το λόγο αυτό, αποτελούν ακόμη και σήμερα έναν στόχο της τεχνολογίας παρόλο που έχουν τεθεί οι πρώτες βάσεις για τη δημιουργία τους.
- Νέφη ειδικών σκοπών : Ειδικότερα στην περίπτωση των IaaS νεφών που προέρχονται από κέντρα δεδομένων και έχουν έναν «γενικότερο σκοπό», τα νέφη αυτά μπορούν να χρησιμοποιηθούν σύμφωνα με τις δυνατότητές τους ώστε να εξυπηρετήσουν συγκεκριμένες περιπτώσεις χρήστης ή τύπους χρηστών. Αντίθετα τα PaaS νέφη, τείνουν να παρέχουν λειτουργίες πιο εξειδικευμένες, γεγονός που σημαίνει ότι χρησιμοποιούν συγκεκριμένες μεθόδους για κάθε περίπτωση και ότι η υποδομή των δεδομένων αλλά και οι διεπαφές που χρησιμοποιούνται είναι συγκεκριμένες για κάθε πελάτη. Εξειδικευμένες λειτουργίες παρέχονται από εταιρίες όπως η Google όπου παρέχει συγκεκριμένες δυνατότητες που αφορούν στην διαχείριση των αρχείων. Αναμένεται από τα

μελλοντικά συστήματα ότι αυτά θα προσφέρουν ακόμη πιο ισχυρές δυνατότητες ώστε να προσελκύσουν συγκεκριμένους χρήστες και να ξεπεράσουν τον ανταγωνισμό που καθημερινά προκύπτει. Τα νέφη ειδικού σκοπού, αποτελούν υπολογιστικά συστήματα νεφών τα οποία παρέχουν επιπλέον ιδιότητες. Η βάση της ανάπτυξης των συστημάτων αυτών είναι προφανής.

1.2 Αρχιτεκτονική του Cloud Computing

Το Cloud Computing αποτελεί μία φυσική επέκταση πολλών σχεδιαστικών αρχών, πρωτοκόλλων, αλλά και συστημάτων που έχουν αναπτυχθεί τα τελευταία 20 χρόνια. Όπως είναι αντιληπτό, ο όρος περιλαμβάνει και πολλές νέες ιδιότητες οι οποίες έχουν ενσωματωθεί στη στοίβα των εφαρμογών και είναι υπεύθυνες για την κλιμάκωση, τον προγραμματισμό και την οπτικοποίηση των πηγών. Μία από τις ιδιότητες που ουσιαστικά διαφοροποιούν το Cloud Computing από οποιαδήποτε άλλη εφαρμογή είναι και αυτή της συνθεσιμότητας (7). Ο όρος αυτός, αναφέρεται στην ιδιότητα της δημιουργίας εφαρμογών από μέρη διαφόρων στοιχείων.

Μία πλατφόρμα, είναι μία υπηρεσία του Cloud Computing που αφορά τόσο στο υλικό όσο και στο λογισμικό και χρησιμοποιείται για τη δημιουργία πιο σύνθετού λογισμικού. Χαρακτηριστικό παράδειγμα των πλατφορμών αυτών είναι οι εικονικές συσκευές που έχουν καταστεί πλέον ως ένα ιδιαίτερα σημαντικό αντικείμενο σε ότι αφορά στην ανάπτυξη Cloud Computing εφαρμογών.

Η λειτουργία του Cloud Computing απαιτεί όπως είναι αντιληπτό, την ύπαρξη διαφόρων πρωτοκόλλων, ώστε το υλικό, το λογισμικό αλλά και οι διάφοροι clients να μπορούν να επικοινωνούν μεταξύ τους (8). Πολλά από αυτά τα πρωτόκολλα, είναι τα παραδοσιακά πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο ενώ την ίδια στιγμή χρησιμοποιείται ένας άλλος, ιδιαίτερα μεγάλος αριθμός πρωτοκόλλων που έχει ως στόχο τη διαχείριση των διαδικασιών που εμπεριέχονται στην επικοινωνία. Τα πλέον γνωστά πρωτόκολλα, όπως είναι το SOAP (Simple Object Access Protocol), κάνουν χρήση της XML ενώ κάποια άλλα που δραστηριοποιούνται στον τομέα της εύρεσης και της περιγραφής των υπηρεσιών χρησιμοποιούν την WSDL (Web Services Description Language) (3).

Το Cloud Computing βασίζεται στην αρχιτεκτονική με την οποία λειτουργούν τα μεγάλα κατανεμημένα δίκτυα πάνω από το διαδίκτυο τα 20 τελευταία χρόνια. Στα παραπάνω λοιπόν, ήδη χρησιμοποιούμενα πρωτόκολλα δικτύωσης, το Cloud Computing προσθέτει τα μοναδικά πλεονεκτήματα των εικονικών συστημάτων, τα οποία έγιναν ιδιαίτερα διάσημα τα τελευταία δέκα χρόνια. Το cloud δημιουργεί ένα σύστημα τέτοιο στο οποίο οι πηγές μπορούν να δεσμευθούν και να χρησιμοποιηθούν ακριβώς όπως απαιτείται. Η αρχιτεκτονική του μπορεί να υποστηρίξει λογισμικά που συνδυάζονται μεταξύ τους και εκτελούνται σε εικονικό υλικό έτσι να προσφέρει υπηρεσία κατ απαίτηση στο χρήστη που θέλει να διαχειριστεί το υλικό και το λογισμικό. Πρόκειται για έναν μοναδικό συνδυασμό αφαιρετικότητας και ταυτόχρονα συνένωσης υπηρεσιών που διαχωρίζει την αρχιτεκτονική των Cloud Computing συστημάτων από αυτή που συναντάται συχνά σε διαδικτυακές εφαρμογές ν-επιπέδων (9).

Οι περισσότερες εφαρμογές που αφορούν στην αρχιτεκτονική του Cloud Computing το διαχωρίζουν σε δύο αρχιτεκτονικά επίπεδα (9):

1. Στο Front End (Client)
2. Στο Back End (Cloud)

Πρόκειται για μία ιδιαίτερα απλοποιημένη βέβαια περιγραφή καθώς τα δύο αυτά επίπεδα αποτελούνται από πολλά και διαφορετικά άλλα επίπεδα που έχουν τελείως διαφορετικές λειτουργίες και εκτελούνται ως μία μίξη σταθερών και εμπορικών πρωτοκόλλων. Το Cloud Computing, διαφοροποιείται κατά πολύ από τα διάφορα παλαιότερα μοντέλο καθώς αυτό περιέχει εμφωλευμένη πληροφορία που ελέγχεται από ένα Application Programming Interface (API), κα προσφέρει διαφοροποιημένη υπηρεσία στο σύνολο του δικτύου (2).

Οι εφαρμογές που δημιουργούνται στο cloud, έχουν συχνά την ιδιότητα να δημιουργούνται από μία συλλογή στοιχείων, η οποία παραπάνω αναφέρθηκε και ως η λειτουργία της συνθεσιμότητας. Ένα σύστημα λοιπόν που μπορεί να συντεθεί χρησιμοποιεί στοιχεία τα οποία εμφωλεύουν υπηρεσίες που μπορούν να τροποποιηθούν ώστε να εξυπηρετήσουν συγκεκριμένους σκοπούς. Κάθε στοιχείο που συντίθεται θα πρέπει να είναι (2):

- Ευέλικτο ώστε να μπορεί να λειτουργεί ως μία ανεξάρτητα μονάδα που θα συνεργάζεται, θα επαναχρησιμοποιείται και θα αντικαθίσταται

- Σταθερό ώστε να μπορεί να εκτελεί όλες τις συναλλαγές χωρίς επιπλέον αιτήματα

Παρόλο που το Cloud Computing δεν απαιτεί τόσο το υλικό όσο και το λογισμικό να έχουν την ικανότητα να συντίθενται, είναι ένα χαρακτηριστικό στο οποίο βασίζονται οι προγραμματιστές, καθώς κάνει το σύστημα ευκολότερο στη διαχείριση, στην εφαρμογή λύσεων, στη φορητότητα και στη διαλειτουργικότητα (3). Την ίδια στιγμή, παρατηρείται η τάση, τα συστήματα αυτά να έχουν όλο και λιγότερο την ιδιότητα της συνθεσιμότητας σε ότι αφορά τους χρήστες, καθώς οι υπηρεσίες ενσωματώνονται πλέον όλο και περισσότερο στις στοίβες του Cloud Computing (5).

Η ιδέα της συνθεσιμότητας, εξαλείφεται καθώς ανεβαίνει κανείς στις στοίβες του Cloud Computing τουλάχιστον σε ότι αφορά στο χρήστη. Στην περίπτωση όμως των SaaS & PaaS παρόχων αυτή εξακολουθεί να παραμένει ένα αρκετά σημαντικό συγκριτικό πλεονέκτημα. Οι Saas και PaaS πάροχοι λαμβάνουν από ένα σύστημα που έχει την ιδιότητα της συνθεσιμότητας πλεονεκτήματα όπως (7):

- Ευκολία στη σύγκλιση των συστημάτων
- Φθηνότερη ανάπτυξη συστημάτων
- Αξιόπιστη λειτουργία
- Μεγαλύτερο αριθμό ικανών developers
- Μεθοδολογία λογικού σχεδιασμού

Όπως μπορεί κανείς πλέον να αντιληφθεί, η τάση πίσω από το σχεδιασμό συστημάτων που θα έχουν την ιδιότητα της συνθεσιμότητας ελλοχεύετε στη διάδοση και την αφομοίωση της αρχιτεκτονικής SOA (Service Oriented Architecture) που είναι εστιασμένη στην υπηρεσία. Βασικό στοιχείο της SOA αρχιτεκτονικής είναι το γεγονός ότι οι υπηρεσίες χτίζονται από ένα σύνολο στοιχείων που χρησιμοποιούν συγκεκριμένες διεπαφές επικοινωνιών και υπηρεσίας (7). Αυτό το οποίο δεν έχει διευκρινιστεί για τα ίδια τα στοιχεία των εφαρμογών είναι ότι αυτά μπορούν να γραφούν σε οποιαδήποτε προγραμματιστική γλώσσα και με όποιο τρόπο επιθυμεί ο προγραμματιστής.

1.3 Υποδομή

Οι μεγαλύτερες υποδομές όπως η υπηρεσία IaaS, βασίζονται κυρίως στην τεχνολογία των εικονικών μηχανών ώστε να κατορθώσουν να υλοποιήσουν του servers που θα

εκτελούν τις εφαρμογές. Οι εικονικοί αυτοί severs, έχουν πολλές φορές χαρακτηριστικά τα οποία είναι αντίστοιχα των πραγματικών servers και περιέχουν ένα συγκεκριμένο αριθμό κύκλων για το μικροεπεξεργαστή, πρόσβαση στη μνήμη αλλά και εύρος δικτύου για τους πελάτες. Το λογισμικό το οποίο εκτελείται στις εικονικές μηχανές, είναι και αυτό το οποίο καθορίζει τη χρησιμότητα του συστήματος του Cloud Computing (7).

Η ιδέα του εικονικού server εισάγει ένα νέο και ευρύ πεδίο και για τον προγραμματιστή καθώς αυτός μπορεί πλέον να εισάγει έναν νέο τρόπο σκέψης στη δημιουργία των προγραμμάτων του (7). Για παράδειγμα, η δημιουργία ενός λογισμικού από έναν προγραμματιστή ενδεχόμενα να απαιτεί παράλληλη εκτέλεση λειτουργιών και έτσι να απαιτείται η συγγραφή κώδικα που θα διαχειρίζεται την εκτέλεση επιπλέον νημάτων τα οποία θα πρέπει και αυτά με τη σειρά τους να είναι εύκολα διαχειρίσιμα από την εφαρμογή. Η χρήση των υπηρεσιών του cloud κατά τη δημιουργία του προγράμματος αυτού αντιμετωπίζει το παραπάνω πρόβλημα καθώς ο προγραμματιστής πλέον μπορεί να χρησιμοποιήσει τις κατάλληλες υπηρεσίες έτσι ώστε η εφαρμογή από μόνη της να προβαίνει σε κλιμάκωση της εκτέλεσης του προγράμματος (10).

Εικάζεται ότι για τις μελλοντικές εφαρμογές, οι προγραμματιστές θα πρέπει εξισορροπούν τις αρχιτεκτονικές ανάγκες των προγραμμάτων τους ώστε οι εφαρμογές τους να παράγουν νέα threads όπου απαιτείται ή να δημιουργούν νέες εικονικές μηχανές. Ακόμη, οι εφαρμογές θα πρέπει να κάνουν αποτελεσματική διαχείριση των πηγών του cloud, να προβαίνουν σε κλιμάκωση όταν απαιτείται και να μην επεκτείνουν τη χρήση του cloud σε περιπτώσεις όπου αυτό δεν είναι αναγκαίο (10).

Το παραπάνω, εισάγει έναν νέο τρόπο σκέψης σε ότι αφορά στην ανάπτυξη των εφαρμογών αλλά και στην ικανότητα αυτές να προβαίνουν σε κλιμάκωση μόνο όταν απαιτείται. Ο τρόπος σκέψης αυτός, θα πρέπει να κυριαρχεί στην εφαρμογή σε όλα τα επίπεδα της δημιουργίας της.

Κεφάλαιο 2
Νέφος-Επικοινωνία

2.1 Πλατφόρμες

Στον τομέα του cloud, μία πλατφόρμα είναι ένα λογισμικό το οποίο χρησιμοποιείται ώστε να δημιουργηθούν υψηλότερα επίπεδα υπηρεσίας. Σήμερα, χρησιμοποιούνται πολλές και διαφορετικές πλατφόρμες, οι πλέον γνωστές όπως είναι (1):

- Salesforce.com's Force.com Platform
- Windows Azure Platform
- Google Apps και Google AppEngine

Οι τρεις αυτές υπηρεσίες, προσφέρουν όλο το υλικό αλλά και το λογισμικό που χρειάζεται ώστε να δημιουργηθούν και αναπτυχθούν διαδικτυακές εφαρμογές ή υπηρεσίες που είναι προσαρμοσμένες στις ανάγκες του προγραμματιστή και μέσα στα πλαίσια πάντα τα οποία η πλατφόρμα επιτρέπει.

Οι πλατφόρμες, αναπαριστούν ουσιαστικά των σύνολο των στοιβών του cloud, με μόνη που απουσιάζει αυτή της παρουσίασης που ουσιαστικά αφορά στη διεπαφή του χρήστη. Αυτό λοιπόν το οποίο ουσιαστικά διαχωρίζει μία πλατφόρμα από μία εικονική συσκευή εντοπίζεται στο λογισμικό που έχει εγκατασταθεί σε αυτήν το οποίο αποτελείται από στοιχεία και υπηρεσίες που ελέγχονται από ένα API (1). Το παραπάνω βασίζεται κυρίως στο γεγονός ότι οι διάφοροι πάροχοι συστημάτων επιθυμούν τα περιβάλλοντα ανάπτυξης που διανέμουν για το cloud να χρησιμοποιούν τις ίδια τεχνολογίες. Οι πλατφόρμες συνήθως συνοδεύονται από εργαλεία και λειτουργίες που βοηθούν στο σχεδιασμό και την ανάπτυξη των εφαρμογών. Έτσι λοιπόν, ανάλογα με τον πάροχο, εντοπίζονται εργαλεία τα οποία βοηθούν σημαντικά στη συνεργασία, στον έλεγχο, στην απόδοση, στις υπηρεσίες Web, στη δημιουργία βάσεων, αλλά και στην αποθήκευση.

Ως εικονική συσκευή χαρακτηρίζεται το λογισμικό το οποίο εγκαθίσταται ως middleware σε μία εικονική μηχανή και εμφανίζεται στο cloud διαμέσου ενός API (1). Οι χρήστες, έχουν τη δυνατότητα να αλληλεπιδράσουν με την πλατφόρμα, να χρησιμοποιήσουν υπηρεσίες διαμέσου του API και να αφήσουν την πλατφόρμα να προβεί μόνη της σε κλιμάκωση της υπηρεσίας. Πολλές από τις πλατφόρμες, προσφέρουν εργαλεία ανάπτυξης διεπαφών χρήστη που βασίζονται στην HTML, στη Javascript και σε πολλές άλλες τεχνολογίες. Έτσι λοιπόν, καθώς ο ιστός εστιάζει όλο και περισσότερο στα πολυμέσα, πολλοί προγραμματιστές, έχουν επιλέξει να εργάζονται σε περιβάλλοντα όπως το Adobe Flash, το Flex, το Air, ή σε εναλλακτικές πλατφόρμες όπως Windows Silverlight (1).

2.2 Πρωτόκολλα Επικοινωνίας

Το Cloud Computing βασίζεται σε υπηρεσίες οι οποίες είναι διαθέσιμες στο διαδίκτυο και επικοινωνούν μεταξύ τους κάνοντας χρήση συγκεκριμένων πρωτοκόλλων διαδικτύου τα οποία υπάγονται στα HTTP και HTTPS πρωτόκολλα μεταφοράς (11). Τα υπόλοιπα πρωτόκολλα και πρότυπα τα οποία ασχολούνται με τους υπολογισμούς και τις πηγές των δεδομένων στο cloud, είτε διαμορφώνουν τα δεδομένα αυτά είτε διαχωρίζουν τα πακέτα επικοινωνίας που αποστέλλονται πάνω από το δίκτυο διαμέσου των πρωτοκόλλων μεταφοράς.

Με στόχο την καλύτερη υπηρεσία σε ότι αφορά στην επικοινωνία client/server, δημιουργήθηκαν τα περασμένα χρόνια αρκετά πρωτόκολλα επικοινωνίας. Διάφορες μορφές υλοποιήσεων PRC (Remote Procedure Call) όπως το Corba, το Java RMI και το DCOM, προσπάθησαν να επιλύσουν τα προβλήματα της δέσμευσης υπηρεσιών και της διαχείρισης συναλλαγών πάνω από το δίκτυο (11).

Καθώς η δημοτικότητα του διαδικτύου ανέβαινε σημαντικά τα τελευταία χρόνια έγιναν ακόμη εντατικότερες οι προσπάθειες βελτίωσης των υπηρεσιών και διαχείρισης των πηγών. Ιδιαίτερα γνωστή προσπάθεια είναι αυτή της δημιουργίας του πρωτοκόλλου SOAP (Simple Object Access Protocol) το οποίο ουσιαστικά αντικαθιστά το XML-RPC. Το SOAP χρησιμοποιεί την XML για τα μηνύματα και τα RPC και HTTP για τη μετάδοσή τους.

Αποτελεί τη βάση των στοιβών πάνω στις οποίες δομούνται οι διαδικτυακές υπηρεσίες σήμερα (10).

Εάν κανείς εξετάσει ένα XML αρχείο που χρησιμοποιείται σε μία SOAP συναλλαγή, θα διαπιστώσει ότι, περιέχει το ίδιο το μήνυμα αλλά και τις κατάλληλες οδηγίες για τον τρόπο που θα χρησιμοποιηθεί αυτό. Το κάθε μήνυμα, περιέχει ένα σύνολο κανόνων που μεταφράζονται σε στιγμιότυπα και τύπους δεδομένων ενώ την ίδια στιγμή καθορίζει τις μεθόδους που πρέπει να χρησιμοποιηθούν ώστε να εκκινήσουν οι κλήσεις αλλά και να υπάρξουν αποκρίσεις (10).

Η εξέλιξη τω τεχνολογιών έφερε τη δημιουργία προτύπων που βασίζονταν σε υπηρεσίες ιστού. Το πλέον γνωστό μοντέλο σε ότι αφορά τα μηνύματα SOAP είναι το WSDL (Web Services Description Language). Το WSDL αφορά σε μία συλλογή τελικών σημείων ή σε θύρες που συνδέονται με συγκεκριμένες διευθύνσεις διαδικτύου και παρέχουν υπηρεσία χρησιμοποιώντας XML μηνύματα (7). Στο πρότυπο αυτό, κάθε υπηρεσία εκτελεί ένα σύνολο λειτουργιών που αφορούν σε πρωτόκολλα διαδικτύου.

Με κοινή χρήση του WSDL αλλά και του SOAP έχει δημιουργηθεί ένας αριθμός επεκτάσεων που επιτρέπει σε διάφορες υπηρεσίες διαδικτύου να περιγράψουν το σύνολο των ιδιοτήτων και των μεθόδων που μπορούν να προσφέρουν. Οι επεκτάσεις αυτές φέρουν τα χαρακτηριστικά γράμματα WS και κάποιες από αυτές είναι (12):

- WS-Διευθυνσιοδότηση
- WS-Ανακάλυψη
- WS-Δημιουργία Σύνδεσης
- WS-Δημιουργία μηνυμάτων
- WS-Ανταλλαγή Metadata
- WS-Ενημέρωση
- WS-Πολιτική
- WS-Διαχείριση Πηγών
- WS-Ασφάλεια
- WS-Μεταφορά
- WS-Εμπιστοσύνη

Κάθε μία από τις παραπάνω WS ιδιότητες αποτελεί και μία διαφορετική κατάσταση ανάπτυξης. Οι WS υπηρεσίες, μεταφέρονται με XML μηνύματα κάνοντας χρήση του

κινητού server εφαρμογών του SOAP πρωτοκόλλου με τρόπους οι οποίοι αυξάνουν διαρκώς την πολυπλοκότητά τους (12).

Καθώς το SOAP αλλά και οι WS υπηρεσίες εξελισσόταν, τα πρωτόκολλα ξεκίνησαν να κάνουν χρήση και άλλων τεχνολογιών. Έτσι λοιπόν, δημιουργήθηκε η ανάγκη της ύπαρξης μίας μεθόδου που θα προτυποποιούσε τη διαχείριση των πηγών στο διαδίκτυο, και εισήχθηκε η ιδέα του REST. Το REST (Representational State Transfer) προσθέτει έναν παγκόσμιο identifier σε κάθε πηγή έτσι ώστε να υπάρχει μία ενιαία μέθοδος πρόσβασης σε αυτήν.

Και ενώ φυσικά το REST χρησιμοποιείται ευρέως, δεν είναι το μοναδικό πρότυπο ανταλλαγής δεδομένα στις υπηρεσίες Cloud. Ιδιαίτερα γνωστό είναι το Atom το οποίο αποτελεί μία μορφή syndication που επιτρέπει στα HTTP πρωτόκολλα να δημιουργούν και να ενημερώνουν τακτικά την πληροφορία.

2.3 Σύνδεση με το Cloud

Οι Clients μπορούν να συνδεθούν με μία υπηρεσία Cloud με πολλούς και διαφορετικούς τρόπους. Οι δύο γνωστότεροι αυτών είναι (12):

- Ένας φυλλομετρητής
- Μία εμπορική εφαρμογή

Οι παραπάνω εφαρμογές, μπορούν να συνδεθούν με μία Cloud υπηρεσία και να εκτελούνται σε έναν sever, σε μία κινητή συσκευή ή σε ένα κινητό τηλέφωνο. Το κοινό χαρακτηριστικό των συσκευών αυτών είναι ότι ανταλλάσσουν δεδομένα πάνω από ένα όχι και τόσο ασφαλές μέσο. Έτσι, προτάθηκαν τρεις βασικοί τρόποι ασφαλούς σύνδεσης (12) :

- Χρήση ενός ασφαλούς πρωτοκόλλου μεταφορά δεδομένων όπως είναι τα SSL (HTTPS), FTPS, ή IPsec, ή διασύνδεση διαμέσου ενός ασφαλούς shell όπως είναι το SSH
- Δημιουργία μιας εικονικής σύνδεσης με χρήση ενός εικονικού ιδιωτικού δικτύου VPN ή διαμέσου ενός ασφαλούς πρωτοκόλλου μεταφοράς όπως τα Microsoft RDP και Citrix ICA, όπου τα δεδομένα προστατεύονται από έναν μηχανισμό tunnelling

- ☞ Κρυπτογράφηση των δεδομένων έτσι ώστε ακόμη και εάν αυτά κλαπούν να μην μπορεί κανείς να τα αναγνώσει

Πολλές από τις συνδέσεις client, χρησιμοποιούν δύο ή και περισσότερες τεχνικές ώστε να συνδεθούν με το cloud. Στην ήδη υπάρχουσα τεχνολογία, οι clients εμπιστεύονται τις υπηρεσίες διαδικτύου και θεωρούν ότι αυτές δημιουργούν ασφαλείς συνδέσεις, στο μέλλον όμως αναμένεται ότι οι clients, θα δρουν από μόνοι τους επιλέγοντας τον ασφαλή τρόπο σύνδεσης που επιθυμούν.

Κεφάλαιο 3
Cloud Computing

3.1 Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής σχετικά με το Cloud Computing

Η εν λόγω επιτροπή, βασιζόμενη πάντα στην ψηφιακή σύγκλιση «Ευρώπη 2020» ασχολήθηκε εντατικά με το θέμα του cloud computing καθώς αναγνώρισε ότι αυτή η πολλά υποσχόμενη εφαρμογή της πληροφορικής κυριάρχησε σε πολλούς και διαφορετικούς τομείς. Στα πλαίσια λοιπόν της ενασχόλησής της αυτής με την τεχνολογία του cloud computing συνέταξε μία γνωμοδότηση ο οποία έχει ως στόχο , να συγκεντρώσει και να διαδώσει τις πρακτικές εμπειρίες τόσο των φορέων που εκπροσωπούνται στην ΕΟΚΕ όσο και της αγοράς αλλά και να διατυπώσει σειρά συστάσεων για να ενθαρρύνει την Ευρώπη να ηγηθεί μέσω πρωτοπόρων επιχειρήσεων σε αυτόν τον πολλά υποσχόμενο τομέα.

Το cloud computing αποτελεί μία ιδιαίτερα ενδιαφέρουσα ψηφιακή αρχιτεκτονική η οποία παρουσιάζει μοναδικά πλεονεκτήματα και υποστηρίζει το παρακάτω πολλά υποσχόμενο οικονομικό πρότυπο (13):

- **Μεγάλος αριθμός δυνητικών χρηστών**: ιδιώτες, επιχειρήσεις, δημόσιες υπηρεσίες κλπ.·
- **Κοινή διαθεσιμότητα** των μέσων και των εργαλείων πληροφορικής, που οδηγεί στη βελτιστοποίηση της χρήσης τους·
- **Διασφάλιση της κινητικότητας**, ώστε ιδιαίτερα οι χρήστες που μετακινούνται συχνά να έχουν ανά πάσα στιγμή πρόσβαση στα δεδομένα τους·

- Απλή, ευέλικτη και διαφανή **ενσωμάτωση** διάφορων τεχνικών στοιχείων όπως Διαδίκτυο, υπηρεσίες διαχείρισης συστημάτων πληροφορικής, κινητές εφαρμογές κλπ.·
- **Χαμηλό κόστος λειτουργίας** καθ' όλη τη διάρκεια ζωής των συστημάτων πληροφορικής, χωρίς υψηλή αρχική επένδυση·
- **Επικέντρωση** των επιχειρήσεων στη βασική τους δραστηριότητα, χωρίς να χρειάζεται να ασχοληθούν με πολύπλοκα συστήματα πληροφορικής·
- Δυνατότητες **ανάπτυξης** μέσω νέων δραστηριοτήτων για σημαντικούς παράγοντες του τομέα, συντονιστές συστημάτων, εκδότες λογισμικών κλπ.

Βέβαια, ένα τέτοιο πρότυπο, καθώς βρίσκεται ακόμη σε φάση ανάπτυξης παρουσιάζει όπως είναι αναμενόμενο και κάποιες αδυναμίες. Σε αυτές συγκαταλέγονται (13) :

- Ο πολύ μεγάλος αριθμός κανόνων για τη ρύθμιση και τον έλεγχο της χρήσης του cloud computing
- Η απουσία αναγνωρίσιμης ευρωπαϊκής **αρχής εποπτείας** της εφαρμογής αυτών των κανόνων·
- Η ακόμη ανεπαρκής εμπειρία των χρηστών και ιδιαίτερα των ιδιωτών, ώστε να μπορούν να αξιολογήσουν σωστά τα **προβαλλόμενα πλεονεκτήματα** και προπαντός τους **ελλοχεύοντες κινδύνους·**
- Ο εγγενώς **ευάλωτος χαρακτήρας** του Διαδικτύου: διακοπή σε περίπτωση βλάβης, κυβερνοεπιθέσεις κλπ.·
- Ο **κορεσμός του Διαδικτύου**: μειωμένη ταχύτητα, μεγάλη αύξηση του όγκου των ανταλλασσόμενων περιεχομένων (αρχεία ήχου, βίντεο, ανεπιθύμητα ηλεκτρονικά μηνύματα/spam), περιορισμοί του συστήματος διευθυνσιοδότησης (IP)·
- Ο **κορεσμός των εξυπηρετητών**: η κοινή διαθεσιμότητα των εξυπηρετητών, με αποτέλεσμα υπεράριθμες συνδέσεις, μπορεί να προκαλέσει συμφόρηση του συστήματος·
- Οι κίνδυνοι που συνεπάγεται η **μεταφορά** δεδομένων ή εφαρμογών **σε τρίτους**·
- Οι κίνδυνοι που συνεπάγεται η **μεταφορά** δεδομένων και εφαρμογών **σε άλλη χώρα** με διαφορετική νομοθεσία·

- Οι κίνδυνοι κοινωνικού χαρακτήρα που συνεπάγεται η συγκέντρωση των δραστηριοτήτων ανάπτυξης, φιλοξενίας και υποστήριξης·
- Τα δικαιώματα και οι υποχρεώσεις τόσο των χρηστών όσο και των παρόχων υπηρεσιών cloud computing παραμένουν αδιευκρίνιστα·
- Η ασαφής διάκριση ανάμεσα στον υπεύθυνο επεξεργασίας και σε αυτόν που εκτελεί την επεξεργασία των προσωπικών δεδομένων·
- Για όσους δεν κατέχουν εξειδικευμένες γνώσεις, οι συμβάσεις παροχής αυτών των υπηρεσιών είναι πολύπλοκες και συχνά δυσνόητες όσον αφορά τη συλλογή, την επεξεργασία, τη μεταφορά των δεδομένων των καταναλωτών καθώς και τα δικαιώματά τους, σύμφωνα με τη νομοθεσία.

Η υλοποίηση του cloud computing γίνεται από συνδυασμό πολλών και διαφορετικών τεχνολογιών και άρα σε κάθε περίπτωση αυτό συμμερίζεται τόσο τα πλεονεκτήματα όσο και τις αδυναμίες που φέρουν οι τεχνολογίες αυτές (14). Βασικά χαρακτηριστικά τα οποία διέπουν το cloud computing και προέρχονται από τις τεχνολογίες που αυτό χρησιμοποιεί είναι η προστασία των δεδομένων προσωπικού χαρακτήρα, τα συστήματα τηλεπικοινωνιών, το διαδίκτυο, η προστασία των χρηστών αλλά και το internet of things.

Η Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής κα Neelie Kroes παρουσιάστη στις 27 Ιανουαρίου 2011 στο Νταβός, τα πλαίσια του παγκόσμιου οικονομικού φόρουμ το εξής όραμα για το cloud computing (13):

«Όσον αφορά το υπολογιστικό νέφος, νομίζω ότι δεν μπορούμε να περιμένουμε έναν παγκοσμίως αναγνωρισμένο ορισμό. Πρέπει να αναλάβουμε δράση (…). Όπως προβλέπεται και στο Ψηφιακό Θεματολόγιο για την Ευρώπη, ξεκίνησα ήδη τη χάραξη μιας πανευρωπαϊκής στρατηγικής για το υπολογιστικό νέφος, η οποία υπερβαίνει τα όρια ενός απλού πολιτικού πλαισίου. Δεν αρκούμαι στη δημιουργία μίας Ευρώπης που να διατίθεται θετικά προς το νέφος («cloud-friendly»), αλλά θέλω μία Ευρώπη που να συμμετέχει ενεργά στον τομέα αυτόν («cloud-active»).»

Τα κυριότερα χαρακτηριστικά του cloud computing είναι (13):

- **Αποϋλοποίηση:** η διάρθρωση, ο τόπος εγκατάστασης και η συντήρηση αυτών των υπηρεσιών πληροφορικής τους πρέπει να είναι όσο το δυνατόν πιο αόρατες για τους χρήστες, είτε για ιδιώτες πρόκειται είτε για επιχειρήσεις.
- **Ευκολία πρόσβασης:** εφόσον διαθέτουν σύνδεση στο Διαδίκτυο, οι χρήστες έχουν πρόσβαση στα δεδομένα και στις εφαρμογές τους από οποιονδήποτε τόπο και από οποιαδήποτε συσκευή, είτε πρόκειται για προσωπικό υπολογιστή, επιπαλάμιο (ταμπλέτα) ή έξυπνο τηλέφωνο (smartphone).
- **Κλιμακωσιμότητα:** ο προμηθευτής προσαρμόζει σε πραγματικό χρόνο την υπολογιστική ισχύ στις ανάγκες του εκάστοτε χρήστη. Αυτό σημαίνει ότι ο χρήστης θα μπορεί να καλύπτει τις ανάγκες του ακόμη και σε περίοδο αιχμής, χωρίς να πρέπει να επενδύσει σε εξοπλισμό πληροφορικής που θα χρησιμοποιεί ελάχιστα ανάμεσα σε δύο περιόδους αιχμής.
- **Κοινή χρήση:** η κλιμακωσιμότητα είναι εφικτή επειδή ο πάροχος θέτει τα εργαλεία πληροφορικής στη διάθεση πολλών χρηστών ταυτόχρονα. Η πρακτική αυτή επιτρέπει τη μέγιστη και καλύτερη δυνατή αξιοποίηση τεράστιων πάρκων εξυπηρετητών με πολλές χιλιάδες ηλεκτρονικούς υπολογιστές.
- **Τιμολόγηση ανάλογη με τη χρήση:** ο χρήστης καταβάλλει μόνον το ποσό που αντιστοιχεί στις υπηρεσίες που χρησιμοποίησε πραγματικά, ανάλογα με τις ανάγκες του σε υπολογιστική ισχύ. Οι συμβάσεις cloud computing είναι συχνά ακόμη εξατομικευμένες, αλλά τείνουν ολοένα και περισσότερο προς την τυποποίηση.

Αρχικά, το cloud computing είχε χρησιμοποιηθεί για απλές εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο, σιγά σιγά όμως, οι εφαρμογές γύρω από αυτό αλλά και η χρήση τους αναπτύχθηκαν ραγδαίως. Μάλιστα, παρατηρείται ότι πλέον αυτό χρησιμοποιείται εντός των επιχειρήσεων ως ένα εργαλείο ανάπτυξης της ευελιξίας αλλά και τις παραγωγικότητας της επιχείρησης. Ειδικότερα, διαμέσου της χρήσης του cloud computing η επιχείρηση κατορθώνει να εστιάσει πλέον στη βασική της δραστηριότητα χωρίς να παρεκκλίνει στο ελάχιστο από αυτή (14). Ακόμη, η συνεργασία με κάποιον εξειδικευμένο πάροχο, σημαίνει ταυτόχρονα, καλύτερη ποιότητα στην υπηρεσία αλλά και γνωμοδότηση από εξειδικευμένο προσωπικό που απασχολείται αποκλειστικά στον τομέα αυτό και έχει συγκεκριμένες γνώσεις. Σύμφωνα με μία πρόσφατη μελέτη, το 70% του κόστους της μονάδας

πληροφορικής μίας επιχείρησης οφείλεται στη διαχείριση υφιστάμενων εφαρμογών (13). Αν ανατεθεί μέρος αυτών των δραστηριοτήτων σε εξωτερικούς παρόχους υπηρεσιών, θα μπορεί η μονάδα αυτή να αφιερώσει χρόνο και ενέργεια στην καινοτομία και στην ανάπτυξη νέων υπηρεσιών.

Ως **πλεονεκτήματα** αναφέρονται συχνά από τις ίδιες τις επιχειρήσεις τα ακόλουθα (13):

- **Χαμηλότερο ύψος αρχικής επένδυσης:** για τις νέες ψηφιακές λύσεις, η καθιέρωση ή η επέκταση ενός συστήματος πληροφορικής δεν συνεπάγεται πλέον σημαντικές επενδύσεις σε αίθουσες μηχανημάτων, εξυπηρετητές, λογισμικά, κατάρτιση στην εφαρμογή λογισμικών συγκεκριμένου παραγωγού κλπ.
- **Ταχύτερη αξιοποίηση και διαθεσιμότητα:** το αρμόδιο για την ανάπτυξη προσωπικό μπορεί να επικεντρωθεί στα ειδικά θέματα της επιχείρησης χωρίς να ασχολείται και με θέματα τεχνικών υποδομών, τα οποία αναλαμβάνει ο πάροχος των υπηρεσιών cloud computing. Υλικοί και ανθρώπινοι πόροι διατίθενται με ευέλικτο τρόπο, ανάλογα με τις εκάστοτε ανάγκες.
- **Λογιστική ταξινόμηση και μείωση του κόστους:** με το cloud computing, οι δαπάνες πληροφορικής εντάσσονται στο μεταβλητό κόστος λειτουργίας και όχι στο πάγιο κόστος της επιχείρησης.
  Το κόστος συντήρησης απορρέει από τη συμφωνία μισθώσεως, στην οποία συμπεριλαμβάνονται υπηρεσίες όπως η περιοδική και διαφανής ενημέρωση του λογισμικού ή του υλικού και η άμεση, επιγραμμική τεχνική υποστήριξη για την επίλυση προβλημάτων από τον παραγωγό του λογισμικού ή τον κατασκευαστή του υλικού.
- **Ενίσχυση του προτύπου παροχής υπηρεσιών:** επειδή η μονάδα πληροφορικής μιας επιχείρησης μπορεί να βασιστεί στις δεσμεύσεις που έχει αναλάβει ο πάροχος cloud computing όσον αφορά την ποιότητα, τη διαθεσιμότητα, την ασφάλεια και την εξέλιξη των συστημάτων, έχει τη δυνατότητα να προσφέρει εντός της επιχείρησης υπηρεσίες βάσει Συμφωνιών περί του Επιπέδου Εξυπηρέτησης (Service Level Agreements)

- **Κινητικότητα του προσωπικού:** το cloud computing διασφαλίζει σε όλους τους υπαλλήλους μιας επιχείρησης, διακινούμενους και μη, ποιοτική και εύκολη πρόσβαση στα δεδομένα.

Οι πάροχοι των υπηρεσιών του cloud computing οφείλουν να παρουσιάσουν μία σειρά ολοκληρωμένων λύσεων για τους πελάτες τους σε συνδυασμό πάντα με την εγκατάσταση αλλά και τη συντήρηση των συστημάτων αυτών. Το κατάλληλα καταρτισμένο προσωπικό τους, αλλά και ικανότητα αυτού να προσαρμόζεται στις απαιτήσεις τους πελάτη, καθιστά τις εταιρίες αυτές να διαδραματίζουν έναν ιδιαίτερα σημαντικό ρόλο στον τομέα της πληροφορικής (15).

Η ραγδαία εξέλιξη στο χώρο των τεχνολογιών οδήγησε με τη σειρά της σε ραγδαία αύξηση της παραγωγικότητας, χωρίς όμως να στερεί από το χώρο της πληροφορικής ούτε τον όγκο της εξέλιξης ούτε το σημαντικό αριθμό των ανθρώπων που εργάζονται σε αυτή. Αντίθετα, ο χώρος της πληροφορικής εξελίσσεται συνεχώς ενώ σε αυτόν εισάγονται σε καθημερινή βάση πολλά και νέα συστήματα. Ως ένα σύστημα πληροφορικής, αντιμετωπίζεται και το cloud computing, το οποίο αναμένεται να δημιουργήσει νέα και μεγάλα πεδία δράσεις για τις επιχειρήσεις του χώρου (15). Μεγάλες εταιρίες του χώρου όπως η Microsoft, η Google, η Oracle, επενδύουν τεράστια ποσά στο χώρο αυτό ώστε να παράγουν νέα προϊόντα που θα ανταποκρίνονται στην αγορά του cloud computing και να προσαρμόσουν τα ήδη υπάρχοντά τους σε αυτή. Για παράδειγμα, η εφαρμογή Office 365 της Microsoft διαφέρει ριζικά από το πρότυπο πωλήσεων που ακολουθούσε μέχρι σήμερα, που συνίστατο στην πώληση της σχετικής άδειας ήδη από την πρώτη χρήση του λογισμικού.

Τα τελευταία χρόνια, υπήρξε σημαντική αύξηση σε ότι αφορά στις υπηρεσίες διαχείρισης συστημάτων πληροφορικής, και ειδικότερο στον τομέα της εξωτερικής ανάθεση και φιλοξενίας, τον επονομαζόμενο και ως hosting (15). Το cloud computing ήρθε για να διευρύνει ακόμη περισσότερο την υπηρεσία αυτή διαθέτοντας ένα σημαντικά μεγάλο αριθμό υπηρεσιών σε έναν ακόμη μεγαλύτερο αριθμό χρηστών. Η έλευση του cloud computing αναμένεται να καινοτομήσει σημαντικά στον τομέα αυτό, καθώς πλέον η τεχνολογία είναι σε θέση τέτοια ώστε να δημιουργήσει τεράστια πάρκα εξυπηρετητών στα οποία θα φιλοξενείται σημαντικά μεγάλος όγκος δεδομένων (13). Η καινοτομία αυτή, όπως

αναμένεται θα αυξήσει τον ανταγωνισμό μεταξύ των παρόχων, ενώ θα οδηγήσει σε συγχωνεύσεις καθώς θα υπάρξει τεράστια ανάγκη για σημαντικές επενδύσεις.

Στο χώρο του cloud computing θα εισέλθει δυναμικά και ο δημόσιος τομέας, ένας τομέας που λειτουργεί σε ένα παρόμοιο όπως θα μπορούσε κανείς να υποστηρίξει πλαίσιο με τον ιδιωτικό. Άρα λοιπόν, βασίζεται και αυτός σε πολύ μεγάλο βαθμό στο ανθρώπινο δυναμικό και τις δομές του, έχοντας πάντα στόχους αλλά και περιορισμούς ως μία επιχείρηση που δραστηριοποιείται σε ένα χώρο. Συνεπαγωγικά, τα όποια πλεονεκτήματα προκύπτουν από τη χρήση του cloud computing στον ιδιωτικό χώρο, προκύπτουν εξίσου και για το δημόσιο τομέα.

Ο δημόσιος τομέας χαρακτηρίζεται, ωστόσο, και από ορισμένες ιδιαιτερότητες (13):

- Το γενικό κλίμα λιτότητας : Συνεπάγεται δημοσιονομική πειθαρχία και περικοπές στα προγράμματα δημόσιων επενδύσεων, συμπεριλαμβανομένου του τομέα της πληροφορικής. Υπό αυτές τις συνθήκες, η αξιοποίηση του ΥΝ δικαιολογείται απόλυτα, διότι επιτρέπει την ανάπτυξη των συστημάτων πληροφορικής χωρίς αρχικές επενδύσεις.
- Η ερευνητική δραστηριότητα στον δημόσιο τομέα : Αν και έρευνα πραγματοποιείται και στον ιδιωτικό τομέα, στον δημόσιο τομέα είναι ιδιαίτερα διαδεδομένη, κυρίως μέσω των εθνικών κέντρων ερευνών, των πανεπιστημίων και των συμπράξεων δημόσιου/ιδιωτικού τομέα. Σε ορισμένες περιπτώσεις, η ερευνητική δραστηριότητα δημιουργεί περιόδους αιχμής όσον αφορά τη ζήτηση υπολογιστικής ισχύος, στις οποίες μπορεί να ανταποκριθεί καλύτερα το cloud computing.
- Οι δημόσιες επενδύσεις : Μέσω της μόχλευσης, οι δημόσιες επενδύνσεις μπορούν να προκαλέσουν και να ενθαρρύνουν τις επενδύσεις στο cloud computing από εθνικούς ή ευρωπαϊκούς ιδιωτικούς φορείς και ιδιαίτερα από οργανισμούς τηλεπικοινωνιών. Στο παρελθόν, ορισμένες επενδύσεις του δημόσιου τομέα λειτούργησαν καταλυτικά για τις επενδύσεις και τη στρατηγική τοποθέτηση του ιδιωτικού τομέα, π.χ. στον τομέα της αεροπορίας και της αεροδιαστημικής, της κινητής τηλεφωνίας, των σιδηροδρόμων υψηλής ταχύτητας κλπ.
- Ορισμένα κράτη μέλη έχουν ήδη πραγματοποιήσει σημαντικές επενδύσεις για την προσαρμογή των λογισμικών της δημόσιας διοίκησής τους στο cloud computing.

Η πλειοψηφία των λύσεων που έχει παρουσιαστεί αφορά κυρίως στου ιδιώτες οι οποίοι έως ένα σημείο παρουσιάζονται να είναι διστακτικοί και να μην προβαίνουν στην αγορά τέτοιων λύσεων (14). Μάλιστα ελάχιστοι από αυτούς είναι διατεθειμένοι ώστε να προβούν σε αγορά εξυπηρετητών ή υποδομών διαδικτύου. Άλλωστε, ακόμη λιγότεροι έχουν τις τεχνικές γνώσεις, ή το εξειδικευμένο προσωπικό ώστε να υποστηρίξουν την αγορά αυτή. Πολλοί από του παρόχους, προβαίνουν σε προσφορά δωρεάν υπηρεσιών έχοντας ως στόχο αφενός την είσοδο στο χώρο πολλών επιχειρήσεων και αφετέρου τη μετέπειτα πραγματοποίηση καταλόγους ιδιωτών χρηστών ως δυνητικών στόχων εμπορίας και διαφημίσεων. Συνήθως διαθέτουν παράλληλα και μία εμπλουτισμένη έκδοση έναντι πληρωμής, με μεγαλύτερη χωρητικότητα, πρόσθετες λειτουργίες κλπ.

Επιπρόσθετα, ιδιαίτερα ελκυστική είναι για τους ιδιώτες και συνεχής πρόσβαση στα δεδομένα οποιαδήποτε στιγμή και από οποιοδήποτε σημείο. Μάλιστα, δεν είναι λίγοι οι προμηθευτές εκείνοι που προσφέρουν στους πελάτες τους τη δυνατότητα να ακούν την αγαπημένη τους μουσική, να βλέπουν τις φωτογραφίες τους κλπ. σχεδόν οπουδήποτε και αν βρίσκονται (14).

Η ραγδαία ανάπτυξη του cloud computing αναμένεται να «χτυπήσει» στο μέγιστο βαθμό τους ειδικούς που δραστηριοποιούνται στο χώρο της πληροφορικής. Για τις επιχειρήσεις που λειτουργούν ως system integrators, δεν αναμένεται σημαντική πτώση ενώ σε κάποιες περιπτώσεις αναμένεται και μία σχετική αύξηση. Ακόμη, ο αριθμός των εργαζομένων στον τομέα της πληροφορικής στις επιχειρήσεις αυτές αναμένεται να παραμείνει ο ίδιος αφού όμως θα υπάρξει καταβολή σοβαρής προσπάθειες ώστε να αποκτήσουν αυτοί νέες δεξιότητες. Αυτοί οι οποίοι πιθανά θα πληγούν στο μέγιστο βαθμό είναι οι τεχνικοί της πληροφορικής οι οποίοι απασχολούνται στην τεχνική υποστήριξη της λειτουργίας των συστημάτων καθώς αναμένεται ότι με την έλευση του cloud computing θα αναπτυχθούν ακόμη περισσότερο οι υπηρεσίες διαχείρισης των συστημάτων από τους τρίτους. Άλλωστε, ο τομέας του cloud computing παρουσιάζει φαινόμενα έντονης συγκέντρωσης αλλά και ιδιαίτερα μεγάλη ευκολία σε ότι αφορά στη μεταφορά των δεδομένων.

Η ανάθεση μέρους των υπηρεσιών πληροφορικής σε τρίτους και εξωτερικούς συνεργάτες «χτυπά» κατά μέτωπο τους ειδικούς πληροφορικής και τους απομακρύνει όλο και

περισσότερο από τις εταιρίες και τους τελικούς χρήστες των συστημάτων (13). Το όλο φαινόμενο, όπως αυτό περιγράφηκε παραπάνω, περιορίζει την αλληλεπίδραση στη σχέση μεταξύ τεχνικών και χρηστών η οποία λόγω της ιδιαίτερης μορφής της, πολλές φορές βασιζόταν καθαρά στην προσωπική επαφή η οποία επέτρεπε σε κάθε ειδικό να κατανοήσει τη δυσκολία του χρήστη και να ανταποκριθεί σε αυτή.

Η σύναψη συμφωνίας μεταξύ πελάτη και παρόχου υπηρεσιών cloud computing διαμορφώνεται με δύο τρόπου οι οποίοι μπορεί να είναι είτε επί πληρωμή είτε δωρεάν παροχή υπηρεσίας. Η διάκριση αυτή δεν είναι ωστόσο πάντα σαφής, διότι οι δωρεάν υπηρεσίες μπορεί να συνεπάγονται μη οικονομικό κόστος όπως η συγκεκριμένη διαφήμιση (contextual advertising) ή η αποδοχή της επαναχρησιμοποίησης των στοιχείων του χρήστη από τον πάροχο (13).

Συνήθως, οι δωρεάν υπηρεσίες απευθύνονται σε ιδιώτες οι οποίοι οφείλουν να προσέξουν ιδιαίτερα στους όρους της ειδικής σύμβασης καθώς αποτελούν μία σοβαρή νομική δέσμευση. Άλλωστε, όποια μορφή και εάν έχει η υπηρεσία που έχουν επιλέξει οι ιδιώτες, τα ευαίσθητα προσωπικά δεδομένα τους μεταφέρονται στο διαδίκτυο και άρα οφείλουν να είναι πλήρως ενημερωμένοι για το τι μπορεί να συμβεί σε περίπτωση απώλειας ή παραποίησης αυτών.

Οι επιχειρήσεις από τη μεριά τους, θα πρέπει και αυτές να είναι ιδιαίτερα προσεκτικές κατά την αποδοχή των όρων που περιγράφονται στις υπηρεσίες του cloud computing και μάλιστα πολλές φορές ενδεχόμενα να ζητούν ακόμη και νομική καθοδήγηση. Ο λόγος που συνίσταται το παραπάνω είναι ότι προσφέρουν στους παρόχους ιδιαίτερα ευαίσθητα και πολύτιμα δεδομένα και οι νομικές κυρώσεις που καλούνται να αντιμετωπίσουν σε οποιαδήποτε περίπτωση παραβίασης αυτών είναι τεράστιες.

Οι συμβάσεις που υπάρχουν στο χώρου του cloud computing συνήθως δεν είναι διαπραγματεύσιμες ενώ ζητείται από τους πελάτες να υπογράψουν μία σύμβαση η οποία ισχύει για όλους και δεν τροποποιείται κατά περίπτωση. Σε κάθε περίπτωση όμως, είτε πρόκειται για δωρεάν είτε για επί πληρωμή υπηρεσίες, η σύμβαση πρέπει να αναφέρει σαφώς τα εξής (13):

- Το επίπεδο της υπηρεσίας ΥΝ (IaaS, PaaS, SaaS)

- Τον εγγυημένο βαθμό διαθεσιμότητας των δεδομένων και την ευθύνη σε περίπτωση απώλειας ή ζημίας
- Την έκταση της κοινής διαθεσιμότητας των πόρων σε πολλούς χρήστες (κίνδυνος υπερφόρτωσης)
- Την ευελιξία των διαθέσιμων και των χρησιμοποιούμενων μέσων πληροφορικής και το τιμολόγιο χρήσης
- Το δικαίωμα ή την υποχρέωση του παρόχου ΥΝ να αποκαλύψει πληροφορίες σε τρίτους, π.χ. σε δικαστική αρχή
- Την ακριβή ταυτότητα του φορέα που προσφέρει πράγματι τις υπηρεσίες, ιδιαίτερα λόγω της συχνά πολυεπίπεδης αρχιτεκτονικής του ΥΝ
- Τη δυνατότητα καταγγελίας της σύμβασης και την τεχνική υποστήριξη που δεσμεύεται να παράσχει ο προμηθευτής κατά τη μεταβατική περίοδο
- Το νομικό καθεστώς (εθνικό ή διεθνές) στο οποίο υπάγεται η σύμβαση, καθώς και το αρμόδιο δικαστήριο σε περίπτωση διαφορών.

Οι υπηρεσίες του cloud computing βασίζονται στο διαδίκτυο και έτσι πολλές φορές τίθενται θέματα ταχύτητας των υπηρεσιών καθώς πλέον σε αυτό εισάγεται καθημερινά τεράστιος αριθμός χρηστών ενώ την ίδια στιγμή μετακινείται υπερβολικά μεγάλος όγκος δεδομένων (15). Η επιθυμία των χρηστών για όλο και μικρότερο χρόνο απόκρισης αυξάνεται διαρκώς γεγονός που ίσως να δημιουργήσει πρόβλημα σε ότι αφορά στη μελλοντική εξέλιξη των επιδόσεων του διαδικτύου. Το cloud computing όπως είναι αντιληπτό επιδεινώνει το παραπάνω πρόβλημα καθώς προβαίνει σε μεταφορά τεράστιου όγκου δεδομένων πάνω από το διαδίκτυο.

Ένα ακόμη πρόβλημα το οποίο συνδέεται με το διαδίκτυο και συζητείται εντόνως σε ότι αφορά στις υπηρεσίες που παρέχει το cloud computing είναι η ανθεκτικότητα του δικτύου και η θωράκιση αυτού απέναντι σε πολλές και σοβαρές απειλές (14). Και φυσικά, ο παραπάνω προβληματισμός δεν περιορίζεται σε καμία περίπτωση στα τεχνικά προβλήματα που ενδεχόμενα να προκύψουν. Αντίθετα, αφορά στο μεγαλύτερο βαθμό του, σε επιθέσεις στον κυβερνοχώρο οι οποίες πλέον είναι ιδιαίτερα συχνές και έχουν ως στόχο την υποκλοπή των δεδομένων που μετακινούνται στο διαδίκτυο. Μάλιστα το cloud computing θα εντείνει ακόμη περισσότερο την ανάγκη ασφάλειας του Διαδικτύου, το οποίο δεν ήταν αρχικά

σχεδιασμένο για εμπορική χρήση. Ιδιαίτερα σημαντική λοιπόν, είναι η ασφάλεια των δεδομένων μέσα στο χώρο του cloud computing όπου και όπως και εάν βρίσκονται αυτά (14).

Η εμπιστευτικότητα των δεδομένων είναι ιδιαίτερα κρίσιμη όταν πρόκειται για δεδομένα υψηλής προστιθέμενης αξίας, λόγω του κινδύνου βιομηχανικής κατασκοπίας. Όπως λοιπόν μπορεί κανείς να συνειδητοποιήσει, οι υπηρεσίες του cloud computing είναι συνεχώς εκτεθειμένες στο χώρο του διαδικτύου και άρα δέχονται συνεχώς επιθέσεις από τους επίδοξους εγκληματίες του κυβερνοχώρου. Άλλωστε, ο χώρος γίνεται ιδιαίτερα ενδιαφέρων πλέον για τους εγκληματίες του διαδικτύου καθώς αυξάνεται συνεχώς το μέγεθος των δεδομένων που μετακινούνται σε αυτό αλλά και η κρισιμότητά τους. Κάποια δεδομένα μάλιστα, είναι ιδιαίτερα σημαντικά και το κόστος υποκλοπής και απόκτησής τους είναι τεράστιο (15).

Για να περιοριστούν οι παραπάνω κίνδυνοι, απαιτείται σημαντικός όγκος δουλειάς και πολλές προσπάθειες από μεριάς των παρόχων οι οποίοι βέβαια είναι ήδη πολύ καλοί γνώστες της κατάστασης αλλά και των κινδύνων που ελλοχεύουν πίσω από το cloud computing.

Ένα άλλο σημαντικό πρόβλημα που προκύπτει στο χώρο του cloud computing και των υπηρεσιών που προσφέρονται από αυτό, είναι η θέσπιση ενός νομικού πλαισίου τέτοιου στο οποίο να υπάγονται όλοι όσοι κινούνται στο χώρο αυτό. Ακόμη, σημαντικό είναι να καθοριστεί, σε Ευρωπαϊκό ή ακόμη και σε παγκόσμιο επίπεδο, ποια είναι η αρχή εκείνη, η οποία θα ασχολείται με την εφαρμογή των κανόνων που θα οριστούν αλλά και θα προβαίνει σε επίλυση οποιονδήποτε διαφορών παρουσιαστούν μεταξύ παρόχου και πελάτης της υπηρεσίας (15).

Η ευρωπαϊκή νομοθεσία όπως αυτή υφίσταται έως και σήμερα, και ιδιαίτερα σε ότι αφορά σε

μεταφορά των δεδομένων εκτός των συνόρων της αποτελεί μια σημαντική τροχοπέδη. Ο ιδιαίτερος διεθνής χαρακτήρας του cloud computing εγείρει σοβαρά ερωτήματα σε ότι αφορά στη μεταφορά των δεδομένων και στην ασφάλεια αυτών και καθώς ακόμη δεν

υπάρχει παγκόσμια ρυθμιστική αρχή που να προβαίνει σε ρυθμίσεις σχετικές με την ασφάλεια αυτών οι προβληματισμοί εντείνονται. Πέραν όμως του θέματος της ασφάλειας των δεδομένων, σοβαρούς προβληματισμούς εγείρει και το θέμα των δικαιωμάτων της πνευματικής ιδιοκτησίας αυτών. Καθώς τα δεδομένα μεταφέρονται γεωγραφικά σε πολλούς και διαφορετικούς servers σε πολλές και διαφορετικές χώρες, είναι ιδιαίτερα δύσκολο να θεσπιστούν σχετικές διατάξεις που θα αφορούν στην προστασία τους, τα πνευματικά δικαιώματα ή ακόμη και τον έλεγχο που ασκείται σε αυτά.

Οι σημαντικές καινοτομίες του διαδικτύου που προσφέρονται καθημερινά στο καταναλωτικό κοινό όπως για παράδειγμα το Facebook ή η μηχανή αναζήτησης της Google, έχουν αποκτήσει ιδιαίτερα σημαντική θέση στην αγορά. Για τον παραπάνω λόγο, η Ευρωπαϊκή Ένωση έχει στραφεί προς την κατεύθυνση αυτή και προσπαθεί με κάθε τρόπο να φροντίσει ώστε καμία από τις παραπάνω εταιρίες να μη θίγει σε καμία περίπτωση τα δικαιώματα των καταναλωτών της (13).

Άλλωστε, το θέμα της φορητότητας των δεδομένων δεν είναι καθαρά τεχνικό καθώς μέσα σε αυτό ελλοχεύει και μία εμπορική σημασία. Απουσία της φορητοτητας, ο πελάτης δεν έχει τη δυνατότητα μεταφοράς των δεδομένων του γεγονός το οποίο περιορίζει στο μέγιστο βαθμό τον ανταγωνισμό που δημιουργείται μεταξύ των παρόχων υπηρεσιών cloud computing. Λύση για το παραπάνω αποτελεί η χρήση των ανοικτών προτύπων η οποία επιτρέπει τη χαμηλού ή και μηδενικού κόστους μετακίνηση από τον ένα πάροχο στον άλλο.

Οι αδυναμίες που περιγράφηκαν παραπάνω ενδεχόμενα να αποτελέσουν ιδιαίτερα σοβαρά εμπόδια σε ότι αφορά στη διάδοση του cloud computing. Ιδιαίτερα το θέμα της ασφάλειας των ευαίσθητων προσωπικών δεδομένων εγείρει πολλούς και σοβαρούς προβληματισμούς. Σε περίπτωση απώλειας κάποιων από αυτά, ο «πόλεμος» που θα δεχόταν μία τέτοια τεχνολογία από το μέσα μαζικής ενημέρωσης θα ήταν τεράστιος και συνεπακόλουθα θα προκαλούνταν σοβαρή βλάβη σε ότι αφορά στην εμπιστοσύνη των χρηστών απέναντι στις υπηρεσίες του cloud computing.

Η Ευρωπαϊκή Επιτροπή έχει θέσει ως στόχο να «συμμετέχει ενεργά» η Ευρώπη στον τομέα του cloud computing («cloud-active»). Όμως, η λέξη «ενεργά» δεν διευκρινίζει αν αφορά την απλή χρήση του cloud computing ή και την ανάπτυξή του. Στην πρώτη περίπτωση πρόκειται

για κατάφωρη έλλειψη φιλοδοξίας. Θα ήταν πολύ σαφέστερο αν ο δηλωμένος στόχος ήταν να καταστεί η Ευρώπη «παραγωγική» στον τομέα του cloud computing («cloud-productive»), που θα σήμαινε ότι η Ευρώπη προσφέρει λύσεις cloud computing και δεν χρησιμοποιεί απλώς τις λύσεις που παράγονται αλλού (13).

Παρά το γεγονός ότι ο ψηφιακός κόσμος κυριαρχείται από επιχειρήσεις που έχουν την έδρα τους σε τρίτες χώρες, η Ευρώπη, έχει κάνει σοβαρές προσπάθειες και έχει καταφέρει να κυριαρχεί στο χώρο των τηλεπικοινωνιών με ένα σημαντικά μεγάλο αριθμό μεγάλων και σοβαρών επιχειρήσεων να στεγάζονται εντός των γεωγραφικών ορίων της. Μάλιστα, ενώ τα τελευταία χρόνια η γηραιά ήπειρος παρουσιάστηκε να κατέχει κυρίαρχη θέση σε πολλούς τεχνολογικούς τομείς, στον τομέα της κινητής τηλεφωνίας έχασε πολύ γρήγορα το προβάδισμά όταν σε αυτόν εισήχθηκαν εταιρίες όπως η Apple και η Samsung. Το cloud computing είναι ο τομέας αυτός που θα της δώσει την ευκαιρία να επανέλθει δυναμικά, να κερδίσει σημαντικά μερίδια αγοράς και ακόμη και να διεκδικήσει ηγετική θέση (13).

Ο παγκόσμιος χαρακτήρας του cloud computing απαιτεί την ύπαρξη διεθνών συνεργασιών και καλεί την Ευρωπαϊκή Ένωση να προβεί στις συνεργασίες αυτές ώστε να είναι πλήρως αρμονική η λειτουργία αυτού. Η Ευρωπαϊκή Ένωση, διαθέτει μία μοναδική σειρά πλεονεκτημάτων στον παγκόσμιο χάρτη που τη φέρνουν στη θέση να ηγηθεί της προσπάθειας αυτής και να προβεί στην ανάπτυξη προτύπων που θα εξασφαλίζουν την προστασία των ευαίσθητων προσωπικών δεδομένων των πελατών καθώς αυτά θα υπάρχουν αλλά και θα διακινούνται στο διαδίκτυο (15). Τα πλεονεκτήματα αυτά είναι (13) :

- Διαθέτει εξαιρετικές υποδομές στον ψηφιακό τομέα. Η τεχνολογία των οπτικών ινών έχει αναπτυχθεί ικανοποιητικά. Τις υποδομές ελέγχει και διαχειρίζεται μικρός αριθμός καθιερωμένων επιχειρήσεων, που μπορούν να επηρεάσουν τόσο τον καθορισμό προτύπων στον τομέα των τηλεπικοινωνιών όσο και τις απαραίτητες επενδύσεις.
- Διαθέτει τις δυνατότητες και την τεχνογνωσία που απαιτούνται για την άσκηση ισχυρής δημόσιας επενδυτικής πολιτικής, ικανής να λειτουργήσει καταλυτικά όσον αφορά τις ιδιωτικές επενδύσεις.

- Οι περιφερειακές και οι εθνικές ΜΜΕ στην Ευρώπη προτιμούν να συνεργάζονται με τοπικούς επιχειρηματικούς εταίρους και, επομένως, θα προτιμούσαν ευρωπαίους πάροχους υπηρεσιών cloud computing.
- Ορισμένοι τομείς (όπως η δημόσια υγεία, οι ένοπλες δυνάμεις, οι δημόσιες συγκοινωνίες, ο δημόσιος τομέας) υπόκεινται σε κανόνες και υποχρεώσεις εθνικού ή ακόμη και ευρωπαϊκού επιπέδου, με αποτέλεσμα να προτιμούν επίσης κατά προτεραιότητα ευρωπαίους ή εθνικούς πάροχους υπηρεσιών cloud computing. Άλλοι τομείς (όπως οι τράπεζες, οι ασφαλιστικές εταιρείες, η ενέργεια, η φαρμακευτική βιομηχανία) δεσμεύονται από μελήματα ασφάλειας των δεδομένων, γεγονός που τους αποτρέπει από την επιλογή παρόχων εκτός της χώρας τους ή της Ευρώπης.

Κεφάλαιο 4
Ασφάλεια Νέφους

4.1 Εισαγωγή

Η έλευση του cloud αποτέλεσε ένα νέο οικονομικό και κοινωνικό φαινόμενο το οποίο έτυχες διεθνούς αναγνώρισης. Μάλιστα, από πολλού θεωρείται μακράν η μεγαλύτερη τεχνολογική επανάσταση που συντελέστηκε τα τελευταία έτη. Το cloud δεν αποτελεί τίποτα περισσότερο από ένα σύνολο τεχνολογιών και υπηρεσιών που εστιάζουν στη διαδικτυακή χρήση και παροχή εφαρμογών τεχνολογίας των πληροφοριών, στη δυνατότητα επεξεργασίας δεδομένων, στην παροχή χώρου αποθήκευσης δεδομένων και στην παροχή μνήμης.

Figure 2 : Αποθήκευση των δεδομένων των χρηστών στο cloud

Όπως είναι αντιληπτό, τα οικονομικά οφέλη που μπορεί να προκύψουν από τη χρήση της τεχνολογίας αυτή είναι τεράστια δεδομένων πάντα των τεραστίων διαστάσεων που έχει λάβει η χρήση της τεχνολογίας αυτής . Πέραν των οικονομικών ωφελειών που απορρέουν

από τη χρήση της τεχνολογίας αυτή, παρουσιάζονται και αρκετά οφέλη σε επίπεδο ασφάλειας καθώς πλέον, ένας μεγάλος αριθμός επιχειρήσεων είναι σε θέση να αποκτήσει σε πολύ μικρό κόστος κορυφαίες τεχνολογίες στις οποίες με διαφορετικές συνθήκες δε θα είχε καμία απολύτως πρόσβαση.

Οι πάροχοι υπηρεσιών cloud προσφέρουν ένα ευρύ φάσμα υπηρεσιών, που κυμαίνεται από συστήματα εικονικής επεξεργασίας και υπηρεσίες που υποστηρίζουν την ανάπτυξη εφαρμογών και προηγμένες δυνατότητες φιλοξενίας, έως διαδικτυακές λύσεις λογισμικού οι οποίες μπορούν να αντικαταστήσουν τις συμβατικές εφαρμογές που εγκαθίστανται συνήθως στους προσωπικούς υπολογιστές των τελικών χρηστών.

4.2 Διάφοροι κίνδυνοι που προκύπτουν από τη χρήση των υπηρεσιών του cloud

Η έλευση μιας τόσο πρωτοποριακής και καινοτόμας πληροφορίας δε θα μπορούσε παρά να αποτελεί στόχο επιτήδειων και φιλόδοξων εγκληματιών κυρίως σε ότι αφορά στην ακεραιτότητα των δεδομένων που χρησιμοποιούνται από αυτή. Στην πλεινότητά τους οι κίνδυνοι αυτοί χωρίζονται σε δύο μεγάλες κατηγορίες :

1. Στην έλλειψη ελέγχου επί των δεδομένων
2. Στην ανεπάρκεια πληροφοριών σχετικά με την ίδια την επεξεργασία

Ο άμεσος κίνδυνος λοιπόν που προκύπτει από τη χρήση των υπηρεσιών του cloud είναι η απώλεια του αποκλειστικού ελέγχου προσωπικών και άλλων δεδομένων που αποθηκεύονται σε αυτό και διακινούνται διαμέσου αυτού.

Η έλλειψη ελέγχου δύναται να εκδηλωθεί με τους ακόλουθους τρόπους (16):

- Έλλειψη διαθεσιμότητας λόγω έλλειψης διαλειτουργικότητας : Πολλές φορές ο χρήστης αδυνατεί να μεταφέρει δεδομένα και έγγραφα μεταξύ συστημάτων κυρίως λόγω ασυμβατότητας ή χρήσης εμπορικών εφαρμογών που προέρχονται από διαφορετικούς πάροχους

- Έλλειψη ακεραιότητας λόγω επιμερισμού των πόρων: Όπως περιγράφηκε σε προηγούμενα κεφάλαια κάθε cloud αποτελείται από συγκεκριμένα συστήματα και υποδομές τα οποία λαμβάνουν και επεξεργάζονται τα δεδομένα. Δυστυχώς πολλά από αυτά και πολλές από τις αρχιτεκτονικές προέρχονται και αφορούν σε διαφορετικούς παρόχους με αποτέλεσμα να υπάρχει ενδεχόμενο σύγκρουσης συμφερόντων.
- Μη τήρηση του απορρήτου σε περίπτωση υποβολής αιτημάτων για σκοπούς επιβολής του νόμου απευθείας σε παρόχους υπηρεσιών cloud: Δεμένου ότι οι αρχές των κρατών έχουν το δικαίωμα με επιβολή νόμου να έχουν άμεση πρόσβαση σε δεδομένα που κυκλοφορούν στο cloud παρουσιάζεται ιδιαίτερα έντονος ο κίνδυνος κοινοποίηση των δεδομένων αυτών στις διάφορες αρχές. Το παραπάνω γεγονός παραβιάζει σημαντικά τα όσα έχουν θεσπιστεί περί προστασίας προσωπικών δεδομένων.
- Αδυναμία παρέμβασης λόγω της πολυπλοκότητας και της δυναμικής της αλυσίδας εξωτερικής ανάθεσης: Η υπηρεσία που προσφέρεται από ένα συγκεκριμένο πάροχο μπορεί σε πολλές περιπτώσεις να προέρχεται από συνδυασμό υπηρεσιών που έχουν προέλθει από περισσότερο από ένα παρόχους και ο αριθμός αυτός να αυξομειώνεται δυναμικά κατά τη διάρκεια ισχύος της σύμβασης του πελάτη. Οι πάροχοι υπηρεσιών cloud είναι πιθανό να μην παρέχουν στον υπεύθυνο της επεξεργασίας τα μέτρα και τα εργαλεία που χρειάζεται για να διαχειρίζεται ευκολότερα τα δεδομένα .
- Έλλειψη απομόνωσης των δεδομένων: Πολλές φορές δίνεται η δυνατότητα στους παρόχους των υπηρεσιών cloud να έχουν τον έλεγχο κα την εποπτεία των δεδομένων ώστε να υπάρχει σύνδεση αυτών με διαφορετικούς πελάτες γεγονός που παραβιάζει και αυτό τους νόμους περί προσωπικών δεδομένων.
- Έλλειψη πληροφοριών όσον αφορά την επεξεργασία (διαφάνεια) : Οι διαδικασίες επεξεργασίας των δεδομένων πολλές φορές δεν περιέχουν επαρκή πληροφορία με αποτέλεσμα αυτή να εγκυμονεί σημαντικούς κινδύνους είτε για τους ανθρώπους που την επεξεργάζονται είτε για τα ίδια τα πρόσωπα στα οποία αφορούν τα δεδομένα. Τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία σε διαφορετικές γεωγραφικές τοποθεσίες εντός του ΕΟΧ, γεγονός που έχει άμεσο αντίκτυπο στη νομοθεσία η οποία διέπει τις διαφορές που ενδέχεται να προκύψουν μεταξύ χρήστη

και παρόχου όσον αφορά την προστασία των δεδομένων. Τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτες χώρες εκτός του ΕΟΧ. Είναι πιθανόν οι τρίτες χώρες να μην εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων και η διαβίβαση των τελευταίων να μην προστατεύεται από κατάλληλα μέτρα (π.χ. τυποποιημένες συμβατικές ρήτρες ή δεσμευτικούς εταιρικούς κανόνες), και, ως εκ τούτου, ενδέχεται να είναι παράνομη.

4.3 Το νομικό πλαίσιο της προστασίας των δεδομένων στην Ευρωπαϊκή Ένωση

Η προστασία των προσωπικών δεδομένων στα πλαίσια της παροχής των υπηρεσιών cloud διέπεται από την οδηγία 95/46/ΕΚ η οποία αφορά σε όλες τις περιπτώσεις στις οποίες γίνεται οποιαδήποτε επεξεργασία προσωπικών δεδομένων. Παρόμοια εφαρμογή έχει και η οδηγία 2002/58/ΕΚ η οποία όμως αφορά στη προστασία της ιδιωτικής ζωής στα πλαίσια των ηλεκτρονικών επικοινωνιών και ισχύει για τις περιπτώσεις εκείνες όπου η επεξεργασία των δεδομένων σχετίζεται άμεσα με την παροχή υπηρεσιών από δημόσια δίκτυα επικοινωνιών.

Η πρώτη οδηγία, δηλαδή η οδηγία 95/46/ΕΚ, και ειδικότερα η παράγραφος 4 που εμπεριέχεται σε αυτή, είναι και αυτή η οποία προσδιορίζει το δίκαιο που εφαρμόζεται. Συγκεκριμένα αφορά στα ένα ή/και περισσότερα σημεία εντός του ΕΟΧ, στα οποία μπορεί δυνητικά να βρίσκεται εγκατεστημένος ο υπεύθυνος επεξεργασίας των δεδομένων ή στις περιπτώσεις όπου αυτός βρίσκεται εκτός ΕΟΧ η επεξεργασία των δεδομένων όμως γίνεται με μέσα εντός ΕΟΧ (17). Στην πρώτη περίπτωση, εφαρμόζεται και ακολουθείται το δίκαιο της χώρας στην οποία είναι εγκατεστημένος ο υπεύθυνος επεξεργασίας των δεδομένων και όχι το δίκαιο της χώρας στην οποία είναι εγκατεστημένος ο πάροχος. Στη δεύτερη περίπτωση, στην περίπτωση όπου ο πάροχος βρίσκεται εγκατεστημένος εντός ΕΟΧ και ο πελάτης εκτός, εφαρμόζεται η νομοθεσία που διέπει τη χώρα στην οποία βρίσκεται εγκατεστημένος ο πάροχος (17).

Όπως είναι αντιληπτό, η παροχή υπηρεσιών cloud, δεν είναι μία απλή διαδικασία και πολλές φορές αφορά στην εμπλοκή πολλών και διαφορετικών φορέων. Εάν λοιπόν στην παροχή αυτή των υπηρεσιών εμπλέκονται και πάροχοι ηλεκτρονικών επικοινωνιών, τότε αυτοί υποχρεούνται να διασφαλίσουν τη συμμόρφωσή τους προς τους κανόνες αλλά και τις υποχρεώσεις που απορρέουν από το απόρρητο των επικοινωνιών αλλά και από την προστασία προσωπικών δεδομένων.

Ο ρόλος του πελάτη σε ότι αφορά την παροχή των υπηρεσιών cloud είναι ιδιαίτερα σημαντικός καθώς αυτός είναι ο μόνος ο οποίος καθορίζει τον τελικό σκοπό της επεξεργασίας και αποφασίζει ή όχι να αναθέσει την επεξεργασία και την εκχώρηση του συνόλου ή μέρους των δραστηριοτήτων επεξεργασίας σε εξωτερικό τρίτο οργανισμό. Ο πελάτης υπηρεσιών cloud ενεργεί, επομένως, ως υπεύθυνος της επεξεργασίας δεδομένων και έχοντας την αρμοδιότητα αυτή, είναι σε θέση ώστε να αναθέσει τον πάροχο τις μεθόδους αλλά και τα μέσα που θα χρησιμοποιηθούν ώστε να γίνει επιτυχής επεξεργασία των δεδομένων (18).

Ο πάροχος των υπηρεσιών από την άλλη, αποτελεί την οντότητα εκείνη που δίνει μορφή στις διάφορες υπηρεσίες cloud. Είναι αυτός ο οποίος παρέχει τόσο τα μέσα όσο και την πλατφόρμα και κατά μία βάση λειτουργεί εκ μέρους του πελάτη. Σε πολλές περιπτώσεις βέβαια, ο πάροχος θεωρείται να είναι υπεύθυνος επεξεργασίας είτε από κοινού με άλλους είτε μόνος του για δικό τους προσωπικό όφελος. Το παραπάνω οφείλεται πάντα στις ανάγκες που προκύπτουν ανάλογα με τις περιστάσεις (18).

Στις περισσότερες των περιπτώσεων οι πελάτες των υπηρεσιών του cloud δεν έχουν τα περιθώρια τροποποίησης των όρων χρήσης αυτών καθώς οι υπηρεσίες παρέχονται βάση τυποποιημένων συμβάσεων. Ο πελάτης είναι, εντούτοις, αυτός που αποφασίζει τελικά να εκχωρήσει ή όχι μέρος ή το σύνολο των διαδικασιών επεξεργασίας σε υπηρεσίες cloud για συγκεκριμένους σκοπούς. Ο πάροχος υπηρεσιών cloud αναλαμβάνει έτσι ρόλο εργολάβου έναντι του πελάτη, και αυτό είναι εν προκειμένω το σημαντικό στοιχείο. Επιπλέον, φέρει τη υποχρέωση με κάθε τρόπο να διασφαλίζει το απόρρητο των δεδομένων του πελάτη.

Αδιαμφισβήτητη σε ότι αφορά στα δεδομένα προσωπικού χαρακτήρα είναι η προστασία με κάθε τρόπο των προσωπικών δεδομένων. Συνεπακόλουθο αυτού είναι η απαγόρευση

οποιασδήποτε επεξεργασίας ή δημοσίευσης με οποιοδήποτε τρόπο δεδομένων προσωπικού χαρακτήρα καθώς από τη διαδικασία αυτή προκύπτει ιδιαίτερα υψηλός κίνδυνος (18). Προκειμένου να ελαχιστοποιηθεί ο κίνδυνος αυτός, προτείνεται μία σύμβαση ανάμεσα στον πάροχο αλλά και στον πελάτη η οποία θα περιλαμβάνει τόσο τεχνικά όσο και οργανωτικά μέτρα μετριασμού του κινδύνου. Η εν λόγω σύμβαση, θα πρέπει φυσικά να προβλέπει την επιβολή αυστηρότατων κυρώσεων για τον πάροχο στην περίπτωση της παραμικρής παραβίασης της νομοθεσίας περί προστασίας των προσωπικών δεδομένων.

Η παράγραφος 6 της οδηγίας 95/46/ΕΚ ορίζει ότι όλα τα προσωπικά δεδομένα οφείλουν να διατηρούνται με μορφή τέτοια η οποία να επιτρέπει αφενός την αναγνώριση της ταυτότητας των προσώπων, για λόγους και πάλι της κοινής ασφάλειες, αφετέρου όμως η χρονική διάρκεια της διατήρησης αυτής να μην υπερβαίνει την προβλεπόμενη που εξυπηρετεί τους στόχους για τους οποίους έχουν συλλεγεί (15). Σε περίπτωση ύπαρξης νομικού κολλήματος που απαγορεύει την οριστική διαγραφή των προσωπικών δεδομένων, θα πρέπει να λαμβάνονται τα μέτρα εκείνα τα οποία θα παρεμποδίζουν με κάθε τρόπο την κάθε μη εξουσιοδοτημένη πρόσβαση σε αυτά. Η αρχή της διαγραφής δεδομένων ισχύει για τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από το εάν αυτά αποθηκεύονται σε σκληρούς δίσκους ή σε άλλα μέσα αποθήκευσης (π.χ. εφεδρικές ταινίες). Καθώς τα δεδομένα αυτά δύναται να βρίσκονται αποθηκευμένα σε πολλές και διαφορετικές τοποθεσίες και έτσι να υπάρχουν πολλά αντίγραφα αυτών, θα πρέπει να διασφαλίζεται με κάθε τρόπο η οριστική διαγραφή τους από όλες τις τοποθεσίες αυτές (15).

Ο πελάτης των υπηρεσιών του cloud οφείλει να είναι ενήμερος σε κάθε περίπτωση, ώστε να γνωρίζει αλλά και να είναι βέβαιος ότι ο πάροχος θα προβεί σε πλήρη διαγραφή των προσωπικών του δεδομένων.

Ο πάροχος με τη σειρά του, και σε ότι αφορά πάντα στην προστασία των δεδομένων, οφείλει να προσλαμβάνει ως διαχειριστή αυτών, πρόσωπο το οποίο θα έχει όλα εκείνα τα χαρακτηριστικά που θα διασφαλίζουν την ακεραιότητα των δεδομένων αλλά και να προβαίνει σε σύναψη σύμβασης που θα θέτει τις ανάλογες δικλείδες ασφαλείας. Η σύμβαση αυτή, ανάμεσα σε άλλα προτείνεται να προβλέπει και τα παρακάτω θέματα (16):

- Αναλυτικές πληροφορίες για τις οδηγίες που πρόκειται να δίνει ο πελάτης στον πάροχο, με ιδιαίτερη έμφαση στις ισχύουσες συμφωνίες επιπέδου εξυπηρέτησης και στις συναφείς κυρώσεις.
- Προσδιορισμός των μέτρων ασφαλείας προς τα οποία πρέπει να συμμορφώνεται ο πάροχος υπηρεσιών cloud, αναλόγως κάθε φορά των κινδύνων που ενέχει η επεξεργασία και της φύσης των δεδομένων που χρήζουν προστασίας.
- Το αντικείμενο και το χρονοδιάγραμμα της υπηρεσίας cloud που πρόκειται να προσφέρει ο πάροχος υπηρεσιών cloud, την έκταση, τον τρόπο και τον σκοπό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τον πάροχο υπηρεσιών cloud, καθώς και τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία.
- Προσδιορισμός των προϋποθέσεων επιστροφής των δεδομένων ή καταστροφής τους μόλις ολοκληρωθεί η παροχή της υπηρεσίας. Ακόμη, πρέπει να υπάρχει μέριμνα για την ασφαλή διαγραφή των δεδομένων προσωπικού χαρακτήρα κατόπιν αιτήματος του πελάτη υπηρεσιών cloud.
- Συμπερίληψη ρήτρας εμπιστευτικότητας, που θα είναι δεσμευτική για τον πάροχο υπηρεσιών cloud και για όσους υπαλλήλους του έχουν ενδεχομένως πρόσβαση στα δεδομένα. Η πρόσβαση στα δεδομένα πρέπει να επιτρέπεται μόνο σε όσους έχουν σχετική άδεια.
- Υποχρέωση του παρόχου να παρέχει στήριξη στον πελάτη όσον αφορά τη διευκόλυνση της άσκησης των δικαιωμάτων που έχουν τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, και συγκεκριμένα των δικαιωμάτων της πρόσβασης στα δεδομένα και της διόρθωσης ή της διαγραφής τους.
- Στη σύμβαση προτείνεται να αναφέρεται ρητά ότι ο πάροχος υπηρεσιών cloud δεν δύναται να κοινοποιεί τα δεδομένα σε τρίτους, ακόμη και για σκοπούς διατήρησης, εκτός και αν προβλέπεται στη σύμβαση η ύπαρξη υπεργολάβων. Σε περίπτωση ύπαρξης υπεργολάβων, και άρα διανομής των δεδομένων, ο πάροχος είναι υποχρεωμένος ώστε να κοινοποιεί τα ονόματα των υπεργολάβων με τους οποίους συνεργάζεται. Ειδικότερα, θα πρέπει να διασφαλίζεται σε κάθε περίπτωση ότι αυτοί θα πρέπει να λειτουργούν αποκλειστικά και μόνο με βάση το συμφέρον των πελατών τους.

- Σαφής καθορισμός των ευθυνών του παρόχου υπηρεσιών cloud όσον αφορά την ενημέρωση του πελάτη υπηρεσιών cloud σε περίπτωση παραβίασης δεδομένων η οποία θίγει τα δεδομένα του τελευταίου.
- Υποχρέωση του παρόχου υπηρεσιών cloud να παρέχει κατάλογο των τοποθεσιών στις οποίες δύναται να γίνεται επεξεργασία των δεδομένων.
- Το δικαίωμα του υπευθύνου της επεξεργασίας να παρακολουθεί τις διαδικασίες επεξεργασίας του παρόχου υπηρεσιών cloud και την αντίστοιχη υποχρέωση του τελευταίου να συνεργάζεται.
- Προτείνεται να καθορίζεται στη σύμβαση ότι ο πάροχος υπηρεσιών cloud πρέπει να ενημερώνει τον πελάτη για συναφείς αλλαγές που αφορούν την εκάστοτε παρεχόμενη υπηρεσία cloud όπως, για παράδειγμα, η εκτέλεση πρόσθετων λειτουργιών.
- Προτείνεται η σύμβαση να προβλέπει την καταγραφή και τον έλεγχο των συναφών διαδικασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα που επιτελούνται από τον πάροχο υπηρεσιών cloud ή τους υπεργολάβους.
- Ενημέρωση του πελάτη υπηρεσιών cloud σχετικά με κάθε νομικά δεσμευτικό αίτημα κοινοποίησης των δεδομένων προσωπικού χαρακτήρα που υποβάλλεται από αρχή επιβολής του νόμου, εκτός αν υπάρχει σχετική απαγόρευση, όπως απαγόρευση συνοδευόμενη από ποινικές κυρώσεις για τη διατήρηση του εμπιστευτικού χαρακτήρα αστυνομικής έρευνας.
- Γενική υποχρέωση του παρόχου να παρέχει διαβεβαιώσεις ότι οι ρυθμίσεις οργάνωσης και επεξεργασίας δεδομένων που εφαρμόζει ο ίδιος συμμορφώνονται προς τις ισχύουσες επιταγές και τα πρότυπα της εθνικής και διεθνούς νομοθεσίας.

Η παράγραφος 2 του άρθρου 17 της οδηγίας 95/46/ΕΚ, οι πελάτες των υπηρεσιών cloud, οφείλουν να ελέγχουν επισταμένως τους πελάτες των υπηρεσιών που χρησιμοποιούν ώστε να βεβαιώνονται για τα μέτρα ασφάλειας που έχουν λάβει αυτοί σχετικά με τα προσωπικά δεδομένα των πελατών τους. Η παραπάνω συμπεριφορά, θεωρείται η πλέον ώριμη και ενδεδειγμένη για τους πελάτες οι οποίοι διαμοιράζονται ευαίσθητα προσωπικά δεδομένα στο διαδίκτυο.

Στους βασικότερους στόχους της προστασίας των δεδομένων υπάγονται (16) :

- ***Η διαθεσιμότητα των δεδομένων*** : Ως εξασφάλιση διαθεσιμότητας νοείται η έγκαιρη και αξιόπιστη πρόσβαση στα ευαίσθητα προσωπικά δεδομένα. Ιδιαίτερα σοβαρή απειλή θα μπορούσε να αποτελέσει οποιαδήποτε απώλεια στη σύνδεση μεταξύ των δύο μερών ή οποιαδήποτε παρακώλυση παροχής της υπηρεσίας λόγω κακόβουλων ενεργειών. Φυσικά, υπάρχουν πάντα και οι αστοχίες του υλικού ή του λογισμικού που πολλές φορές καθίστανται ιδιαίτερα επικίνδυνες σε ότι αφορά στην προστασία των δεδομένων.
- ***Η ακεραιότητα των δεδομένων :*** Πρόκειται για την ιδιότητα που παρουσιάζουν τα δεδομένα ώστε να διατηρούν τη γνησιότητα τους και να μην υπόκεινται σε καμία μορφή τροποποίησης όταν αυτή προέρχεται από κακόβουλη ενέργεια. Η έννοια της ακεραιότητας μπορεί να επεκταθεί σε συστήματα τεχνολογιών της πληροφορίας, με την προϋπόθεση να παραμένει αμετάβλητη η επεξεργασία δεδομένων προσωπικού χαρακτήρα στα συστήματα αυτά. Επιθυμητές είναι μονάχα οι μεταβολές των δεδομένων όταν γίνονται από κρυπτογραφικούς αλγόριθμους και με στόχο να διασφαλιστεί ακόμη περισσότερο η ακεραιότητά τους.
- ***Το απόρρητο :*** Η κρυπτογράφηση είναι μία ιδιαίτερα επιτυχημένη τεχνική σε ότι αφορά στην αποτελεσματική προστασία των δεδομένων. Προτείνεται για όλες τις περιπτώσεις όπου τα δεδομένα βρίσκονται εν κινήσει, μετακινούνται δηλαδή μέσα στο διαδίκτυο. Μάλιστα, η τεχνική της κρυπτογράφησης, συνίσταται κυρίως για την επικοινωνία μεταξύ παρόχου αλλά και πελάτη υπηρεσιών. Ο πελάτης των υπηρεσιών του cloud θα πρέπει να έχει υπ όψιν του ότι σε περίπτωση επεξεργασίας των δεδομένων, οι αλγόριθμοι κρυπτογράφησης παύουν να υφίστανται και άρα αυτή δε θα πρέπει να είναι σε καμία περίπτωση ιδιαίτερα εκτεταμένη.
- ***Διαφάνεια :*** Βασικό στόχο της λειτουργίας των υπηρεσιών του cloud αποτελεί η προστασία των δεδομένων προσωπικού χαρακτήρα και άρα για να είναι αυτό εφικτό, θα πρέπει σε κάθε περίπτωση να διασφαλίζεται η απομόνωση αυτών. Για να γίνει το παραπάνω, θα πρέπει οπωσδήποτε να τεθούν νομικές δικλείδες που θα προστατεύουν την άμεση πρόσβαση. Γενικότερα, οι διαχειριστές και οι χρήστες πρέπει να έχουν πρόσβαση μόνο στις πληροφορίες που είναι αναγκαίες για τους νόμιμους σκοπούς τους οποίους καλούνται να επιτελέσουν. Στα πλαίσια της διαφάνειας, υπάγεται και η έννοια της παρέμβασης που αναφέρεται στη διόρθωση,

τη διαγραφή, το κλείδωμα και την αντίταξη των δεδομένων. Ο πελάτης των υπηρεσιών cloud θα πρέπει να είναι ενήμερος για της ενέργειες στις οποίες προβαίνει ο πάροχος ώστε να διασφαλίζει ότι δε θίγονται άμεσα τα δικαιώματά του. Η φορητότητα των δεδομένων, αποτελεί και αυτή με τη σειρά της μία ιδιότητα των δεδομένων η οποία υπάγεται στα πλαίσια της διαφάνειας. Έως σήμερα, η πλειοψηφία των παρόχων υπηρεσιών cloud, δεν υποστηρίζει φορητότητα των δεδομένων και έτσι σε περίπτωση όπου ο πελάτης αποφασίσει να αλλάξει πάροχο, η μεταφορά των δεδομένων καθίσταται σχεδόν αδύνατη. Μία ακόμη οντότητα είναι και αυτή της λογοδοσίας. Ως λογοδοσία νοείται η ικανότητα απόδειξης των ενεργειών που πραγματοποιήθηκαν ώστε ο πελάτης να είναι σε θέση να εξετάσει τους τρόπους και τις τεχνικές με τους οποίους προστατεύθηκαν ή όχι τα δεδομένα του. Η οντότητα αυτή είναι ιδιαίτερα σημαντική καθώς μπορεί να διερευνήσει αλλά και να εντοπίσει όλες τις παραβιάσεις που μπορεί να έχουν γίνει εις βάρος της προστασίας των προσωπικών δεδομένων.

- ***Διεθνής παραβίαση των δεδομένων :*** Τα άρθρα 25 και 26 της οδηγίας 95/46/ΕΚ προβλέπουν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός του ΕΟΧ μόνο εάν οι χώρες αυτές ή ο αποδέκτης παρέχουν επαρκές επίπεδο προστασίας των δεδομένων. Όπως είναι αντιληπτό, καθώς πρόκειται για υπηρεσίες που βασίζονται αποκλειστικά στο cloud, ο καθορισμός της τοποθεσίας είναι μία έννοια η οποία στην ουσία δεν υφίσταται. Τα δεδομένα ταξιδεύουν διαρκώς πάνω από το διαδίκτυο και άρα ο εκάστοτε πελάτης δεν είναι ποτέ σε θέση ώστε να γνωρίζει που ακριβώς βρίσκονται αυτά, από τοπολογικής πάντα άποψης. Ως εκ τούτου, τα παραδοσιακά νομικά μέσα που διέπουν τη διαβίβαση δεδομένων σε τρίτες χώρες εκτός ΕΕ οι οποίες δεν παρέχουν επαρκή προστασία, έχουν περιορισμένο πεδίο εφαρμογής. Στο παραπάνω πλαίσιο υπάγονται και οι δεσμευτικοί εταιρικοί κανόνες οι οποίοι δεν αποτελούν τίποτε παραπάνω από κώδικα δεοντολογίας τις επιχειρήσεις που προβαίνουν σε διαβίβαση των δεδομένων εντός του ομίλου τους. Η διαβίβαση αυτή, μπορεί να γίνεται μόνο εντός της εταιρίας και μόνο προς όφελος των πελατών. Υπό το πρίσμα αυτό, ο πελάτης θα είναι σε θέση ώστε να εμπιστεύεται τα ευαίσθητα προσωπικά του δεδομένα εάν και μόνο του

παρέχεται η διαβεβαίωση ότι τα δεδομένα αυτά τυγχάνουν της προστασίας που απαιτείται.

4.4 Συμπεράσματα επί του Ευρωπαϊκού Νομικού Πλαισίου

Όλα όσα αναφέρθηκαν στην προηγούμενη ενότητα οδηγούν αναπόφευκτα στο συμπέρασμα ότι τόσο οι επιχειρήσεις όσο και οι διοικητικές αρχές που επιθυμούν να κάνουν χρήση των υπηρεσιών του cloud, οφείλουν εξ αρχής να προβαίνουν σε διεξοδική ανάλυση των κινδύνων που προκύπτουν από τη χρήση αυτού. Τα δεδομένα τα οποία μεταφέρονται μέσω των υπηρεσιών του cloud, είναι ιδιαίτερα ευαίσθητα και η οποιαδήποτε υποψία υποκλοπής αυτών εγείρει προφανώς πρόσθετες ανησυχίες. Ως εκ τούτου, απαιτούνται πρόσθετες εγγυήσεις, με την επιφύλαξη πάντοτε των εθνικών νομοθεσιών.

Σε ότι αφορά στους πελάτες αλλά και τους παρόχους υπηρεσιών του cloud ισχύουν τα παρακάτω (16):

- Στη σχέση μεταξύ πελάτη και παρόχου υπηρεσίας, ο πάροχος φέρει την πλήρη ευθύνη για την επεξεργασία και τη διαβίβαση των δεδομένων και θα πρέπει να τηρεί πάντα όλες τις υποχρεώσεις που ορίζονται από το νόμο και απορρέουν από τις οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ.
- Εάν ο πελάτης με τη σειρά του προβαίνει σε οποιαδήποτε επεξεργασία δεδομένων, τότε θα πρέπει να αποδέχεται την πλήρη ευθύνη των ενεργειών του αλλά και να συμμορφώνεται σε όλους τους κανόνες που αφορούν στην προστασία των προσωπικών δεδομένων όπως αυτοί αναφέρονται στις οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ. Συνίσταται στον πελάτη, να επιλέγει τον πάροχο εκείνο ο οποίος θα του παρέχει όλες τις απαραίτητες εγγυήσεις διασφάλισης προσωπικών δεδομένων αλλά και όλες τις αποδείξεις συμμόρφωσης με τα θεσμικά πλαίσια της Ευρωπαϊκής Ένωσης.
- Στην περίπτωση της συνεργασίας με υπεργολάβους, θα πρέπει να αναφέρεται ρητά στη σύμβαση ότι η επεξεργασία των δεδομένων θα καθίσταται εφικτή, μονάχα

κατόπιν συγκατάθεσης που μπορεί να προέρχεται από τον αρμόδιο επεξεργασίας και να αποσκοπεί στην πλήρη εναρμόνιση των κανονισμών. Η κάθε σύμβαση μεταξύ παρόχου και υπεργολάβου θα πρέπει να περιέχει ιδιαίτερα αυστηρές ρήτρες προστασίας των δεδομένων. Μάλιστα, η προστασία απέναντι στον πελάτη θα πρέπει να είναι τέτοια ώστε ο πελάτης να έχει τη δυνατότητα να καταφεύγει στη δικαιοσύνη στην περίπτωση όπου παραβιάζονται τα δικαιώματά του.

- Η συμμόρφωση προς τις θεμελιώδης αρχές προστασίας των δεδομένων περιλαμβάνει (19):
    - Διαφάνεια
    - Προσδιορισμό και περιορισμό του σκοπού ώστε να υπάρχει διαβεβαίωση ότι δεν γίνεται περαιτέρω επεξεργασία των δεδομένων
    - Διατήρηση δεδομένων
- Οι συμβατικές εγγυήσεις περιλαμβάνουν
    - Επαρκή μέτρα ασφάλειας
    - Πρόσβαση σε δεδομένα μόνο από εξουσιοδοτημένα άτομα
    - Κοινοποίηση δεδομένων μονάχα κατόπιν νομικά δεσμευτικού αιτήματος
    - Υποχρεώσεις συνεργασίας οι οποίες ορίζουν την πλήρη και αποτελεσματική συνεργασία ανάμεσα σε πάροχο και πελάτη
    - Διασυνοριακή μεταβίβαση δεδομένων σε περιοχές όπου η νομιμότητα αυτών προστατεύει τα δεδομένα του πελάτη
    - Καταγραφή και έλεγχος της επεξεργασίας στην οποία υπόκεινται τα δεδομένα τόσο από τον πάροχο όσο και από τον υπεργολάβο
    - Τεχνικά και οργανωτικά μέτρα που έχουν ως στόχο την εξάλειψη των κινδύνων

Προκειμένου να διασφαλιστούν στο έπακρο τα δεδομένα που διακινούνται μέσα στο cloud θα πρέπει να υφίστανται (19) :

- Η ανεξάρτητη επαλήθευση ή πιστοποίηση από ευυπόληπτο τρίτο φορέα
- Οι επιμέρους έλεγχοι των δεδομένων που φιλοξενούνται σε πολυμερές, εικονικοποιημένο περιβάλλον διακομιστή ή η διενέργεια συναφούς ελέγχου από τρίτο φορέα της επιλογής του υπευθύνου της επεξεργασίας

- Η θέσπιση προτύπων και πιστοποιήσεων ειδικά για την προστασία της ιδιωτικής ζωής
- Τα πρότυπα και οι πιστοποιήσεις που προαναφέρονται προτείνεται να προβλέπουν τεχνικά μέτρα και διαδικασίες διασφάλισης της προστασίας των δεδομένων στους κόλπους των παρόχων υπηρεσιών cloud.

Η ομάδα η οποία επιμελήθηκε το ιδιαίτερα κρίσιμο άρθρο 29, έχει επίγνωση της κατάστασης και αντιλαμβάνεται ότι οι συστάσεις που έχει προτείνει σε κάποιες περιπτώσεις δεν επαρκούν κυρίως λόγω του πολύπλοκου χαρακτήρα του cloud. Παρακάτω, παρατίθενται κάποια από τα ζητήματα τα οποία χρήζουν άμεσης αντιμετώπισης ώστε να ενισχυθεί η προστασία των δεδομένων που μεταδίδονται διαμέσου του cloud.

- Καλύτερη εξισορρόπηση ευθυνών μεταξύ υπευθύνου της επεξεργασίας και εκτελούντος την επεξεργασία
- Πρόσβαση σε δεδομένα προσωπικού χαρακτήρα για σκοπούς εθνικής ασφάλειας και επιβολής του νόμου
- Ειδικές προφυλάξεις εκ μέρους του δημόσιου τομέα
- Ευρωπαϊκή εταιρική σχέση για την παροχή υπηρεσιών cloud

Κεφάλαιο 5

Ελληνικό Νομοθετικό Πλαίσιο

5.1 Το Ελληνικό Νομοθετικό Πλαίσιο

Η ραγδαία εξέλιξη στο χώρο στο cloud computing κυριάρχησε όπως αναμενόταν και στον ελληνικό χώρο. Οι ελληνικές νομοθετικές αρχές έχουν κάνει σοβαρές προσπάθειες ώστε να ενημερώσουν το κοινό αλλά και τους αρμόδιους φορείς για τα θέματα που προκύπτουν αναφορικά πάντα με την ασφάλεια των προσωπικών δεδομένων.

Βασικός νόμος στη χώρα που αφορά στην προστασία των προσωπικών δεδομένων είναι ο 2472/1997 που συνάδει με το Ευρωπαϊκό νομοθετικό πλαίσιο. Παρόλα αυτά όμως, υπάρχουν πολλοί και διάφοροι ακόμη, που με τη σειρά τους ενισχύουν τα διάφορα σχετικά ζητήματα που προκύπτουν. Ειδικότερα :

- Ο ν. 2472/1997 συμπληρώνεται από τον ν. 3471/06 για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών που αντικατέστησε τον προ-ισχύσαντα ν. 2774/1999 για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα. Ο νόμος αυτός, ενσωματώνοντας την Οδηγία 2002/58/ΕΚ, αποσκοπεί στην εισαγωγή ειδικών ρυθμίσεων που αφορούν τόσο το απόρρητο της επικοινωνίας και την προστασία της ιδιωτικότητας των χρηστών από πρακτικές, όπως π.χ. η εγκατάσταση κατασκοπευτικού λογισμικού (spyware) όσο και την οργάνωση της προστασίας των δεδομένων των συνδρομητών και χρηστών έναντι των παρόχων (20).

- Με τον ν. 4070/2012 τροποποιήθηκε ο ν. 3471/2006 για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Οι τροποποιήσεις αφορούν στη νομιμότητα της επεξεργασίας των δεδομένων κίνησης και θέσης, στην γνωστοποίηση περιστατικών παραβίασης προσωπικών δεδομένων, στις ανεπιθύμητες ηλεκτρονικές επικοινωνίες και στην υποχρέωση των παρόχων για την λήψη κατάλληλων μέτρων και στην εγκατάσταση cookies (21).
- Το προεδρικό διάταγμα 150/2001, σχετικά με τις ηλεκτρονικές υπογραφές, που προσαρμόζει την ελληνική νομοθεσία στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης, σχετικά με το Κοινοτικό πλαίσιο για τις Ηλεκτρονικές Υπογραφές. Με το παρών διαμορφώνεται ένα ενιαίο πλαίσιο αντιμετώπισης νομικών ζητημάτων που προκύπτουν από τη χρήση της ηλεκτρονικής υπογραφής και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (22).
- Ο ν. 3115/2003, σχετικά με την σύσταση Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών με σκοπό την προστασία του απορρήτου των επιστολών34, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και πληροφοριών (23).
- Ο ν. 3917/2011, σχετικά με την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις (24).
- Ο ν. 3979/2011, σχετικά με την αναγνώριση του δικαιώματος των φυσικών και νομικών προσώπων ιδιωτικού δικαίου να επικοινωνούν και να συναλλάσσονται με φορείς του δημοσίου τομέα με χρήση τεχνολογικών πληροφορικής και επικοινωνιών (ΤΠΕ) και η ρύθμιση της χρήσης των ΤΠΕ από τους φορείς του δημόσιου τομέα εντός του πλαισίου και για τις ανάγκες της λειτουργίας τους και την υποστήριξη της άσκησης των αρμοδιοτήτων και συναλλαγών τους (25).

5.2 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Το σημαντικότερο σημείο στο νόμο 2742/1997 είναι η θέσπιση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η οποία λειτουργεί ως μοχλός εφαρμογής όλων των σχετικών νομοθετικών ρυθμίσεων. Η Αρχή είναι προσανατολισμένη στο πρότυπο της Ανεξάρτητης Διοικητικής Αρχής και στη διαδικασία επιλογής των μελών της εμπλέκεται το Κοινοβούλιο, και δεν υπόκεινται σε οποιονδήποτε διοικητικό έλεγχο (26). Αποστολής της είναι η εποπτεία των νόμων αλλά και των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την άσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά. Ο θεσμικός ρόλος και η εν γένει λειτουργία της Αρχής για το σύστημα προστασίας προσωπικών δεδομένων, καταδεικνύεται από το γεγονός ότι η αρχή αυτή είναι κατοχυρωμένη και σε συνταγματικό επίπεδο (26).

Σύμφωνα με τις επικείμενες διατάξεις, η Αρχή, έχει ένα ευρύτατο πεδίο αρμοδιοτήτων που συνδέονται άμεσα με το σύστημα γνωστοποίησης όλων των αρχείων προσωπικών δεδομένων και την άσκηση προληπτικού ελέγχου, όταν πρόκειται για τη δημιουργία, τήρηση ή διασύνδεση αρχείων με ευαίσθητα δεδομένα καθώς και τη διαβίβασή τους σε μη κοινοτική χώρα.

Η Αρχή μπορεί να συνδέσει την άδεια που δίνει με την επιβολή όρων και ειδικότερων προϋποθέσεων «για την αποτελεσματικότερη προστασία του δικαιώματος της ιδιωτικής ζωής των υποκειμένων ή τρίτων» και επομένως να αντιμετωπίσει τα προβλήματα εν τω γενέσθαι. Εκτός από τις αρμοδιότητες προληπτικού ελέγχου, ο οποίος έγκειται στη μετάθεση της απόφασης και κατά συνέπεια της ευθύνης σε ένα όργανο το οποίο βρίσκεται εκτός εκτελεστικής εξουσίας, η Αρχή διαθέτει ευρύτατες κανονιστικές αρμοδιότητες (27). Εκδίδει οδηγίες με σκοπό την ενιαία εφαρμογή των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και κανονιστικές πράξεις

Σημαντικότατες επίσης είναι οι λειτουργίες της σχετικά με το γνωμοδοτικό και συμβουλευτικό της ρόλο προς το Κοινοβούλιο, καθώς και η συμμετοχή της στην εκπόνηση

κανόνων δεοντολογίας από τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών και νομικών προσώπων και η ενημέρωση και ευαισθητοποίηση του κοινού σε θέματα προστασίας προσωπικών δεδομένων. Τέλος, η Αρχή λειτουργεί ως συμπαραστάτης του πολίτη στις περιπτώσεις που συναντά δυσκολίες κατά την άσκηση δικαιωμάτων που του αναγνωρίζει ο νόμος και επιβάλει διοικητικές κυρώσεις (27).

5.3 Ενσωμάτωση Κοινοτικών Οδηγιών στην Ελληνική Νομοθεσία

Οι κοινοτικές οδηγίες που έχουν ενσωματωθεί στην ελληνική νομοθεσία είναι :

- Η **Οδηγία 95/46/ΕΚ :** Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική Οδηγία στο εσωτερικό δίκαιο. Το ελληνικό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, τον νόμο 2472/97 (ΦΕΚ Α' 50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (28). Ο βασικός σκοπός του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σκοπός του η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Οι διατάξεις και επιταγές του νόμου καταλαμβάνουν, χωρίς διαφοροποιήσεις και τον δημόσιο και ιδιωτικό τομέα. Ο ν. 2472/97 συνιστά ένα πλαίσιο κανόνων που εδράζεται σε τέσσερις πυλώνες (29) :
    - Σε ένα σύστημα ουσιαστικών ρυθμίσεων που θέτει αφενός τις προϋποθέσεις νομιμότητας της επεξεργασίας προσδιορίζοντας δεσμευτικά το σημείο ισορροπίας μεταξύ των αντιτιθεμένων δικαιωμάτων και συμφερόντων και αφετέρου τις βασικές αρχές του νόμου με έμφαση στην αρχή του σκοπού και της αναλογικότητας (άρθρα 4-10)
    - Στην απονομή δικαιωμάτων στα πρόσωπα ώστε να προστατεύσουν τα δικαιώματα και συμφέροντά τους (άρθρα 11-14)

- Στην εισαγωγή και οργάνωση ανεξάρτητου θεσμικού ελέγχου της προστασίας προσωπικών δεδομένων ώστε να εξασφαλίζεται η εφαρμογή της νομοθεσίας (άρθρα 15-20)
- Στους κανόνες που προβλέπουν διοικητικές, ποινικές και αστικές κυρώσεις σε περιπτώσεις παράβασης του νόμου (άρθρα 21- 23).

- Η **Οδηγία 97/66/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, η οποία εισήχθη στο ελληνικό δίκαιο με το **ν. 2774/1999**, "Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα". Από τις σημαντικότερες ρυθμίσεις που επιβάλλονται από την οδηγία και από το άρθρο 9 του Ν. 2774/97συνίσταται ότι η αποστολή ηλεκτρονικών μηνυμάτων "για κάθε είδους διαφημιστικούς σκοπούς" είναι επιτρεπτή μόνο στην περίπτωση συνδρομητών που έχουν δώσει εκ των προτέρων τη ρητή συγκατάθεσή τους. Έτσι η αποστολή μη ζητηθέντος ηλεκτρονικού μηνύματος συνιστά παράνομη επεξεργασία, εφόσον τα υποκείμενα δεν είχαν δώσει ρητή συγκατάθεσή τους προηγουμένως (30)
- Η **Οδηγία 2002/58/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 αποτελεί μέρος των ρυθμίσεων για τις τηλεπικοινωνίες και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Ο βασικός σκοπός είναι ότι ο πάροχος υπηρεσιών ηλεκτρονικών υπηρεσιών να εξασφαλίζει την πρόσβαση στα προσωπικά δεδομένα έχει μόνο εξουσιοδοτημένο προσωπικό και διασφαλίζει ότι τα δεδομένα αυτά από τυχαία καταστρέφει η αλλοίωση. Επίσης θέτει ότι για φυσικά πρόσωπα η συγκατάθεση των αντικειμένων εμπορικής επικοινωνίας είναι υποχρεωτική ενώ για τα νομικά πρόσωπα δίδεται στα κράτη-μέλη η κατά διακριτική ευχέρεια δυνατότητα επιλογής μεταξύ ενός συστήματος (31).
- **Η Οδηγία 2009/136/ΕΚ** τροποποίησε την παραπάνω οδηγία και θέτει ότι παρόλο τη ενημέρωση του χρήστη μέσω των όρων πολιτικής απορρήτου της ιστοσελίδας πλέον καθίσταται υποχρεωτική η συγκατάθεση του. Η συγκατάθεση του χρήστη

μπορεί να δίνεται μέσω ρυθμίσεων στον φυλλομετρητή ή μέσω άλλων εφαρμογών. Ο νόμος εξουσιοδοτεί την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) για τον προσδιορισμό των τρόπων παροχής πληροφοριών και δήλωσης της συγκατάθεσης. Στο πεδίο εφαρμογής εμπίπτουν τα cookies που χρησιμοποιούνται για διαφήμιση είτε αυτά εγκαθίστανται από τον ίδιο τον κάτοχο της ιστοσελίδας, είτε από άλλα διαφημιστικά δίκτυα μέσω της επισκεπτόμενης ιστοσελίδας (32).

Κεφάλαιο 6
Πάροχοι Υπηρεσιών

6.1 Πάροχοι Υπηρεσιών Υπολογιστικού Νέφους

Η αγορά του cloud computing αποτελεί μία ιδιαίτερα ελπιδοφόρα βιομηχανία που επεκτείνεται συνεχώς προσελκύοντας όλο και περισσότερες επιχειρήσεις να εισέλθουν σε αυτή. Το παραπάνω γεγονός φυσικά, σε καμία περίπτωση δε θα μπορούσε να αφήσει αδιάφορες εταιρίες – πυλώνες του χώρου των τεχνολογιών που φυσικά εισήλθαν και στο πεδίο του cloud computing και προσέφεραν μοναδικές λύσεις.

- ***Amazon*** :

Το μεγαλύτερο εμπορικό σήμα του χώρου αυτού αποτελεί η εταιρία Amazon.com η οποία ξεκίνησε από ένα on-line βιβλιοπωλείο σε μια πλατφόρμα γενικής λιανικής πώλησης και έχει μετατραπεί στον κορυφαίο προμηθευτή cloud computing. Η εισαγωγή της στο χώρο του cloud computing έγινε το 2006 με την απλή υπηρεσία αποθήκευσής (Simple Storage Service Amazon S3) και το ελαστικό υπολογίζουν σύννεφο (Elastic Compute Cloud Amazon EC2). Η Amazon είναι πρωτοπόρος στις IaaS προσφορές cloud. Ο γενικός διευθυντής τεχνολογίας της Amazon, Werner Vogels, είναι ένα βαθύ τεχνικό μυαλό και έχει συμβάλλει στην κατεύθυνση της στρατηγικής cloud της Amazon και χρησιμεύει συχνά ως το δημόσιο πρόσωπο της εταιρίας. Ως εταιρία έχει επαινεθεί για τη στρατηγική που ακολουθεί στο cloud και θεωρείται ο βιομηχανικός ηγέτης στη ανερχόμενη αγορά. Το 2008 απονεμήθηκε στο Vogels ο τίτλος του «προϊστάμενος του έτους» από το περιοδικό InformationWeek και ενώ παράλληλα έλαβε και το βραβείο «καλύτερου επιχειρηματικού ξεκινήματος» στα βραβεία «Crunchies» για την Amazon. Εάν το cloud computing απογειώθηκε σαν

βιομηχανία, πολλοί παρατηρητές προβλέπουν ότι τα μελλοντικά λιανικά εισοδήματα της Amazon θα επισκιαστούν από τις cloud προσφορές τους (33).

Ο Larry Dignan του ZDNet δήλωσε ότι «η Amazon θα είναι όπως ένα κατάστημα βιβλίων όπου τα βιβλία θα είναι ακριβώς μια βιτρίνα να καλύψει τον προϋπολογισμό της και για να πουλήσουν την αποθήκευση και το cloud computing.» Τα προϊόντα που προσφέρονται από την εταιρία εμπίπτουν μιας ομάδας συμπληρωματικών προϊόντων, «Amazon Web Services», Amazon Elastic Compute Cloud (Amazon EC2), Amazon SimpleDB, Amazon Elastic Block Store (EBS), Amazon Simple Storage Service (Amazon S3), Amazon Cloud Front, Amazon Simple Queue Service (Amazon SQS), AWS Premium Support).

Το **Elastic Compute Cloud (EC2)** είναι η κυριότερη προσφορά της Amazon Cloud. Το EC2 επιτρέπει την on-demand ενοικίαση εικονικών μηχανών υπολογιστικών πόρων. Προσφέρεται επί μισθώσει σε μονάδες που ονομάζονται στιγμιότυπα, κάθε μια από τις οποίες αντιπροσωπεύει ένα εικονικό διακομιστή με ειδικές προδιαγραφές του υλικού. Από την πλευρά του χρήστη, είναι σαν να ενοικιάζει φυσικούς servers με την ώρα σε οποιαδήποτε ποσότητα. Υπάρχουν πέντε είδη των διαφοροποιημένων στιγμιότυπα προς ενοικίαση με διαφορετική δύναμη της CPU, της μνήμης του σκληρού δίσκου και των I/O επιδόσεων. Οι εφαρμογές που απαιτούν ένα σημαντικό ποσό της μνήμης RAM ή τις επιδόσεις της CPU μπορούν να νοικιάσουν πιο ακριβά αλλά πιο ισχυρά στιγμιότυπα, ενώ ένα δίκτυο με προορισμό την εφαρμογή, όπως ένας web server, μπορούν να χρησιμοποιήσουν φθηνότερες και λιγότερο ισχυρά στιγμιότυπα. Ενώ το EC2 παρέχει μετρημένες υπολογιστικές εγκαταστάσεις προσωρινής τοπικής αποθήκευσης, τρία προϊόντα του Amazon παρέχουν δοσομετρικές μόνιμες εγκαταστάσεις αποθήκευσης: το Elastic Block Store (EBS), το Simple Storage Service (S3) και το SimpleDB (33).

Το **Elastic Block Store (EBS)** λειτουργεί σε συνδυασμό με το EC2 και προσφέρουν επιπλέον υψηλές επιδόσεις, μόνιμης αποθήκευσης με EC2 στιγμιότυπα εικονικής μηχανής. Τα EC2 στιγμιότυπα έχουν τοπική αποθηκευτική ικανότητα, με το χώρο να είναι προσωρινός και διαθέσιμος μόνο όταν ένα στιγμιότυπο συνεχίζει να λειτουργεί. Το EBS παρέχει αποθήκευση παρόμοια με έναν εικονικό δίσκο (αποθήκευση block), η οποία μπορεί να συνδεθεί με ένα συγκεκριμένο στιγμιότυπο EC2.

Το **Simple Storage Service (S3)** ήταν η πρώτη υποδομή σε επίπεδο web υπηρεσιών της Amazon, που ξεκίνησε στις αρχές του 2006. Το S3 παρέχει ισχυρή αποθήκευση αντικείμενων μετρημένη ανά gigabyte ανά μήνα. Η πρόσβαση γίνεται ανεξάρτητα από τα EC2 στιγμιότυπα και έτσι μπορεί να το χρησιμοποιήσει ως ένα χώρο αποθήκευσης (33).

Το **CloudFront** είναι πιο η πιο καινοτόμα υπηρεσία της Amazon, που δημιουργήθηκε τον Νοέμβριο του 2008. Πρόκειται για ένα δίκτυο διανομής περιεχομένου (Content Delivery Network), το οποίο λειτουργεί με τα δεδομένα που αποθηκεύονται στο S3. Το CDN, ενισχύει την παράδοση των δεδομένων προς τους καταναλωτές τους παρέχοντας τους πιο κοντινές τοποθεσίες για τη διανομή τους.

Η **Simple Queue Service (SQS)** της Amazon παρέχει αξιόπιστη ανταλλαγή μηνυμάτων μεταξύ στοιχειών διανεμημένου λογισμικού. Χρησιμοποιείται συχνά σε συνδυασμό με την EC2 για να συντονίσει τις δράσεις σε διαφορετικά στιγμιότυπα ή σε διαφορετικές συνιστώσες μιας μεγαλύτερης εφαρμογή που τρέχει στο EC2.

Η **AWS Premium Support** δεν είναι ένα τεχνικό προϊόν. Είναι μια υπηρεσία υποστήριξης και συμβουλευτικής που σχετίζονται με τις υπηρεσίες cloud της Amazon. Η εταιρία, θέλοντας να παρέχει βοήθεια αλλά και τεχνική υποστήριξη σε θέματα που αφορούν σε ανάπτυξη του λογισμικού της δημιούργησε την υπηρεσία αυτή στοχεύοντας στην καλύτερη εξυπηρέτηση των πελατών της.

- ***Google*** :

Πρόκειται για τη μεγαλύτερη, πλέον σύγχρονη αλλά και σημαντικότερη επιχείρηση που δραστηριοποιείται στο διαδίκτυο σήμερα. Οι ταξινομήσεις των μηχανών αναζήτησης δείχνουν ότι το μερίδιο αγοράς της Google είναι σχεδόν τα δύο τρίτα της συνολικής αγοράς αναζήτησης, εναντίον περίπου 20% για τη Yahoo και 10% ή λιγότερων για τη Microsoft, οι επόμενοι μεγαλύτεροι ανταγωνιστές της. Με την πείρα της του να τρέχει τη δημοφιλέστερη μηχανή αναζήτησης παγκόσμιος και την απέραντη, βιομηχανία-οδηγός στην υποδομή για να υποστηρίξει την ιστοσελίδα με την μεγαλύτερη επισκεψιμότητα, το να επεκταθεί στις υπηρεσίες cloud computing είναι μια φυσική εξέλιξη. Η τρομερή επιτυχία της σε ότι αφορά στις μηχανές αναζήτησης δεν την εμπόδισε να εισέλθει και στο χώρο του cloud computing με την πλατφόρμα Google App την οποία και ενημερώνει συνεχώς (34).

Η **App Engine** της Google είναι διαμετρικά αντίθετη αντιμετώπιση του cloud computing. Στοχεύει σε κλασσικές διαδικτυακές εφαρμογές και επιβάλει δόμηση της εφαρμογής με ξεκάθαρο διαχωρισμό μεταξύ του υπολογιστικού επιπέδου, που είναι χωρίς κατάσταση, και του αποθηκευτικού επιπέδου που έχει καταστάσεις. Η App Engine δεν μπορεί να έχει τόσο ευρεία χρήση όπως το EC2, καθώς δεν επιτρέπει ευελιξία στην υποδομή του συστήματος. Παρέχοντας την υποδομή αυτή απαλλάσσει τους δημιουργούς από τις ανάγκες διαχείρισης και τα προβλήματα που έχει η εγκατάσταση μεγάλων κατανεμημένων εφαρμογών. Η App Engine αναλαμβάνει την τοποθέτηση της εφαρμογής σε ένα cluster, την παρακολούθηση αυτού και την επαναφορά σε περίπτωση αποτυχίας (34).

Περιορισμοί που επιβάλλονται από την App Engine (34):

- Οι developers έχουν μόνο read δικαιώματα στο σύστημα αρχείων της App Engine.
- Εκτός από προγραμματισμένες εργασίες υποβάθρου (background tasks) η App Engine μπορεί να εκτελέσει μόνο κώδικα που καλείτε από HTTP αιτήματα.
- Οι χρήστες μπορούν να ανεβάζουν αυθαίρετα modules αλλά μόνο αν είναι γραμμένα σε καθαρή python.
- Η App Engine περιορίζει τις μέγιστες επιστρεφόμενες εγγραφές από τη βάση δεδομένων σε 1000 ανά κλήση.
- Οι Java εφαρμογές μπορούν να χρησιμοποιήσουν μόνο ένα μέρος του JRE.

- ***Microsoft*** :

Η Microsoft είναι ένας ισχυρός προμηθευτής επιχειρησιακού λογισμικού, αλλά οι προσπάθειες της σε ότι αφορά στην παροχή υπηρεσιών διαδικτύου έχουν επισκιαστεί σε πολύ μεγάλο βαθμό από τους ανταγωνιστές της όπως η Google και το Yahoo. Παρά την ανικανότητά της να μετατοπίσει τους σύγχρονους πρωτοπόρους στην αγορά υπηρεσιών Διαδικτύου, η Microsoft έχει τη σημαντική υποδομή και τη λειτουργική εμπειρία για να τρέξει και να εισβάλει δυναμικά στο χώρο των υπηρεσιών διαδικτύου. Οι προσπάθειες της Microsoft σε αυτήν την νέα περιοχή είναι μερικώς αμυντικές και πολλοί παρατηρητές ήταν δύσπιστοι απέναντι στη Microsoft για την είσοδο της στην υποδομή και στα επίπεδο-πλατφόρμας που προσφέρει το Cloud. Η αρχική εισβολή της Microsoft στο cloud computing

ήταν υπό μορφή προσφορών λογισμικού ως υπηρεσία. Ωστόσο, υπάρχει η προσφορά **Microsoft Azure Services Platform** που περιέχει διάφορα στοιχεία: Live Services, SQL Services, .NET Services, SharePoint Services, Dynamics CRM Services (35).

Βασικό στοιχείο της **πλατφόρμας Azure** είναι ότι επιτρέπει στους χρήστες να τρέχουν ελεγχόμενο κώδικα σε μια εικονική μηχανή σε φιλοξενούμενους και συντηρούμενους διακομιστές της Microsoft. Οι χρήστες πρέπει να επιλέξουν ρόλους Web ή ρόλους εργαζομένων για τις στιγμιότυπο εφαρμογές: ρόλοι Web είναι κατάλληλοι για φιλοξενούμενες εφαρμογές που αλληλοεπιδρούν με τον έξω κόσμο διαμέσου του διαδικτύου, ενώ οι ρόλοι των εργαζομένων είναι κατάλληλοι για τον κώδικα που απλά εκτελείται (35)**.**

Εκτός από τη βασική πλατφόρμα Azure, οι συμπληρωματικές υπηρεσίες περιλαμβάνουν τα ακόλουθα:

SQL Υπηρεσίες: Η υπηρεσίες δεδομένων SQL επιτρέπει στους πελάτες να φιλοξενούν βάσης δεδομένων. Το λογισμικό βασίζεται σε μια σχεσιακή βάση δεδομένων του συστήματος διαχείρισης της Microsoft SQL server, αλλά εκθέτει ένα ελαφρώς διαφορετικό περιβάλλον από αυτή της κοινής σχεσιακής βάσης δεδομένων. Αυτή η υπηρεσία είναι παρόμοια με αυτή της Amazon SimpleDB.

Υπηρεσίες .NET: Η .NET υπηρεσία περιλαμβάνει τρία στοιχεία: την υπηρεσία ελέγχου πρόσβασης, την υπηρεσία Bus και την υπηρεσία ροής εργασίας. Αυτές είναι βοηθητικές υπηρεσίες που χρησιμοποιούνται για την κατασκευή πολύπλοκων εφαρμογών που χρησιμοποιούν το Azure.

Live Υπηρεσίες: Πρόκειται για μία σειρά υπηρεσιών όπως το MSN Hotmail, το Live Messenger, το Live Search και άλλα.

- ***SalesForce*** :

Ιδρύθηκε το 1999 και ξεκίνησε ως προμηθευτής λογισμικού Customer Relationship Management (CRM) Σήμερα, συγκαταλέγεται ανάμεσα στις 50 μεγαλύτερες εταιρίες λογισμικού στον κόσμο. Αρχικά η εταιρία ήταν πρωτοπόρος στα συστήματα SaaS, η έναρξη

όμως τη Force.com, ενός συστήματος PaaS, εισήγαγε την εταιρία στο χώρο της παροχής υπηρεσιών χαμηλότερων επιπέδων Cloud (36).

Η ίδια η εταιρία, περιγράφει το προϊόν της ως PaaS και παρέχει ένα υψηλότερου επιπέδου πλαίσιο εφαρμογής WEB και τις βοηθητικές υπηρεσίες) με στόχο να κατασκευάσει ορισμένα προσανατολισμένα στις επιχειρήσεις, που φιλοξενούνται στο cloud της προϊόντα PaaS. Η εστίαση αυτή στην παροχή συγκεκριμένης υπηρεσίας, δίνει ένα μοναδικό πλεονέκτημα στη Saleforce καθώς εισάγεται πλέον στην αγορά με τη γενίκευση ενός προϊόντος PaaS (36).

Salesforce είναι μια Customer Relationship Management (CRM) προμηθευτής λογισμικού, που παραδίδει το λογισμικό του ως υπηρεσία online (SaaS). Το Force.com είναι μια μοναδική PaaS που προσφέρει και επιτρέπει στους προμηθευτές του να δημιουργήσουν τις επιχειρηματικές εφαρμογές τους και αυτές να παραδίδονται στη υπάρχουσα υποδομή Salesforce. Το Salesforce αναφέρει σαν στόχους του force.com τις περιοχές εφαρμογής του στη διαχείριση των προγραμματιστικών πόρων (ERP / Enterprise Resource Planning), διαχείριση πόρων ανθρώπινου δυναμικού (HRM / Human Resource Management) και διαχείριση εφοδιαστικής αλυσίδας (SCM / Supply Chain Management) (36).

Κεφάλαιο 7
Τύποι Επιθέσεων

7.1 Τύποι επιθέσεων που πραγματοποιούνται στο χώρο του Cloud Computing

Κύριος προβληματισμός λοιπόν που προκύπτει για κάθε επιχείρηση σε ότι αφορά στη χρήση του cloud computing είναι φυσικά η ασφάλεια και η ακεραιότητα των πολύ ευαίσθητων δεδομένων της καθώς οποιαδήποτε παραβίαση ή απώλεια αυτών φέρνει την επιχείρηση αντιμέτωπη με ιδιαίτερα σοβαρά προβλήματα.

Τα δεδομένα λοιπόν τα οποία διακινούνται στο cloud είναι τριών μορφών :

1. Δεδομένα που μεταφέρονται
2. Δεδομένα που αποθηκεύονται
3. Δεδομένα προς επεξεργασία

Όσο αυτά βρίσκονται στο «χώρο» του cloud, κινδυνεύουν να γίνουν στόχος επίδοξων εισβολέων στο δίκτυο και άρα αυτό που απαιτείται άμεσα είναι η θωράκισή τους. Οι διάφοροι πάροχοι υπηρεσιών cloud computing, προσπαθούν να προστατέψουν με κάθε τρόπο τους πελάτες τους και για το λόγο αυτό αναπτύσσουν συστήματα ασφαλείας και ελέγχου που αποσκοπούν στη μέγιστη δυνατή ασφάλεια των δεδομένων.

Συνίσταται λοιπόν σε κάθε πελάτη, όταν αυτός ενδιαφέρεται να χρησιμοποιήσει την υπηρεσία του cloud computing να εξετάζει κάποια από τα παρακάτω θέματα ασφάλειας :

- ✓ Οι διαδικασίες ασφάλειας του παρόχου υπηρεσιών cloud θα πρέπει να είναι το ίδιο καλές ή καλύτερες από τις διαδικασίες που χρησιμοποιεί η επιχείρηση. Ο έλεγχος των

διαδικασιών του πάροχου, θα πρέπει να γίνεται περιοδικά, συμπεριλαμβανομένων ενδεχομένως των επιδιορθώσεων και των ενημερώσεων ασφάλειας (updates) για τα μεμονωμένα συστατικά που χρησιμοποιούνται.

- ✓ Ο πάροχος θα πρέπει να εξασφαλίζεται την απομόνωση των υποδομών και των δεδομένων από τους υπόλοιπους χρήστες. Ανάλογα με το είδος της εργασίας που ζητείται να εκτελεστεί στο cloud, αυτή η ρύθμιση μπορεί ή δεν μπορεί να γίνει αποδεκτή από έναν χρήστη cloud. Σε τέτοιες περιπτώσεις, ο πάροχος υπηρεσιών cloud θα πρέπει να έχει τη δυνατότητα να παρέχει χωριστούς φυσικούς servers για συγκεκριμένους πελάτες.
- ✓ Οι λειτουργίες ασφαλείας μπορεί να τρέξουν ως εικονικές συσκευές από τους host σε περιβάλλον cloud. Έτσι, είναι δυνατό για τους χρήστες cloud σε ένα περιβάλλον IaaS να φορτώσουν και να διαμορφώσουν το δικό τους τείχος προστασίας ή άλλης ασφαλούς εικονική συσκευή για να τρέξει μέσα στο cloud.
- ✓ Θα πρέπει να γίνεται καταγραφή και ιστορικό ελέγχων για τις αιτήσεις που είναι σημαντικές για τις επιχειρήσεις να κατανοήσουν τόσο την απόδοση των εφαρμογών καθώς και τα κενά ασφαλείας. Οι πάροχοι υπηρεσιών cloud computing θα πρέπει να επιτρέψουν την πρόσβαση στην παρακολούθηση της εφαρμογής και των χαρακτηριστικών εργαλείων τους, ανάλογα με την περίπτωση.
- ✓ Οι μηχανισμοί ελέγχου ταυτότητας θα πρέπει να υφίστανται και στα δύο άκρα των επιπέδων παροχής σύνδεσης, τόσο στο χρήστη όσο και στο cloud. Ο χρήστης και ο διαχειριστής πρέπει να συμφωνήσουν σε προγράμματα όπως ο έλεγχος ταυτότητας με τα ψηφιακά πιστοποιητικά και αρχές έκδοσης πιστοποιητικών.
- ✓ Επειδή, οι υπηρεσίες cloud είναι εκτεθειμένες στον έξω κόσμο, οι πόροι του cloud θα πρέπει να υποστηρίζουν λειτουργίες ασφάλειας, όπως η ανίχνευση εισβολής και πρόληψης, το firewal για την πρόληψη της μη επιτρεπόμενης κυκλοφορίας, καθώς και Denial of Service (DoS) πρόληψη. Οι υπηρεσίες cloud είναι ευάλωτες σε Distributed Denial of Service (DDoS), με αποτέλεσμα οι χρήστες να μην έχουν πρόσβαση στις υπηρεσίες Cloud.

Όλα στα παραπάνω, συγκλίνουν προς τον ιδιαίτερα σημαντικό παράγοντα για το cloud computing που καλείται ασφάλεια και χαρακτηρίζει μονοσήμαντα την ποιότητα των υπηρεσιών. Απουσία αυτής, τα δεδομένα εκτίθενται σε ιδιαίτερα μεγάλο κίνδυνο και στο στόχαστρο επίδοξων κυβερνοεγκληματιών. Πολλές από τις επιθέσεις των εισβολέων αυτών μπορούν να χαρακτηριστούν ως παθητικές καθώς αφορούν μονάχα σε παρακολούθηση των πληροφοριών ενώ άλλες είναι ενεργές και αποσκοπούν στο να υποκλέψουν, να αλλοιώσουν ή ακόμη και να καταστρέψουν τα δεδομένα. Οι γνωστότερες κατηγορίες επιθέσεων απέναντι στο cloud computing είναι :

- ***Eavesdropping*:** Η επικοινωνία μέσω διαδικτύου γίνεται στο μεγαλύτερο βαθμό της με τη μορφή ενός απλού κειμένου γεγονός που επιτρέπει σε κάθε επίδοξο εισβολέα να αποκτήσει πρόσβαση στα δεδομένα χρησιμοποιώντας έναν πολύ απλό sniffer ο οποίος θα παρακολουθεί το διαδίκτυο. Εάν λοιπόν τα δεδομένα δεν είναι αυστηρά προστατευμένα με ιδιαίτερα αποδοτικούς κρυπτογραφικούς αλγόριθμους τότε είναι εύκολα αναγνώσιμα από όποιον παρακολουθεί το διαδίκτυο (37).
- ***Data Modification :*** Αφού λοιπόν υποκλαπούν τα δεδομένα από το διαδίκτυο με τον τρόπο που συζητήθηκε παραπάνω, επόμενο βήμα είναι ανάγνωσή τους χωρίς κανένα από τα εμπλεκόμενα κατά τη μεταφορά τους μέρη να το γνωρίζει. Η διαδικασία αυτή είναι ιδιαίτερα απλή για έναν επίδοξο εισβολές καθώς με πολύ απλές τεχνικές μπορεί να προβεί σε ανάγνωση αυτών, δεδομένου ότι δεν υποστηρίζονται με κρυπτογραφικούς αλγορίθμους (38) .
- ***Identity Spoofing (IP Address Spoofing):*** Η κίνηση του δικτύου βασίζεται στη χρήση της IP διεύθυνσης, ώστε τα δεδομένα να μεταφερθούν από τον αποστολέα προς το δυνητικό παραλήπτη. Με τη χρήση της τεχνικής του identity spoofing, οι επίδοξοι εισβολείς, προσποιούνται να είναι οι παραλήπτες χρησιμοποιώντας την ίδια IP διεύθυνση με αυτούς. Με τον τρόπο αυτό τα δεδομένα ακολουθούν διαφορετική διαδρομή και έτσι υποκλέπτονται ή τροποποιούνται (39).
- ***Password Based Attacks :*** Πρόκειται για μορφές επιθέσεων που αφορούσαν κυρίως στα παλαιότερα και όχι ιδιαίτερα προστατευμένα συστήματα. Στόχο έχουν με τη χρήση ενός sniffer να υποκλέπτουν τα αδύναμα passwords και να τα χρησιμοποιούν ώστε να έχουν άμεση πρόσβαση στα δεδομένα. Κάθε φορά που ένας εισβολέας

βρίσκει έναν έγκυρο λογαριασμό χρήστη, αποκτά την ίδια στιγμή ακριβώς τα ίδια δικαιώματα με το χρήστη και ως εκ τούτου μπορεί να πραγματοποιήσει οποιαδήποτε κακόβουλη ενέργεια επιθυμεί. Μετά την απόκτηση πρόσβασης στο δίκτυο του χρήστη, με ένα έγκυρο λογαριασμό, ο εισβολέας μπορεί να κάνει οποιοδήποτε από τα ακόλουθα: να αποκτήσει τους καταλόγους των έγκυρων ονομάτων χρηστών ηλεκτρονικών υπολογιστών και πληροφορίες δικτύου, να τροποποιήσει τον server και δικτύου, συμπεριλαμβανομένων των ελέγχων πρόσβασης και των πινάκων δρομολόγησης, να τροποποιήσει, να αναδρομολογήσει, ή να διαγράψει τα δεδομένα του χρήστη (40).

- ***Denial of Service Attack (DoS) :*** Πρόκειται για τη μορφή της επίθεσης η οποία εμποδίζει ολοσχερώς την παροχή υπηρεσιών από το cloud computing προς τους χρήστες του. Ο εισβολέας κατορθώνει να στείλει στο server έναν υπερβολικό αριθμό αιτημάτων προς εξυπηρέτηση υπερφορτώνοντας το δίκτυο και προκαλώντας διακοπής της λειτουργίας αυτού. Ιδιαίτερα γνωστό είδος επίθεσης DoS, είναι η επίθεση SYN Flood, κατά την οποία ο εισβολέας στέλνει πολλά πακέτα TCP SYN προς στον θύμα για να πραγματοποιήσει σύνδεση, εκμεταλλευόμενος το TCP 3-way handshake. Βασική προϋπόθεση ώστε να είναι πραγματοποιήσιμη η επίθεση αυτή είναι η άμεση δέσμευση των πόρων του συστήματος με την παραλαβή του ACK πακέτου. Ο διακομιστής αντιλαμβάνεται τα πακέτα ως προερχόμενα από κανονικό χρήστη και απαντά με τα ανάλογα SyN – ACK για να διατηρήσει την επικοινωνία. Ο επιτιθέμενος δεν απαντά ανάλογα και καθυστερεί την επικοινωνία ξοδεύοντας έτσι πολύτιμους υπολογιστικούς πόρους για το TCP και κωλύοντας την εξυπηρέτηση των νόμιμων χρηστών. Η παραπάνω επίθεση, μπορεί να προληφθεί εάν γίνει χρήση αυστηρής πρόσβασης στο cloud και εάν χρησιμοποιηθούν όλα τα πρωτόκολλα εκείνα που θα εξασφαλίζουν έγκυρη και ασφαλή πρόσβαση (41).
- ***Man in the Middle :*** Ο τύπος αυτός επίθεσης είναι αντίστοιχος του ονόματος που του έχει δοθεί. Ο εισβολέας βρίσκεται ανάμεσα στο χρήστη και στο άτομο με το οποίο επικοινωνεί και ουσιαστικά παρακολουθεί και ελέγχει όλη την επικοινωνία. Οι επιθέσεις αυτές παρουσιάζονται κυρίως σε περιπτώσεις όπου το πρωτόκολλο SSL δε

λειτουργεί αποτελεσματικά και άρα η επικοινωνία είναι αφύλακτη απέναντι σε οποιαδήποτε επίδοξο εισβολέα (42).

- ***XML Signature Element :*** Η XML υπογραφή στοιχείου, περιγράφει τον τρόπο δημιουργίας και αναπαράστασης των κρυπτογραφημένων δεδομένων XML, καθώς και του τρόπου αποκρυπτογράφησης ενώ παράλληλα μπορεί να υποστηρίξει την κρυπτογράφηση ενός ολόκληρου κειμένου XML ή μόνο επιλεγμένων κομματιών του. Η μορφή αυτή της επίθεσης απέναντι στις υπηρεσίες του cloud computing περιλαμβάνει κακόβουλο λογισμικό και παρόλο που χρησιμοποιείται η XML υπογραφή για την ασφάλεια των στοιχείων δυστυχώς δεν υπάρχει επαρκής προστασία. Ένας εισβολέας είναι σε θέση να χειριστεί ένα μήνυμα SOAP (Simple Object Access Protocol) αντιγράφοντας το στοιχείο στόχου και εισάγοντας οτιδήποτε θεωρεί ότι χρειάζεται και το αρχικό στοιχείο οπουδήποτε αλλού στο μήνυμα SOAP (το SOAP είναι ένα πρωτόκολλο βασισμένο στην XML το οποίο επιτρέπει στις εφαρμογές να ανταλλάσσουν πληροφορία πάνω από κοινώς χρησιμοποιούμενα πρωτόκολλα του διαδικτύου. Αυτή η τεχνική μπορεί να εξαπατήσει την υπηρεσία δικτύου για να επεξεργαστεί το κακόβουλο μήνυμα που δημιουργείται από την επίθεση. Τα παρακάτω σχήματα απεικονίζουν ένα παράδειγμα επίθεσης XML signature element wrapping (43).
- ***Cloud Malware Injection Attack :*** Πρόκειται για τον τύπο επίθεσης ο οποίος επιχειρεί να εισχωρήσει σε μία εφαρμογή ή σε μία εικονική μηχανή ανάλογα πάντα με το μοντέλο της cloud υπηρεσίας (SaaS, PaaS ή IaaS). Ο εισβολέας επιχειρεί να δημιουργήσει τη δική του εικονική μηχανή ή υπηρεσία και να την προσθέσει στο σύστημα που χρησιμοποιείται. Το κακόβουλο λογισμικό που χρησιμοποιείται επιχειρεί να ξεγελάσει την ασφάλεια του cloud και συνεπακόλουθα να αναγνωριστεί η μηχανή που προστέθηκε ως μη κακόβουλη. Σε περίπτωση επιτυχίας της επίθεσης αυτής, οι χρήστες χρησιμοποιούν την υπηρεσία χωρίς να γνωρίζουν τον κίνδυνο και παρέχουν με ιδιαίτερη ευκολία τα ευαίσθητα δεδομένα τους στον κακόβουλο εισβολέα (44).

Κεφάλαιο 8
Ευρωπαϊκό Νομοθετικό Πλαίσιο

8.1 Νομοθετικό πλαίσιο των Ευρωπαϊκών Χωρών

8.1.1 Αυστρία

Στις 14 Ιουλίου 2009 ο Άρειος Πάγος, λαμβάνοντας υπόψη του την απάντηση του ΔΕΚ στο προδικαστικό ερώτημα που είχε υποβάλει, απέρριψε αίτημα Οργανισμού Συλλογικής Διαχείρισης προς Αυστριακό φορέα παροχής σύνδεσης στο διαδίκτυο να αποκαλύψει την ταυτότητα χρηστών βάσει δυναμικών διευθύνσεων IP οι οποίοι ήταν ύποπτοι για παράνομη ανταλλαγή αρχείων με προστατευόμενο περιεχόμενο. Η απόφαση του στηρίχτηκε στο γεγονός ότι στο αυστριακό δίκαιο δεν προβλέπεται ρητά η δυνατότητα αποθήκευσης και επεξεργασίας των δεδομένων κίνησης με σκοπό την εξιχνίασης προσβολών δικαιωμάτων πνευματικής ιδιοκτησίας (45).

8.1.2 Βέλγιο

Στις 27 Ιανουαρίου 2011 προτάθηκε, χωρίς ωστόσο να ευοδωθεί, στο Βέλγιο η υιοθέτηση ενός νόμου «τεσσάρων σταδίων» ακολουθώντας το παράδειγμα του γαλλικού νόμου των «τριών» σταδίων σε σχέση με τις προσβολές της πνευματικής ιδιοκτησίας στο διαδίκτυο. Βάσει της πρότασης αυτής αρχικά θα αποστέλλεται μια ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείου στους παραβάτες ενώ σε περίπτωση κατ' εξακολούθηση προσβολών προβλέπεται διαδοχικά η επιβολή διοικητικού προστίμου, η παραπομπή στο δικαστήριο, η

επιβολή χρηματικού προστίμου, ο περιορισμός της σύνδεσης στο διαδίκτυο του χρήστη και τελικά ο διπλασιασμός του προστίμου και η πλήρης διακοπή της σύνδεσης στο διαδίκτυο (45).

Τον Ιούνιο 2006 στην υπόθεση Sabam vs. Scarletto πρωτοβάθμιο δικαστήριο Βρυξελλών διέταξε τον φορέα παροχής διαδικτυακών υπηρεσιών να λάβει όλα τα κατάλληλα μέτρα, ακόμα και την χρήση φίλτρων, για την παύση/άρση της προσβολής των δικαιωμάτων της πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων, η οποία γινόταν με την παράνομη ανταλλαγή μουσικών αρχείων μεταξύ των συνδρομητών της με τη χρήση συστημάτων P2P.

Το 2008 'ανέβηκε' στο YouTube χωρίς την απαιτούμενη άδεια από τους δικαιούχους μια ταινία μικρού μήκους με τον τίτλο *Fait d ' Hiver .* Η δικαιούχος παραγωγός κίνησε τις διαδικασίες για να βρεθεί το πρόσωπο που είχε ανεβάσει την ταινία, όμως αυτό δεν κατέστη δυνατό. Η ίδια ταινία όμως βρέθηκε διαθέσιμη και σε μία ιστοσελίδα, στην οποία ο ιδιοκτήτης της είχε ενσωματώσει την ταινία από την ιστοσελίδα του YouTube . Ο ιδιοκτήτης κατηγορήθηκε για προσβολή του νόμου περί πνευματικής ιδιοκτησίας. Στις 23 Μαΐου 2012 το πρωτοβάθμιο ποινικό δικαστήριο τον αθώωσε, ο Εισαγγελέας όμως και η δικαιούχος παραγωγός άσκησαν έφεση (45).

8.1.3 Γαλλία

Στις 23 Νοεμβρίου 2007 η Γαλλική Κυβέρνηση ανακοίνωσε την πρόθεσή της να δημιουργήσει μια ανεξάρτητη εποπτική αρχή, η οποία με τη συνδρομή των παρόχων υπηρεσιών Internet, θα στέλνει προειδοποιήσεις σε όσους ανταλλάσσουν παράνομα αρχεία στο διαδίκτυο και συνεπώς παραβιάζουν το δίκαιο περί πνευματικής ιδιοκτησίας. Σε περίπτωση άρνησης συμμόρφωσης του παραβάτη η ανεξάρτητη αρχή θα έχει το δικαίωμα να διακόπτει τη σύνδεση προσωρινά ή οριστικά. Το σχέδιο σύστασης της Επιτροπής βασίσθηκε σε πρόταση του Dennis Olivennes ο οποίος ηγήθηκε αυτής (45).

Μάλιστα η Γαλλία είναι μια από τις τελευταίες χώρες που διέταξαν τη διακοπή παροχής πρόσβασης στην ιστοσελίδα Pirate Bay βάσει απόφασης δικαστηρίου του Παρισιού. Η απόφαση εκδόθηκε στις 4 Δεκεμβρίου 2014 μετά από 10 μήνες ακρόασης της υπόθεσης που

ξεκίνησε με αίτημα του οργανισμού συλλογικής διαχείρισης δικαιωμάτων παραγωγών δίσκων SCPP. Η απόφαση διατάσσει 4 γαλλικούς ISPs (Orange, Bouygues Telecom, Free and SFR) να παρεμποδίσουν την πρόσβαση στην ιστοσελίδα The Pirate Bay και σε άλλες ιστοσελίδες «mirror» ή «proxies» (72 domain names συνολικά). Η απόφαση βασίζεται στο άρθρο του γαλλικού κώδικα πνευματικής ιδιοκτησίας L. 336-2 of the French Intellectual Property Code που προβλέπει ότι οι δικαιούχοι μπορούν να αιτηθούν στο δικαστήριο να διατάξει κάθε αναγκαίο μέτρο για την παύση των προσβολών των δικαιωμάτων τους. Στις 28 Νοεμβρίου 2013 είχαν ξανά διαταχθεί ISPs να διακόψουν την παροχή πρόσβασης σε ιστοσελίδες που μετέδιδαν με την τεχνική του streaming οπτικοακουστικά έργα (υπόθεση "Allostreaming") (45).

8.1.4 Γερμανία

Με τροποποίηση του γερμανικού νόμου για την πνευματική ιδιοκτησία το 2009 ενσωματώθηκε το δικαίωμα πληροφόρησης που προβλέπει η Οδηγία 2004/48 για την επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας. Βάσει της γερμανικής ρύθμισης (αρ. 101 παρ. 9 γερμανικού νόμου για την πνευματική ιδιοκτησία) όταν οι αναγκαίες πληροφορίες για την προσβολή του δικαιώματος πνευματικής ιδιοκτησίας ή του συγγενικού μπορούν να ληφθούν μόνο μέσω χορήγησης δεδομένων κίνησης (IP address) απαιτείται προηγουμένως δικαστική εντολή κατόπιν αιτήσεως του θιγόμενου. Τα έξοδα έκδοσης της εντολής τα επιβαρύνεται ο θιγόμενος. Η απόφαση για την αποδοχή ή απόρριψη της αίτησης εκδίδεται εντός δύο εβδομάδων. Προβλέπεται ένδικο μέσο κατά της σχετικής απόφασης ενώ δεν θίγονται οι προβλέψεις της γερμανικής νομοθεσίας για την προστασία των προσωπικών δεδομένων (45).

8.1.5 Δανία

Η χρήση υπερσυνδέσμων τύπου deep links προκειμένου να προβληθούν σελίδες από βάσεις δεδομένων που βρίσκονται σε άλλες ιστοσελίδες ισοδυναμεί με προσβολή των δικαιωμάτων

επί της βάσης δεδομένων. Αυτό απεφάνθη δανέζικο δικαστήριο επί της υπόθεσης *Danish Newspaper Publishers' Association v. Newsbooster.com ApS*, το οποίο εξέδωσε διαταγή με την οποία απαγορεύθηκε στην ιστοσελίδα Newsbooster.com να παρέχει στους συνδρομητές της υπηρεσίες, οι οποίες τους έδιναν τη δυνατότητα βάσει λέξεων κλειδιών να συγκεντρώνουν στην ιστοσελίδα Newsbooster.com νέα από άλλες ιστοσελίδες. Στους κατηγορούμενους απαγορεύθηκε να παρέχουν δυνατότητες αναζήτησης με την τεχνική του deep linking, να αναπαράγουν τους τίτλους ειδήσεων άλλων ιστοσελίδων και να διανέμουν ηλεκτρονικά ενημερωτικά δελτία με υπερσυνδέσμους τύπου deep linking (45).

8.1.6 Ελβετία

Την 1η Φεβρουαρίου 2013 με τη συνεργασία του Ελβετικού Συλλόγου Διαδικτυακής Βιομηχανίας (Swiss Internet Industry Association - SIMSA) υιοθετήθηκε από τους παρόχους υπηρεσιών διαδικτύου στην Ελβετία ένας νέος κώδικας Δεοντολογίας, με στόχο να αποσαφηνίσει τον ρόλο των ISPs στην παράνομη διακίνηση έργων πνευματικής ιδιοκτησίας. Ο ελβετικός νόμος δεν παρέχει συγκεκριμένες διατάξεις για την αστική και ποινική ευθύνη των παρόχων υπηρεσιών διαδικτύου (ISPs) και όταν υποθέσεις διαδικτυακής προσβολής πνευματικής ιδιοκτησίας έρχονται ενώπιον των ελβετικών δικαστηρίων, επιλύονται βάσει των γενικών κανόνων του Αστικού Κώδικα περί προστασίας δικαιωμάτων προσωπικότητας. Ως εκ τούτου η υιοθέτηση ενός Κώδικα Δεοντολογίας επί αυτών των ζητημάτων, αν και δεν αποτελεί νομικώς δεσμευτικό κείμενο, παρόλαυτά κινείται προς την σωστή κατεύθυνση, διότι θέτει ένα πλαίσιο λειτουργίας των ISPs, το οποίο τους «αυτοδεσμεύει» και επιφέρει μια σχετική ασφάλεια δικαίου. Ο Κώδικας αναφέρεται μεταξύ άλλων σε διαδικασίες παρόμοιες με αυτές που ισχύουν στην Ε.Ε., της οποίας μέλος δεν είναι η Ελβετία, όπως τη διαδικασία ‘ notice and take down ’ (45).

8.1.7 Ηνωμένο Βασίλειο

Στις 19 Νοεμβρίου 2009 συζητήθηκε για πρώτη φορά στο Βρετανικό Κοινοβούλιο το βρετανικό νομοσχέδιο για την ψηφιακή οικονομία. Το βασικότερο ζήτημα πνευματικής ιδιοκτησίας που θίγει το νομοσχέδιο είναι οι διατάξεις για την αντιμετώπιση των

διαδικτυακών προσβολών πνευματικής ιδιοκτησίας. Βάσει αυτών θεσπίζεται υποχρέωση ενημέρωσης των συνδρομητών μιας διαδικτυακής υπηρεσίας εκ μέρους του φορέα παροχής σύνδεσης στο διαδίκτυο για την ύπαρξη αναφοράς για προσβολή δικαιώματος πνευματικής ιδιοκτησίας. Η ενημέρωση μπορεί να λάβει χώρα είτε στην ηλεκτρονική διεύθυνση είτε στην διεύθυνση κατοικίας του συνδρομητή την οποία έχει στη διάθεση του ο πάροχος. Στο νομοσχέδιο περιγράφεται το ελάχιστο περιεχόμενο που πρέπει να έχουν τόσο η αναφορά για την προσβολή όσο και η ειδοποίηση προς τον συνδρομητή. Στο πλαίσιο της ενημέρωσης μπορεί να γνωστοποιηθεί στο συνδρομητή η δυνατότητα του δικαιούχου του δικαιώματος που προσβάλλεται να ζητήσει να μάθει από τον πάροχο ποιες από τις αναφορές του συνδέονται με τα στοιχεία χρήσης της υπηρεσίας του συνδρομητή και κατόπιν αιτήματος ενώπιον δικαστηρίου να λάβει πλήρη ενημέρωση για την ταυτότητα του (του συνδρομητή). Ο θιγόμενος δικαιούχος έχει το δικαίωμα επιπλέον να ζητήσει και να λάβει από τον φορέα παροχής της υπηρεσίας λίστες από τις οποίες προκύπτει η σύνδεση του ύποπτου συνδρομητή με τη διενέργεια προσβολών πνευματικής ιδιοκτησίας χωρίς ωστόσο να επιτρέπει την ταυτοποίηση του συνδρομητή αυτού. Προϋπόθεση είναι να έχει τεθεί σε ισχύ ο κώδικας υποχρεώσεων που προβλέπεται στο βρετανικό νόμο Communications Act 2003. Τον κώδικα αυτό τον εγκρίνει το βρετανικό Γραφείο Επικοινωνιών μετά από τη συναίνεση του Γραμματέα του Κράτους. Ομοίως και κάθε μεταγενέστερη τροποποίηση ή και απόσυρση της έγκρισης του κώδικα. Στο νομοσχέδιο προβλέπεται επίσης μια σειρά αναφορών εκ μέρους του Γραφείου Επικοινωνιών ανά τακτά χρονικά διαστήματα για την εφαρμογή της διαδικασίας αναφορών εναντίον των συνδρομητών υπηρεσίας σύνδεσης στο διαδίκτυο. Σε περιόδους που δεν υπάρχει εγκεκριμένος κώδικας υποχρεώσεων το Γραφείο Επικοινωνιών με διάταγμα του υιοθετεί έναν σχετικό κώδικα για να ρυθμίσει τις υποχρεώσεις αυτές. Στο πλαίσιο του κώδικα μπορεί να τεθεί περιορισμός στον αριθμό των αναφορών που μπορεί να υποβάλει κάθε δικαιούχος και απαίτηση προκαταβολής μιας συνεισφοράς για τα έξοδα στα οποία θα υποχρεωθεί ο φορέας παροχής. Μπορεί ιδιαίτερα να προβλεφθεί η διαδικασία ενημέρωσης να ενεργοποιείται μετά από έναν συγκεκριμένο αριθμό αναφορών εντός συγκεκριμένης χρονικής περιόδου (45).

8.1.8 Ιρλανδία

Τον Φεβρουάριο του 2012 τέθηκε σε ισχύ ως νόμος ο ιρλανδικός Κανονισμός (The European Union (Copyright and Related Rights) Regulations) S.I. No. 59/2012. Σκοπός του Κανονισμού είναι να παρέχει έναν σαφή μηχανισμό που θα διευκολύνει τους δικαιούχους να λάβουν ασφαλιστικά μέτρα εναντίον ενός παρόχου που παρέχει μέσα διευκόλυνσης στους χρήστες των υπηρεσιών του, τα οποία μπορούν να χρησιμοποιηθούν για προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας στο διαδίκτυο (45).

8.1.9 Ισπανία

Στις 31 Δεκεμβρίου 2011 δημοσιεύθηκε στην Ισπανική Εφημερίδα της Κυβέρνησης το Βασιλικό διάταγμα 1889/2011 που αναλύει τις αρμοδιότητες της Ισπανικής Επιτροπής Πνευματικής Ιδιοκτησίας και θέτει σε εφαρμογή τη διαδικασία ενημέρωσης και γνωστοποίησης των περιπτώσεων προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας στο διαδίκτυο που προβλέπεται στον αμφιλεγόμενο νόμο με την ονομασία “Sinde Act”. Η διαδικασία γνωστοποίησης και απόσυρσης περιεχομένου εφαρμόζεται: α) όταν οι επίμαχες πράξεις γίνονται με σκοπό το κέρδος και έχουν σαν αποτέλεσμα την οικονομική ζημία των δικαιούχων και β) όταν οι υπηρεσίες του παρόχου εμπίπτουν στην έννοια της «υπηρεσίας της κοινωνίας της πληροφορίας» που προβλέπεται στον ισπανικό νόμο ο οποίος ενσωμάτωσε την οδηγία για το ηλεκτρονικό εμπόριο (45).

8.1.10 Ιταλία

Στις 17 Δεκεμβρίου 2010 η Ιταλική Αρχή Επικοινωνιών έθεσε τις προτάσεις της για την προστασία της πνευματικής ιδιοκτησίας στα δίκτυα ηλεκτρονικών επικοινωνιών προς διαβούλευση με καταληκτική ημερομηνία για την υποβολή σχολίων την 4η Μαρτίου 2011. Οι βασικές θέσεις της Ιταλικής κρατικής πολιτικής όπως εμφανίζονται στο κείμενο αυτό αφορούν: την ανάγκη προαγωγής της διαθεσιμότητας νόμιμου ψηφιακού περιεχομένου, την δυνατότητα ενημέρωσης και εκπαίδευσης των διαδικτυακών χρηστών σχετικά με την παραβατικότητα στο διαδίκτυο, την διαδικασία που θα πρέπει να ακολουθούν οι δικαιούχοι

προστασίας πνευματικής ιδιοκτησίας για την αναφορά της προσβολής των δικαιωμάτων τους και την απομάκρυνση του σχετικού παράνομου περιεχομένου και τα μέτρα που προτίθεται να λάβει η Αρχή για την προστασία της πνευματικής ιδιοκτησίας (45).

8.1.11 Νορβηγία

Σύμφωνα με πρόσφατο δημοσίευμα ένας νέος νόμος σχετικά με τα πνευματικά δικαιώματα και τον διαμοιρασμό αρχείων στο διαδίκτυο, αναμένεται να τεθεί σε ισχύ από την 1η Ιουλίου στην Νορβηγία. Ο νέος νόμος, ο οποίος ήταν στα σκαριά για δυο περίπου χρόνια, προβλέπει την δημιουργία μιας ομάδας για την αποτελεσματική καταπολέμηση της διαδικτυακής πειρατείας. Η ομάδα, η οποία βρίσκεται ακόμη σε στάδιο σχηματισμού, έχει σκοπό να θέσει σε εφαρμογή τις νέες διατάξεις, προς όφελος των κατόχων πνευματικών δικαιωμάτων. Ο γενικός γραμματέας του Videograms Association της Νορβηγίας Willy Johansen, ανέφερε χαρακτηριστικά: “Η νέα ομάδα που θα συγκροτηθεί θα διεξάγει έρευνες σχετικά με την παραβίαση των πνευματικών δικαιωμάτων. Ελπίζουμε στην δημιουργία μιας πολύ ισχυρής οργάνωσης, με πολλά μέλη που κατέχουν πνευματικά δικαιώματα ενταγμένα σε αυτή” (45).

8.1.12 Πορτογαλία

Τον Δεκέμβριο του 2010 το πορτογαλικό Υπουργείο Πολιτισμού υπέγραψε πρωτόκολλο συνεργασίας με την πορτογαλική φωνογραφική Ένωση προκειμένου να παρασχεθεί εκπαίδευση σε υπηρεσίες του Υπουργείου για την εξακρίβωση των περιπτώσεων πειρατείας. Στο πρωτόκολλο αποκαλύφθηκε ότι περιέχονται ρυθμίσεις δημιουργίας παγίδων γνωστών ως «honeypots» για τους χρήστες που ανταλλάσσουν προστατευόμενα αρχεία μέσω συστημάτων peer to peer προκειμένου να διευκολυνθεί η καταγραφή των IP διευθύνσεων τους. Ο όρος "Honeypots" χρησιμοποιείται για τις ιστοσελίδες που δημιουργούνται προκειμένου να θέλξουν τους χρήστες να προβούν σε τηλεφόρτωση προστατευόμενων αρχείων ώστε να τους παγιδεύουν και μετά να στραφούν εναντίον τους (45).

8.1.13 Σουηδία

Την 1η Απριλίου 2009 τέθηκε σε ισχύ ο στις νόμος για την πνευματική ιδιοκτησία στη Σουηδία, ο οποίος ενσωματώνει την Οδηγία 2004/48 για την επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας. Ο νόμος επιτρέπει στους φορείς παροχής διαδικτυακών υπηρεσιών να αποκαλύπτουν την ταυτότητα στις χρήστη στον οποίο αντιστοιχεί η IP Address σε σχέση με την οποία υφίστανται υποψίες ότι γίνονται παράνομες ανταλλαγές αρχείων με προστατευόμενο με δικαίωμα πνευματικής ιδιοκτησίας περιεχόμενο (45).

Κεφάλαιο 9
Το Νέφος στην Ελλάδα

9.1 Το υπολογιστικό νέφος στην Ελλάδα

Το σημαντικότερο έργο που έχει υλοποιηθεί στην Ελλάδα στα πλαίσια της τεχνολογίας του cloud computing, και σε ότι αφορά στο δημόσιο τομέα είναι η δημιουργία του κόμβου G-Cloud από την Γενική Γραμματεία Πληροφοριακών Συστημάτων. Το έργο δημιουργήθηκε υπό την αιγίδα του Επιχειρησιακού Προγράμματος «Ψηφιακή Σύγκλιση» και αφορά στις Κεντρικές Υπολογιστικές Γραμμές της κοινωνίας της Πληροφορίας. Το κόστος υλοποίησής του ανέρχεται στα 16,3 εκατομμύρια ευρώ ενώ το αντικείμενο του είναι ο σχεδιασμός και η υλοποίηση δύο Κεντρικών Υπολογιστικών Κέντρων για την Κοινωνία της Πληροφορίας αλλά και τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (46). Τα δύο αυτά κέντρα, θα έχουν τεράστια υπολογιστική και αποθηκευτική ισχύ ενώ θα λειτουργούν αυτόνομα. Οι υποδομές που θα αναπτυχθούν θα χρησιμοποιηθούν για την προσφορά υπηρεσιών οι οποίες θα καλύπτουν τις ανάγκες της ευρύτερης Δημόσιας Διοίκησης, πιο συγκεκριμένα, τις ανάγκες σε υπολογιστική και αποθηκευτική ισχύ των κεντρικών συστημάτων πρωτίστως δράσεων για τις οποίες οι Φορείς Λειτουργίας του Έργου είναι οι τελικοί δικαιούχοι στα πλαίσια της τέταρτης προγραμματικής περιόδου αλλά και λοιπών κεντρικών συστημάτων τρίτων Φορέων της Δημόσιας Διοίκησης που θα υποδειχθούν (46).

Η εγκατάσταση των κέντρων αυτών θα γίνει σε ειδικό χώρο που θα φέρει κατάλληλο εξοπλισμό. Ο εξοπλισμός αυτός θα πρέπει να είναι άρτιος αλλά και ο πλέον σύγχρονος ώστε τα κέντρα δεδομένων να παρέχουν υπηρεσίες υψηλής ποιότητας προς όλους τους συνεργαζόμενους φορείς με ασφαλή, ευέλικτο αλλά και αποτελεσματικό τρόπο.

Η ολοκλήρωση του έργου, θα φέρει τους Φορείς Λειτουργίας του σε σημείο ώστε να έχουν καθορίσει όλες εκείνες τις απαραίτητες διαδικασίες ώστε να υπάρξει άριστη διαχείριση των παρεχόμενων υπηρεσιών. Ακόμη, θα έχουν τη δυνατότητα πρόσβασης σε προηγμένες υπηρεσίες που θα βασίζονται σε τεχνολογίες αιχμής και θα τους παρέχουν τα παρακάτω οφέλη (46):

- Αύξηση της διαθεσιμότητας και της απόδοσης των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης με την υιοθέτηση του μοντέλου ευέλικτων και αποτελεσματικών κέντρων δεδομένων τα οποία παρέχουν πόρους ελαστικά και με βελτιωμένη ανθεκτικότητα σε αστοχίες και άλλες καταστροφές.
- Αύξηση της αποδοτικότητας και της ασφάλειας των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης.
- Οικονομίες κλίμακας μέσω της μείωσης του συνολικού κόστους που προκύπτει από την διαχείριση και συντήρηση πληροφοριακών συστημάτων.
- Βελτίωση της συνολικής "εμπειρίας του Πολίτη", λόγω της κεντρικής υπόστασης των υπηρεσιών των Κέντρων Δεδομένων, μέσω της οποίας θα επιτυγχάνεται μικρότερο χρονικό διάστημα για την παροχή των εφαρμογών και κατ' επέκταση άμεση ανταπόκριση στην αύξηση των αναγκών κλπ.
- Βελτίωση της δυνατότητας διαλειτουργικότητας και διασυνδεσιμότητας των φιλοξενούμενων πληροφοριακών συστημάτων και ως εκ τούτου διευκόλυνση της εφαρμογής ψηφιακών υπηρεσιών προστιθέμενης αξίας για τις επιχειρήσεις και τους πολίτες της χώρας.

Ο υποψήφιος Ανάδοχος θα πρέπει να λάβει ειδική μέριμνα και να δρομολογήσει τις κατάλληλες δράσεις για (46):

- Την ασφάλεια των Πληροφοριακών Συστημάτων, Εφαρμογών, Μέσων και Υποδομών του κάθε Κέντρου Δεδομένων
- Την προστασία της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που αφορούν στην λειτουργία των υποδομών του κάθε Κέντρου Δεδομένων (infrastructure data)

- Την προστασία τυχόν προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων στις βάσεις δεδομένων της υποδομής ή αλλού των αναζητώντας και εντοπίζοντας με μεθοδικό τρόπο τα τεχνικά μέτρα και τις οργανωτικό- διοικητικές διαδικασίες που απαιτούνται.

Επιπλέον για τον σχεδιασμό και την υλοποίηση των τεχνικών μέτρων ασφαλείας του έργου, ο ανάδοχος θα πρέπει να λάβει υπόψη του (46):

- Το θεσμικό και νομικό πλαίσιο που ισχύει (π.χ. προστασία των προσωπικών δεδομένων Ν. 2472/97, προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα Ν. 2774/99)
- Τις σύγχρονες εξελίξεις στις ΤΠΕ
- Τις βέλτιστες πρακτικές στο χώρο της Ασφάλειας στις ΤΠΕ
- Τα επαρκέστερα διατιθέμενα προϊόντα λογισμικού και υλικού
- Τυχόν πρότυπα (ISO27001) τα οποία θα περιλαμβάνονται στο «Πλάνο Ενεργειών για τη Ασφάλεια και προστασία των συστημάτων και των δεδομένων της υποδομής των Κέντρων Δεδομένων» που θα παραδοθεί από τον Ανάδοχο στην Αναθέτουσα Αρχή

Ο ανάδοχος, στην πρόταση του, θα πρέπει να διατυπώσει τη μεθοδολογία ανάλυσης και αντιμετώπισης των ζητημάτων ασφαλείας που άπτονται των παραπάνω ζητημάτων, περιγράφοντας τους μηχανισμούς ελέγχου και τις τεχνολογικές λύσεις που περιέχονται στην προτεινόμενη λύση. Κατ' ελάχιστον θα πρέπει να γίνει καταγραφή των εξής:

- Καταγραφή Απαιτήσεων Συμμόρφωσης με Θεσμικό, Νομικό και Κανονιστικό Πλαίσιο
- Συμφωνία πεδίου εφαρμογής της Διαχείρισης της Ασφάλειας
- Ανάλυση Επιχειρηματικών Επιπτώσεων, απειλών και αδυναμιών
- Ανάπτυξη Σχεδίου Διαχείρισης Κινδύνων ISO27001
- Ανάπτυξη Πολιτικών Ασφάλειας Πληροφοριών
- Ανάπτυξη Διαδικασιών Ασφάλειας

9.2 Προτάσεις για τη μελλοντική διαχείριση του Cloud Computing στην Ελλάδα

Όπως προαναφέρθηκε στα προηγούμενα κεφάλαια, ο χώρος του cloud computing αποτελεί μία σύγχρονη τεχνολογία αιχμής η οποία εισέρχεται όλο και περισσότερο στους διάφορους τομείς της καθημερινότητας. Οι δύσκολες κοινωνικοπολιτικές αλλά και οικονομικές συνθήκες που επικρατούν στην Ελλάδα, δεν έχουν επιτρέψει στο χώρα να ακολουθήσει το φρενήρη ρυθμό της τεχνολογίας αυτής, να κάνει χρήση της στο δημόσιο και ιδιωτικό τομέα αλλά και να θεσπίσει νόμους και πολιτικές προς αυτήν την κατεύθυνση.

Αντίθετα, πολλές από τις Ευρωπαϊκές χώρες, έχουν προβεί στην ανάληψη έργων που αφορούν στο cloud computing ενώ θέτουν ήδη γερές βάσεις για τη μετανάστευση προς αυτόν τον τομέα. Για παράδειγμα, η Ιταλία και το Ηνωμένο Βασίλειο, έχουν θεσπίσει αυστηρές πολιτικές που αφορούν στη χρήση των υπηρεσιών που προσφέρει το cloud computing αλλά και στην προστασία των τόσο ευαίσθητων προσωπικών δεδομένων που κινούνται στο χώρο αυτό. Η Ελλάδα, όπως προαναφέρθηκε, δεν έχει θεσπίσει συγκεκριμένες στρατηγικές ώστε να περιορίσει τα όποια προβλήματα μπορεί να δημιουργηθούν από το χώρο του cloud computing, ενώ έχει περιοριστεί μονάχα στη δράση και τη λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Έτσι, συχνά δεν τηρούνται οι όποιοι νόμοι και ταυτόχρονα παρατηρούνται παραβιάσεις.

Η Ελλάδα, στα πλαίσια του εκσυγχρονισμού της και με στόχο να συμβαδίσει με τις υπόλοιπες Ευρωπαϊκές χώρες, οφείλει να υιοθετήσει την τεχνολογία και τις υπηρεσίες που προσφέρει το cloud computing αλλά και να προβεί σε ανάλογες εξελίξεις που σχετίζονται με αυτές. Δεδομένου ότι η χρήση της τεχνολογίας του cloud computing οφείλει να διασφαλίζει την ακεραιότητα των δεδομένων που διακινούνται στο χώρο θα πρέπει να υπάρχουν ανάλογες διαπιστεύσεις ότι οι υπηρεσίες αυτές είναι και θα παραμείνουν ασφαλής. Οι πάροχοι των υπηρεσιών του cloud computing, σε συνεργασία πάντα με το κράτος οφείλουν να ενημερώνουν αλλά και να διαβεβαιώνουν τους χρήστες ότι θα λάβουν όλα τα μέτρα αλλά και τις προφυλάξεις προς αυτήν την κατεύθυνση. Άλλωστε, στη χώρα υπάρχει και το παράρτημα του ENISA (European Network and Information Security Agency) το οποίο μπορεί να προσφέρει ουσιαστική βοήθεια προς την κατεύθυνση αυτή.

Οποιαδήποτε πρωτοβουλία θα ληφθεί από τους Ελληνικούς αρμόδιους φορείς οφείλει να ξεκινήσει φυσικά με την καταπολέμηση της οποιαδήποτε μορφής απάτης μπορεί να συντελεστεί μέσα στους χώρους του cloud computing. Οι χρήστες θα πρέπει να αισθάνονται ασφαλείς για την τεχνολογία που χρησιμοποιούν αλλά και να την εμπιστεύονται χωρίς ενδοιασμούς και δεύτερες σκέψεις. Κακόβουλες ενέργειες όπως κλοπές, εξαπατήσεις αλλά και hacking θα πρέπει να καταστέλλονται άμεσα. Άλλωστε, αυτό απαιτείται ώστε να μπορεί να αναγνωριστεί το μέγεθος και ο αριθμός των απειλών αλλά και τα μέτρα που πρέπει να λαμβάνονται προς αυτήν την κατεύθυνση. Συνίσταται λοιπόν να προάγεται η διαφάνεια σε ότι αφορά τις τεχνικές των υπηρεσιών του cloud computing, να υπάρχει συμμόρφωση των παρόχων των υπηρεσιών αυτών με όσα ορίζει ο ENISA, να ενισχυθεί και να γίνει αυστηρότερη η νομοθεσία που αφορά στην παραβίαση των δεδομένων, να δημιουργηθούν δράσεις απέναντι στις κυβερνοαπειλές, αλλά και να γίνουν πιο αυστηρές οι ποινές για τους hackers.

Για να μπορούν να αναπτυχθούν στο έπακρο οι απεριόριστες δυνατότητες που προσφέρουν οι υπηρεσίες του cloud computing, θα πρέπει να τηρούνται, να ακολουθούνται αλλά και να εφαρμόζονται οι κανόνες που θα θεσπιστούν στο έπακρο. Έτσι λοιπόν, θα πρέπει να υπάρξει μία αναθεώρηση που θα αφορά στο πλαίσιο της προστασίας των δεδομένων αλλά και θα ξεκαθαρίζει όλους τους νόμους και τους κανόνες που θα αφορούν σε αυτή και θα σχετίζονται με το χώρο του cloud computing. Ασφαλώς και συνίσταται η εναρμόνιση και η συμμόρφωση με τους κανόνες που έχουν οριστεί από την Ευρωπαική Ένωση και ειδικότερα από την οδηγία 95/46/ΕΚ. Το παραπάνω, είναι ιδιαίτερα σημαντικό καθώς του cloud computing έχει διεθνείς διαστάσεις με τα δεδομένα να ταξιδεύουν αλλά και να αποθηκεύονται σε πολλά και διαφορετικά σημεία της γης.

Ιδιαίτερα σημαντική για τον Ελλαδικό χώρο είναι και η εξάλειψη της γραφειοκρατίας σε ότι αφορά τον τομέα του cloud computing που θα δώσει τη δυνατότητα σε παρόχους να προσφέρουν έναν μεγαλύτερο αριθμό υπηρεσιών αλλά και να εστιάσουν προς τη διασφάλιση των δεδομένων και τη μέγιστη εξυπηρέτηση του χρήστη. Επιπρόσθετα, η νομοθεσία που θα οριστεί οφείλει να είναι τέτοια που δε θα περιέχει αντικρουόμενους νόμους αλλά και διατάγματα που θα αποτελούν τροχοπέδη το ένα για το άλλο και τελικά θα εμποδίζουν την ανάπτυξη των υπηρεσιών του cloud computing στην Ελλάδα.

Ένας ακόμη τομέας που θα πρέπει να ληφθεί σοβαρά υπ όψιν στον ελλαδικό χώρο είναι αυτός της φορητότητας των δεδομένων αλλά και της διαλειτουργικότητας των διαφόρων περιβαλλόντων και των διαφόρων συσκευών. Η διαλειτουργικότητα είναι ένας ιδιαίτερα σοβαρός τομέας και οι τεχνολογικές εξελίξεις οφείλουν να στρέφονται προς την κατεύθυνση αυτή προσδίδοντας έτσι προστιθέμενη αξία στο χώρο του cloud computing. Οι διάφοροι πάροχοι υπηρεσιών του χώρου θα πρέπει να συνεργάζονται μεταξύ τους υπό ένα κοινό νομοθετικό πλαίσιο ώστε να παρέχουν τη βέλτιστη υπηρεσία στο χρήστη σε ένα ανοικτό και συνεργατικό περιβάλλον.

Επιπρόσθετα, ο χώρος του cloud computing είναι ένας χώρος που στοχοποιείται από μία σειρά επίδοξων κακοποιών και άρα πολλές φορές αρκετοί από αυτούς καταφέρνουν να επιτύχουν το σκοπό τους, προσφέροντας στο χρήστη διάφορες μορφές κακόβουλου λογισμικού. Η ελεύθερη διακίνηση και η ελεύθερη προσφορά του όποιου λογισμικού ίσως να μη φαίνεται ύποπτη και να μην εγείρει προβληματισμούς στο χρήστη, πολλές φορές όμως είναι. Στα παραπάνω πλαίσια, θα πρέπει να υπάρχει στενή συνεργασία του κράτους, των αρμόδιων φορέων αλλά και των παρόχων ώστε να εντοπίζονται τα λογισμικά αυτά, και να αποσύρονται άμεσα από το δίκτυο. Φυσικά, αυτό θα πρέπει να συνοδεύεται από εντοπισμό και σύλληψη του επίδοξου εγκληματία αλλά και από επιβολή των ανάλογων κυρώσεων.

Όλα τα παραπάνω εάν ακολουθηθούν και εφαρμοστούν πιστά θα συντελέσουν στην εξέλιξη της τεχνολογίας στον ελληνικό χώρο, θα προάγουν την επιχειρηματικότητα και θα προσφέρουν τη βέλτιστη δυνατή υπηρεσία στο χρήστη. Φυσικά για να εφαρμοστεί αυτό θα πρέπει να υπάρχει άριστη συνεργασία κράτους, φορέων και παρόχων αλλά και εναρμόνιση με τους νόμους και τις οδηγίες που ορίζονται από την Ε.Ε. σχετικά με την προστασία των δεδομένων.

Κεφάλαιο 10
Αποτελέσματα Έρευνας

10.1 Συμπεράσματα

Ο χώρος του Cloud Computing αποτελεί τεχνολογία αιχμής και εξελίσσεται σε έναν τεράστιο κλάδο παροχής υπηρεσιών που εξασφαλίζουν υψηλές ταχύτητες και χαμηλότερο λειτουργικό κόστος. Ο κλάδος επεκτείνεται διαρκώς δημιουργώντας νέες αγορές και θέσεις εργασίας σε παγκόσμιο επίπεδο. Τα ιδιαίτερα χαρακτηριστικά της Ευρωπαϊκής Ηπείρου, ειδικότερα σε ότι αφορά στον κλάδο των τηλεπικοινωνιών την καθιστούν ηγέτη του κλάδου ενώ την ίδια στιγμή της δίνουν τη δυνατότητα να καλύψει το χαμένο έδαφος που προήλθε από το χώρο των τηλεπικοινωνιών.

Ως γνωστόν, κάθε νόμισμα έχει δύο όψεις και για το λόγο αυτό, όσο σύγχρονη και εξυπηρετική και αν είναι η τεχνολογία του cloud computing, ελλοχεύει μία σειρά κινδύνων που αφορούν κυρίως στην ασφάλεια των δεδομένων που ταξιδεύουν μέσα στο δίκτυο. Στην πλειοψηφία τους τα δεδομένα αυτά είναι ευαίσθητα και θα πρέπει να θωρακίζονται με τρόπο τέτοιο ώστε να μην αποτελούν στόχους των επίδοξων εγκληματιών. Οι μηχανισμοί που θα αναπτύσσονται γύρω από την τεχνολογία αυτή θα πρέπει να ενισχύονται καθημερινά, να βασίζονται σε άριστους κρυπτογραφικούς αλγορίθμους και να προστατεύουν στο μέγιστο δυνατό βαθμό την ακεραιότητα των δεδομένων και την ασφάλεια των πελατών στο χώρο του διαδικτύου.

Σύσσωμη η Ευρωπαϊκή Ένωση προβαίνει σε μία σειρά δράσεων ώστε τόσο να προωθηθεί ο τομέας του cloud computing και να εισχωρήσει στο χώρο των επιχειρήσεων ως παροχή υπηρεσιών όσο και να ενισχυθεί με το βέλτιστο δυνατό βαθμό η τεχνολογία αυτή και η ασφάλεια που θα προσφέρει στο δυνητικό καταναλωτικό κοινό της. Κάθε χώρα ξεχωριστά,

αλλά και ολόκληρη η Ευρωπαϊκή Ένωση προβαίνουν στη θέσπιση νόμων και κανονισμών που θα προστατεύουν την πνευματική ιδιοκτησία με στόχο πάντα την ενίσχυση της αξιοπιστίας του cloud computing αλλά και της εμπιστοσύνης των καταναλωτών προς την υπηρεσία αυτή.

Το κανονιστικό πλαίσιο που έχει τεθεί από την Ευρωπαϊκή Ένωση ορίζει τον τρόπο με τον οποίο θα πρέπει να λειτουργεί ο κάθε πάροχος, οι υποχρεώσεις που έχει αυτός, τα μέτρα που οφείλει να λαμβάνει αλλά τη σχέση που θα πρέπει να έχει με τον πελάτη. Η οδηγία 95/46/ΕΚ ορίζει όλες εκείνες τις ενέργειες στις οποίες οφείλουν να προβαίνουν οι πάροχοι σε ότι αφορά στη μετακίνηση, την επεξεργασία και την αποθήκευση των δεδομένων σε χώρε εντός και εκτός της Ευρωπαϊκής Ένωσης.

Καθώς οι απειλές που προκύπτουν από το διαδίκτυο είναι πολλές αλλά και οι επίδοξοι εισβολείς αναρίθμητοι, κάθε πάροχος οφείλει να προβεί στη δημιουργία μηχανισμών τέτοιων που θα διαφυλάσσουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων ενώ την ίδια στιγμή θα προσφέρουν έναν ιδιαίτερα υψηλό επίπεδο υπηρεσιών.

Μάλιστα, είναι σημαντικός ο αριθμός των παραβιάσεων που έχουν σημειωθεί γεγονός που συχνά κλονίζει την εμπιστοσύνη των καταναλωτών απέναντι στο cloud και οδήγησε την κάθε χώρα ξεχωριστά στη λήψη αυστηρών μέτρων προστασίας των προσωπικών δεδομένων.

Ο χώρος του cloud computing αποτελεί μία ιδιαίτερα υποσχόμενη τεχνολογία, η οποία θα αποτελέσει αντικείμενο σημαντικών μελετών και ερευνών στα επόμενα χρόνια τόσο για τα ιδιαίτερα και μοναδικά χαρακτηριστικά της όσο και για τους κινδύνους που φαίνεται να αντιμετωπίζει.

Η Ελλάδα λόγω των δύσκολων οικομικοκοινωνικών προβλημάτων που αντιμετωπίζει παρουσιάζεται να είναι ουραγός στην υιοθέτηση και την εξέλιξη της ιδιαίτερα χρήσιμης αυτής τεχνολογίας αλλά και στη θέσπιση κανόνων σχετικά με αυτή. Απαιτείται έντονη προσπάθεια ώστε να προωθηθούν οι υπηρεσίες που προέρχονται από το χώρο του cloud computing αλλά και συνεργασία ιδιωτικών και δημόσιων φορέων ώστε να διασφαλιστεί στο μέγιστο δυνατό βαθμό η ακεραιότητα των δεδομένων προσωπικού χαρακτήρα ενώ την ίδια στιγμή θα προσφέρεται η βέλτιστη υπηρεσία στο χρήστη.

Βιβλιογραφία

1. **Buyya, Rajkumar, και συν.** Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems.* 06 2009, σσ. 599-616.

2. **Marston, Sean, και συν.** Cloud computing — The business perspective. *Decision Support Systems.* 04 2011, σσ. 176-189.

3. **Quan, Chen και Deng, Qian Ni.** Cloud computing and its key techniques. *Journal of Computer Applications.* 2009.

4. **Subahini, S και Kavitha, V.** A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications.* 01 2011, σσ. 1-11.

5. **Dihn, Hoang, και συν.** A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing.* 12 2013, σσ. 1587-1611.

6. **Caroll, Marianna.** Secure cloud computing : Benefits, risks and controls. *2011 Information Security for South Africa.* 08 2011, σσ. 1-9.

7. **Kevis, Michael.** *Architecturing the cloud.* s.l. : Wiley, 2014.

8. **Berl, Andreas, και συν.** Energy-Efficient Cloud Computing. *The computer journal.* 08 2009, σσ. 1045-1051.

9. **Kang, Chen και Zheng, Wei - Min.** Cloud Computing: System Instances and Current Research.

10. **Vaquero, Luis M., και συν.** A break in the clouds : Towards a cloud definition. *ACM SIGCOMM Computer Communication Review.* 01 2009, σσ. 50-55.

11. **Lenk, Alexander, και συν.** What's inside the Cloud? An architectural map of the Cloud landscape. *CLOUD '09 Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing .* 2009, σσ. 23-31.

12. **Bojanova, Irena και Samba, Augustine.** Analysis of cloud computing architecture models. *2011 Workshops of International Conference on Advanced Information Networking and Applications.* 2011, σσ. 453-458.

13. Ευρωπαική Οικονομική και Κοινωνική Επιτροπή. *webapi.eesc.europa.eu.* [Ηλεκτρονικό] 15 02 2016. https://webapi.eesc.europa.eu/.../ces1606-2011_ac_el.doc.

14. *European Cloud Initiative - Building a competitive data and knowledge economy in Europe.* Brussels : European Commission, 2016.

15. Europa Eu. *eur-lex.europa.eu.* [Ηλεκτρονικό] 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1461148525752&uri=COM:2016:178:FIN.

16. ENISA. *www.enisa.com.* [Ηλεκτρονικό] 2016. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view.

17. *www.dataprotection.ie.* [Ηλεκτρονικό] 2016. https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm.

18. eur-lex.europa.eu. [Ηλεκτρονικό] 2016. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

19. **European, Union.** *Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική.* s.l. : ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ, 2012.

20. www.nis.gr. [Ηλεκτρονικό] 1997. http://www.nis.gr/npimages/docs/2472-1997.pdf.

21. www.yme.gr. [Ηλεκτρονικό] 2012. www.yme.gr/getfile.php?id=4582.

22. dide.flo.sch.gr. [Ηλεκτρονικό] 2001. dide.flo.sch.gr/Plinet/Nomothesia-Internet/PD.150-2001.pdf.

23. dide.flo.sch.gr. [Ηλεκτρονικό] 2003. dide.flo.sch.gr/Plinet/Nomothesia.../ADAE-Systasi-N.3115-2003.pdf.

24. www.katraslaw.gr. [Ηλεκτρονικό] 2011. http://www.katraslaw.gr/ki/nomothesia/244-2011-01-14-17-57-09.

25. www.minadmin.gov.gr. [Ηλεκτρονικό] 2011. www.minadmin.gov.gr/?p=1806.

26. ikee.lib.auth.gr. [Ηλεκτρονικό] 2010. http://ikee.lib.auth.gr/record/115356/files/GRI-2010-4583.pdf.

27. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. [Ηλεκτρονικό] 2016. www.dpa.gr.

28. ec.europa.eu. [Ηλεκτρονικό] 2016. ec.europa.eu/justice/data-protection/article-29/.../files/.../wp196_el.pdf.

29. ikee.lib.auth.gr. [Ηλεκτρονικό] 2015. ikee.lib.auth.gr/record/269763/files/GRI-2015-14652.pdf.

30. eur-lex.europa.eu. [Ηλεκτρονικό] 1997. http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:31997L0066.

31. www.dpa.gr. [Ηλεκτρονικό] 2002. http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/THEMATIKES_ENOTITES/ODHGIA%202002_58_EK%20_3.PDF.

32. www.adae.gr. [Ηλεκτρονικό] 2009. http://www.adae.gr/fileadmin/docs/nomoi/Odigies_EE/LexUriServ_2009.pdf.

33. **Ζεάκης, Γρηγόριος.** *Ανάλυση τεχνολογιών υποδομής για συστήματα και υπηρεσίες μεγάλης κλίμακας.* Ηράκλειο : ΤΕΙ Κρήτης.

34. computer.howstuffworks.com. [Ηλεκτρονικό] 2016. http://computer.howstuffworks.com/cloud-computing/google-cloud.htm.

35. Microsoft. *azure.microsoft.com.* [Ηλεκτρονικό] 2016. https://azure.microsoft.com/en-us/overview/what-is-azure/.

36. www.slideshare.net. [Ηλεκτρονικό] 2016. http://www.slideshare.net/deepusnath/q-burst-cloud-seminarbasics-of-cloud-computing-salesforcecom.

37. **Kuhn, Markus.** Eavesdropping attacks on computer displays. *Information Security Summit.* 2006, σσ. 1-11.

38. **Wang, Con, και συν.** Ensuring Data Storage Security in Cloud Computing. σσ. 1-9.

39. **Tanase, Mathew.** IP Spoofing: An Introduction. *www.symantec.com.* [Ηλεκτρονικό] 2003. http://www.symantec.com/connect/articles/ip-spoofing-introduction.

40. **Grimes, Roger.** Types of Password Attacks . *windowsitpro.com.* [Ηλεκτρονικό] 2006. http://windowsitpro.com/security/types-password-attacks.

41. **Rouse, Margaret.** denial of service (DoS). *searchsoftwarequality.techtarget.com.* [Ηλεκτρονικό] 2016. http://searchsoftwarequality.techtarget.com/definition/denial-of-service.

42. OWAS. *www.owasp.org.* [Ηλεκτρονικό] 2015. https://www.owasp.org/index.php/Man-in-the-middle_attack.

43. **Gajek, Sebastian, και συν.** Analysis of Signature Wrapping Attacks and Countermeasures. σσ. 1-8.

44. **Singh, Shikha, και συν.** Cloud Computing Attacks: A Discussion with solutions. *OPEN JOURNAL OF MOBILE COMPUTING AND CLOUD COMPUTING.* 08 2014, σσ. 1-10.

45. Οργανισμός Πνευματικής Ιδιοκτησίας. *www.opi.gr.* [Ηλεκτρονικό] 2016. http://www.opi.gr/index.php/2013-10-03-12-23-43/2013-10-29-08-47-46.

46. Κοινωνία της Πληροφορίας. *www.ktpae.gr.* [Ηλεκτρονικό] 2016. http://www.ktpae.gr/index.php?option=com_ktpcontests&task=Details&id=367&Itemid=13.