

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Υπολογιστική νέφους (Cloud Computing) – Νομικά ζητήματα με έμφαση στην ασφάλεια και στην προστασία προσωπικών δεδομένων»

Δημακογιάννης Γεώργιος
Μ3100010

ΑΘΗΝΑ, ΜΗΝΑΣ ΕΤΟΣ

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Υπολογιστική νέφους (Cloud Computing) – Νομικά ζητήματα με έμφαση στην ασφάλεια και στην προστασία προσωπικών δεδομένων»

Δημακογιάννης Γεώργιος

M3100010

Επιβλέπουσα Καθηγήτρια: Μήτρου Ευαγγελία
Εξωτερικός Κριτής: Τσούμας Βασίλειος

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΘΗΝΑ, ΜΗΝΑΣ ΕΤΟΣ

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Περιεχόμενα

Ευχαριστίες 6

Περίληψη 7

Abstract 11

Κεφάλαιο 1ο – Εισαγωγή στο Cloud Computing 14

1.1 Ορισμός Υπολογιστικού Νέφους (Cloud Computing) 14

1.2 Βασικά συστατικά Cloud Computing 14

1.2.1 Clients 15

1.2.2 Datacenter – Κέντρο Δεδομένων 16

1.2.3 Distributed Servers 16

1.3 Ουσιώδη Χαρακτηριστικά του Cloud Computing 17

1.4 Μοντέλα Υπηρεσίας Cloud Computing 19

1.4.1 Software as a Service (Λογισμικό νέφους ως υπηρεσία) 19

1.4.2 Infrastructure as a Service (Δομή του νέφους ως υπηρεσία) 20

1.4.3 Platform as a Service (Πλατφόρμα νέφους ως υπηρεσία) 21

1.5 Μοντέλα Ανάπτυξης Cloud Computing 22

1.5.1 Public Cloud (Δημόσιο νέφος) 22

1.5.2 Private Cloud (ιδιωτικό νέφος) 23

1.5.3 Community Cloud (Νέφος κοινότητας) 23

1.5.4 Hybrid Cloud (Υβριδικό νέφος) 24

1.6 Αρχιτεκτονική Cloud Computing 25

1.7 Υλοποιήσεις Cloud Computing 25

1.7.1 Amazon EC2 (Elastic Compute Cloud) 26

1.7.2 Google App Engine 26

1.7.3 Microsoft Azure services Platform 27

Κεφάλαιο 2ο – Το Cloud Computing στον Δημόσιο και Ιδιωτικό τομέα 30

2.1 Προσδοκίες από το Cloud Computing 30

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.2 Το Cloud Computing στο Δημόσιο Τομέα 30
2.2.1 Μείωση του κόστους των Δημόσιων Υπηρεσιών με την χρήση Cloud Computing 31
2.2.2 Οφέλη για τους συναλλασσόμενους με Δημόσιες Υπηρεσίες..... 32
2.2.3 Όλοι οι Δημόσιοι Οργανισμοί ή Φορείς μπορούν να υιοθετήσουν τεχνολογίες Cloud Computing 33
2.2.4 Προϋποθέσεις Υιοθέτησης του Cloud Computing στην Ελλάδα 34
2.2.5 Οφέλη του Cloud Computing στο περιβάλλον 35
2.2.6 Πρόσφατες έρευνες για το Cloud Computing 36
Παγκόσμια έρευνα της AMD αναδεικνύει την αναπτυσσόμενη αποδοχή του Cloud Computing 36
Έρευνα της CSA και της HP για τις απειλές αφάλειας στο Cloud Computing 38
2.3 Το Cloud Computing στον Ιδιωτικό Τομέα 41
2.3.1 Προϋποθέσεις υιοθέτησης του Cloud Computing από μία επιχείρηση . 42
2.3.2 Πλεονεκτήματα και Μειονεκτήματα υιοθέτησης του Cloud Computing για μία επιχείρηση 43
2.3.3 Υπηρεσίες Cloud Computing για τις επιχειρήσεις 47
2.3.4 Προσδιορισμός της καταλληλότητας μιας επιχείρησης για την υιοθέτηση στρατηγικών Cloud Computing 49
2.4 Δέκα από τα σημαντικότερα εμπόδια μετάβασης στο Cloud Computing 50
Κεφάλαιο 3ο – Τήρηση κι επεξεργασία δεδομένων στο Cloud Computing 54
3.1 Δεδομένα ενός πελάτη στο Cloud Computing 54
3.2 Ο κύκλος ζωής των δεδομένων 55
3.3 Ειδικά ζητήματα του κύκλου ζωής των δεδομένων στο Cloud Computing . 56
Κεφάλαιο 4ο – Ασφάλεια στο Cloud 60
4.1 Πιθανές Επιθέσεις στο Cloud Computing 60
4.2 Αρχές Ασφάλειας στο Cloud Computing 62
4.3 Ποσοτικοποίηση Κινδύνου και Πρότυπα Ασφάλειας 63

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κεφάλαιο 5ο – Ζητήματα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων: εφαρμοστέο δίκαιο, κατανομή ρόλων και ευθύνης....66
5.1 Ιδιωτικότητα και Απόρρητο....66
5.2 Ζητήματα Ιδιωτικότητας και Ασφάλειας των Δεδομένων στο Cloud Computing....67
5.3 Προσωπικά Δεδομένα....73
5.3.1 Σε ποιόν "ανήκουν" τα δεδομένα....74
5.3.2 Η προστασία των προσωπικών δεδομένων ως συνταγματικό δικαίωμα....75
5.3.3 Η Αρχή Προστασίας Προσωπικών Δεδομένων....77
5.3.4 Το δικαίωμα προστασίας των προσωπικών δεδομένων σε διεθνές επίπεδο....78
5.3.5 Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών....80
5.4 Προστασία Προσωπικών Δεδομένων στο πλαίσιο του Cloud Computing....81
5.4.1 Επεξεργασία Προσωπικών Δεδομένων....81
5.4.2 Δεδομένα Κίνησης....84
5.4.3 Τοποθεσία Παρόχου Υπηρεσιών Cloud Computing....84
5.5 Νομοθετικό Πλαίσιο στην Ελλάδα....87
5.6 Κατανομή Ρόλων και Ευθύνης....92
5.6.1 Ορισμός Υπευθύνου και του Εκτελούντος την Επεξεργασία....92
Κεφάλαιο 6ο - Προτάσεις/Συστάσεις....94
Επίλογος....98
Εικόνες....99
Βιβλιογραφία....101

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ευχαριστίες

Η εκπόνηση της παρούσας διπλωματικής εργασίας πραγματοποιήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος Σπουδών στα Πληροφοριακά Συστήματα του Οικονομικού Πανεπιστημίου Αθηνών, υπό την επίβλεψη της Επίκουρης Καθηγήτριας κα. Λίλιαν Μήτρου.

Θα ήθελα να εκφράσω τις βαθύτερες ευχαριστίες μου προς την κα. Λίλιαν Μήτρου τόσο για την ανάθεση του θέματος όσο και για την καθοδήγηση και τις χρήσιμες συμβουλές που μου παρείχε καθ' όλη τη διάρκεια της συνεργασίας μας.

Θα ήθελα επίσης να ευχαριστήσω τον Διδάκτορα κ. Βασίλειο Τσούμα για το ενδιαφέρον του και τη βοήθειά του σε ζητήματα που προέκυψαν.

Και τέλος, να εκφράσω την ευγνωμοσύνη μου στους γονείς μου και τα αδέρφια μου για την υποστήριξη και την κατανόησή τους καθ' όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

Περίληψη

Η παρούσα διπλωματική εργασία αποτελεί μια ενδελεχή έρευνα στην Υπολογιστική Νέφους (Cloud Computing) και στα νομικά ζητήματα που προκύπτουν με έμφαση στην ασφάλεια και στην προστασία των προσωπικών δεδομένων. Το Cloud Computing είναι μια καινούρια και πρωτοποριακή τεχνολογία η οποία έχει αρχίσει να αναπτύσσεται και να εδραιώνεται με ταχύτατους ρυθμούς στον τομέα της πληροφορικής και των τηλεπικοινωνιών. Εξαιτίας της καινοτομικής συμπεριφοράς που προβάλει η συγκεκριμένη τεχνολογία, οι ορισμοί που περιγράφουν την τεχνολογία του Cloud Computing είναι πολλοί, εμείς θέλοντας να περιγράψουμε με όσο το δυνατόν απλούστερη ορολογία την έννοια του Cloud Computing, θα λέγαμε ότι είναι η ανάθεση των τεχνολογιών πληροφορικής (Βάση Δεδομένων, Υπολογιστική Πόροι Εξυπηρετητές, Αποθηκευτικοί πόροι, Εφαρμογές, Υπηρεσίες, Δίκτυα κ.α.) μιας εταιρείας ή ενός οργανισμού σε τρίτους, με στόχο την υποστήριξη της εύκολης δικτυακής πρόσβασης. Ειδικότερα δίνεται η δυνατότητα σε μια εταιρεία ή οργανισμό να λαμβάνει όλες τις υπηρεσίες πληροφορικής που χρειάζεται, από κάποιον τρίτο και ανάλογα με τις απαιτήσεις που προκύπτουν να ρυθμίζει το μέγεθος αυτών των υπηρεσιών. Με την υιοθέτηση λοιπόν του Cloud Computing επιτυγχάνουμε μείωση στο κόστος των υπηρεσιών αλλά και του χρόνου διεκπεραίωσης τους.

Από τον απλούστατο ορισμό που δώσαμε παραπάνω, γίνεται σαφές ότι οι ανάθεση οποιουδήποτε είδους πληροφορίας σε τρίτους επιφέρει και αρκετούς κινδύνους. Οι κίνδυνοι που προκύπτουν από την τεχνολογία του Cloud Computing επικεντρώνονται σε ζητήματα ασφάλειας των υπηρεσιών που παρέχει, αλλά και σε ζητήματα ανασφάλειας των δεδομένων που διακινούνται, με αποτέλεσμα να πρέπει να οριστεί το νομικό πλαίσιο προστασίας των εταιρειών ή οργανισμών απο αυτούς του κινδύνους.

Εξαιτίας της ταχύρυθμης ανάπτυξης των τεχνολογιών Cloud Computing, σχεδόν όλες οι χώρες όπως και η Ελλάδα, έχουν προσαρμόσει τις νομοθετικές τους ρυθμίσεις με στόχο να προλαμβάνουν τους κινδύνους που περιγράψαμε παραπάνω. Καθίσταται λοιπόν αναγκαίο από εμάς, εκτός της τεχνικής ανάλυσης της εν λόγω τεχνολογίας, να αναλύσουμε και το νομικό πλαίσιο που την διέπει, με στόχο να παρέχεται στον αναγνώστης της παρούσας διπλωματικής εργασίας μια γενικότερη εικόνα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Αρχικά, στο 1ο Κεφάλαιο της παρούσας διπλωματικής εργασίας, προσπαθήσαμε να αναλύσουμε την έννοια του Cloud Computing και επικεντρωθήκαμε στον ορισμό της νέας τεχνολογίας. Παραθέσαμε τα βασικά συστατικά από τα οποία αποτελείται (Client, Datacenters, Distributed Servers, κ.α.) και αναλύσαμε τα ουσιώδη χαρακτηριστικά του. Εν συνεχεία, περιγράψαμε τα μοντέλα υπηρεσιών του Cloud Computing (Software as a Service, Infrastructure as a Service, Platform as a Service) και το πώς το καθένα συμβάλλει στην ανάπτυξη και προώθηση της εν λόγω τεχνολογίας. Εμβαθύναμε στα μοντέλα ανάπτυξης του Cloud Computing (Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud), στην δομή του κάθε σταδίου και στη συσχέτιση που μπορεί να προκύψει μεταξύ των σταδίων με στόχο την αποκόμιση μέγιστου κέρδους, από την εφαρμογή της νέας τεχνολογίας. Αναφερθήκαμε συνοπτικά στην αρχιτεκτονική της τεχνολογίας του Cloud Computing και ολοκληρώσαμε το κεφάλαιο με την ανάλυση κάποιων από τις πιο γνωστές υλοποιήσεις τεχνολογιών Cloud computing, από μεγάλες εταιρείες του χώρου (Amazon EC2, Google App Engine, Microsoft Azure Services Platform).

Στο 2ο Κεφάλαιο, επικεντρωθήκαμε στην εφαρμογή της τεχνολογίας του Cloud Computing στον δημόσιο και στον ιδιωτικό τομέα. Εστιάζοντας στον δημόσιο τομέα, αναφέρουμε τις προσδοκίες από το Cloud Computing, την μείωση των δημοσίων δαπανών που μπορεί να επιφέρει η εφαρμογή της εν λόγω τεχνολογίας και τα οφέλη που προκύπτουν για τους συναλλασσόμενους με τις δημόσιες υπηρεσίες. Επίσης αναλύουμε τις προϋποθέσεις κάτω από τις οποίες μπορεί ένας δημόσιος οργανισμός να υιοθετήσει τεχνολογίες Cloud υπηρεσιών και το αν μπορούν όλοι οι οργανισμοί να προσχωρήσουν στην νέα τεχνολογία. Αναφέρουμε τα οφέλη που θα είχε στο περιβάλλον η ευρεία εφαρμογή του Cloud Computing και παραθέτουμε 2 έρευνες μεγάλης κλίμακας που έγιναν από μεγάλους οργανισμούς (AMD, CSA, HP) και εστιάζουν στην αναπτυσσόμενη αποδοχή του Cloud Computing και τις απειλές ασφάλειας που προκύπτουν. Όσον αφορά τον ιδιωτικό τομέα περιγράφουμε τις προϋποθέσεις υιοθέτησης της τεχνολογίας του Cloud Computing από μια επιχείρηση, τα πλεονεκτήματα και τα μειονεκτήματα που μπορεί να επιφέρει η εφαρμογή της εν λόγω τεχνολογίας και αναφέρουμε συνοπτικά τις υπηρεσίες Cloud Computing που παρέχονται για τις επιχειρήσεις. Προσδιορίσαμε την καταλληλότητα μιας επιχείρησης για την υιοθέτηση στρατηγικών Cloud Computing και ολοκληρώσαμε το κεφάλαιο με

την παράθεση των δέκα από τα σημαντικότερα εμπόδια μετάβασης για μια επιχείρηση στην τεχνολογία του Cloud Computing.

Στο 3^{ο} Κεφάλαιο της παρούσας διπλωματικής εργασίας, εστιάσαμε την προσοχή μας στην τήρηση και επεξεργασία των δεδομένων στα πλαίσια της τεχνολογίας του Cloud Computing. Αναφερθήκαμε στα δεδομένα ενός πελάτη στο Cloud Computing, αναλύσαμε τον κύκλο ζωής των δεδομένων και ειδικότερα εστιάσαμε σε κάποια συγκεκριμένα ζητήματα που προκύπτουν όσον αφορά την βιωσιμότητα των δεδομένων στο Cloud Computing.

Στο 4^{ο} Κεφάλαιο, προσπαθήσαμε να αναδείξουμε ένα καθαρά τεχνικό ζήτημα της τεχνολογίας του Cloud Computing, την ασφάλεια. Περιγράψαμε τις πιθανές επιθέσεις που μπορεί να προκύψουν από κακόβουλους χρήστες, τις αρχές ασφάλειας που πρέπει τηρούνται στα πλαίσια του Cloud Computing και εφαρμόσαμε συγκεκριμένες διαδικασίες με στόχο την ποσοτικοποίηση του κινδύνου. Τέλος, ολοκληρώσαμε το συγκεκριμένο κεφάλαιο με την παράθεση κάποιων προτύπων ασφαλείας, των οποίων η εφαρμογή καθίσταται απαραίτητη για την ορθή και ασφαλή εφαρμογή της τεχνολογίας του Cloud Computing.

Στο 5^{ο} Κεφάλαιο της παρούσας διπλωματικής εργασίας, επικεντρωθήκαμε σε ζητήματα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων στα πλαίσια της τεχνολογίας του Cloud Computing και εστιάσαμε στο εφαρμοστέο δίκαιο, την κατανομή των ρόλων και της ευθύνης. Προσπαθήσαμε να ορίσουμε τις έννοιες της ιδιωτικότητας και του απορρήτου, να περιγράψουμε τα ζητήματα ιδιωτικότητας και ασφάλειας που προκύπτουν όσον αφορά τα δεδομένα στο Cloud Computing και να αναλύσουμε ειδικότερα τα προσωπικά δεδομένα που μπορεί να διακινηθούν μέσω της εν λόγω τεχνολογίας. Συγκεκριμένα, αναφέρουμε την προστασία των προσωπικών δεδομένων ως συνταγματικό δικαίωμα, το δικαίωμα προστασίας των προσωπικών δεδομένων σε διεθνές επίπεδο και περιγράφουμε τις πολύ σημαντικές αρχές που έχουν συσταθεί στην Ελλάδα για την τήρηση της προστασίας των προσωπικών δεδομένων, την Αρχή Προστασίας Προσωπικών Δεδομένων και τη Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών. Εν συνεχεία, επικεντρωθήκαμε στην επεξεργασία των προσωπικών δεδομένων, την τοποθεσία του παρόχου υπηρεσιών Cloud Computing και στην ανάλυση σε βάθος του νομοθετικού πλαισίου που υπάρχει στην Ελλάδα, με στόχο την ορθή και νόμιμη εφαρμογή και προώθηση της τεχνολογίας του Cloud Computing στη χώρα μας. Τέλος, ολοκληρώσαμε το

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συγκεκριμένο κεφάλαιο με τον ορισμό του υπευθύνου και του εκτελούντος την επεξεργασία των δεδομένων στα πλαίσια του Cloud Computing με απώτερο σκοπό την κατανομή των ρόλων και της ευθύνης.

Στο 6^{ο} Κεφάλαιο, με το οποίο ολοκληρώνουμε την συγγραφή της παρούσας διπλωματικής εργασίας θεωρήσαμε σωστό να παραθέσουμε κάποιες Προτάσεις/Συστάσεις προς τον αναγνώστη, με στόχο να τον αφυπνίσουμε και να τον ενημερώσουμε για την ορθολογική εφαρμογή, της καινοτόμας και πρωτοποριακής τεχνολογίας του Cloud Computing.

Abstract

The current thesis is a thorough investigation on Cloud Computing and the legal issues that arise, emphasis is given on safety and protection of personal data. Cloud Computing is a new and innovative technology that is being developed and established rapidly in the computers and telecommunications field.

Due to the innovative nature of this technology, the definitions that describe Cloud Computing are several. In an effort to describe Cloud Computing in a more simplified way, we would describe it as the assignment of computer technologies (Database, Computational Resources, Servers, Storage Resources, Applications, Services, Networks etc.) of a corporation or an organization to third parties, aiming to the support of easy network access.

Specifically, a corporation or an organization is given the possibility to receive the computer services desired from a third party and to control the size of these services according to the requirements. Therefore adopting Cloud Computing leads to cost and time reduction of the services.

From the definition given above it becomes obvious that assigning any kind of data to third parties also includes risks. The major risks of Cloud Computing involve security issues of the services but also the security of the data transferred. As a result, the legal frame for the protection of the corporations/organizations from these risks must be defined.

Since the Cloud Computing technologies are being developed rapidly, almost every country including Greece have adapted their legislations to prevent the aforementioned risks. Besides the analysis of this technology from a technical perspective, it is imperative to analyze the legal framework that surrounds it so that the reader of this thesis can form a global opinion/overview

In Chapter1 an attempt to analyze the concept of Cloud Computing and to define the new technology was made. Its basic parameters are illustrated and its most vital characteristics are examined. Further on, the models of the services of Cloud Computing (Client, Datacenters, Distributed Servers, etc.) and their contribution to the development and promotion of this technology were described. Aiming to obtain the maximum benefits from the implementation of Cloud Computing emphasis was given models of its development (Public Cloud, Private Cloud, Community Cloud,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Hybrid Cloud), the construction of each stage and correlation that may exist between the stages. Finally, the first chapter includes a brief reference to the architecture of the Cloud Computing technology and the analysis of some application examples, the implementation of the new technology to big corporations such as Amazon EC2, Google App Engine and Microsoft Azure Services Platform was studied.

Chapter 2 mainly deals with the implementation of the technology to the public and the private sector. Regarding the public sector, the prospects of Cloud Computing, the reduction of public expenditures and the benefits it induces to the civilians are analyzed. Additionally, the conditions under which an organization can adopt Cloud services and if all organizations can adopt them are investigated. The benefits on the environment of the wide range implementation of Cloud computing are mentioned and the results of two large scale investigations that were carried out by big organizations (AMD, CSA, HP) and focused on the constantly increasing acceptance of Cloud Computing and the security threats from its use are given. As far as the private sector is concerned, the requirements for use of the Cloud Computing are described, the advantages and disadvantages from its use and a brief reference is made to the services Cloud Computing can provide to corporations. The capability of a corporation to adopt Cloud Computing strategies is defined and finally, ten of the most important drawbacks for the use of Cloud Computing are given.

In the 3rd chapter of the current thesis, we focus on maintaining and processing the data under Cloud computing technology. We made reference to the data of a client in Cloud Computing, we analyzed life cycle of these data and more specifically we focused on certain issues that deal with data existence in Cloud Computing.

In Chapter 4, a purely technical issue of Cloud Computing, safety, is highlighted. The possible assaults from bad users, the security principles that must be followed are described and certain procedures for the quantification of threat are applied. This Chapter ends with some security standards that are necessary for the correct and safe implementation of Cloud Computing.

The 5th Chapter deals with the protection of personal data and privacy in the framework of Cloud Computing technology and with the legislations, the distribution of responses. The concept of privacy was analyzed and in particular the personal data that may be transferred through this technology. Protection of personal data is defined

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

as a constitutional right, this right exists in internationally. The most important authorities for the protection of personal data in Greece, the Data Protection Authority and the Assurance of confidentiality of communications Authority, are described. The processing of personal data, the service provider and the analysis of the relative legislation in Greece are examined, aiming to the correct and legal implementation and promotion of the Cloud Computing technology. The chapter is finished with the definition of the person in charge of the processing of the data, the distribution of roles and responsibilities.

To conclude, in the 6th and final Chapter of this thesis, some suggestions/recommendations are given to the readers, in an attempt to draw their attention and inform them on the correct implementation of the new and innovative technology of Cloud Computing.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κεφάλαιο 1ο – Εισαγωγή στο Cloud Computing

1.1 Ορισμός Υπολογιστικού Νέφους (Cloud Computing)



Το Cloud Computing έχει λάβει το όνομα του ως μια επέκταση της αφηρημένης εικόνας του σύννεφου (Cloud), με την όποια απεικονίζουμε το Internet. Αυτό το εικονίδιο του σύννεφου (Cloud) αναφέρεται σε "όλα τα άλλα πράγματα" που καθιστούν ένα δίκτυο λειτουργικό. Θα έλεγε κάνεις ότι αποτελεί το ανάλογο του ceteris paribus που χρησιμοποιείται στην Οικονομική Επιστήμη, είναι δηλαδή είδος "κλπ" για το κόσμο των υπολογιστών[1].



Στη σημειολογία του κόσμου της πληροφορικής τεχνολογίας, το σύννεφο (Cloud) σημαίνει μια περιοχή του διαδικτυακού διαγράμματος που αποτελεί μέλημα κάποιου άλλου.

Η βασική αρχή του Cloud Computing εστιάζεται στην υποστήριξη της εύκολης δικτυακής πρόσβασης σε μια ομάδα από παραμετροποιήσιμους υπολογιστικούς πόρους (όπως δίκτυα, εξυπηρετητές, αποθηκευτικούς πόρους, εφαρμογές, υπηρεσίες). Οι υπολογιστικοί πόροι είναι διαθέσιμοι με την ελάχιστη προσπάθεια διαχείρισης και αλληλεπίδρασης από τον πάροχο της συγκεκριμένης υπηρεσίας. Το συγκεκριμένο μοντέλο προωθεί την διαθεσιμότητα και αποτελείται από έξι σημαντικά χαρακτηριστικά, τρία μοντέλα υπηρεσίας και τέσσερα μοντέλα ανάπτυξης.

1.2 Βασικά συστατικά Cloud Computing



Σε μια απλή τυπολογικά αναπαράσταση ενός συστήματος Cloud συναντάμε τα ακόλουθα στοιχεία: υπολογιστές-πελάτες, datacenter και διακομιστές διανομής. Κάθε στοιχείο έχει ένα σκοπό και παίζει ένα συγκεκριμένο ρόλο στην αποτελεσματική λειτουργία μια εφαρμογής που «τρέχει» σε περιβάλλον cloud.

1.2.1 Clients

Οι υπολογιστές-πελάτες σε μια αρχιτεκτονική Cloud Computing, παίζουν τον ίδιο ρόλο με αυτόν στα κλασσικά συστήματα τοπικού δικτύου (LAN). Είναι, συνήθως, οι υπολογιστές που απλώς βρίσκονται στο γραφείο μας, αλλά και νέοι τύποι υπολογιστικών μηχανών, όπως φορητοί υπολογιστές, υπολογιστές tablet, κινητά τηλέφωνα ή PDA. Γενικά ως υπολογιστές-πελάτες λογίζονται όλες οι συσκευές με τις οποίες οι τελικοί χρήστες αλληλεπιδρούν και διαχειρίζονται πληροφορίες που βρίσκονται στο Cloud.

Οι υπολογιστές-πελάτες εμπίπτουν εν γένει σε μια από τις ακόλουθες κατηγορίες:

- **Φορητοί/Mobile:** Οι φορητές συσκευές περιλαμβάνουν τα PDA ή smartphones, Blackberry, Windows Mobile Smartphone ή το iPhone.
- **Thin Clients:** Οι υπολογιστές που δεν διαθέτουν εσωτερικές μονάδες σκληρού δίσκου, αλλά χρησιμοποιούν κάποιον διακομιστή για να επεξεργαστεί τα δεδομένα, και στη συνέχεια εμφανίζονται οι πληροφορίες.
- **Thick Clients:** Αυτός ο τύπος πελάτη είναι ένας πλήρης υπολογιστής, που χρησιμοποιεί ένα πρόγραμμα περιήγησης στο web όπως Firefox ή Internet Explorer, για να συνδεθεί με το Cloud. Οι Thin Clients γίνονται όλο και πιο δημοφιλή λύση, λόγω της τιμής και της περιορισμένης επιβάρυνσης του περιβάλλοντος. Επιπρόσθετα μπορούμε να εντοπίσουμε ορισμένα πρόσθετα πλεονεκτήματα από την χρήση thin client.

  1. **Χαμηλότερο κόστος υλικού**, οι thin clients είναι φθηνότεροι από τους κλασικούς υπολογιστές-πελάτες επειδή περιέχουν λιγότερο εξοπλισμό, ενώ έχουν μεγαλύτερη διάρκεια ζωής, καθότι αντικαθίστανται πολύ αργότερα (απαξιώνονται με πολύ αργό ρυθμό)
  2. **Ασφάλεια:** εφόσον η επεξεργασία λαμβάνει χώρα στο διακομιστή και δεν υπάρχει καμία μονάδα σκληρού δίσκου, υπάρχει μικρότερη πιθανότητα κάποιο κακόβουλο λογισμικό να πλήξει τη συσκευή. Επίσης, οι thin clients δε λειτουργούν χωρίς διακομιστή και άρα δεν υπάρχει κίνητρο κλοπής τους.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3. **Ασφάλεια Δεδομένων:** δεδομένου ότι τα δεδομένα είναι αποθηκευμένα στο διακομιστή, υπάρχει μικρότερη πιθανότητα να χαθούν εάν χαλάσει η συσκευή ή αν ο υπολογιστής-πελάτης κλαπεί
4. **Μικρότερη κατανάλωση ενέργειας :** οι thin clients καταναλώνουν λιγότερη ενέργεια από τους κλασικούς υπολογιστές-πελάτες. Αυτό σημαίνει μικρότερο κόστος λειτουργίας, και λιγότερη έκκληση θερμότητας στο περιβάλλον.
5. **Ευκολία στην επισκευή ή την αντικατάσταση:** όταν ένας thin client ολοκληρώσει τον κύκλο ζωή του είναι εύκολο να αντικατασταθεί. Απλά αντικαθιστάμε τη συσκευή και σε μηδενικό χρόνο ο σταθμός μπαίνει σε παραγωγική φάση, ακριβώς όπως ήταν πριν από την αστοχία[4,5].

1.2.2 Datacenter – Κέντρο Δεδομένων

Το κέντρο δεδομένων αποτελεί τη συλλογή διακομιστών που «φιλοξενούν» τις εφαρμογές που εκτελούμε. Το datacenter θα μπορούσε να είναι είτε ένα μεγάλο δωμάτιο στο υπόγειο του κτιρίου ή ένα δωμάτιο γεμάτο από διακομιστές στην άλλη μεριά της γης, στο οποίο έχουμε πρόσβαση μέσω του διαδικτύου. Μια αυξανόμενη τάση στον κόσμο πληροφορικής αποτελεί η χρήση εικονικών διακομιστών. Δηλαδή, το λογισμικό μπορεί να εγκατασταθεί σε ένα μονό φυσικό τμήμα του διακομιστή, επιτρέποντας σε άλλες εφαρμογές να «τρέχουν» άλλες εικονικές συσκευές. Με αυτόν τον τρόπο μπορούμε να έχουμε πολλούς εικονικούς διακομιστές που εκτελούνται σε φυσικό διακομιστή[6].

1.2.3 Distributed Servers

Οι διακομιστές δεν βρίσκονται πάντα στην ίδια φυσική τοποθεσία. Συχνά, οι servers είναι σε διαφορετικές γεωγραφικά θέσεις. Παραταύτα, για το συνδρομητή του Cloud, αυτοί οι διακομιστές λειτουργούν σαν να ήταν μια φυσική οντότητα.

Αυτό δίνει στην υπηρεσία μεγαλύτερη ευελιξία σε επιλογές και ασφάλεια. Για παράδειγμα, η Amazon προσφέρει μια λύση Cloud χρησιμοποιώντας διακομιστές που βρίσκονται κατανεμημένοι σε διάφορα σημεία σε όλον τον

κόσμο. Έτσι, αν κάτι συμβεί σε μία τοποθεσία και προκαλέσει μία αστοχία, η υπηρεσία θα εξακολουθεί να είναι προσβάσιμη μέσω μιας άλλης τοποθεσίας. Επίσης, εάν υπάρξει απότομη αύξηση της ζητούμενης επεξεργαστικής ισχύος (cpu time), δεν χρειάζεται να «αγοράσουμε» νέες μηχανές, αλλά αρκεί απλά να μεταφερθούμε, μέσω διαδικτυακών πόρων, σε μια άλλη τοποθεσία, για την εξυπηρέτηση της τρέχουσας ανάγκης[7].

1.3 Ουσιώδη Χαρακτηριστικά του Cloud Computing

Υπάρχουν έξι ουσιώδη χαρακτηριστικά του Cloud Computing, τα οποία εξηγούν τη σχέση και τη διαφορά που υφίσταται συγκριτικά με τις παραδοσιακές υπολογιστικές μεθόδους[20].

1. **On-demand self-service (Αυτό - εξυπηρέτηση κατά απαίτηση)**
   Ο χρήστης μπορεί μονομερώς να χρησιμοποιεί υπολογιστικούς πόρους όπως χρόνος του εξυπηρετητή και αποθηκευτικούς πόρους δικτύου, αυτόματα, ανάλογα με τις ανάγκες του, χωρίς να απαιτείται διάδραση από τον πάροχο της συγκεκριμένης υπηρεσίας
2. **Broad network access (Ευρεία πρόσβαση στο δίκτυο)**
   Οι δυνατότητες / πόροι είναι διαθέσιμοι μέσα από το δίκτυο στο οποίο μπορεί κανείς να έχει πρόσβαση μέσα από γνωστούς μηχανισμούς, οι οποίοι προωθούν την χρήση ετερογενών τερματικών συσκευών στην πλευρά του τελικού χρήστη
3. **Resource pooling (Διάθεση πόρων)**
   Οι υπολογιστικοί πόροι του πάροχου είναι συγκεντρωμένοι έτσι ώστε να μπορούν να εξυπηρετήσουν παράλληλα πολλούς πελάτες χρησιμοποιώντας το μοντέλο multi-tenant, να χρησιμοποιήσουν διαφορετικούς φυσικούς και εικονικούς πόρους οι οποίοι θα έχουν αντιστοιχηθεί δυναμικά ανάλογα με τη ζήτηση του κάθε πελάτη. Ο χρήστης δεν έχει τον έλεγχο ή την γνώση για την ακριβή τοποθεσία (όπως χώρα, περιοχή ή data center). Οι πόροι μπορεί να είναι αποθηκευτικός χώρος, υπολογιστική ισχύς, μνήμη, εύρος ζώνης και εικονικές μηχανές
4. **Rapid elasticity (Ταχεία ελαστικότητα)**
   Οι πόροι αυτοί μπορούν με πιό ευέλικτο τρόπο να αυξηθούν πολύ γρήγορα, σε πολλές περιπτώσεις, με αυτόματο τρόπο, έτσι ώστε να μην υπάρχει διάδραση με τον πελάτη με σκοπό την αποφυγή χρονοβόρων διαδικασιών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

5. **Measured service (Μετρούμενη υπηρεσία)**

   Τα Cloud συστήματα έχουν την δυνατότητα αυτόματα να ελέγχουν και να βελτιώνουν τους διαθέσιμους πόρους χρησιμοποιώντας ένα μηχανισμό μέτρησης, ανάλογα με τον τύπο της προσφερόμενης υπηρεσίας. Οι χρησιμοποιούμενοι πόροι μπορούν να ελέγχονται και να παρακολούθούνται χωρίς να γίνονται αντιληπτοί τόσο στον πάροχο όσο και στον χρήστη της χρησιμοποιούμενης υπηρεσίας

6. **Sharing of infrastructure (Κοινή χρήση των υποδομών)**

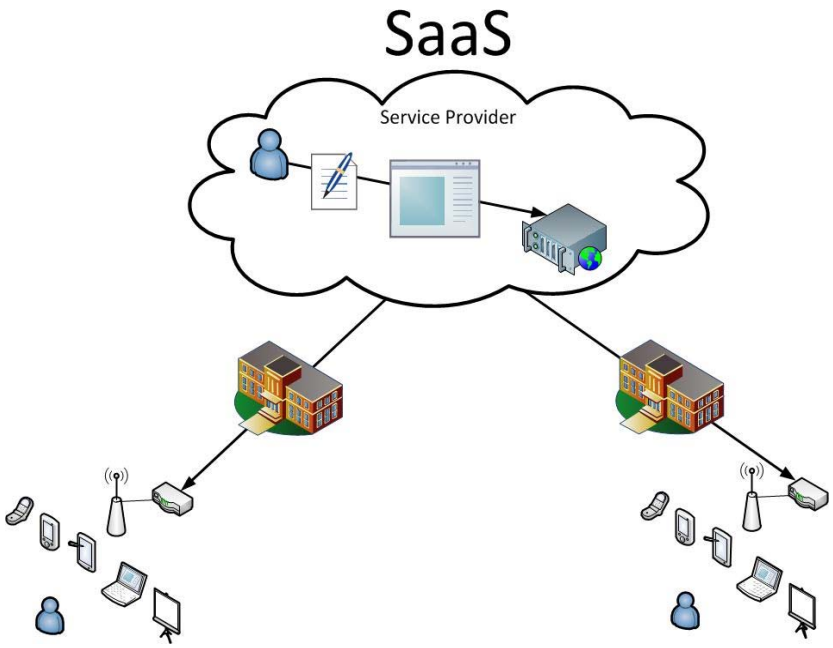
   Το φυσικό hardware που εκτελεί το λογισμικό δεν έχει αντιστοίχηση 1:1, δηλαδή ο εξυπηρετητής (server) μπορεί να εκτελεί λειτουργίες πολλών εικονικών εξυπηρετητών επιτρέποντας την εξοικονόμηση πόρων. Άρα οι τελικοί χρήστες μπορούν να έχουν περισσότερα οφέλη με λιγότερους πόρους (hardware) και μπορεί τώρα ο πάροχος της υπηρεσίας να πουλήσει τους ανεκμετάλλευτους πόρους αλλού, αν το επιθυμεί

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

1.4 Μοντέλα Υπηρεσίας Cloud Computing

Το Cloud Computing είναι μια έννοια που περικλείει διάφορες υλοποιήσεις με βασικότερες τις εξής:

1.4.1 Software as a Service (Λογισμικό νέφους ως υπηρεσία)



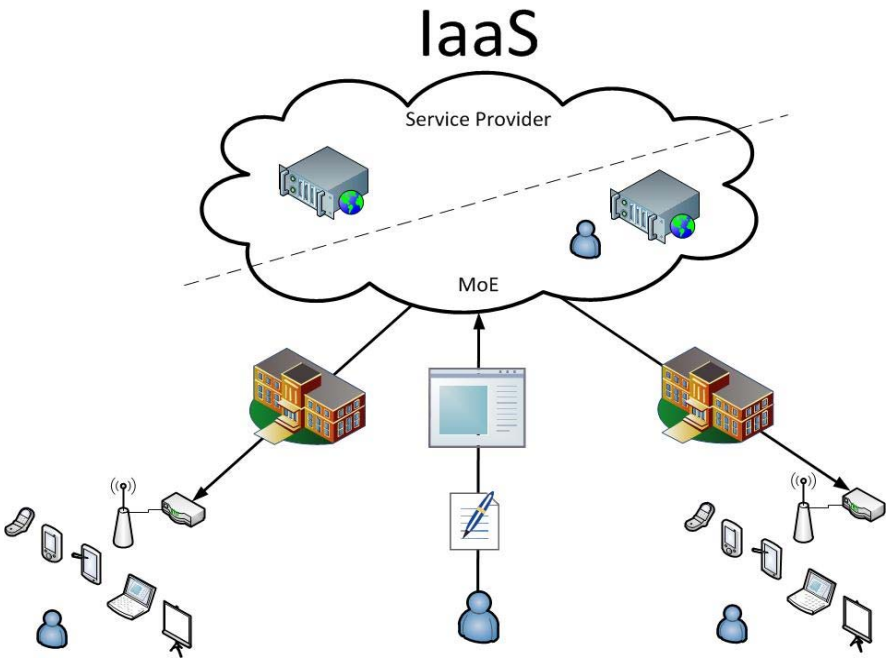
Εικόνα 1

Πρόκειται για όλες τις εφαρμογές λογισμικού που λειτουργούν με την μορφή υπηρεσίας μέσω του internet. Το λογισμικό ως υπηρεσία (Software as a Service - SaaS) είναι το μοντέλο κατά το οποίο η εφαρμογή φιλοξενείται σε κεντρικούς διακομιστες και για την πρόσβασή τους οι πελάτες χρησιμοποιούν φυλομετρητές τύπου Internet Explorer ή chrome. Όταν το λογισμικό φιλοξενείται εκτός της εταιρίας, ο πελάτης δεν χρειάζεται να δαπανά χρήματα για την υποστήριξη των εφαρμογών. Από την άλλη πλευρά, χάνουμε τον έλεγχο των δεδομένων/εφαρμογών και τον παραχωρούμε σε τρίτους.

Για τους προμηθευτές, η πλατφόρμα SaaS γίνεται ελκυστική, καθότι παρέχει αποτελεσματικότερη προστασία της πνευματικής ιδιοκτησίας, ενώ παράλληλα δημιουργούν μια συνεχή ροή εισοδήματος. Υπάρχουν πολλοί τύποι λογισμικού που προσφέρονται για το μοντέλο SaaS. Συνήθως, λογισμικό το οποίο εκτελεί μια απλή εργασία χωρίς μεγάλη ανάγκη αλληλεπίδρασης με

άλλα συστήματα καθίσταται ιδανικό για παροχή μέσω SaaS. Οι πελάτες που δεν έχουν την τάση να αναπτύσσουν το δικό τους λογισμικό, αλλά έχουν ανάγκη από εφαρμογές με υψηλές απαιτήσεις σε υπολογιστικούς πόρους, μπορούν να επωφεληθούν επίσης από την πλατφόρμα SaaS (Customer resource management (CRM), Video conferencing, IT,service management, Accounting, Web analytics, Web content management)[8].

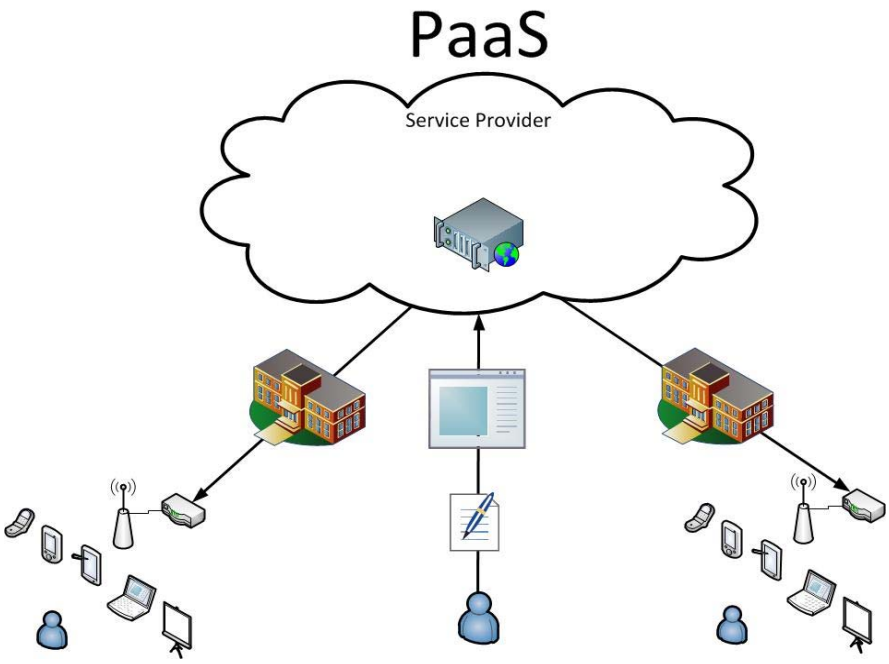
1.4.2 Infrastructure as a Service (Δομή του νέφους ως υπηρεσία)



Εικόνα 2

Αυτή είναι μια δυνατότητα που παρέχεται στον καταναλωτή, η οποία τον εφοδιάζει με λειτουργίες επεξεργασίας, αποθήκευσης, δικτύου και άλλους θεμελιώδεις υπολογιστικούς πόρους στους οποίους ο χρήστης είναι ικανός να αναπτύξει και να τρέξει οποιασδήποτε μορφής λογισμικού, όπως λειτουργικά συστήματα ή προγράμματα[13,14].

1.4.3 Platform as a Service (Πλατφόρμα νέφους ως υπηρεσία)



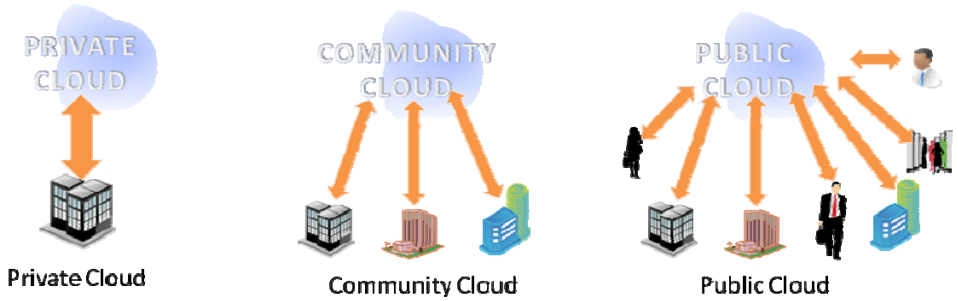
Εικόνα 3

Πρόκειται για τη διαχειριστική πλατφόρμα, μέσω της οποίας γίνεται όλη η διαχείριση και απομακρυσμένη παραμετροποίηση του IaaS, καθώς και των SaaS εφαρμογών που είναι εγκατεστημένες στο IaaS. Επίσης συμπεριλαμβάνει τα APIs (Application Programming Interface) που επιτρέπουν τη διασύνδεση δυνατοτήτων servers, χωρίς την προϋπόθεση να στηθούν ξεχωριστά για την χρήση τους από οποιοδήποτε SaaS μας ενδιαφέρει. Για παράδειγμα εδώ μπορούμε να πούμε ότι κάποιος IT Manager δεν είναι υποχρεωμένος να στήσει έναν ξεχωριστό mail server αλλά να χρησιμοποιήσει το ανάλογο API του PaaS ώστε να καλύψει την ανάγκη της εφαρμογής του.

Η πλατφόρμα PaaS περιλαμβάνει τη σχεδίαση, ανάπτυξη, δοκιμή και φιλοξενία εφαρμογών. Άλλες υπηρεσίες περιλαμβάνουν συνεργατικές υποδομές, ενοποίηση υπηρεσιών παγκοσμίου ιστού, βάσεις δεδομένων, ασφάλεια, αποθήκευση, διαχείριση και τήρηση ιστορικού εκδόσεων (versioning)[5].

1.5 Μοντέλα Ανάπτυξης Cloud Computing

Υπάρχουν τέσσερα μοντέλα ανάπτυξης του Cloud Computing και χωρίζονται στις εξής κατηγορίες:



Εικόνα 4

1.5.1 Public Cloud (Δημόσιο νέφος)

Η υποδομή του Cloud μπορεί είναι διαθέσιμη στο κοινό ή σε μια μεγάλη ομάδα από οργανισμούς / επιχειρήσεις και ανήκει σε ένα οργανισμό που διαχειρίζεται υπηρεσίες Cloud. Στην απλούστερη εκδοχή του ένα δημόσιο σύννεφο είναι διαθέσιμο εξωτερικά στον τελικό χρήστη με μικρό περιορισμό για το ποιός μπορεί να γίνει χρήστης της υπηρεσίας επι πληρωμή. Οι πιο κοινές μορφές του public Cloud είναι προσβάσιμες μέσω διαδικτύου. Τα τελευταία χρόνια έχει υπάρξει τεράστια ανάπτυξη του public Cloud με αποτέλεσμα να υπάρχει μεγάλη προσφορά σε υπηρεσίες IaaS από εταιρίες όπως η Amazon με την EC2, την IBM BlueCloud και την Rackspace Cloud offering. Άλλες μορφές προσφοράς public Cloud σε υπηρεσίες PaaS γίνονται από την Google με το AppEngine & το Windows Azure.

Στο βασικό επίπεδο, τα δημόσια σύννεφα έχουν μοναδικά στοιχεία ασφαλείας και κριτήρια αξιολόγησης. Τα public Cloud μπορούν να διαμορφωθούν από τους παρόχους υπηρεσιών που θέλουν μια υποδομή μεγάλης δυναμικότητας και ένα ευρύ φάσμα πελατών. Ως αποτέλεσμα τα δεδομένα μπορούν να αποθηκευτούν σε κοινά μέσα αποθήκευσης, κάτι που καθιστά απαραίτητη την κωδικοποίηση των δεδομένων για μεγαλύτερη ασφάλεια. Πρέπει να αναφερθεί πως η υπηρεσία του public Cloud αντιμετωπίζεται με εμπιστοσύνη από τούς συνδρομητές τέτοιων υπηρεσιών[19].

1.5.2 Private Cloud (ιδιωτικό νέφος)

Η υποδομή του Cloud λειτουργεί αποκλειστικά για ένα οργανισμό, ο οποίος την διαχειρίζεται ο ίδιος ή την αναθέτει σε κάποιον τρίτο. Επίσης δίνεται η δυνατότητα η υποδομή του Cloud να βρίσκεται στις κτιριακές υποδομές του ίδιου του οργανισμού. Σε αντίθεση με τα Public Clouds, τα Private Clouds είναι εσωτερικά φιλοξενούμενα. Τα Private Clouds ανταπεξέρχονται αρκετά καλά στα πρότυπα ασφάλειας των δεδομένων, ακριβώς όμως επειδή είναι ιδιωτικά δεν σημαίνει ότι είναι και πιο ασφαλή. Στο Private Cloud, εκτιμήσεις όπως εξασφάλιση του εικονικού περιβάλλοντος (που είναι το λογισμικό, το φυσικό υλικό "hardware", και το "firmware") γίνονται από τον πελάτη, εν αντίθεση με το Public Cloud, που όλα αυτά τα αναλαμβάνει ο πάροχος υπηρεσίας.

Κατά συνέπεια, σε συγκρίσεις του Private με το Public Cloud, είναι δύσκολο να κάνουμε γενικεύσεις για το ποιό είναι ασφαλέστερο απο τα δύο. Το πραγματικό πλεονέκτημα ενός ιδιωτικού Cloud είναι ότι ο πάροχος της υπηρεσίας καλείται να κάνει το περιβάλλον της διεπαφής να βρίσκεται περισσότερο κοντά στις ανάγκες του εκμισθωτή[19].

1.5.3 Community Cloud (Νέφος κοινότητας)

Η υποδομή του Cloud είναι διαμοιρασμένη σε διάφορους οργανισμούς και υποστηρίζει προκαθορισμένες κοινότητες που μπορεί να έχουν κοινές απαιτήσεις, σε επίπεδο ασφάλειας, λειτουργικότητας, αποστολής. Η υποδομή Cloud σε αυτήν την περίπτωση διαχειρίζεται από τον οργανισμό ή από κάποιον εξωτερικό πάροχο και μπορεί να βρίσκεται στις κτιριακές υποδομές του οργανισμού. Η υπόσχεση των Community Clouds είναι ότι επιτρέπουν πολλαπλές ανεξάρτητες οντότητες για να κερδίσουν τα κόστη-κέρδη ενός κοινού μη δημοσίου σύννεφου, αποφεύγοντας την ασφάλεια και ρυθμιστικές ανησυχίες που μπορούν να υπάρξουν σε ένα κοινό σύννεφο που δεν τα έχει προβλέψει στο SLA (Service-level agreement) του.

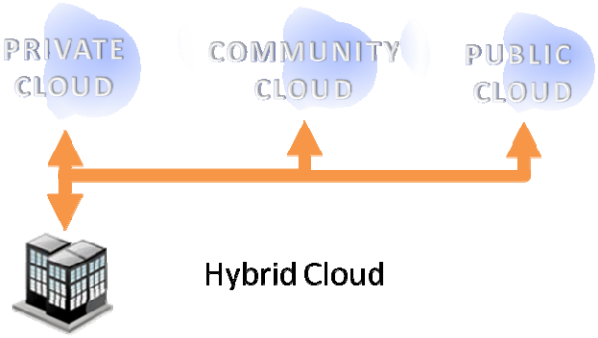
Αυτό το πρότυπο έχει τεράστιες δυνατότητες για τις οντότητες ή τις επιχειρήσεις που υπόκεινται σε ρυθμιστικές συμμορφώσεις ή περιορισμούς. Τα διάφορα Community Clouds θεωρούνται από τις Ηνωμένες Πολιτείες και την Ευρωπαϊκή Ένωση ως τοπικά επίπεδα. Αυτό έχει μεγάλο νόημα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δεδομένου ότι υπάρχουν πολλαπλάσια οφέλη και στα δύο ως μεμονωμένες οντότητες καθώς επίσης και συλλογικά[19].

1.5.4 Hybrid Cloud (Υβριδικό νέφος)

Η Cloud υποδομή είναι μια σύνθεση από ένα ή περισσότερα Clouds (private, community, or public) τα οποία είναι ξεχωριστές οντότητες και επιτρέπουν τη μεταφορά τόσο των δεδομένων όσο και των εφαρμογών (e.g. Cloud bursting for load-balancing between Clouds)



Εικόνα 5

Στην παραπάνω εικόνα μπορούμε να δείξουμε πως ένας οργανισμός μπορεί να εκμεταλλευτεί τις δυνατότητες του ιδιωτικού του Cloud και να εκτείνει τις δυνατότητες του κοινού Cloud έτσι ώστε να δημιουργήσει ένα υβριδικό μοντέλο. Τα υβριδικά σύννεφα είναι ότι ακριβώς περιγράφει το όνομα τους. Τα σύννεφα αυτά διαμορφώνονται από τους οργανισμούς όταν δημιουργούν ιδιωτικά σύννεφα, και θέλουν οι κοινότητες τους να έχουν διασύνδεση με τα δημόσια σύννεφα τους για συγκεκριμένους σκοπούς. Η διασύνδεση του ιδιωτικού με το δημόσιο σύννεφο για την εξυπηρέτηση συγκεκριμένων σκοπών δημιουργεί το υβριδικό σύννεφο. Πραγματικά ένα υβριδικό Cloud μπορεί να δημιουργηθεί από την σύνδεση τριών Cloud, ένα δημόσιο, ένα ιδιωτικό και ένα community. Πολλοί οργανισμοί επεκτείνουν το εσωτερικό ιδιωτικό τους Cloud για την κρίσιμη υποδομή τους και ικανοποιούν ανάγκες που δεν είναι οικονομικές για να δημιουργηθούν εσωτερικά[19].

1.6 Αρχιτεκτονική Cloud Computing

Οι περισσότερες υλοποιήσεις του Cloud Computing σήμερα βασίζονται στην παροχή αξιόπιστων υπηρεσιών με την χρήση data centers τα οποία είναι χτισμένα με την χρήση διαφόρων επιπέδων τεχνολογιών εικονικοποίησης (virtualization). Οι Cloud υπηρεσίες είναι προσβάσιμες σε όλους του χρήστες του διαδικτύου. Επίσης τα Clouds προσφέρουν ένα σημείο εισόδου για κάθε υπηρεσία καθώς αποτελούν κατανεμημένα συστήματα αδιαφανή προς τους χρήστες, δηλαδή ο χρήστης δεν είναι σε θέση να γνωρίζει ποιος εξυπηρετητής του προσφέρει την υπηρεσία που λαμβάνει καθώς αυτός είναι κάπου μέσα στο Cloud. Τα Clouds γενικότερα προσφέρουν συγκεκριμένα πρότυπα ποιότητας υπηρεσίας (QoS) και στους εμπορικούς πελάτες τους προσφέρουν Συμφωνίες Επιπέδου Υπηρεσίας (Service Level Agreements). Τα ανοιχτά πρότυπα και το λογισμικό ανοιχτού κώδικα γενικότερα έχουν προσφέρει ιδιαίτερα στην ανάπτυξη πολλών υλοποιήσεων του Cloud Computing μέχρι σήμερα[15].

1.7 Υλοποιήσεις Cloud Computing

Στην ενότητα αυτή θα αναφερθούμε σε κάποιες από τις πιο δημοφιλείς υλοποιήσεις του Cloud Computing και θα συγκρίνουμε τις διαφορές μεταξύ τους έτσι ώστε να δώσουμε ένα έμπρακτο παράδειγμα λειτουργίας του Cloud Computing.

Cloud Computing	Cloud storage
Amazon	Amazon S3
Microsoft	Intermap XIP Cloud Storage
Flexiant	Nirvanix
Google	Windows Azure
OneNet	PhoneKlone
Joyent	Dropbox
Rackspace Cloud	Box.net
Salesforce	

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Skytap	
Jitscale	
Tata IAAS	
Dedicated Now	

Συγκεντρωτικός πίνακας παρόχων υπηρεσιών Cloud Computing

1.7.1 Amazon EC2 (Elastic Compute Cloud)

Το βασικό μοντέλου του EC2 δίνει την δυνατότητα στον χρήστη να νοικιάζει υλικό, πάνω στο οποίο μπορούν να τρέξουν εικονικές μηχανές (virtual machines). Ο χρήστης έχει την δυνατότητα να δημιουργήσει, να εκτελέσει και να τερματίσει την λειτουργία εικονικών μηχανών κατά βούληση, όπως αυτός θέλει πληρώνοντας με την ώρα χρήσης. Επίσης μπορεί να έχει κάποιες περιορισμένες επιλογές στο επίπεδο του hardware, πάνω στο οποίο θα τρέχουν οι εικονικές μηχανές. Αρχικά προσέφερε εικονικές μηχανές, που έτρεχαν GNU/Linux, Open Solaris και τελευταία προσέθεσε την δυνατότητα δημιουργίας εικονικών μηχανών με Microsoft Windows.

Από άποψη αρχιτεκτονικής το EC2 χρησιμοποιεί την μηχανή Xen[16] για την δημιουργία και διαχείριση των εικονικών μηχανών. Κάθε εικονική μηχανή λειτουργεί ως εικονικός εξυπηρετητής και ανάλογα με τις υπολογιστικές δυνατότητες, την κύρια μνήμη που διαθέτουν και τον αποθηκευτικό χώρο, που έχουν οι εικονικές μηχανές χωρίζονται σε μικρές, μεσαίες και μεγάλες[10].

1.7.2 Google App Engine

Η App Engine της Google είναι διαμετρικά αντίθετη αντιμετώπιση του Cloud Computing. Το AppEngine είναι στοχευόμενο 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[17].

Η App Engine δεν μπορεί να έχει τόσο ευρεία χρήση όπως το EC2 καθώς δεν επιτρέπει ευελιξία στην υποδομή του συστήματος αλλά παρέχοντας αυτή την υποδομή απαλλάσσει τους δημιουργούς από τις ανάγκες διαχείρισης και τα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

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.

Περιορισμοί που επιβάλλονται από την App Engine:

- 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 python modules αλλά μόνο αν είναι γραμμένα σε καθαρή python.
- Η App Engine περιορίζει τις μέγιστες επιστρεφόμενες εγγραφές από την βάση δεδομένων σε 1000 ανά κλήση.
- Οι Java εφαρμογές μπορούν να χρησιμοποιήσουν μόνο ένα μέρος του JRE.
- Οι Java εφαρμογές δεν μπορούν να δημιουργήσουν καινούργια νήματα.

Όπως είναι προφανές η App Engine αποτελεί μια τελείως διαφορετική υλοποίηση Cloud Computing[11].

1.7.3 Microsoft Azure services Platform

Η πλατφόρμα υπηρεσιών Azure της Microsoft είναι μια ενδιάμεση υλοποίηση ευέλικτη και παράλληλα προσφέρει στους προγραμματιστές έτοιμες δυνατότητες. Οι βιβλιοθήκες, που προσφέρει, δίνουν την δυνατότητα για αυτόματη ρύθμιση του δικτύου και ανάνηψη από λάθη, αλλά προϋποθέτουν από τον χρήστη να ρυθμίσει κάποιες παραμέτρους[17].

Το Azure τρέχει πάνω σε datacenters, που έχει δημιουργήσει η Microsoft για το σκοπό αυτό. Παρέχει ένα Cloud λειτουργικό σύστημα, που ονομάζεται Windows Azure, που επιτρέπει την εκτέλεση εφαρμογών και παρέχει ένα σύνολο υπηρεσιών, που επιτρέπουν την εγκατάσταση, τον έλεγχο και την φιλοξενία εφαρμογών, που τρέχουν εκτός των datacenters της Microsoft.

Βασικό στοιχείο της αρχιτεκτονικής των Azure είναι ο Fabric Controller, που λειτουργεί ως εικονική δεξαμενή πολλών υπολογιστικών συστημάτων και αυτόματα διαχειρίζεται τους πόρους αλλά και ισορροπεί των φόρτο εργασίας

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αυτών. Επίσης ελέγχει την ύπαρξη αντιγράφων των δεδομένων ανά γεωγραφική περιοχή[12,18].

	Amazon Web Services	Microsoft Azure	Google AppEngine
Computation model (VM)	• x86 Instruction Set Architecture (ISA) via Xen VM • Computation elasticity allows scalability, but developer must build the machinery, or third party VAR such as RightScale must provide it	• Microsoft Common Lan-guage Runtime (CLR) VM; common intermediate form executed in managed envi-ronment • Machines are provi-sioned based on declarative descriptions (e.g. which "roles" can be replicated); automatic load balancing	• Predefined application structure and framework; programmer-provided "han-dlers" written in Python, all persistent state stored in MegaStore (outside Python code) • Automatic scaling up and down of computation and storage; network and server failover; all consistent with 3-tier Web app structure
Storage model	• Range of models from block store (EBS) to augmented key/blob store (SimpleDB) • Automatic scaling varies from no scaling or sharing (EBS) to fully au-tomatic (SimpleDB, S3), depending on which model used • Consistency guarantees vary widely depending on which model used • APIs vary from standardized (EBS) to proprietary	• SQL Data Services (re-stricted view of SQL Server) • Azure storage service	• MegaStore/BigTable
Networking model	• Declarative specification of IP-level topology; internal placement details concealed • Security Groups enable restricting which nodes may communicate • Availability zones provide ab-straction of independent	• Automatic based on pro-grammer's declarative de-scriptions of app compo-nents (roles)	• Fixed topology to ac-commodate 3-tier Web app structure • Scaling up and down is automatic and programmer-invisible

Εικόνα 6

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κεφάλαιο 2^{ο} – Το Cloud Computing στον Δημόσιο και Ιδιωτικό τομέα

2.1 Προσδοκίες από το Cloud Computing



Οι τεχνολογίες Cloud Computing δημιουργούν προσδοκίες για περικοπή του κόστους λειτουργίας και κεφαλαίου, αφαιρώντας παράλληλα το άγχος για την εύρυθμη λειτουργία από τον οργανισμό και μεταφέροντάς το στους παρόχους υπηρεσιών Cloud Computing (Cloud Service Provider -CSP).

Στην ουσία, Cloud Computing είναι μια δομή που επιτρέπει την πρόσβαση σε εφαρμογές, οι οποίες βρίσκονται σε διαφορετική θέση από τον υπολογιστή μας ή την όποια άλλη συσκευή χρησιμοποιούμε για να συνδεθούμε στο Internet[2].

Επιπρόσθετα η άδεια χρήσης του λογισμικού στοιχίζει το ίδιο στον οργανισμό, είτε ο υπάλληλος χρησιμοποιεί την εφαρμογή μια φορά το μηνά, είτε συνεχώς. Στα παραπάνω αν προσθέσουμε το νέο εξοπλισμό, που συνήθως χρειάζονται οι νέες εκδόσεις για να λειτουργήσουν αποδοτικά, οδηγούμαστε σε ακόμη μεγαλύτερες επενδύσεις κεφαλαίου. Επενδύσεις που σε περιβάλλον Cloud δεν είναι καθόλου αυτονόητες, καθότι εκεί εφαρμόζεται το μοντέλο pay as you go, και ανά πασά χρονική στιγμή υπάρχει χρηματική καταβολή μονό για τα facilities που χρησιμοποιούνται, με αποτέλεσμα την ορθολογικότερη χρήση των πόρων του οργανισμού[3]. Επιπρόσθετα η καθολική πρόσβαση, ανεξάρτητα από το σημείο φυσικής παρουσίας μας, οδηγεί σε νέα εργαλεία και μεθόδους παροχής υπηρεσιών με σημαντικό όφελος τόσο για τον εργαζόμενο όσο και τον οργανισμό[1].

2.2 Το Cloud Computing στο Δημόσιο Τομέα



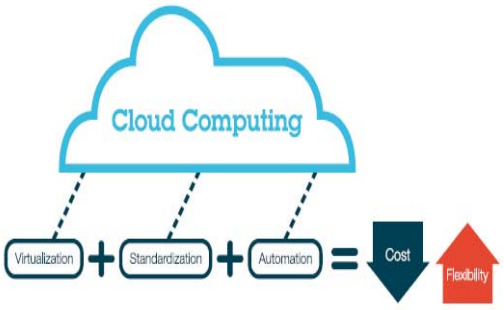
Το Cloud Computing αποτελεί τη νέα τάση στην πληροφορική, η οποία συμβάλλει στην εξοικονόμηση κόστους, πόρων και ενέργειας, αποτελώντας ειδικά σήμερα - λόγω της κρίσης- στρατηγική επιλογή για επιχειρήσεις, οργανισμούς και κυβερνήσεις. Όπως έχουμε αναφέρει, η συγκεκριμένη τεχνολογία προσφέρει στον χρήστη ένα πλήθος δυνατοτήτων επικοινωνίας, συνεργασίας και καταχώρησης πληροφοριών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

σε μια κοινή βάση. Τα δεδομένα δεν αποθηκεύονται σε σκληρούς δίσκους, αλλά σε «σύννεφα» που βρίσκονται στο ίντερνετ ή σε τοπικά δίκτυα. Το Cloud Computing παρέχει ευκολία και αξιοπιστία στην διαχείριση, αποθήκευση και ανταλλαγή σχεδόν απεριόριστου όγκου δεδομένων, τα οποία είναι προσβάσιμα από οπουδήποτε. Ήδη εταιρείες όπως η IBM, η Google και η Yahoo έχουν επενδύσει τεράστια κεφάλαια στην νέα αυτή τεχνολογική δομή ενώ εστιάζουν όλο και περισσότερο τις υπηρεσίες τους έτσι ώστε να εκμεταλλεύονται τις επαναστατικές δυνατότητες του Cloud Computing στο έπακρο. Η αγορά υπηρεσιών Cloud Computing εκτιμάται σήμερα σε περίπου 50 δις δολάρια, ενώ σύμφωνα με την Merrill Lynch την επόμενη 5ετία αναμένεται να ξεπεράσει τα 100 δις δολάρια[24].

Η χρήση λοιπόν της δομής του Cloud Computing από τις Δημόσιες Υπηρεσίες θα μπορούσε να μειώσει σε σημαντικότατο βαθμό το κόστος λειτουργίας όλου του Δημόσιου Τομέα. Παράλληλα θα μπορούσε να ενοποιήσει διαφορετικές Δημόσιες Υπηρεσίες σε ένα περιβάλλον γρήγορης ανταλλαγής πληροφοριών απλοποιώντας γραφειοκρατικές και κοστοβόρες λειτουργίες που ταλαιπωρούν καθημερινώς τους πολίτες και συνάμα τους επιβαρύνουν με επιπλέον φόρους[24].

2.2.1 Μείωση του κόστους των Δημόσιων Υπηρεσιών με την χρήση Cloud Computing



Πολλοί χαρακτηρίζουν το Cloud Computing ως ένα μέσο για τη μείωση του πληροφοριακού κόστους. Στην πραγματικότητα, η μείωση του κόστους προέρχεται από την υιοθέτηση πρότυπων διαδικασιών, εργαλείων και υπηρεσιών που βασίζονται σε πρότυπες κοινές υποδομές. Συνεπώς, η μείωση του κόστους προέρχεται από τη μετάβαση από πολύπλοκα, ετερογενή, υπολογιστικά μοντέλα, σε περιβάλλοντα που επιτρέπουν την άμεση και κοινή αξιοποίηση πόρων. Οι διαδικασίες ενοποίησης, απλοποίησης και εικονικοποίησης μπορούν επίσης να συμβάλλουν στη μείωση του κόστους μιας υποδομής πληροφορικής[21].

Η υιοθέτηση της εν λόγω τεχνολογίας περιλαμβάνει μικρότερους και πιο φθηνούς υπολογιστές ,συνεπώς η χρήση της επιτυγχάνει σημαντική μείωση του κόστους. Σύμφωνα με πρόσφατη εκτίμηση της εταιρείας iQ Studies, η χρήση αυτής της τεχνολογίας σε μια μικρή επιχείρηση 10 ατόμων μπορεί να οδηγήσει σε εξοικονόμηση 2.000 - 4.000 ευρώ τον χρόνο. Επιπλέον, μπορεί να αποφέρει κέρδη έως και 177,3 δισ. ευρώ τον χρόνο στις ισχυρές οικονομίες της Ευρώπης μέχρι το 2015, σύμφωνα με την εταιρεία συμβούλων CEBR[24].

Το Cloud Computing μπορεί να χρησιμοποιηθεί από ένα ευρύ φάσμα φορέων του ιδιωτικού και του δημόσιου τομέα, από νοσοκομεία και σχολεία, μέχρι υπουργεία και οργανισμούς τοπικής αυτοδιοίκησης. Το Υπουργείο Παιδείας εγκαινίασε πρόσφατα ηλεκτρονικές υπηρεσίες που βασίζονται στο Cloud Computing. Εκτιμάται ότι η πλήρης λειτουργία τους θα έχει όφελος 4 εκατ. ευρώ από την προμήθεια εξοπλισμού και 6 εκατ. ευρώ από τη μείωση της κατανάλωσης ηλεκτρικής ενέργειας[23][24].

Ωστόσο, η υποδομή είναι μόλις ένα μικρό μέρος των ποσών που δαπανούν οι κυβερνητικοί οργανισμοί για υπηρεσίες. Μπορεί να υπάρξει ακόμη μεγαλύτερη εξοικονόμηση, αν το Cloud Computing χρησιμοποιηθεί για τη βελτίωση των εσωτερικών διαδικασιών των κυβερνητικών φορέων και του τρόπου με τον οποίο συναλλάσσονται και επικοινωνούν με τους πολίτες.

2.2.2 Οφέλη για τους συναλλασσόμενους με Δημόσιες Υπηρεσίες

Με την υιοθέτηση πρακτικών Cloud Computing, βεβαίως και μπορούν να προκύψουν οφέλη για τους πολίτες, τους συναλλασσόμενους και τους κοινωνικούς εταίρους. Αυτό οφείλεται στο γεγονός ότι το Cloud Computing προσφέρει νέες μεθόδους για την ανάπτυξη διαδικασιών, γεγονός που βελτιώνει την εξυπηρέτηση των πολιτών και συνολικότερα τις διαδικασίες του Δημόσιου Τομέα, ο οποίος μπορεί να προσαρμόζεται συνεχώς με βάση αυτή την αλληλεπίδραση. Αυτό σημαίνει ότι η υιοθέτηση μοντέλων Cloud για την ανάπτυξη εφαρμογών που βασίζονται σε υπηρεσίες, μπορεί να οδηγήσει σε υπηρεσίες που θέτουν τον πολίτη στο επίκεντρο, αλλά και σε στενότερη συνεργασία μεταξύ φορέων και τρίτων παρόχων. Έτσι, δημιουργούνται ευκαιρίες από τη μείωση της γραφειοκρατίας, του χρόνου και του κόστους των εσωτερικών διαδικασιών του Δημοσίου, καθώς και από το γεγονός ότι οι

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πολίτες συναλλάσσονται και επικοινωνούν με το Δημόσιο ταχύτερα και απλούστερα.

Παραδοσιακά, οι διαδικασίες του Δημοσίου είναι απομονωμένες μεταξύ τους και απαιτούν από τον πολίτη είτε να συμπληρώσει πολλές αιτήσεις, είτε να επισκεφθεί ο ίδιος τις δημόσιες υπηρεσίες. Αυτά μπορούν να αντικατασταθούν από υπηρεσίες που επιτρέπουν στους πολίτες να εισάγουν οι ίδιοι τις απαραίτητες πληροφορίες ή να προωθήσουν τα αιτήματα τους μέσω του Internet, όποτε και όπως τους βολεύει. Η υποστήριξη υπηρεσιών web και απομακρυσμένων συσκευών, καθώς και η υιοθέτηση τυποποιημένων υπηρεσιών για διαδικασίες καταγραφής στοιχείων, δημιουργούν συνολικότερες διαδικασίες στις οποίες ασχολείται ενεργά ο πολίτης. Παράλληλα, μειώνεται το κόστος συλλογής και επεξεργασίας δεδομένων και οι δημόσιοι οργανισμοί μπορούν να εξυπηρετήσουν καλύτερα τους πολίτες.

Επιπλέον, οι λύσεις Cloud, προσφέρουν καλύτερη ενοποίηση των διαδικασιών που χρησιμοποιούν οι δημόσιες υπηρεσίες, οι προμηθευτές τους και όσοι συναλλάσσονται με αυτές, γεγονός που μειώνει το κόστος και βελτιώνει τη ροή της πληροφόρησης συνολικά. Πέρα όμως από τα παραπάνω, η αλλαγή των εσωτερικών διαδικασιών του Δημοσίου και των διαδικασιών συναλλαγής και επικοινωνίας με τους κοινωνικούς εταίρους, μπορούν να οδηγήσουν και στη μείωση του περιβαλλοντικού αντίκτυπου, καθώς απαιτούνται λιγότερες μετακινήσεις και λιγότεροι πόροι για την παροχή μιας υπηρεσίας[21].

2.2.3 Όλοι οι Δημόσιοι Οργανισμοί ή Φορείς μπορούν να υιοθετήσουν τεχνολογίες Cloud Computing

Η ταχύτητα μετάβασης στο Cloud Computing διαφέρει από οργανισμό σε οργανισμό. Τα επίπεδα εξυπηρέτησης και ασφάλειας που χρειάζεται ο κάθε οργανισμός θα επηρεάσουν και τη δυνατότητα του να υιοθετήσει Cloud λύσεις. Συνεπώς, υπάρχει ευελιξία στην υιοθέτηση αυτών των τεχνολογιών, καθώς οι οργανισμοί μπορούν να τις υλοποιήσουν ακριβώς εκεί που τις χρειάζονται και όπου μπορούν να δημιουργήσουν προστιθέμενη αξία. Η διαδικασία αυτή δεν είναι μια αλλαγή που γίνεται μια κι έξω.

Από πολλές απόψεις, η κατάσταση γύρω από το Cloud Computing μοιάζει πολύ με τα πρώτα στάδια υιοθέτησης του Internet. Με αυτό εννοούμε ότι όταν πρωτοεμφανίστηκε το Internet, οι επιχειρήσεις δεν ήξεραν ακριβώς πώς

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

θα μπορούσαν να το αξιοποιήσουν προς όφελος των δραστηριοτήτων τους. Οι περισσότερες επιχειρήσεις πέρασαν από διάφορα στάδια υιοθέτησης web λύσεων, οι οποίες εξελίχθηκαν βαθμιαία τόσο όσο προς την πολυπλοκότητα, όσο και ως προς τις δυνατότητες συνεργασίας που προσέφεραν στους τελικούς χρήστες.

Το Cloud Computing βρίσκεται σε μια παρόμοια κατάσταση. Ενώ το μοντέλο των υποδομών που το αφορά γίνεται ολοένα και πιο ξεκάθαρο, οι μέθοδοι με τις οποίες μπορεί να αξιοποιηθεί καλύτερα από τις επιχειρήσεις και τους δημόσιους οργανισμούς βρίσκονται ακόμη σε πρώιμο στάδιο ανάπτυξης. Αυτός είναι ίσως και ο λόγος που πολλοί οργανισμοί πιστεύουν ότι μπορούν να ανακαλύψουν το Cloud Computing και τα οφέλη του μέσω ιδιωτικών και όχι μέσω δημοσίας χρήσης συστημάτων Cloud. Ενώ τα δημόσιας χρήσης Cloud συστήματα φαίνονται ιδιαίτερα ελκυστικά από άποψη κόστους, οι οργανισμοί έχουν σοβαρές επιφυλάξεις σχετικά με την ασφάλεια τους. Επιπλέον, ενώ τα δημόσιας χρήσης Cloud συστήματα προσφέρουν ένα κοινό επίπεδο υπηρεσιών, οι επιχειρήσεις συχνά θέλουν πιο εξατομικευμένα μοντέλα για τις κρίσιμες πληροφορίες και εφαρμογές τους[21].

2.2.4 Προϋποθέσεις Υιοθέτησης του Cloud Computing στην Ελλάδα

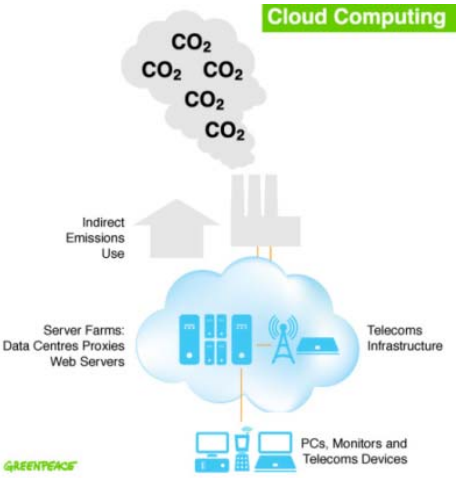
Για να υιοθετήσουν Cloud συστήματα στην χώρα μας, οι δημόσιοι οργανισμοί οφείλουν να αλλάξουν τη νοοτροπία με την οποία αντιμετωπίζουν τις διαδικασίες προμηθειών. Δεν πρέπει αποκλειστικά να αναζητούν τρόπους για να βελτιστοποιήσουν αυτή τη διαδικασία σε όρους τιμής και επιλογής hardware για κάθε έργο πληροφορικής. Το Cloud Computing απαιτεί τη μετάβαση των οργανισμών προς ένα μοντέλο κοινών υπηρεσιών και μεθόδων για την αξιοποίηση πόρων.

Το μοντέλο αυτό μειώνει την πολυπλοκότητα και το κόστος. Νέες εφαρμογές μπορούν να αναπτυχθούν με βάση πρότυπα, επιτρέποντας και στα Cloud συστήματα να αξιοποιηθούν για νέες υπηρεσίες. Δεν πιστεύουμε ότι το Cloud Computing αποτελεί πανάκεια, ούτε ότι θα αντικαταστήσει όλες τις λύσεις πληροφορικής. Η διαφορά είναι ότι οι επιχειρήσεις και οι οργανισμοί θα είναι σε θέση να αξιοποιήσουν την εκάστοτε λύση με τον καλύτερο δυνατό τρόπο – σε όρους κόστους, εξυπηρέτησης και ασφάλειας – δημιουργώντας υβριδικά μοντέλα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Με αυτό τον τρόπο, ένα Cloud σύστημα θα μπορεί να υποστηρίξει διάφορες λύσεις hardware και λογισμικού. Ωστόσο, το πιο σημαντικό κομμάτι ενός Cloud συστήματος είναι να μπορεί να δημιουργήσει υπηρεσίες που μπορούν να αξιοποιηθούν μεμονωμένα και όχι στο πλαίσιο μιας και μοναδικής, ενιαίας λύσης, όπως συνέβαινε στο παρελθόν. Η Cloud υποδομή μπορεί να υποστηρίξει πολλαπλά λειτουργικά συστήματα, βάσεις δεδομένων κλπ., τα οποία όμως αποτελούν μέρος μιας ελεγχόμενης γκάμας standard υπηρεσιών που δεν επιτρέπουν σε μεγάλο βαθμό στον εκάστοτε χρήστη να επιλέξει την κάθε λύση ανεξάρτητα[21]

2.2.5 Οφέλη του Cloud Computing στο περιβάλλον



Τα πλεονεκτήματα από την χρήση της τεχνολογίας Cloud Computing είναι μεγάλα, τόσο για τους τελικούς χρήστες όσο και για το περιβάλλον. Σύμφωνα με έκθεση του Climate Group, το Cloud Computing μπορεί το 2020 να συνεισφέρει στην μείωση των εκπομπών διοξειδίου του άνθρακα κατά περίπου 7,8 γιγατόνους, αριθμός που αντιστοιχεί στο 15% των εκπομπών παγκοσμίως. Επίσης εκτιμάται ότι αν σήμερα η εν λόγω τεχνολογία χρησιμοποιούνταν πλήρως από όλους τους χρήστες πληροφορικής οι ατμοσφαιρικοί ρύποι στον πλανήτη θα μπορούσαν να μειωθούν έως και 5% συνολικά ή αλλιώς 2,5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO2). Σημειώνεται ότι η επιβάρυνση του περιβάλλοντος από την χρήση συστημάτων πληροφορικής ενδέχεται να διπλασιαστεί την επόμενη 10ετία, άρα η μείωση των ατμοσφαιρικών ρύπων παγκόσμια θα μπορούσε να μειωθεί σε βάθος χρόνου έως και 5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO2) ετησίως[24].

2.2.6 Πρόσφατες έρευνες για το Cloud Computing

Παγκόσμια έρευνα της AMD αναδεικνύει την αναπτυσσόμενη αποδοχή του Cloud Computing

Η **AMD** παρουσίασε τα αποτελέσματα της έρευνας που διενέργησε σε παγκόσμιο επίπεδο, με σκοπό να μελετήσει την τάση του υπολογιστικού νέφους (**Cloud Computing**).

Η έρευνα εστίασε στην αποδοχή, την στάση και τις προσεγγίσεις του κοινού απέναντι στο **Cloud Computing**, λαμβάνοντας υπόψη τις απόψεις υψηλά ιστάμενων στελεχών του IT κλάδου σε δημόσιο και ιδιωτικό τομέα σε ΗΠΑ, Ευρώπη, Ασία και σε χώρες του Ειρηνικού Ωκεανού.

Τα ευρήματα της έρευνας αποκαλύπτουν παγκόσμιες αλλά και τοπικές τάσεις του Cloud Computing, τονίζοντας την σπουδαιότητα τόσο των υποδομών όσο και του φόρτου εργασίας για την υποστήριξη του μοντέλου Cloud Computing.

Πιο συγκεκριμένα:

- Το Cloud Computing ωριμάζει ραγδαία, με το 70% των ερωτηθέντων να αναφέρουν πως το χρησιμοποιούν ήδη ή μαθαίνουν για αυτό ώστε να τους φανεί χρήσιμο για τις εφαρμογές που χρησιμοποιούν από απόσταση ή την αποθήκευση δεδομένων.
- Οι οργανισμοί που έχουν ήδη αναπτύξει λύσεις Cloud, σε ποσοστό 60% αναφέρουν πως έχει μεγάλη αξία για τις επιχειρήσεις τους.
- Ανάμεσα στους ήδη υπάρχοντες χρήστες του Cloud, το 92% απαντά πως οι υποδομές αποτελούν ένα σημαντικό παράγοντα για την ανάπτυξη του μοντέλου Cloud Computing.

Δεδομένα αξίας άνω του 1 δις δολαρίων βρίσκονται αποθηκευμένα στο Cloud.

Όσο η υιοθέτηση του Cloud αυξάνεται, τόσο μεγαλώνει αντίστοιχα και η χρηματική αξία των δεδομένων που αποθηκεύονται στο Cloud. Γενικά, το 63% των αποθηκευμένων δεδομένων στο Cloud είναι αξίας πάνω από $250.000, ενώ με βάση την έρευνα υπολογίζεται πως τα ενεργά δεδομένα που είναι αποθηκευμένα στο Cloud έχουν αξία άνω του $1 δις.

Η **AMD**, μελέτησε τη στάση του Δημόσιου τομέα απέναντι στο Cloud. Στις ΗΠΑ οι συμμετέχοντες στην έρευνα από το δημόσιο τομέα απάντησαν πως οι περιπτώσεις που υιοθέτησαν το Cloud είναι διπλάσιες εκείνων που δεν το έχουν αποδεχτεί, ως ένα κύριο μέσο να μειώσουν τα κόστη. Το **50%** περίπου των ερωτηθέντων από το δημόσιο τομέα παγκοσμίως αναφέρει πως η ραγδαία ανάπτυξη των λύσεων του Cloud οφείλεται στον περιορισμένο προϋπολογισμό των οργανισμών.

Ένα βασικό εμπόδιο, που παραμένει ακόμα για το δημόσιο τομέα προκειμένου να υιοθετήσει πλήρως το Cloud computing, είναι η ελλιπής απαραίτητη τεχνογνωσία στην πληροφορική για να υποστηριχθεί η ανάπτυξη ανάλογων λύσεων. Πιο συγκεκριμένα, το **43%** των ερωτηθέντων του δημοσίου τομέα απάντησαν πως δε διαθέτουν τις κατάλληλες γνώσεις για να υποστηρίξουν τις ανάγκες του Cloud, σε αντίθεση με το **23%** των ερωτηθέντων του ιδιωτικού τομέα[22].

Σημαντικά σημεία της έρευνας αναφέρουν:

- **Ανάπτυξη του Cloud:** Το 74% των οργανισμών στις ΗΠΑ χρησιμοποιούν ή αναζητούν να μάθουν για τις λύσεις του Cloud και ακολουθούν η Ασία με ποσοστό 68% και η Ευρώπη με ποσοστό 58%.
- **Εμπιστοσύνη στο Cloud:** Ένας στους δέκα οργανισμούς στις ΗΠΑ υπολογίζει ότι αποθηκεύει στο Cloud δεδομένα αξίας άνω των $10 εκατομμυρίων. Εντούτοις, το 63% των ερωτηθέντων παγκοσμίως υποστηρίζει πως το ζήτημα της ασφάλειας των δεδομένων είναι ο μεγαλύτερος κίνδυνος του μοντέλου του Cloud.
- **Κατανόηση και Προετοιμασία για το Cloud:** Για όσους χρησιμοποιούν ήδη το Cloud, το 75% κατέχει τις απαραίτητες γνώσεις πληροφορικής για να υποστηρίξει τις ανάγκες του, σε αντίθεση με το 39% των ερωτηθέντων που μελετούν τις λύσεις του Cloud.
- **Οι Χρήστες του Cloud:** Οι χρήστες του Cloud έχουν πρόσβαση στις υπηρεσίες του Cloud μέσω: PCs (90%), smartphones (56%), ταμπλέτες (37%) και thin clients (32%).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Έρευνα της CSA και της HP για τις απειλές αφάλειας στο Cloud Computing



Η συμμαχία **Cloud Security Alliance** (CSA), ένας αναγνωρισμένος μη κερδοσκοπικός οργανισμός, και η **HP** ανακοινώνουν την έκδοση μιας νέας έρευνας που περιγράφει αναλυτικά τους πιθανούς κινδύνους για την ασφάλεια υπηρεσιών και περιβαλλόντων Cloud Computing.

Η έρευνα ανατέθηκε στην **CSA** από την **HP** και είχε ως στόχο την καλύτερη ενημέρωση και την ενίσχυση της κατανόησης σχετικά με υπάρχουσες και μελλοντικές απειλές. Ακόμη, στόχος της έρευνας ήταν η παρουσίαση στρατηγικών για την επαναφορά συστημάτων και την ανάκτηση πληροφοριών. Οι επιχειρήσεις μπορούν να αξιοποιήσούν αυτές τις στρατηγικές για την απρόσκοπτη και ασφαλή συνέχεια των διαδικασιών που εκτελούνται σε περιβάλλοντα Cloud Computing.

Η έρευνα με τίτλο "**Top Cloud Security Threats Report**" στηρίχθηκε σε εκτενείς συνεντεύξεις εξειδικευμένων στελεχών από **29 επιχειρήσεις**, παρόχους λύσεων ασφάλειας και εταιρείες παροχής συμβουλευτικών υπηρεσιών, που καλούνται να διαχειριστούν τα πιο πολύπλοκα περιβάλλοντα Cloud Computing στον κόσμο. Τα βασικά ευρήματα της έρευνας παρουσιάστηκαν στο **Cloud Security Summit** που διεξήχθη στο πλαίσιο του συνεδρίου **RSA**.

Σήμερα, η υιοθέτηση υπηρεσιών Cloud Computing αυξάνεται με ολοένα και ταχύτερους ρυθμούς, παρότι η ασφάλεια θεωρείται ο βασικός παράγοντας που αποτρέπει τις επιχειρήσεις από την αξιοποίηση τους. Με τη νέα έρευνα, οι επιχειρήσεις που αξιοποιούν αυτές τις υπηρεσίες μπορούν να αποκτήσουν μεγαλύτερη ορατότητα πάνω σε θέματα ασφάλειας, αλλά και να εκτιμήσουν καλύτερα τους κινδύνους και τα οφέλη που προκύπτουν από την υλοποίηση στρατηγικών Cloud Computing.

"*Οι υπηρεσίες Cloud Computing είναι σίγουρα η επόμενη γενιά τεχνολογιών πληροφορικής που πρέπει να διαχειριστούν αποτελεσματικά οι επιχειρήσεις. Ως κλάδος, έχουμε συνολικά την ευθύνη να κατανοήσουμε τις απειλές που πιθανώς*

να συνοδεύουν τη χρήση αυτών των υπηρεσιών και να εφαρμόσουμε βέλτιστες πρακτικές για τη μείωση των κινδύνων για την ασφάλεια τους", δήλωσε ο **Jim Reavis**, ιδρυτής της Cloud Security Alliance. "*Ο στόχος της έρευνας δεν ήταν απλώς η αναγνώριση των απειλών που απασχολούν πιο πολύ τα τμήματα πληροφορικής. Προσπαθήσαμε να βοηθήσουμε τους οργανισμούς να κατανοήσουν πως μπορούν να προστατευθούν έγκαιρα από αυτές», συμπλήρωσε. Και συνέχισε λέγοντας: «Αυτό ήταν το πρώτο μέρος της ερευνητικής μας πρωτοβουλίας. Η έρευνα θα ανανεώνεται τακτικά, ώστε να αντανακλάται η αύξηση της συμμετοχής των στελεχών, αλλά και η εξέλιξη των απειλών*".

Η έρευνα αναγνωρίζει τα τρωτά σημεία που αν προσβληθούν, θα εμποδίσουν την πλήρη αξιοποίηση των υπηρεσιών Cloud Computing. Για παράδειγμα, οι επιχειρήσεις πρέπει να είναι ενήμερες γύρω από προγράμματα και πρακτικές "κατάχρησης ή επιβλαβούς χρήσης του Cloud Computing", όπως το κακόβουλο δίκτυο Zeus και τα trojan horses InfoStealing, τα οποία εκμεταλλεύονται με ιδιαίτερη επιτυχία ευαίσθητους ιδιωτικούς πόρους και δεδομένα που υπάρχουν σε περιβάλλοντα Cloud Computing.

Ωστόσο, αξίζει να σημειωθεί ότι οι απειλές ασφάλειας δεν είναι απαραίτητα προϊόν κακόβουλων προθέσεων. Καθώς οι μηχανισμοί κοινωνικής δικτύωσης εξελίσσονται, όλο και περισσότερες ιστοσελίδες στηρίζονται σε interfaces προγραμματισμού εφαρμογών (APIs), δηλαδή σε ένα σετ λειτουργιών που επιτρέπουν την αλληλεπίδραση μεταξύ προγραμμάτων λογισμικού για την ανταλλαγή δεδομένων από διαφορετικές πηγές. Οι ιστοσελίδες που στηρίζονται σε πολλά APIs συχνά αντιμετωπίζουν προβλήματα λόγω του φαινομένου του «πιο αδύναμου κρίκου», στο οποίο ένα μη ασφαλές στέλεχος μπορεί να έχει αρνητική επίδραση στο ευρύτερο σύνολο των APIs. Έτσι, μπορεί να δημιουργηθεί ένα συνδυασμός τρωτών σημείων και να αναπτυχθούν κακόβουλες τεχνικές που θέτουν σε κίνδυνο την ασφάλεια των συστημάτων και των δεδομένων.

Η έρευνα ανέδειξε και άλλες απειλές για περιβάλλοντα Cloud computing, μεταξύ των οποίων περιλαμβάνονται:

- Εισβολείς με κακόβουλες προθέσεις

- Τρωτά σημεία τεχνολογιών που χρησιμοποιούνται από κοινού
- Περιπτώσεις απώλειας ή διαρροής δεδομένων
- Δραστηριότητες πειρατείας λογαριασμών και υπηρεσιών

Ως μέλος της συμμαχίας CSA, η HP προχώρησε στη χορηγία της έρευνας, με στόχο την ενημέρωση και την εκπαίδευση των εταιρειών γύρω από πιθανές απειλές για περιβάλλοντα Cloud Computing και την εφαρμογή βέλτιστων πρακτικών για την αποφυγή τους. Επιπλέον, η HP προσφέρει ένα ενοποιημένο χαρτοφυλάκιο λύσεων ασφάλειας που περιλαμβάνει εξειδικευμένα προϊόντα, υπηρεσίες συμβουλευτικής υποστήριξης και εκπαίδευσης, καθώς και ειδικές υπηρεσίες για τη μείωση της πολυπλοκότητας και του ρίσκου.

"*Για τη διασφάλιση της προστασίας των data center τους, οι εταιρείες πρέπει να επενδύσουν χρόνο και πόρους. Έτσι, θα ελαχιστοποιήσουν το επιχειρηματικό ρίσκο που συνδέεται με περιβάλλοντα Cloud Computing*", δήλωσε ο **Archie Reed**, Chief Technologist for Cloud Security, HP Secure Advantage, και μέλος της εκτελεστικής επιτροπής της CSA. "*Το ολοκληρωμένο χαρτοφυλάκιο λύσεων ασφάλειας της HP περιλαμβάνει hardware, λογισμικό και ειδικές υπηρεσίες συμβουλευτικής υποστήριξης, οι οποίες είναι σχεδιασμένες για να ελαχιστοποιήσουν τις περιπτώσεις παραβίασης της ασφάλειας των δεδομένων σε περιβάλλοντα Cloud Computing*", συμπλήρωσε [44].

2.3 Το Cloud Computing στον Ιδιωτικό Τομέα



Η μηχανογράφηση επιχειρήσεων με εκμετάλλευση των πλεονεκτημάτων που προσφέρει σήμερα το Cloud Computing παρουσιάζει ιδιαίτερα μεγάλους ρυθμούς ανάπτυξης. Η ανάπτυξη αυτή ενισχύεται ασφαλώς και από τις επιπτώσεις της τρέχουσας οικονομικής κρίσης, με δεδομένη την αδυναμία των περισσότερων επιχειρήσεων να προχωρήσουν σε επενδύσεις με σημαντικές οικονομικές επιβαρύνσεις και αυξημένες αρχικές εκροές κεφαλαίων. Οι ιδιαίτερες συνθήκες λειτουργίας των επιχειρήσεων επιβάλλουν την αναζήτηση ευέλικτων και οικονομικών λύσεων μηχανογράφησης που θα ικανοποιήσουν τις ανάγκες τους με πληρότητα, ασφάλεια και χωρίς ποιοτικούς συμβιβασμούς.

Η μηχανογράφηση στο Cloud δίνει μια ουσιαστική λύση στα προβλήματα που αντιμετωπίζουν σήμερα πολλές επιχειρήσεις. Και εκτός από σημαντική μείωση του λειτουργικού κόστους, η χρήση λογισμικού με τη μορφή συνδρομητικής υπηρεσίας μέσω internet είναι σε θέση να προσφέρει στις επιχειρήσεις και μια σειρά από άλλα πλεονεκτήματα που θα τις καταστήσουν περισσότερο ανταγωνιστικές στον τομέα που δραστηριοποιούνται. Κι αυτό γιατί το Cloud δεν αφορά μόνο στον τρόπο με τον οποίο υλοποιούνται πληροφοριακές υποδομές, αλλά επηρεάζει καταλυτικά τα επιχειρησιακά μοντέλα λειτουργίας και δημιουργεί προστιθέμενη αξία για την αναπτυξιακή προοπτική των επιχειρήσεων.

Η αμεσότητα πρόσβασης στο λογισμικό, η δυνατότητα αξιοποίησης πραγματικού-χρόνου (real-time) δεδομένων, η επικέντρωση στο core business, η ευελιξία χρήσης και οι οικονομίες κλίμακας που επιτυγχάνονται είναι σε θέση να δημιουργήσουν ισχυρό πλεονέκτημα για την επιχείρηση και να τη διαφοροποιήσουν αποτελεσματικά σε σχέση με τον ανταγωνισμό της. Με το Cloud Computing και τη μηχανογράφηση στο «σύννεφο» ανοίγονται άλλες δυνατότητες και προοπτικές για την επιχείρηση που επιθυμεί να συμμετάσχει με αξιώσεις στο σύγχρονο επιχειρηματικό γίγνεσθαι[25].

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.3.1 Προϋποθέσεις υιοθέτησης του Cloud Computing από μία επιχείρηση



Μία επιχείρηση προτού λάβει την απόφαση να υιοθετήσει την νέα τεχνολογία πρέπει να ενημερωθεί προσεκτικά σχετικά με την συνολική πολιτική που εφαρμόζει ένας προμηθευτής, όσον αφορά την αποφυγή της πρόσβασης στα δεδομένα της επιχείρησης από κάποιον μη εξουσιοδοτημένο χρήστη. Η πολιτική αυτή θα πρέπει να προβλέπει τόσο τη «**φυσική**» όσο και την «**ηλεκτρονική**» ασφάλεια των δεδομένων.

Με τον όρο «**φυσική**» ασφάλεια εννοούμε την προστασία των δεδομένων από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση που μπορεί πιθανόν να αποκτήσει κάποιο άτομο στους φυσικούς servers και το δικτυακό εξοπλισμό του data center όπου είναι αποθηκευμένα τα δεδομένα. Για να επιτευχθεί αυτό το είδος ασφαλείας, θα πρέπει να έχουν δημιουργηθεί από τον πάροχο τα απαιτούμενα διαβαθμισμένα επίπεδα ασφαλείας που αφορούν την πρόσβαση στις κτιριακές εγκαταστάσεις, την είσοδο στο data center και την πρόσβαση στον εξοπλισμό. Η πρόσβαση στο κτίριο που στεγάζει το data center είναι σημαντικό να είναι ελεγχόμενη μέσω ενός συστήματος ταυτοποίησης των εισερχομένων ατόμων και η περίμετρος του κτιρίου να παρακολουθείται. Η είσοδος στο data center μπορεί να γίνεται μέσω ειδικών μαγνητικών καρτών που διαθέτει μόνο το εξουσιοδοτημένο προσωπικό, έτσι ώστε οι πληροφορίες πρόσβασης του προσωπικού να καταγράφονται και να είναι εύκολο να ελεγχθούν από κάποιον υπεύθυνο ασφαλείας. Τέλος, η πρόσβαση στον εξοπλισμό του data center, όπως σε Rack Cabinets, αποθηκευτικά μέσα, κεντρικό server και συσκευές δικτύου, είναι χρήσιμο να προστατεύεται με την τοποθέτηση τους σε ειδικούς χώρους (π.χ. computer room), στους οποίους έχει πρόσβαση μόνο το αρμόδιο προσωπικό.

Με τον όρο «**ηλεκτρονική**» ασφάλεια αντίστοιχα, εννοούμε την προστασία των δεδομένων από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση που μπορεί πιθανόν να αποκτήσει κάποιο άτομο στο δίκτυο του data center μέσω του internet. Για να επιτευχθεί τέτοιου τύπου ασφάλεια ο προμηθευτής θα πρέπει να έχει δημιουργήσει τα απαιτούμενα επίπεδα απομόνωσης του εσωτερικού

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δικτύου και των κρίσιμων δεδομένων από το internet με τη χρήση εξελιγμένων συστημάτων προστασίας (firewalls, intrusion detection systems, antivirus software, antispam/antimalware software), καθώς και ειδικών συστημάτων κρυπτογράφησης και ασφαλείας των πρωτόκολλων επικοινωνίας που χρησιμοποιούνται ευρέως. Ακόμη, τα επιχειρηματικά δεδομένα που κρίνονται ως «ευαίσθητα» θα πρέπει να τυγχάνουν αυξημένης προστασίας, μέσω της αποθήκευσής τους σε ειδικά αποθηκευτικά μέσα στα οποία ο έλεγχος πρόσβασης των χρηστών είναι αυστηρότερος.

Στα παρακάτω κεφάλαια θα επικεντρωθούμε περισσότερο και θα αναλύσουμε σε βάθος τα ζητήματα ασφάλειας και το κανονιστικό πλαίσιο που ισχύει στην Ελλάδα[26].

2.3.2 Πλεονεκτήματα και Μειονεκτήματα υιοθέτησης του Cloud Computing για μία επιχείρηση



Το Cloud Computing θεωρείται ακόμη μια νέα και σχετικά μη εδραιωμένη τεχνολογία από τις επιχειρήσεις. Τα πλεονεκτήματα που προσφέρει όμως ιδιαίτερα στις μικρές & μεσαίες επιχειρήσεις είναι σημαντικά και δεν θα έπρεπε να παραβλέπονται. Παρακάτω συνοψίζονται τα βασικότερα πλεονεκτήματα που προσφέρει η νέα τεχνολογία για μια επιχείρηση[28,9]:

1. **Οικονομία**

   Αντί να διατηρούν ένα data center με ακριβό εξοπλισμό και λογισμικό που μπορεί να μένουν αχρησιμοποίητα ή χρησιμοποιούμενα μόνο εν μέρει για χρόνια, οι επιχειρήσεις μπορούν να νοικιάζουν υπολογιστικούς πόρους, όταν και όσους χρειάζονται και για τη διάρκεια που αυτοί είναι απαραίτητοι. Έτσι, αντί για μεγάλες επενδύσεις σε συστήματα πληροφορικής πληρώνουν μια μικρή, μηνιαία ή ετήσια συνδρομή στρέφοντας τις επένδύσεις τους σε πραγματικές ευκαιρίες ανάπτυξής τους.

   Παράλληλα, στο Cloud δεν υπάρχουν κρυφά κόστη (αυξημένοι λογαριασμοί ηλεκτρικής ενέργειας, μετακινήσεις στελεχών σε υποκαταστήματα για εγκαταστάσεις, συντηρήσεις, κ.α.). Επίσης,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αποκλείεται η περίπτωση αγοράς πλεονάζοντος εξοπλισμού, λογισμικού ή ισχύος καθώς στο Cloud οι επιχειρήσεις πληρώνουν ακριβώς για αυτά που χρησιμοποιούν, ενώ ανά περίοδο συνδρομής μπορούν τα μεγέθη αυτά να τα αυξομειώνουν ανάλογα με τις εκάστοτε ανάγκες τους. Θεωρείται ότι οι δαπάνες κεφαλαίου μετατρέπονται σε (σαφώς μικρότερων μεγεθών) έξοδα λειτουργίας, ενώ γίνεται εφικτή η εφαρμογή πληθώρα προγραμμάτων με απαγορευτικά υψηλό κόστος προμήθειας.

2. **Πολυπλοκότητα Vs Απλότητα**

   Η διατήρηση ενός τοπικού data center κοστίζει αρκετά και επιβάλλει τη συνεργασία "ειδικών" από διαφορετικούς τομείς (HW, SW, DB, κτλ). Ακόμη και στην περίπτωση που οι επιχειρήσεις προχωρήσουν σε outsourcing των IT εργασιών απαιτείται σημαντική προσπάθεια για project management, διαχείριση προϋπολογισμών και χρονοδιαγραμμάτων, disaster recovery σχεδιασμούς και ελέγχους. Όλη η διαδικασία αυτή μπορεί γρήγορα να γίνει αρκετά πολύπλοκη. Αντιθέτως στο Cloud όλα τα παραπάνω είναι λυμένα, είναι δεδομένα ενώ και "οι όποιες αλλαγές απαιτούνται είναι απλώς θέμα μερικών κλικ." Επίσης όσων αφορά τη απλότητα με pay – as – you – go υπηρεσίες, υπάρχει σχεδόν πραγματικού-χρόνου (real-time) δυναμική αντιστοίχηση πόρων ανάλογα με την ζήτηση από πλευράς του πελάτη.

3. **Ταχύτητα υλοποίησης**

   Σε μια on-premise εγκατάσταση η υλοποίηση ενός καινούριου πληροφοριακού συστήματος (καθορισμός προδιαγραφών, παραγγελία, παραλαβή, εγκατάσταση, ρυθμίσεις, έλεγχοι, system integration…) μπορεί να πάρει μήνες. Στο Cloud, αντίστοιχες υποδομές μπορούν να αρχίσουν να λειτουργούν σε λίγα λεπτά, ενώ ολόκληρη η λύση μπορεί να υλοποιηθεί σε κάποιες ώρες. Επίσης μια επιχείρηση αντί να χρειαστεί να επενδύσει σε υλικό και λογισμικό, να εγκαταστήσει και να ρυθμίσει τις εφαρμογές που τρέχουν στις ανάγκες της, καθώς και να στήσει back-up υπηρεσίες ασφαλείας, μπορεί απλά να προμηθευτεί μεσαίας απόδοσης υπολογιστές και μια σύνδεση στο Internet και να έχει έτοιμο ένα παραγωγικό περιβάλλον μέσω Cloud Computing.

4. **Αυξημένη Ευελιξία**

Μακροπρόθεσμες υποχρεώσεις όπως η αγορά λογισμικού ή η προμήθεια υποδομών απαιτούν ακριβή σχεδιασμό για μακροπρόθεσμες ανάγκες. Αντίθετα, στην περίπτωση του Cloud Computing ο πελάτης δεν δεσμεύεται με συμβόλαια μεγάλων χρονικών διαστημάτων και ο προγραμματισμός γίνεται για μικρότερες χρονικές περιόδους, επομένως αυξομειώσεις στη ζήτηση υπολογιστικών πόρων καλύπτονται όταν παρουσιαστούν και για όσο οι πόροι αυτοί είναι αναγκαίοι. Επίσης ο πάροχος Cloud υπηρεσιών είναι ικανός να προσφέρει εργαλεία μέτρησης της χρήσης και των απαιτήσεων σε πόρους του πελάτη σε χρονοδιαγράμματα.

Τόσο το λογισμικό όσο και το υλικό αναβαθμίζονται και συντηρούνται από τον πάροχο του Cloud και είναι διαθέσιμα «με το επόμενο log – in» δίχως καθυστερήσεις ή ρίσκα ασυμβατότητας, ενώ προσφέρονται χιλιάδες TBytes αποθηκευτικού χώρου εν αντιθέσει των μόλις μερικών μιας επιχείρησης.

Τέλος ο πελάτης κάνει log – in στις υπηρεσίες του, δίχως να ενδιαφέρεται για την υλική πλατφόρμα που τρέχει το λογισμικό , όπου και το λογισμικό είναι επιλογή του παρόχου άρα και ευθύνη του η ικανοποιητική και αποδοτική παραμετροποίηση του.

5. **Περισσότερες επιλογές – Χαμηλότερες τιμές**

   Όταν ξεκίνησαν οι Web υπηρεσίες της Amazon προσέφεραν on-line storage σε ένα μόνο data center. Σήμερα η Amazon έχει τέσσερα σε τρεις ηπείρους και σε σημαντικά χαμηλότερες τιμές. Αντίστοιχα, όταν ξεκίνησαν οι Web υπηρείες της Amazon ούτε καν ο όρος Cloud Computing δεν χρησιμοποιούνταν. Σήμερα πλέον δραστηριοποιούνται δυναμικά στο Cloud μεγάλες εταιρίες, όπως η Microsoft και η Rackspace αλλά και hosting εταιρίες που αρχίζουν να έχουν Cloud offerings. Ποιος κερδίζει από όλο αυτό; Μα φυσικά ο πελάτης, οι μικρές & μεσαίες επιχειρήσεις αφού οι επιλογές τους συνεχώς αυξάνονται και γίνονται πιο ελκυστικές.

6. **Ασφάλεια & αξιοπιστία**



   Πολλές επιχειρήσεις ανησυχούν για την ασφάλεια και την αξιοπιστία των Cloud υπηρεσιών. Ωστόσο,

είναι σαφές ότι οι Cloud πωλητές είναι πολύ ευκολότερο να σχεδιάσουν καλύτερες πολιτικές ασφάλειας από μια μικρομεσαία επιχείρηση γιατί αφενός μεν χρησιμοποιούν ειδικούς εμπειρογνώμονες και αφετέρου ακολουθούν πιστοποιημένες διαδικασίες ασφαλείας. Επίσης, επειδή ακριβώς εξειδικεύονται στο αντικείμενο αυτό, είναι πολύ ευκολότερο να χτίσουν συστήματα υψηλής αξιοπιστίας ώστε να προστατεύουν και να υποστηρίζουν τα συστήματα χιλιάδων αντίστοιχων επιχειρήσεων.

Ωστόσο η υιοθέτηση τεχνολογίας Cloud Computing ελλοχεύει μία σειρά από κινδύνους, γιαυτό και πρέπει να ληφθούν υπόψη και τα μειονεκτήματα που προκύπτουν από την εφαρμογή της. Τα κυριότερα μειονεκτήματα είναι τα εξής[9]:

1. **Ασφάλεια:** Η ασφάλεια θα μπορούσε από μια άλλη οπτική γωνία να θεωρηθεί μειονέκτημα από την άποψη ότι όσον αφορά ειδικά τα ευαίσθητα – κρίσιμα δεδομένα, δεν έχει τον έλεγχο η επιχείρηση.
2. **Κόστος μετάβασης:** Το κόστος αλλαγής πάροχου Cloud υπηρεσιών, αλλά και μετακίνησης του περιεχομένου, σε αρκετές περιπτωσεις είναι απαγορευτικό.
3. **Απάιτηση αδιάλειπτης πρόσβασης στο Internet:** Λόγω της φύσης της υπηρεσίας, απαιτείται μόνιμη σύνδεση στο Internet, ενώ οποιαδήποτε διακοπή δημιουργεί πλήρη αδυναμία πρόσβασης και επεξεργασίας των δεδομένων μιας εταιρίας ή ενός χρήστη.
4. **Εξάρτηση από τον πάροχο:** Αν ο πάροχος Cloud για κάποιον λόγο δεν μπορεί να εξυπηρετήσει τους πελάτες του, η επιχείρηση βρίσκεται μετέωρη.
5. **Έλλειψη QoS:** Δεν υπάρχουν σαφείς δεσμεύσεις για δείκτες ποιότητας υπηρεσιών (uptime, availability).
6. **Πιθανή οριστική απώλεια δεδομένων:** Εγείρεται το ερώτημα σε περίπτωση που ο Cloud πάροχος για κάποιο λόγο τερματίσει την επιχειρηματική δραστηριότητα του, αν θα επιστραφούν τα δεδομένα στον ιδιοκτήτη τους.
7. **Πρόσβαση στα δεδομένα:** Έχει ουσιαστικά μόνο ο πελάτης εξουσιοδοτημένη πρόσβαση στα δεδομένα του;

8. **Αποδοχή:** Εξαιτίας του ότι υπάρχει έλλειψη αναφορών χρήσης Cloud Computing από μεγάλες εταιρίες, διατηρείται η επιφιλακτικότητα από το αγοραστικό κοινό. Επίσης κατά κάποιο τρόπο είναι «ντροπιαστικό» μια εταιρία που ασχολείται με την πληροφορική να εξαρτάται από μια άλλη.
9. **Ταχύτητα συνδέσεων & bandwidth:** Επιγραμματικά το Cloud Computing, δεν μπορεί να δουλέψει με αργές συνδέσεις, ενώ η χρήση μισθωμένων γραμμών Internet για τις ζωτικής σημασίας υπηρεσίες μιας εταιρίας, λόγω του μεγάλου traffic μπορούν να εκτοξεύσουν το παράπλευρο κόστος του Cloud Computing.

2.3.3 Υπηρεσίες Cloud Computing για τις επιχειρήσεις

Παρακάτω αναφέρονται συνοπτικές περιγραφές από τις υπηρεσίες που προσφέρονται σήμερα μέσω του Cloud αλλά και των υπηρεσιών που αναπτύσσονται και θα είναι σύντομα διαθέσιμες[32].

Cloud Desktop

Το περιβάλλον εργασίας μέσω του Cloud αφαιρεί την ανάγκη του παραδοσιακού υπολογιστή γραφείου και ουσιαστικά μηδενίζει το κόστος συντήρησης τους. Ένα Cloud περιβάλλον εργασίας είναι και λειτουργεί, όπως ένας κανονικός υπολογιστής γραφείου, με το λογισμικό και τα δεδομένα του να βρίσκονται σε απομακρυσμένα, ιδιαίτερα ασφαλή data centers. Οι χρήστες μπορούν, με απλό τρόπο, να έχουν πρόσβαση στο περιβάλλον εργασίας τους από οποιοδήποτε σημείο του κόσμου, μέσω μιας σύνδεσης με το διαδίκτυο, χρησιμοποιώντας είτε ένα υπάρχον PC είτε ένα laptop είτε, για μέγιστη οικονομία, μια ιδιαίτερη συσκευή αποκαλούμενη thin client. Το τυπικό περιβάλλον εργασίας περιλαμβάνει Microsoft Windows XP/7, Microsoft Office, Antivirus ενώ μπορούν να προστεθούν εφαρμογές ERP, CRM και Document Managment.

Cloud Mail



Δεδομένου ότι οι περισσότερες επιχειρήσεις ψάχνουν για μια ασφαλή, αξιόπιστη λύση ηλεκτρονικού ταχυδρομείου που δεν θα κοστίζει υπερβολικά και θα

καλύπτει και πρόσθετες ανάγκες όπως της αρχειοθέτησης επαφών, τήρησης ημερολογίου, κοινών φακέλων, κ.α. όλο και περισσότερες έχουν την ανάγκη εγκατάστασης ενός mail server. Με την διάθεση του mail server, ως Cloud εφαρμογή, δίνεται η δυνατότητα πλέον και σε μικρές επιχειρήσεις να απολαμβάνουν τα οφέλη του χωρίς να πρέπει να επενδύσουν σε δαπανηρές υποδομές. Τα δεδομένα του ηλεκτρονικού ταχυδρομείου αποθηκεύονται σε ιδιαίτερα ασφαλή data centers τα οποία παρέχουν συνεχή διαθεσιμότητα και πρόσβαση από οποιοδήποτε σημείο και πάντα μέσω του διαδικτύου.

Cloud Storage



Με την υπηρεσία Cloud storage διατίθεται χώρος αποθήκευσης δεδομένων παρέχοντας ασφάλεια, δυναμική επεκτασιμότητα και πρόσβαση μέσω διαδικτύου, χωρίς να απαιτείται αγορά εξοπλισμού από την εταιρεία, με μηνιαίο κόστος που προκύπτει ανάλογα με την χωρητικότητα που χρησιμοποιείται. Ολοι οι χρήστες μίας εταιρείας που χρησιμοποιούν Cloud desktop έχουν κοινή, διαβαθμισμένη, πρόσβαση στον ίδιο αποθηκευτικό χώρο ενισχύοντας την συνεργασία εντός και εκτός του χώρου εργασίας.

Cloud Servers

Οι διαδικτυακοί διακομιστές είναι η επόμενη γενιά των servers οι οποίοι απαρτίζουν σήμερα ένα τυπικό computer room. Μέσω του διαδικτύου παρέχονται οι απαραίτητοι πόροι για να δημιουργηθεί ένας διακομιστής, ο οποίος με την σειρά του είναι πλήρως επεκτάσιμος.

Με την έννοια επεκτάσιμος εννοούμε ότι τα χαρακτηριστικά του διακομιστή, όπως είναι η μνήμη ή ο επεξεργαστής του, μπορούν να αλλάξουν δυναμικά οποιαδήποτε στιγμή για να καλύψουν μόνιμες ή περιστασιακές ανάγκες μίας εταιρείας χωρίς να χρειάζεται να επιβαρυνθεί οικονομικά η εταιρεία για εξοπλισμό που δεν της είναι συνεχώς απαραίτητος. Ακόμη και στις περιπτώσεις που ο διακομιστής χρειάζεται αλλαγή, όταν βρίσκεται στο Cloud, αντιμετωπίζεται ως μία επέκταση εκμηδενίζοντας έτσι όλα τα κόστη υπηρεσιών που θα χρειαζόντουσαν σε κάθε άλλη περίπτωση.

Cloud Telephony

Αναφέρεται στη χρήση των τηλεφωνικών υπηρεσιών οι οποίες πραγματοποιούνται δια μέσω του διαδικτύου για οποιεσδήποτε κλήσεις. Από την άποψη της χρήσης δεν υπάρχει καμία διαφορά σε σχέση με την παραδοσιακή τηλεφωνία, αλλά έχει ευδιάκριτα πλεονεκτήματα όσον αφορά το κόστος καθώς και την παρεχόμενη λειτουργικότητα. Το φιλοξενούμενο τηλεφωνικό σύστημα μηδενίζει το κόστος τηλεφωνικής υποδομής, εγκατάστασης και προμήθειας ακριβών γραμμών, προσφέροντας μια εναλλακτική απλή λύση που διατίθεται με μηνιαία συνδρομή.

Με τη τεχνολογία αυτή, η πρόσβαση στις τηλεφωνικές επικοινωνίες γίνεται με την απλή σύνδεση ενός προ-ρυθμισμένου τηλεφώνου στο εταιρικό δίκτυο, με ένα Laptop η με ένα κινητό τηλέφωνο.

2.3.4 Προσδιορισμός της καταλληλότητας μιας επιχείρησης για την υιοθέτηση στρατηγικών Cloud Computing

Η λήψη της απόφασης για την μετάβαση του εταιρικού περιβάλλοντος από την παραδοσιακή In-house δομή σε ένα από τα διαθέσιμα μοντέλα Cloud Computing, έχει υψηλή σημασία για τον ίδιο τον οργανισμό και τον τρόπο λειτουργίας του. Για το λόγο αυτό, είναι χρήσιμο να εξετάσουμε προσεκτικά τα ειδικά χαρακτηρίστηκα του οργανισμού ώστε να καταλήξουμε σε εκείνο το μίγμα που προσφέρει τα μέγιστα οφέλη με βάση αντικειμενικά κριτήρια και όχι τα trends της εποχής.

Ειδικότερα πολύ ερευνητές προτείνουν την αξιολόγηση των πόρων που διαθέτει ο οργανισμός, τα ειδικά στοιχειά του κλάδου στον οποίο δραστηριοποιείται και την φύση των δεδομένων που διαχειρίζεται, ώστε να κριθεί τελικά η ορθότητα μετάβασης αλλά και το μοντέλο Cloud που ταιριάζει καλύτερα στις ανάγκες του υπό εξέταση φορέα.

Πίνακας 1 Στοιχεία αξιολόγησης για την μετάβαση σε περιβάλλον Cloud Computing

1. Το μέγεθος των πόρων που χαρακτηρίζει το τμήματα πληροφορικής

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2. Η πολιτική οργάνωσης και λειτουργίας του τμήματος πληροφορικής
3. Η φύση των δεδομένων που διαχειρίζεται ο οργανισμός
4. Η σημασία/ κρισιμότητα του κάθε πόρου που προσφέρετε από το τμήμα πληροφορικής για την εύρυθμη λειτουργία του οργανισμού

Στον παραπάνω πίνακα συγκεντρώσαμε τα τέσσερα πιό σημαντικά κριτήρια τα οποία πρέπει να λάβει υπόψη του μία επιχείρηση όσον αφορά το λειτουργικό της κομμάτι με στόχο την λήψη απόφασης για την υιοθέτηση ή μη της τεχνολογίας Cloud Computing. Καταλήγουμε λοιπόν στο συμπέρασμα ότι το Cloud Computing είναι πιο κατάλληλο για μικρές και μεσαίες επιχειρήσεις.[49]

2.4 Δέκα από τα σημαντικότερα εμπόδια μετάβασης στο Cloud Computing

Υπάρχουν δέκα βασικοί παράγοντες οι οποίοι καθιστούν διστακτικό έναν δημόσιο ή ιδιωτικό οργανισμό να μεταβεί σε τεχνολογία Cloud Computing. Αυτοί οι παράγοντες είναι οι εξής[47]:

1. **Διαθεσιμότητα της υπηρεσίας (Availability of a Service)**
   Οι οργανισμοί ανησυχούν για το αν οι υπηρεσίες που χρειάζονται καθημερινώς, θα έχουν επαρκές επίπεδο διαθεσιμότητας, το οποίο καθορίζεται από τον πάροχο τεχνολογίας Cloud Computing. Αυτό σημαίνει ότι αν για κάποιο λόγο ο πάροχος δεν θα μπορούσε να παρέχει τις υπηρεσίες του Cloud στον οργανισμό, άμεσα ο οργανισμός θα ερχόταν αντιμέτωπος με καταστροφικές συνέπειες όσον αφορά την βιωσιμότητα του ίδιου του οργανισμού.
2. **Δέσμευση των δεδομένων στο Cloud (Data Lock-In)**
   Η δυσκολία εξαγωγής δεδομένων από το Cloud και η ασυμβατότητα των δεδομένων για χρήση τους σε διαφορετικές υπηρεσίες στο διαδίκτυο, καθιστά τους οργανισμούς αρκετά επιφυλακτικούς ως προς την υιοθέτηση της νέας τεχνολογίας. Οι οργανισμοί θεωρούν ότι αν μεταβούν σε

τεχνολογίες Cloud Computing τα δεδομένα τους θα δεσμευτούν (Data Lock-In) μέσα στο σύννεφο, οπότε αυτόματα θα γίνουν και αυτοί δέσμιοι του παρόχου υπηρεσιών Cloud Computing. Έτσι θα έρθουν αντιμέτωποι με πολλούς κινδύνους όπως είναι οι εκβιαστικές αυξήσεις των τιμών του παρόχου, η αμφισβήτηση της αξιοπιστίας των υπηρεσιών του παρόχου καθώς και ο κίνδυνος πτώχευσης του παρόχου.

3. **Εμπιστευτικότητα των δεδομένων και δυνατότητα ελέγχου (Data Confidentiality and Auditability)**

   Όσον αφορά την εμπιστευτικότητα των δεδομένων πολλοί θεωρούν ότι επειδή οι τωρινές υπηρεσίες Cloud Computing παρέχονται μέσα από δημόσια δίκτυα, τα δεδομένα τους γίνονται άμεσα εκτεθειμένα σε επιθέσεις. Ωστόσο κάτι τέτοιο δεν είναι σωστό καθώς γνωρίζουμε ότι κρυπτογραφημένα δεδομένα αποθηκευμένα σε κάποιο Cloud ίσως να είναι πιο ασφαλή από δεδομένα μη-κρυπτογραφημένα σε τοπικους χώρους αποθήκευσης. Ομοίως για τον έλεγχο παρέχεται η δυνατότητα ευκολότερου οικονομικού ελέγχου των υπηρεσιών καθώς και του ελέγχου των εικονικών λειτουργικών συστημάτων που παρέχονται από τον πάροχο Cloud Computing. Καταλήγουμε λοιπόν στο συμπέρασμα ότι δεν υπάρχουν ουσιαστικά εμπόδια μετάβασης στο Cloud Computing, όσον αφορά την εμπιστευτικότητα και τον έλεγχο καθώς οι υπηρεσίες Cloud Computing μπορούν να γίνουν τόσο ασφαλείς όσο οι τοπικές υποδομές ενός οργανισμού.

4. **Προβλήματα μεταφοράς των δεδομένων (Data Transfer Bottlenecks)**
   Σημαντικό πρόβλημα των οργανισμών είναι τα κόστη που προκύπτουν όσον αφορά τις χρεώσεις μεταφοράς των δεδομένων. Οι οργανισμοί θα πρέπει να υπολογίσουν τα σχετικά κόστη σε όλα τα επίπεδα μεταφοράς των δεδομένων στο Cloud με στόχο να ελαχιστοποιήσουν το γενικότερο κόστος της υπηρεσίας. Ωστόσο τα τελευταία χρόνια εξαιτίας της ταχύτατης ανάπτυξης της τεχνολογίας έχουν μειωθεί οι καθυστερήσεις μεταφοράς των δεδομένων, οι συνδέσεις είναι αξιόπιστες και τα κόστη μεταφοράς εξαιτίας του αυξημένου εύρους ζώνης (bandwidth) είναι αρκετά χαμηλά.
5. **Αδυναμία πρόβλεψης της απόδοσης (Performance Unpredictability)**

Στην τεχνολογία Cloud Computing πολλαπλές εικονικές μηχανές (Virtual Machines) μπορούν να μοιραστούν αρκετά αποδοτικά, επεξεργαστική ισχύ και κύρια μνήμη. Ωστόσο, όσον αφορά τα Inputs/Outputs (I/O's) η πολυπλοκότητα της νέας τεχνολογίας αυξάνεται, γι'αυτό και καθίσταται δύσκολος ο υπολογισμός ξεκάθαρης απόδοσης και αντίστοιχης χρέωσης. Η ταχύτατη όμως ανάπτυξη της τεχνολογίας μας δίνει την ικανότητα να πιστεύουμε ότι αυτά τα εμπόδια είναι θέμα χρόνου κ θα ξεπεραστούν στα επόμενα χρόνια πλήρως.

6. **Κλιμακωτή αποθήκευση (Scalable Storage)**

   Με τον όρο κλιμακωτή αποθήκευση εννοούμε ότι θέλουμε να κατασκευάσουμε ένα σύστημα αποθήκευσης το οποίο θα συνδυάζει τρόπους δέσμευσης των πόρων και των δεδομένων με τέτοιο τρόπο ώστε ο κάθε οργανισμός να λαμβάνει κάθε φορά «όσο χρειάζεται» και να του γίνεται και η αντίστοιχη χρέωση. Οι τρείς στόχοι που θέλουμε να πετύχουμε με αυτό τον τρόπο είναι οι εξής:

   1. Δέσμευση όσων πόρων χρειάζονται κάθε φορά
   2. Κανένα αρχικό κόστος
   3. Απεριόριστος αποθηκευτικός χώρος

7. **Σφάλματα σε μεγάλης κλίμακας κατανεμημένα συστήματα (Bugs in Large-Scale Distributed Systems)**

   Τα συστήματα που χρησιμοποιούνται για την υποστήριξη των τεχνολογιών Cloud Computing είναι μεγάλης κλίμακας κατανεμημένα συστήματα, οπότε η εύρεση των λαθών και αποσφαλμάτωση του όλου συστήματος είναι μια αρκετά πολύπλοκη και δύσκολη διαδικασία η οποία πέρνει χρόνο ο οποίος ειναι υψίστης οικονομικής σημασίας για τον οργανισμό.

8. **Γρήγορη Κλιμάκωση (Scaling Quickly)**

   Οι οργανισμοί επιθυμούν να τους παρέχεται ελαστικότητα όσον αφορά την χρήση της υπηρεσίας αλλα και το κόστος. Γι'αυτό τον λογό επιθυμούν να έχουν ταχύτατη κλιμάκωση των υπηρεσιών με στόχο την μέγιστη ελαχιστοποίηση του κόστους αλλά και την διατήρηση των πόρων που τους είναι διαθέσιμοι από τον πάροχο Cloud Computing. Με τον όρο κλιμάκωση εννοούμε χρεώσης ανα-ώρα, ανα-byte κ.λ.π. έτσι ώστε να μπορεί ο οργανισμός να επικεντρώνει το ενδιαφέροντου στην αποδοτικότητα του συστήματος Cloud Computing.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

9. **Φήμη του παρόχου διαμορφωμένη από ενέργειες χρηστών (Reputation Fate Sharing)**

   Οι οργανισμοί που αποφασίζουν να μεταβούν σε τεχνολογία Cloud Computing θα πρέπει να είναι διατεθειμένοι να αντιμετωπίσουν και συμπεριφορές άλλων κακόβουλων χρηστών οι οποίοι χρησιμοποιούν τον ίδιο πάροχο Cloud υπηρεσιών. Για παράδειγμα ένας κακόβουλος χρήστης θα μπορούσε να προβεί σε κακόβουλες ενέργειες εναντίον των πελατών του παρόχου, με αποτέλεσμα να καταστρέφει την φήμη του παρόχου και την αξιοπιστία των υπηρεσιών του. Ωστόσο υπάρχουν πλέον μηχανισμοί οι οποίοι αποτρέπουν την πραγματοποίηση τέτοιων συμπεριφορών.

10. **Παραχώρηση αδειών χρήσης λογισμικού (Software Licensing)**

    Οι άδειες λογισμικών περιορίζουν τους υπολογιστές στους οποίους θα τρέχει ένα λογισμικό και οι χρεώσεις για τα λογισμικά που χρησιμοποιούνται ανα υπολογιστή είναι αρκετά αυξημένες, έτσι δημιουργείται ένα πρόβλημα για το πώς ένας πάροχος Cloud υπηρεσιών θα μπορέσει να παρέχει στους οργανισμούς όλων των ειδών τα λογισμικά χωρις να υπάρχουν υπέρογκες χρεώσεις.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κεφάλαιο 3^{ο} – Τήρηση κι επεξεργασία δεδομένων στο Cloud Computing

3.1 Δεδομένα ενός πελάτη στο Cloud Computing

Όταν ένας πελάτης συνάψει σύμβαση με μία εταιρεία υπηρεσιών Cloud Computing τότε αρκετές πληροφορίες που αφορούν τον πελάτη γίνονται διαθέσιμες στην εταιρεία. Οι πληροφορίες των πελατών μπορεί να είναι «δεδομένα χρήστη» ή/και «προσωπικά δεδομένα». Τα δεδομένα χρήστη είναι πληροφορίες που συλλέγονται από τον πελάτη και συμπεριλαμβάνουν:

- Δεδομένα που συλλέγονται απευθείας από κάποιον πελάτη (π.χ. συμπληρώνονται από τον πελάτη μέσω της διαπεφής μιας εφαρμογής)
- Δεδομένα σχετικά με κάποιον πελάτη που συγκεντρώνονται έμμεσα (π.χ. μεταδεδομένα σε έγγραφα)
- Δεδομένα σχετικά με την συμπεριφορά χρήσης του πελάτη
- Δεδομένα που σχετίζονται με το σύστημα του πελάτη (π.χ διεύθυνση IP)

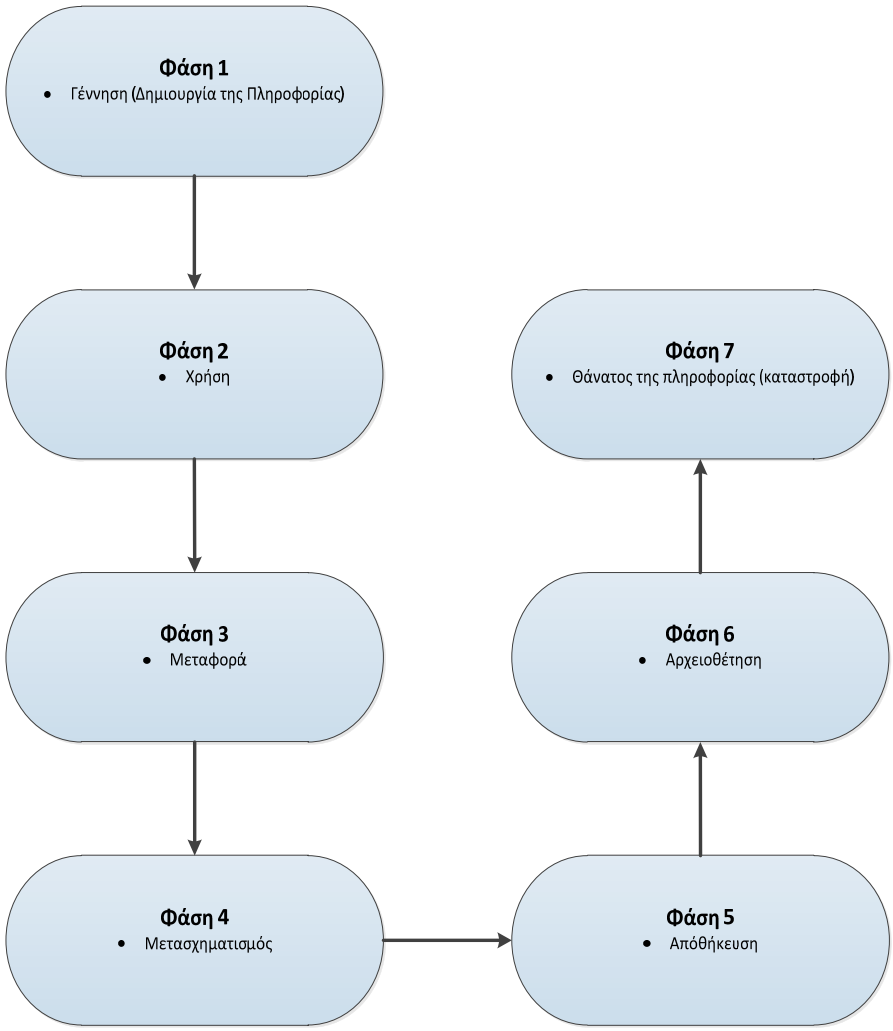
Να σημειωθεί πως τα δεδομένα χρήστη μπορεί να είναι και προσωπικά δεδομένα, εφόσον πρόκειται για φυσικό πρόσωπο και τα δεδομένα αναφέρονται στο πρόσωπο αυτό.

Όσον αφορά στα δεδομένα προσωπικού χαρακτήρα (μερικές φορές ονομάζονται και προσωπικά στοιχεία) περιλαμβάνεται κάθε δεδομένο που μπορεί πιθανώς να χρησιμοποιηθεί αυτόνομο ή σε συνδυασμό με άλλες πηγές, για να ταυτοποιήσει μοναδικά, να σχετίσει ή να εντοπίσει ένα μόνο πρόσωπο. Δεν θα αναλύσουμε περαιτέρω τα προσωπικά δεδομένα σε αυτή την ενότητα διότι θα εμβαθύνουμε στο κεφάλαιο 5.2 στο ζήτημα των προσωπικών δεδομένων στο Cloud Computing.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.2 Ο κύκλος ζωής των δεδομένων

Για να κατανοήσουμε καλυτέρα τις απαιτούμενες πολιτικές είναι χρήσιμο, να κάνουμε μια γρήγορη ανασκόπηση του κύκλου ζωής των δεδομένων (Data Life Cycle). Ο κύκλος ζωής των δεδομένων αναφέρεται στην διαδρομή που ακολουθεί, η πληροφορία από τη στιγμή που γίνετε αρχικά διαθέσιμή έως την τελική της αποδόμηση («θάνατο»). Στο σχεδιασμό της στρατηγικής του οργανισμού αναφορικά με τη πολιτική Προστασίας των προσωπικών δεδομένων, θα πρέπει να εξετασθεί ο αντίκτυπος του Cloud για καθεμία από τις ακόλουθες φάσεις όπως αναφέρονται αναλυτικά στο γράφημα[2,30,31].



Εικόνα 7

3.3 Ειδικά ζητήματα του κύκλου ζωής των δεδομένων στο Cloud Computing

Όπως αναφέραμε στο κεφάλαιο 3.2 ο κύκλος ζωής των δεδομένων αποτελείται από επτά στάδια. Σε καθένα από τα στάδια αυτά εγείρονται ποικίλα ερωτήματα τα οποία πρέπει να απαντηθούν για την εξασφάλιση της ορθής ροής των δεδομένων και των πληροφοριών από την δημιουργία μέχρι και την αποδόμηση τους. Παρακάτω θα αναλύσουμε τα ερωτήματα που προκύπτουν ξεχωριστά σε κάθε στάδιο του κύκλού ζωής των δεδομένων.

Φάση 1 : Δημιουργία της πληροφορίας

- Ιδιοκτησία: ποιος από τον οργανισμό είναι ο κύριος υπεύθυνος των προσωπικών δεδομένων, και πως η ιδιοκτησία των δεδομένων διατηρείται εάν ο οργανισμός χρησιμοποιεί τεχνολογίες Cloud Computing;
- Ταξινόμηση: πώς και πότε ένα προσωπικό δεδομένο καταχωρίζεται. Υπάρχουν περιορισμοί σχετικά με τη χρήση και επεξεργασία συγκεκριμένων κατηγοριών δεδομένων σε περιβάλλον Cloud;
- Διακυβέρνηση: υπάρχει μια δομή στην εταιρική διακυβέρνηση που να διασφαλίζει την διαχείριση και προστασία των προσωπικών δεδομένων συμφώνα με τις πρότυπες πολιτικές του οργανισμού; Και αν ναι, η δομή αυτή μπορεί να εξασφαλίσει την ροη έλεγχου για τα δεδομένα που μεταναστεύουν στο Cloud;

Φάση 2 : Χρήση

- Εσωτερική και εξωτερική χρήση: Τα προσωπικά δεδομένα χρησιμοποιούνται μόνο στο πλαίσιο του φορέα που αρχικά τα συλλέγει ή χρησιμοποιούνται και εκτός του οργανισμού (π.χ., υπηρεσίες ΤΕΙΡΕΣΙΑΣ Α.Ε);
- Τρίτα μέρη: είναι οι πληροφορίες που ο οργανισμός «μοιράζεται» από κοινού με τρίτους (π.χ., τους υπεργολάβους ενός προγράμματος πληροφορικής). Είναι πληροφορίες του οργανισμού οι οποίες είναι αναγκαίο να παρέχονται σε τρίτα πρόσωπα για την εύρυθμη λειτουργία των επιχειρησιακών διαδικασιών.

- Ορθότητα: είναι η χρήση των πληροφοριών ορθή και συμφωνεί με τον σκοπό για τον οποίο έχουν συλλεχθεί; Είναι ορθή η χρήση των δεδομένων όταν αυτά βρίσκονται σε περιβάλλον Cloud, και είναι σύμφωνη με τις νομικές (κατ' ελάχιστον) δεσμεύσεις που έχει αναλάβει ο οργανισμός απέναντι στα υποκείμενα των δεδομένων;
- Αποκάλυψη/Συμμόρφωση : Γίνεται η διαχείριση, των πληροφοριών που βρίσκονται, στο Cloud με τέτοιο τρόπο, ώστε να είναι εφικτή η συμμόρφωση του οργανισμού με νομικές απαιτήσεις σε περίπτωση δικαστικής διερεύνησης, η προστατευτικών μέτρων;

Φάση 3 : Μεταφορά

- Δημόσια ή Ιδιωτικά δίκτυα: όταν οι πληροφορίες μεταφέρονται σε ένα περιβάλλον Cloud αυτό είναι δημόσιο, και επίσης προστατεύεται καταλλήλως. (Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται πάντοτε, επιστάμενα προκειμένου να αποφευχθούν διαρροές που αφορούν στοιχεία του τελικού πελάτη και οι νομικές συνέπειες που ακολουθούν).
- Απαιτήσεις κρυπτογράφησης: Τα προσωπικά δεδομένα κρυπτογραφούνται; Τι ισχύει, αναφορικά με την κρυπτογράφηση για όσα δεδομένα ταξιδεύουν στο Cloud;
- Έλεγχος πρόσβασης: Υπάρχουν επαρκείς μηχανισμοί έλεγχου πρόσβασης (ποιος μπορεί να έχει πρόσβαση) σε δεδομένα προσωπικού χαρακτήρα;

Φάση 4 : Μετασχηματισμός

- Εξαγωγή ειδικών χαρακτηριστικών: Οι αρχικές δομές έλεγχου πρόσβασης και οι περιορισμοί χρήσης, διατηρούνται όταν τα προσωπικά δεδομένα μεταναστεύουν στο διαδίκτυο και μορφοποιούνται για περαιτέρω επεξεργασία (λ.χ συσχετισμός κάρτα αγορών και στοιχεία ταυτότητας στη γενική γραμματεία πληροφοριακών συστημάτων του ΥΠΟΙΚ);
- Συγκέντρωση-συσχέτιση: Τα δεδομένα όταν μεταφερθούν σε πλατφόρμα Cloud συνεχίζουν να σχετίζονται με ένα αναγνωρίσιμο άτομο (και αρά διατηρούν το χαρακτήρα του προσωπικού δεδομένου);

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

- Ακεραιότητα: η ακεραιότητα των προσωπικών δεδομένων διατηρείτε όταν αυτά πλέον υπάρχουν στο Cloud[29];

Φάση 5 : Αποθήκευση

- Έλεγχος πρόσβασης: Υπάρχουν δομές έλεγχου πρόσβασης για τα δεδομένα προσωπικού χαρακτήρα, που να διασφαλίζουν ότι όταν πλέον αυτά αποθηκεύονται στο Cloud, μόνο τα άτομα που είναι αναγκαίο και μόνο αυτά, θα μπορούν να έχουν πρόσβαση σε αυτά;
- Δομημένη έναντι αδόμητης αποθήκευσης: Με ποια μεθοδολογία αποθηκεύονται τα δεδομένα, και πως μπορεί ο οργανισμός να έχει μελλοντικά πρόσβαση και να τα διαχειριστεί;
- Ακεραιότητα/διαθεσιμότητα/εμπιστευτικότητα: Με ποιους μηχανισμούς εξασφαλίζεται η ακεραιότητα των δεδομένων, ποια η διαθεσιμότητα τούς και επιτυγχάνεται η διατήρηση της εμπιστευτικότητα τους όταν αυτά αποθηκεύονται σε περιβάλλον Cloud;
- Κρυπτογράφηση: πολλές νομοθετικές και κανονιστικές διατάξεις, σε διάφορες χώρες προβλέπουν, ότι ορισμένοι τύποι προσωπικών δεδομένων, πρέπει να αποθηκεύονται σε κρυπτογραφημένη μορφή. Γεννάται λοιπόν το ερώτημα, αν και σε ποιο βαθμό, ο πάροχος των υπηρεσιών Cloud είναι σε θέση να προσφέρει υπηρεσίες συμφώνα με την παραπάνω νομική απαίτηση.

Φάση 6 : Αρχειοθέτηση

- Νομικές Δεσμεύσεις: Τα προσωπικά δεδομένα υπόκεινται σε ρυθμίσεις που υπαγορεύουν για πόσο χρόνο θα πρέπει να αποθηκευτούν και να αρχειοθετηθούν; Είναι λοιπόν ζωτικής σημασίας η πλήρης συμμόρφωση του παρόχου προς της απαιτήσεις αυτές.
- Τεχνικοί προβληματισμοί: Το αποθηκευτικό μέσο που χρησιμοποιείται για την αρχειοθέτηση των πληροφοριών, θα είναι προσπελάσιμο και στο μέλλον (λ.χ οι δισκέτες 5,2’ δεν μπορούν πλέον να διαβαστούν γιατί οι σχετικές συσκευές ανάγνωσης έχουν αποσυρθεί). Ποιος ελέγχει τα μέσα μαζικής ενημέρωσης και ποια είναι η ικανότητα του οργανισμού για την ανάκτηση των φυσικών από τον παροχή Cloud;

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

- Διατήρηση: για πόσο καιρό τα δεδομένα θα διατηρούνται από τον πάροχο; Η περίοδος διατήρησης είναι συνεπής με την πολιτική του οργανισμού-πελάτη;

Φάση 7 : Θάνατος της πληροφορίας

- Ασφαλής καταστροφή: Η πολιτική αποδόμησης και καταστροφής της πληροφορίας γίνεται με τον ενδεδειγμένο τρόπο ώστε να είναι αδύνατη η μη εξουσιοδοτημένη επανάκτηση της ;
- Αποτελεσματικότητα: Οι πληροφορίες καταστρέφονται ολοσχερώς και με τρόπο που να κάνει αδύνατη την ανάκτηση τους από τον οποιοδήποτε;

Κεφάλαιο 4ο – Ασφάλεια στο Cloud

4.1 Πιθανές Επιθέσεις στο Cloud Computing

Το μεγαλύτερο ζήτημα του Cloud Computing είναι η ασφάλεια. Πολλοί είναι οι κακόβουλοι χρήστες οι οποίοι έχουν σκοπό να βλάψουν είτε τον πάροχο της υπηρεσίας Cloud Computing είτε τον ίδιο τον πελάτη. Παρακάτω θα σας παραθέσουμε μερικές από τις συνηθέστερες τεχνικές επίθεσης:

1. **Denial of service attacks:** Μια από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι με στόχο τη διακοπή παροχής υπηρεσιών από ένα δικτυακό κόμβο ή πληροφοριακό σύστημα είναι οι επιθέσεις τύπου Denial of service. Τα προγράμματα που συνήθως χρησιμοποιούν οι επιτιθέμενοι ακολουθούν την τακτική μαζικής αποστολής μηνυμάτων-αιτημάτων στο στόχο ώστε να προκαλέσουν την αποτυχία ανταπόκρισης του και την κατάρρευση του συστήματος.
2. **Επιθέσεις μεταμφίεσης (Spoofing):** Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, «μεταμφιέζεται» σε κάποιο νόμιμο χρήστη, ώστε να αποκτήσει πρόσβαση σε μια εφαρμογή. Δηλαδή ο επιτιθέμενος κάνει χρήση των στοιχείων πρόσβασης ενός εξουσιοδοτημένου χρήστη. Αυτό μπορεί να είναι αποτέλεσμα των εξής: α) οι εξουσιοδοτημένοι χρήστες δεν ακολουθούν τους κανόνες προστασίας των κωδικών πρόσβασης, β) οι κωδικοί πρόσβασης είτε διακινούνται μέσω του δικτύου, είτε αποθηκεύονται χωρίς κρυπτογράφηση, και γ) οι χρήστες χρησιμοποιούν εύκολους κωδικούς.
3. **E-mail Spoofing:** Το e-mail spoofing αποτελεί πρακτική παραποίησης ή απόκρυψης της πραγματικής πηγής από την οποία προήρθε το μήνυμα ηλεκτρονικού ταχυδρομείου. Χρησιμοποιείται συνήθως για να παραπλανήσει το χρήστη ώστε να συλλεχθούν από αυτόν χρήσιμα δεδομένα. Ενδεικτικά αποστέλλονται μηνύματα με υποτιθέμενο αποστολέα τον διαχειριστή του συστήματος, ζητώντας από το χρήστη να επιβεβαιώσει το password που χρησιμοποιεί.
4. **Επιθέσεις παρακολούθησης (Sniffing):** Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά συστημάτων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα «προγράμματα sniffing». Έτσι

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Οι συσκευές με δυνατότητες sniffing μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών IDS (Intrusion Detection System). Συνεπώς τέτοιου είδους συσκευές είναι χρήσιμες και απαραίτητες. Ωστόσο, είναι προφανές ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις υπηρεσίες που προσφέρουν τα προγράμματα sniffing για την υλοποίηση των παράνομων δραστηριοτήτων τους. Υπάρχουν ειδικά προγράμματα sniffing, ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση: α) password, β) στοιχείων οικονομικών συναλλαγών (π.χ. κωδικοί πιστωτικών καρτών), γ) εμπιστευτικών δεδομένων (π.χ. προσωπικά στοιχεία χρηστών, e-mail).

5. **Ιοί (viruses) - σκουλήκια (worms):** Οι ιοί είναι προγράμματα ή εντολές που προσαρτώνται σε προγράμματα ή δεδομένα και εκτελούνται παράλληλα με αυτά. Μπορούν να προκαλέσουν την αλλοίωση ή καταστροφή δεδομένων. Τα σκουλήκια αντίστοιχα, είναι προγράμματα που κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Και οι δύο κατηγορίες προγραμμάτων έχουν ως στόχο να πλήξουν το σύστημα στο οποίο εκτελούνται, προκαλώντας ζημιές όπως διαγραφή δεδομένων.
6. **Buffer overflow attacks (υπερχείλιση καταχωρητή):** Οι επιθέσεις αυτού του τύπου έχουν σαν στόχο να πλήξουν τις εφαρμογές που αποθηκεύουν δεδομένα σε προσωρινό χώρο μνήμης (buffer) μέχρι να έρθει η ώρα τους για επεξεργασία. Οι επιτιθέμενοι βάζουν κώδικα δικής τους κατασκευής στο πακέτο που στέλνεται για αποθήκευση στον καταχωρητή με σκοπό την αντικατάσταση μέρους του κώδικα της εφαρμογής με τις δικές τους εντολές. Σε περίπτωση επιτυχημένης εκτέλεσης των εντολών, οι επιτιθέμενοι αποκτούν προνόμια πρόσβασης μεγαλύτερα ενός απλού χρήστη της εφαρμογής και καταφέρνουν να αποκτήσουν τον έλεγχο του συστήματος.
7. **Cookie Poisoning:** Τα Cookies είναι αρχεία υπολογιστών που αποθηκεύονται στον σκληρό δίσκο του υπολογιστή του πελάτη ή στην μνήμη cache, κατά την πρόσβαση του σε μια εφαρμογή διαδικτύου μέσω ενός browser. Αυτά τα αρχεία περιέχουν πληροφορίες, όπως όνομα χρήστη, κωδικός πρόσβασης και στοιχεία συνόδου. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες με σκοπό τη χρήση του υπολογιστή του πελάτη για κακόβουλες

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πράξεις. Τα Cookies χωρίζονται σε δύο κατηγορίες: αυτά που μένουν στον υπολογιστή του χρήστη μόνο κατά τη διάρκεια της επίσκεψης του χρήστη στην εφαρμογή διαδικτύου, και αυτά που έχουν ημερομηνία λήξης και παραμένουν στον σκληρό δίσκο του πελάτη μέχρι την ημερομηνία λήξης τους οπότε και διαγράφονται[37].



4.2 Αρχές Ασφάλειας στο Cloud Computing

Για να μπορέσουν οι πάροχοι να προσφέρουν υπηρεσίες ποιότητας, θα πρέπει να ακολουθήσουν κάποιες βασικές αρχές ασφάλειας με στόχο να ελαχιστοποιήσουν τον κίνδυνο. Οι βασικές αρχές ασφάλειας πρέπει να εφαρμόζονται σε κάθε είδους εφαρμογές, ανεξάρτητα από την τεχνολογία της κάθε εφαρμογής.

Οποιοσδήποτε ασχολείται με την ασφάλεια των web εφαρμογών πρέπει να τηρεί τις παρακάτω βασικές αρχές ασφάλειας:

1. **Ελάχιστα δυνατά προνόμια:** Θα πρέπει να παραχωρούνται στους χρήστες ελάχιστα προνόμια και δικαιώματα πρόσβασης, ούτως ώστε οι επιτιθέμενοι να έχουν περιορισμένες ικανότητες σε περίπτωση που καταφέρουν να παραβιάσουν την ασφάλεια της εφαρμογής.
2. **Έλεγχος εγκυρότητας εισαγόμενων δεδομένων:** Τα δεδομένα τα οποία εισάγονται στην εφαρμογή από τους χρήστες αποτελούν δίοδο εχθρικού λογισμικού προς την εφαρμογή. Τα δεδομένα αυτά αποτελούν το αρχικό όπλο του επιτιθέμενου στην προσπάθεια του να εισβάλει στην εφαρμογή. Τα εισερχόμενα προς την εφαρμογή δεδομένα θα πρέπει να ελέγχονται. Η πιο ασφαλής τακτική ελέγχου είναι να θεωρούνται όλα τα δεδομένα εισαγωγής κακόβουλα μέχρι να αποδειχθεί το αντίθετο και να γίνεται έλεγχος επικύρωσης όλων των δεδομένων, ώστε η εφαρμογή να αποδέχεται μόνο ασφαλή δεδομένα και να απορρίπτει τα υπόλοιπα.
3. **Έλεγχος στην πύλη:** Όλοι οι επισκέπτες θα πρέπει να αυθεντικοποιούνται κατά την είσοδο τους στο σύστημα.
4. **Αποτυχία με ασφάλεια:** Σε περίπτωση που αποτύχει η εφαρμογή τα ευαίσθητα δεδομένα δεν θα πρέπει να παραμένουν προσιτά σε τρίτους. Θα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πρέπει να επιστρέφονται φιλικά μηνύματα σφάλματος στους χρήστες τα οποία να μην εκθέτουν τις εσωτερικές λεπτομέρειες του συστήματος και γενικά να μην περιλαμβάνουν λεπτομέρειες που θα μπορούσαν να βοηθήσουν τους επιτιθέμενους να εκμεταλλευτούν τις ευπάθειες τις εφαρμογής.

5. **Δημιουργία ασφαλών προεπιλογών:** Οι λογαριασμοί προεπιλογής (default account) θα πρέπει εξ ορισμού να είναι εκτός λειτουργίας και σε περίπτωση ανάγκης να επιτρέπεται ρητά η χρήση τους. Όταν εμφανίζεται ένα λάθος θα πρέπει τα ευαίσθητα δεδομένα να μην διαρρέουν πίσω στον χρήστη ο οποίος ενδεχομένως θα μπορεί να τα χρησιμοποιήσει ενάντια στο σύστημα.
6. **Μείωση περιοχής επιθέσεων:** Θα πρέπει να μειώνεται η διαθέσιμη περιοχή για επιθέσεις. Αυτό μπορεί να γίνει θέτοντας εκτός λειτουργίας ή αφαιρώντας αχρησιμοποίητες συσκευές και πρωτόκολλα[37].

4.3 Ποσοτικοποίηση Κινδύνου και Πρότυπα Ασφάλειας

Οι προσεγγίσεις ως προς την ασφάλεια πρέπει να είναι αντικειμενικές κυρίως όσον αφορά τον έλεγχο του συστήματος και τη λειτουργικότητά του. Αυτό που εννοούμε είναι ότι δεν είναι κατάλληλη η ίδια αρχιτεκτονική και ο ίδιος έλεγχος για διαφορετικές εφαρμογές ασφάλειας. Σε ότι αφορά την Cloud τεχνολογία, δεν πρέπει να αναμείξουμε τραπεζικές με εφαρμογές κοινωνικής δικτύωσης, σε ένα δημόσιο σύννεφο (Cloud). Από τη φύση τους κάποιες εφαρμογές χαμηλού κινδύνου ασφάλειας, θα μπορούσαν να συνυπάρξουν με άλλες εφαρμογές με ανάλογες ανάγκες ασφάλειας.

Για να μπορέσουμε να ποσοτικοποιήσουμε τον κίνδυνο θα λέγαμε ότι έχει εξάρτηση από τις ευπάθειες του συστήματος, τις απειλές που δέχεται το σύστημα καθώς και από τα μέτρα πρόληψης που λαμβάνουμε για να αντιμετωπίσουμε τις καταστάσεις αυτές.

$$\text{Risk} = \left(\frac{\text{Threats} \times \text{Vulnerabilities}}{\text{Countermeasures}}\right) \times (\text{Asset value})$$

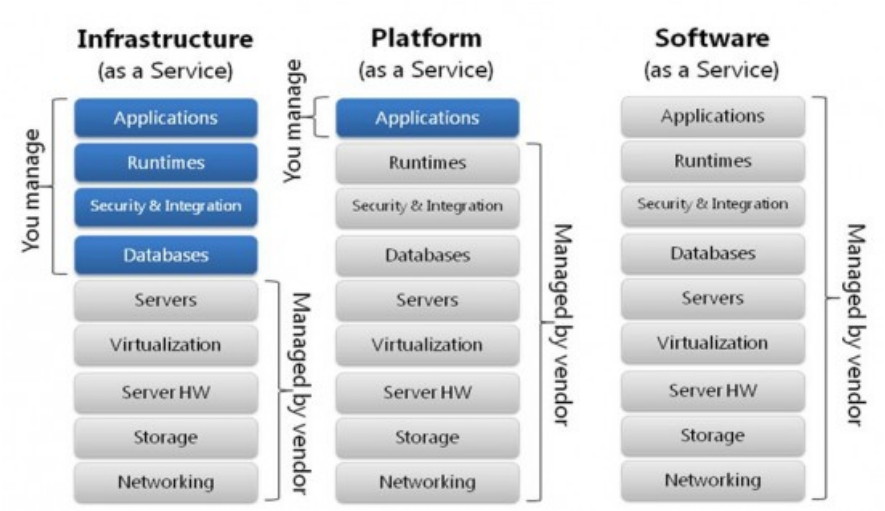
Ο υπολογισμός του κίνδυνου από τον παραπάνω τύπο μας βοηθάει να ποσοτικοποιήσουμε τις ευπάθειες του συστήματος μας, κάτι το οποίο είναι αρκετά δύσκολο να γίνει.



Υπάρχει ένα ευρύ φάσμα μοντέλων και προτύπων που ισχύουν για να παρέχουν ασφάλεια σε Λογισμικό / λύσεις ασφάλειας / συστήματα Ανάπτυξης Κύκλου Ζωής (System Development Life Cycle - SDLC). Αρκετές από αυτές μπορούν να χρησιμεύσουν ως πρότυπα αναφοράς για την τεχνολογία συστημάτων ασφαλείας, αρχιτεκτονική ασφαλείας, τις διαδικασίες ασφάλειας, και σίγουρα για την ασφάλεια στο Cloud. Ορισμένα από αυτά τα μοντέλα είναι:

- **ISO 27001 through ISO 27006F:** Αυτή η σειρά διεθνών προτύπων για την ασφάλεια των πληροφοριών καλύπτει την διαχείριση, τις βέλτιστες πρακτικές, τις απαιτήσεις και τις τεχνικές. Αυτά έχουν σημαντική αξία ως προς τις δυνατότητες εφαρμογής τους στην ασφάλεια του Cloud.
- **European Network and Information Security Agency (ENISA):** Είναι ένας Ευρωπαϊκός οργανισμός ασφάλειας του διαδικτύου.
- **Information Technology Infrastructure Library (ITIDI:** Η διαχείριση ασφάλειας στο ITIL είναι βασισμένη στο ISO/IEC 27002.
- **Control Objectives for Information and related Technology (COBIT):** Πρόκειται για ένα σύνολο από γενικά αποδεκτές καλύτερες πρακτικές και μέτρα ασφάλειας.

Ανάλογα με το είδος της υπηρεσίας που εκτελείται στο Cloud (IaaS, PaaS ή IaaS) ο πελάτης έχει και διαφορετικό έλεγχο αυτής της υπηρεσίας.



Εικόνα 8

Με το SaaS, η ασφάλεια αναλαμβάνεται από τον πάροχο υπηρεσιών του Cloud. Αντίθετα με το PaaS, προσφέρεται μεγαλύτερη επεκτασιμότητα και έλεγχος από τους πελάτες.

Κεφάλαιο 5ο – Ζητήματα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων: εφαρμοστέο δίκαιο, κατανομή ρόλων και ευθύνης

5.1 Ιδιωτικότητα και Απόρρητο

Μία από τις πιο συνήθεις προσλήψεις της έννοιας της ιδιωτικότητας είναι ότι αυτή συνίσταται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτήν την έννοια η ιδιωτικότητα προσβάλλεται με την αποκάλυψη απόρρητης πληροφορίας . Ιδίως η «κλασική» προσέγγιση της ιδιωτικότητας ως refugium (καταφυγίου) παρουσιάζει στοιχεία ταύτισης ή και σύγχυσης με την έννοια του απορρήτου (secrecy) και της εμπιστευτικότητας (confidentiality).

Οι όροι αυτοί, αν και συχνά γίνονται αντιληπτοί και χρησιμοποιούνται ως ισοδύναμοι, εκφράζοντας σε τελευταία ανάλυση παρεμφερείς αξιώσεις προστασίας, εντούτοις δεν ταυτίζονται: Η έννοια του απόρρητου (secrecy) αναφέρεται είτε στη μη προσπελασιμότητα ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης (όπως το ιατρικό απόρρητο ή το τραπεζικό απόρρητο) είτε τις κατέχουν επί τη βάσει της θέσης και της αρμοδιότητάς τους (όπως το υπηρεσιακό απόρρητο). Εάν μάλιστα πρόκειται για πληροφορία που εμπίπτει στη δημόσια σφαίρα δεν είναι νοητή η προστασία από το απόρρητο. Για να είναι απόρρητη/εμπιστευτική η πληροφορία θα πρέπει να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.λπ.

Το «απόρρητο» αποκλείει τους (περαιτέρω) τρίτους από τη γνώση, τη χρήση και αξιοποίηση των πληροφοριών, εφόσον δεν συντρέχει κάποιος νόμιμος λόγος και η αντίστοιχη διαδικασία που επιτρέπουν την άρση του απορρήτου. Αξίζει πάντως να σημειωθεί ότι σε ορισμένες έννομες τάξεις, όπως αυτή των ΗΠΑ, ήδη το γεγονός ότι ένα πρόσωπο εμπιστεύεται μία πληροφορία που το αφορά σε ένα άλλο πρόσωπο ή οργανισμό οδηγεί στη στέρηση της προστασίας που επιφυλάσσεται στην ιδιωτικότητα. Η άποψη αυτή συνδέεται με κρίσιμες για τα πρόσωπα συνέπειες, όπως π.χ. το εύρος και οι προϋποθέσεις για περαιτέρω κοινοποίηση των πληροφοριών αυτών. Το Supreme Court (Ανώτατο Δικαστήριο των ΗΠΑ)

έκρινε ότι ένα πρόσωπο δεν έχει εύλογη προσδοκία ιδιωτικότητας (reasonable expectation of privacy), όσον αφορά πληροφορίες που αποκάλυψε εθελοντικά σε ένα τρίτο πρόσωπο ή οργανισμό και στη συνέχεια διαβιβάστηκαν από αυτό σε μία δημόσια αρχή, ακόμη και εάν η πληροφορία δόθηκε αρχικά με την υπόθεση ότι θα χρησιμοποιηθεί για έναν περιορισμένο σκοπό. Στο σημείο αυτό εντοπίζεται μία βασική ατέλεια της επίκλησης της ιδιωτικότητας ως πληροφοριακής απομόνωσης: η χρησιμότητά της (και συνακόλουθα η προστασία του υπό συζήτηση αγαθού) εν τέλει παύει να υφίσταται κατά τη στιγμή που η πληροφορία «παραδίδεται» σε κάποιον άλλον, «διαφεύγει» από το πρόσωπο που αφορά και παύει να είναι «μυστική».[46]

5.2 Ζητήματα Ιδιωτικότητας και Ασφάλειας των Δεδομένων στο Cloud Computing

Το Cloud Computing είναι μια καινούρια τεχνολογία, η οποία περιλαμβάνει αρκετά οφέλη αλλά και αρκετούς κινδύνους. Είναι κάτι καινοτόμο και πρωτοποριακό και γι' αυτό προκαλεί διστακτικότητα στους χρήστες όσον αφορά τα θέματα ιδιωτικότητας και ασφάλειας δεδομένων. Προτού όμως αναφερθούμε σε θέματα ιδιωτικότητας και ασφάλειας δεδομένων στο Cloud Computing, επιβάλλεται να ορίσουμε τις δύο έννοιες σε νομικό αλλά και σε πληροφοριακό επίπεδο. Με τον όρο ιδιωτικότητα σε **νομικό επίπεδο** αναφερόμαστε σε ένα σύνολο δικαιωμάτων τα οποία έχουν καταχυρωθεί κατά τον 20^{ο} αιώνα . Η ιδιωτικότητα συγκροτείται από ορισμένα επιμέρους δικαιώματα ή εκφάνσεις [45]:

1. το δικαίωμα σε ιδιωτική ζωή
2. ο περιορισμός της προσβασιμότητας
3. ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο (ή άσυλο της κατοικίας)
4. η ελαχιστοποίηση των "παρεμβάσεων" (intrusiveness)
5. η προσδοκία της εχεμύθειας
6. το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της – υπό στενή έννοια - ιδιωτικότητας (intimacy)
7. της ανωνυμίας και της απόσυρσης (reserve)

Με τον όρο ιδιωτικότητα σε **πληροφοριακό επίπεδο** αναφερόμαστε στην συσχέτιση ανάμεσα στην συλλογή και διάδοση των δεδομένων και στα νομικά

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ζητήματα που προκύπτουν από αυτό. Η δυνατότητα να ελέγχει κάποιος ποιές πληροφορίες αποκαλύπτονται για τον ίδιον μέσω του Διαδικτύου, και ποιος μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, αποτελεί ένα ζήτημα αυξανόμενης ανησυχίας. Τα πεδία της ασφάλειας δεδομένων και της ασφάλειας πληροφοριών σχεδιάζουν και χρησιμοποιούν υλικό, λογισμικό και ανθρώπινους πόρους για να αντιμετωπίσουν αυτό το ζήτημα[40].

Όσον αφορά τον τομέα της ασφάλειας των πληροφοριών/δεδομένων σε **πληροφοριακό επίπεδο**, η κοινότητα της τεχνολογίας των πληροφοριών, ώς ασφάλεια ορίζει:

> «**Ασφάλεια Πληροφοριών** είναι η προστασία και τήρηση της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των πληροφοριών»

Όπου:

> **Εμπιστευτικότητα** (Confidentiality) είναι η διασφάλιση της προσπέλασης της πληροφορίας μόνο από εξουσιοδοτημένους χρήστες.
>
> **Ακεραιότητα** (Integrity) είναι η διασφάλιση της ακρίβειας και πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας της.
>
> **Διαθεσιμότητα** (Availability) είναι η διασφάλιση της προσπέλασης στην πληροφορία εξουσιοδοτημένων χρηστών, σε εύλογα προσδοκώμενο χρόνο.

Όσον αφορά τον ορισμό της ασφάλειας σε **νομικό επίπεδο**, θεωρούμε την ασφάλεια συνιστώσα της προστασίας των δεδομένων και της ιδιωτικότητας, ενώ εστιάζεται στην έγκαιρη αναγνώριση πιθανών κινδύνων και απειλών και την ανάπτυξη προληπτικών μέτρων και διαδικασιών για τη διάγνωση, την αποφυγή αλλά και τον εντοπισμό της επέλευσής τους. Φαίνεται να μην υπάρχει κάποιο πεδίο στην πληροφορική το οποίο να μην επηρεάζεται από το Cloud Computing. Τα δύο πιο σημαντικά προβλήματα που αφορούν την ιδιωτικότητα των δεδομένων στο Cloud Computing είναι:

1. Η απώλεια του ελέγχου στα δεδομένα και
2. Η εξάρτηση από τον πάροχο των υπηρεσιών Cloud Computing (αλλά και ο προσδιορισμός των υποχρεώσεων και των ευθυνών του)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Τα παραπάνω προβλήματα αναλύονται σε μία σειρά από ειδικότερα νομικά προβλήματα καθώς και ζητήματα ασφάλειας που σχετίζονται με την υποδομή (infrastructure), την διαχείριση ταυτότητας (identity management), τον έλεγχο πρόσβασης, τη διαχείριση ρίσκου (risk management), την κανονιστική και νομοθετική συμμόρφωση στο νόμο (regulatory and legislative compliance), τον έλεγχο ακεραιότητας (integrity control) όπως επίσης και τους κινδύνους που εξαρτώνται από τον συγκεκριμένο πάροχο υπηρεσιών Cloud Computing.

Μερικά προβλήματα που σχετίζονται με την απώλεια ελέγχου των δεδομένων είναι[34][35]:

Προβλήματα που αφορούν την ιδιωτικότητα:

1. Οι περισσότεροι πελάτες γνωρίζουν τους κινδύνους που σχετίζονται με την παραχώρηση του ελέγχου και αποθήκευσης των δεδομένων τους σ'έναν πάροχο υπηρεσιών νεφουπολογιστικής (Cloud Computing Provider). Τα δεδομένα μπορούν κάλλιστα να υποκλαπούν από τον Cloud Computing Provider, όπως επίσης και από άλλες ανταγωνιστικές εταιρίες, οι οποίες έχουν τον ίδιο πάροχο.
2. Υπάρχει μια έλλειψη διαφάνειας (προς τον πελάτη) όσον αφορά τον τρόπο, τον χρόνο και τον τόπο διαχείρισης των δεδομένων. Αυτό αντιτίθεται στην απαίτηση προστασίας δεδομένων που συνιστά οι πελάτες να γνωρίζουν τι συμβαίνει με τα δεδομένα τους.
3. Τεχνικά, πολλοί πάροχοι υπηρεσιών Cloud Computing είναι ικανοί να κάνουν εξόρυξη δεδομένων (data mining) και να επεξεργαστούν και να αναλύσουν τα δεδομένα. Είναι μια πολύ λεπτή λειτουργία και ακόμα περισσότερο όταν οι χρήστες αποθηκεύουν και διαχειρίζονται τα δεδομένα αυτά μέσω υπηρεσιών Cloud Computing. Αυτό γίνεται πιό κατανοητό με τις εφαρμογές των μέσων κοινωνικής δικτύωσης (social media) όπου χρήστες ενθαρρύνονται να δημοσιεύσουν στοιχεία της ιδιωτικής τους ζωής, όπως για παράδειγμα προσωπικές φωτογραφίες[33].

4. Η προστασία δεδομένων και η νομοθεσία περί ιδιωτικότητας δεν είναι παρόμοιες στις περισσότερες χώρες του κόσμου ενώ το Cloud Computing είναι η παγκόσμια υπηρεσία του μέλλοντος. Συνεπώς προβλήματα και κίνδυνοι οι οποίοι επηρεάζουν τους κανόνες προστασίας των δεδομένων πρέπει να ληφθούν σοβαρά υπόψην όταν οι πλατφόρμες των υπηρεσιών Cloud Computing βρίσκονται σε διακομιστές (servers) εκτός των Ευρωπαικών χωρών.

Προβλήματα που αφορούν την ασφάλεια:

1. Οι φορητές συσκευές (mobile devices) και ειδικότερα ο περιορισμένος αποθηκευτικός χώρος και οι δυνατότητες που έχουν, οδηγούν στην ανάγκη χρησιμοποίησης υπηρεσιών που στηρίζονται στο Cloud Computing και όχι στο λογισμικό (software) των Η/Υ. Ακόμη και όταν πρέπει να μεταφερθούν δεδομένα από μια φορητή συσκευή σε μια άλλη τοπική συσκευή, συχνά χρησιμοποιούνται εφαρμογές Cloud, όταν η συσκευή έχει τέτοιες δυνατότητες και υπηρεσίες. Ως εκ τούτου οι χρήστες βάζουν τον εαυτό τους σε κίνδυνο χωρίς να το συνειδητοποιήσουν αφού πιστεύουν ότι η μεταφορά των δεδομένων γίνεται τοπικά.
2. Από την στιγμή που το Cloud είναι μια υπηρεσία ,είναι προσβάσιμη εξ' αποστάσεως, η σύνδεση μεταξύ παρόχου υπηρεσιών Cloud Computing και του πελάτη δεν προστατεύεται πάντα επαρκώς. Προκύπτουν κίνδυνοι ασφάλειας οι οποίοι απειλούν την μεταφορά δεδομένων και μπορεί να περιέχουν υποκλοπές, πλαστογράφηση του DNS (DNS spoofing), καθώς και επιθέσεις Denial-of-Service.
3. Η στροφή προς το Cloud Computing καθιστά τη χρήση των παραδοσιακών προσεγγίσεων διαχείρισης κινδύνων δύσκολη έως και αδύνατη. Ανεξάρτητα από το γεγονός ότι ο έλεγχος των δεδομένων μεταφέρεται στον πάροχο των υπηρεσιών Cloud Computing, η διαχείριση των κινδύνων όπως επίσης και τα θέματα συμμόρφωσης καταμερίζονται μεταξύ του πελάτη, του παρόχου υπηρεσιών Διαδικτύου (ISP) και του παρόχου υπηρεσιών Cloud Computing. Επιπρόσθετα, η συμμόρφωση με το νόμο είναι ένας πολύ σημαντικός παράγοντας μεταξύ του πελάτη και του παρόχου υπηρεσιών Cloud Computing. Την ώρα που οι περισσότερες ρυθμιστικές και νομοθετικές συμφωνίες είναι συνήθως προβληματικές. Τα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

data centers των υπηρεσιών Cloud μπορούν να εξαπλωθούν γεωγραφικά, επομένως η νομοθετική δικλείδα δεν έχει ακόμα αποσαφηνιστεί. Ειδικότερα, ενώ οι περισσότερες χώρες έχουν ψηφίσει νόμους όσον αφορά τα νομικά ζητήματα του Cloud Computing, ο πάροχος των υπηρεσιών Cloud Computing, μπορεί κάλλιστα να μεταφέρει τις υποδομές του εκτός συνόρων έτσι ώστε η εταιρεία του μαζί με τα δεδομένα που διαχειρίζεται να μην εντάσσεται στο κανονιστικό πλαίσιο της αντίστοιχης χώρας.

4. Αφού όλος ο τεχνικός έλεγχος ανατίθεται στον πάροχο υπηρεσιών Cloud Computing, οι πελάτες συχνά θέλουν να γίνεται εξωτερικός έλεγχος του παρόχου αυτού. Επομένως, οι πληροφορίες που σχετίζονται με τον έλεγχο πρόσβασης και την καταγραφή θα πρέπει να αποθηκευτούν και να προστατευτούν με απώτερο σκοπό να επαληθευτούν. Η κατάλληλη καταγραφή μπορεί να παρέχει την δυνατότητα για επιστημονική εξερεύνηση σε περίπτωση κάποιου απροόπτου.
5. Υπάρχουν ανησυχίες που σχετίζονται με την διαγραφή των δεδομένων καθώς είναι δύσκολο να διαγράψεις όλα τα ηλεκτρονικά αντίγραφα μιας πληροφορίας/ενός δεδομένου αφού δεν μπορείς να τα βρείς όλα, αυτό προκύπτει διότι είναι τόσο μεγάλος ο όγκος των πληροφοριών τα οποία δέχονται επεξεργασία από διαφορετικές υπηρεσίες, που καθιστά πολύ δύσκολη έως αδύνατη την εύρεση όλων των αντιγράφων με στόχο την διαγραφή τους. Είναι αδύνατον να εγγυηθείς την πλήρη διαγραφή όλων των δεδομένων. Ως αποτέλεσμα, είναι πολύ δύσκολο να επιβάλλεις την υποχρεωτική διαγραφή των δεδομένων. Ωστόσο, η υποχρεωτική διαγραφή δεδομένων πρέπει να συμπεριληφθεί στον προκείμενο κανονισμό των υπηρεσιών Cloud Computing , αλλά ακόμα δεν μπορούμε να στηριχθούμε σε αυτόν: αν υπήρξε ποτέ εποχή με «Εγγυημένη συνολική διαγραφή δεδομένων», έχει πια περάσει. Αυτή η παράμετρος θα πρέπει να λαμβάνεται υπόψη πολύ σοβαρά, όταν τα δεδομένα συλλέγονται και αποθηκεύονται.
6. Το Cloud Computing εξαρτάται από την έμπιστη και ασφαλή χρήση του τηλεπικοινωνιακού δικτύου το οποίο διασφαλίζει και εγγυάται την διεκπεραίωση των τερματικών χρηστών από τις παρεχόμενες υπηρεσίες του Cloud από τον πάροχο των υπηρεσιών Cloud Computing. Οι

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

τηλεπικοινωνιακοί πάροχοι συχνά διαφέρουν από τους παρόχους υπηρεσιών Cloud Computing.

Τυπικά ζητήματα σχετικά με την εξάρτηση στον πάροχο υπηρεσιών Cloud Computing συμπεριλαμβάνουν[35][36]:

1. Μια μεγάλη ανησυχία σχετικά με τον βαθμό εξάρτησης ενός συγκεκριμένου παροχέα υπηρεσιών Cloud Computing είναι η διαθεσιμότητα. Αν ο πάροχος οδεύει προς την «χρεοκοπία» και σταματήσει να παρέχει υπηρεσίες, ο πελάτης, μπορεί να αντιμετωπίσει προβλήματα πρόσβασης στα δεδομένα του και ως εκ τούτου κα στην συνέχεια του κύκλου εργασιών της επιχείρησης.
2. Μερικές διαδεδομένες εφαρμογές Cloud Computing υπηρεσιών (όπως το Google Docs) δεν συμπεριλαμβάνουν κάποιο συμφωνητικό, ή σύμβαση ανάμεσα στον πελάτη και τον πάροχο. Ως αποτέλεσμα ο πελάτης δεν έχει κανένα αποδεικτικό στην περίπτωση πιθανού προβλήματος κι εν γένει δεν αποτυπώνονται/ προβλέπονται δεσμευτικά τα δικαιώματά του και οι υποχρεώσεις-ευθύνες του παρόχου.
3. Οι υπηρεσίες Cloud Computing είναι υπηρεσίες παρόμοιες με άλλες παραδοσιακές υπηρεσίες και εφαρμογές (π.χ. τηλεπικοινωνίες, τραπεζικές συναλλαγές, ηλεκτρικό ρεύμα, νερό κ.λ.π.). Και οι παραδοσιακές αλλά και οι υπηρεσίες Cloud Computing είναι υπηρεσίες οι οποίες παρέχονται από μεγάλους πάροχους και «φιλοξενούν» μικρούς πελάτες. Επομένως οι πελάτες εξαρτώνται συχνά από τους παρόχους επειδή είναι δύσκολο να αλλάξουν πάροχο εάν η αλλαγή αυτή είναι εφικτή. Ως συνέπεια οι παραδοσιακές υπηρεσίες ρυθμίζονται συχνά αναφορικά με την έκταση των λειτουργιών όπως η τιμολόγηση, η αξιοπιστία του παρόχου κ.λ.π.

Το Cloud ενισχύει την τάση ότι η ασφάλεια στην Πληροφορική δεν είναι ένα καθαρό τεχνικό ζήτημα αλλά ένα ζήτημα μεταξύ ατόμων και οργανισμών και για αυτό τον λόγο περιλαμβάνει πολλές ανθρώπινες και οργανωτικές προοπτικές όπως τη διαχείριση, τα συμφωνητικά και τη νομική προστασία.

Στο σημείο αυτό θα μιλήσουμε για το μεγαλύτερο πρόβλημα που προκύπτει για την ιδιωτικότητα, το οποίο είναι η αμφισβήτηση της.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Η αμφισβήτηση της ιδιωτικότητας ή η αμφισβήτηση της εμβέλειας και των μέσων της, οφείλονται σε ποικίλες αιτίες:

1. τον νομικό πολιτισμό μιας χώρας
2. τις κυρίαρχες αντιλήψεις για τη σχέση ιδιωτικής-δημόσιας σφαίρας
3. την έμφαση σε άλλες πολιτικο-οικονομικές επιδιώξεις, στις οποίες η προστασία της ιδιωτικότητας προυποθέτει την εκπλήρωση άλλων δικαιωμάτων και συμφερόντων

Τα όρια της ιδιωτικότητας και της προστασίας της καθορίζονται από:

1. τεχνολογικούς παράγοντες
2. την παγκοσμιοποίηση της επεξεργασίας και της επικοινωνίας
3. τις αλλαγές των αντιλήψεων τόσο των ατόμων όσο και των κρατικών και κοινωνικών οργανώσεων ως προς το περιεχόμενο της ιδιωτικότητας όσο και ως προς τη σχέση της με άλλα δημόσια και ιδιωτικά αγαθά και επιδιώξεις

Η πληροφοριακή ιδιωτικότητα διάγει περίοδο κρίσεως που οφείλεται τόσο στην περιρρέουσα πολιτικο-οικονομική πραγματικότητα όσο και σε βασικά δομικά χαρακτηριστικά των ΤΠΕ, όπως αυτές εξελίσσονται και λειτουργούν[46].

5.3 Προσωπικά Δεδομένα

Στα δεδομένα προσωπικού χαρακτήρα (μερικές φορές ονομάζονται και προσωπικά στοιχεία) περιλαμβάνεται κάθε δεδομένο που μπορεί πιθανώς να χρησιμοποιηθεί αυτόνομο ή σε συνδυασμό με άλλες πηγές, για να ταυτοποιήσει μοναδικά, να σχετίσει ή να εντοπίσει ένα μόνο πρόσωπο. Παραδείγματα προσωπικών δεδομένων είναι:

- Πληροφορίες επικοινωνίας (όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, τηλέφωνο, ταχυδρομική διεύθυνση)
- Μορφές ταυτοποίησης (ταυτότητα, δίπλωμα οδήγησης, διαβατήριο, δαχτυλικά αποτυπώματα)
- Δημογραφικές πληροφορίες (ηλικία, φύλο, εθνικότητα, θρησκευτικές πεποιθήσεις, σεξουαλικές προτιμήσεις, ποινικό μητρώο)
- Επαγγελματικές πληροφορίες (θέση, όνομα εταιρείας)

- Πληροφορίες υγειονομικής περίθαλψης (κατάσταση υγείας, πάροχοι, ασφάλιση, γενετικές πληροφορίες)
- Χρηματοοικονομικές πληροφορίες (τραπεζικούς και πιστωτικούς/ χρεωστικούς αριθμούς λογαριασμών, ιστορικό αγορών)
- Online δραστηριότητα (διεύθυνση IP, αγορές, επαφές, επισκέψεις, ηλεκτρονικοί φίλοι...)

Ένα υποσύνολο των προσωπικών δεδομένων ορίζεται ως ευαίσθητα προσωπικά δεδομένα και απαιτεί ένα μεγαλύτερο επίπεδο ελέγχου όσο αφορά την συλλογή, χρήση, γνωστοποίηση και προστασία. Παραδείγματα πληροφοριών που αποτελούν ευαίσθητα προσωπικά δεδομένα είναι: 1) θρησκευτικές πεποιθήσεις 2) πολιτικές ιδέες και 3) πληροφορίες που αφορούν την υγεία. Τα ευαίσθητα προσωπικά δεδομένα περιλαμβάνουν και κάποιες μορφές ταυτοποίησης, όπως ο αριθμός κοινωνικής ασφάλισης, ορισμένα δημογραφικά δεδομένα, και πληροφορίες που μπορούν να χρησιμοποιηθούν για να αποκτήσει κάποιος πρόσβαση σε χρηματοοικονομικούς λογαριασμούς, όπως αριθμοί πιστωτικών καρτών και αριθμοί λογαριασμών σε συνδυασμό με οποιονδήποτε απαιτούμενο κωδικό ασφαλείας ή κωδικό πρόσβασης.

5.3.1 Σε ποιόν “ανήκουν” τα δεδομένα

Υπάρχουν σημαντικά ερωτήματα που ο νομοθέτης πρέπει να επιλύσει καθώς αυτός έχει την όλη ευθύνη της ορθής εφαρμογής του κανονιστικού πλαισίου που αφορά το Cloud Computing.

Πρώτον, ποιος είναι ο κύριος των δεδομένων: ποιά είναι δηλαδή τα πρόσωπα τα οποία αφορούν τα δεδομένα; και δεύτερον αν το κανονιστικό πλαίσιο που θα εφαρμοστεί θα δίνει απαντήσεις σχετικά με την ιδιωτικότητα των προσώπων.

Ένα μεγάλο πρόβλημα είναι ότι άτομα που χρησιμοποιούν υπηρεσίες Cloud, δεν αντιλαμβάνονται τις επιπλοκές που επιφέρει στο προσωπικό τους απόρρητο η μεταφορά προσωπικών δεδομένων, σε κοινόχρηστες υποδομές, ενώ παράλληλα δεν είναι κατάλληλα εκπαιδευμένοι να αντιμετωπίζουν τις προσκλήσεις ασφάλειας που συνεπάγεται η κατοχή ενός λογαριασμού e-mail, LinkedIn ή MySpace σε υποδομή Cloud.

Στο εξωτερικό και συγκεκριμένα στις ΗΠΑ η τρέχουσα νομολογία τείνει στην παραδοχή ότι τα ιδιωτικά δεδομένα που είναι αποθηκευμένα στο Cloud δεν μπορούν να απολαμβάνουν το ίδιο επίπεδο προστασίας προσωπικών δεδομένων με τα δεδομένα που είναι αποθηκευμένα σε προσωπικό υπολογιστή, αλλά αντίθετα θα πρέπει εύκολα και γρήγορα να είναι προσβάσιμα από της αρχές ασφάλειας των ΗΠΑ.[50]

5.3.2 Η προστασία των προσωπικών δεδομένων ως συνταγματικό δικαίωμα

Στη διάταξη του άρθρου 9Α του Ελληνικού Συντάγματος ορίζεται ότι: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».

Με τη διάταξη αυτή, κατοχυρώνεται σε επίπεδο Συντάγματος, δηλαδή, στο ανώτατο επίπεδο της εθνικής έννομης τάξης, ένα νέο ατομικό δικαίωμα που αποσκοπεί στην προστασία του ατόμου από τις δυνατότητες της τεχνολογικής εξέλιξης στα πλαίσια μιας κοινωνίας που θεμελιώνει τις αποφάσεις της στην ελεύθερη ροή και επεξεργασία των πληροφοριών.

Η ρυθμιστική εμβέλεια του άρθρου 9Α καταλαμβάνει ιδίως την καταχώρηση και χρήση των προσωπικών δεδομένων μέσω ηλεκτρονικών υπολογιστών. Η κατά τη διάταξη αυτή «προστασία» των προσωπικών δεδομένων δεν σημαίνει, ότι απαγορεύεται γενικά η συλλογή, επεξεργασία και χρήση τους και ούτε ασφαλώς παρέχει τη δυνατότητα στον κοινό νομοθέτη να καθιερώσει τέτοια απόλυτη απαγόρευση, αφού το ενδεχόμενο αυτό θα ερχόταν σε αντίθεση προς το άρθρο 5Α του Συντάγματος (δηλαδή στο δικαίωμα πληροφόρησης). Η συνταγματική προστασία των προσωπικών δεδομένων υποχρεώνει, όμως, τον κοινό νομοθέτη να διαμορφώσει ένα περιοριστικό, λειτουργικό θεσμικό status, στα πλαίσια του οποίου και μόνο καθίσταται θεμιτή η συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων.

Το δικαίωμα πληροφοριακής αυτοδιάθεσης ή πληροφοριακού αυτοπροσδιορισμού αποτελεί πρωτίστως ένα ατομικό αμυντικό δικαίωμα,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

που θεμελιώνει πρωτίστως αξίωση αποχής από τη συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων κυρίως σε δύο διακεκριμένα επίπεδα. Σε ένα πρώτο επίπεδο στο συνδυασμό του άρθρου 9Α προς την κατά περίπτωση συναφή ειδική συνταγματική διάταξη θεμελιώνεται η απαγόρευση και απλής καταγραφής ακόμη συγκεκριμένων δεδομένων σε συγκεκριμένες περιπτώσεις, π.χ. η απαγόρευση αναγραφής του θρησκεύματος στις αστυνομικές ταυτότητες. Σε ένα δεύτερο επίπεδο ο κάθε πολίτης δικαιούται να αρνηθεί την παροχή προσωπικών πληροφοριών, εάν η νομοθετική πρόβλεψη της παροχής τους π.χ. στο πλαίσιο μιας γενικής απογραφής του πληθυσμού, δεν συνοδεύεται παράλληλα από την πρόβλεψη ενός ελάχιστου ορίου οργανωτικών και διαδικαστικών εγγυήσεων.

Εκτός, όμως, από την αμυντική του λειτουργία, με το ουσιαστικό περιεχόμενο της διάταξης αυτής προβλέπεται και το δικαίωμα του κάθε πολίτη να καθορίζει ο ίδιος, κατά τρόπο ενεργό τη ροή των πληροφοριών που τον αφορούν και να νομιμοποιεί την επεξεργασία των προσωπικών του δεδομένων. Όπως τονίζεται στην καθοριστική απόφασή του το Γερμανικό Ομοσπονδιακό Δικαστήριο, που αφορούσε στην απογραφή του πληθυσμού, ο πολίτης έχει τη δυνατότητα να αποφασίζει μόνος του για την επεξεργασία και χρήση των προσωπικών του δεδομένων.

Παράλληλα, η κατοχύρωση ενός τέτοιου δικαιώματος δεν έχει μόνον ατομική διάσταση, δηλαδή, δεν αφορά μόνον την ελεύθερη ανάπτυξη της προσωπικότητας του κάθε πολίτη αλλά αποτελεί και την απαραίτητη προϋπόθεση για τη δημοκρατική πληροφοριακή συγκρότηση μιας σύγχρονης πολιτείας.

Σε συγκεκριμένες περιπτώσεις, το δικαίωμα στην προστασία των προσωπικών δεδομένων ενδέχεται να συγκρούεται με το δικαίωμα στην πληροφόρηση, που κατοχυρώνεται και αυτό ρητά (άρθρο 5Α Συντ.).

Πρέπει, καταρχήν να αποσαφηνισθεί, ότι τόσο η προστασία των προσωπικών δεδομένων όσο και η ελευθερία της πληροφόρησης συνιστούν παραμέτρους της δημοκρατικής δομής του κράτους και της κοινωνίας. Η επεξεργασία και διάθεση των πληροφοριών θεωρούνται ως οι λειτουργικές βάσεις μιας πλουραλιστικής δημοκρατίας που βασίζεται στη σχέση μεταξύ

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μιας πληροφορημένης κοινής γνώμης και της σταθερότητας των πολιτικών συστημάτων, καθώς μόνο ο πληροφορημένος πολίτης μπορεί να είναι ενεργός πολίτης. Πρόκειται, συνεπώς για δύο δικαιώματα, τα οποία δεν είναι ex principio ανταγωνιστικά, αφού στην ουσία αποτελούν εκφάνσεις του δικαιώματος ανάπτυξης της προσωπικότητας. Η ad hoc σύγκρουσή τους δεν επιλύεται με μια in abstracto επιλογή αλλά μέσω μιας στάθμισης in concreto με γνώμονα τα εκάστοτε πραγματικά δεδομένα και με απώτερο σκοπό την πρακτική εναρμόνιση της άσκησης των συγκρουόμενων αγαθών[41].

5.3.3 Η Αρχή Προστασίας Προσωπικών Δεδομένων

Κεντρικό ρόλο στο σύστημα που εισήγαγε ο Ν. 2472/1997, για τον οποίο θα μιλήσουμε παρακάτω στο κεφάλαιο 5.5, διαδραματίζει η Αρχή Προστασίας Προσωπικών Δεδομένων που συστάθηκε ως ανεξάρτητη διοικητική αρχή, αρμόδια για την εφαρμογή του νόμου.

Ο θεσμικός ρόλος και η εν γένει λειτουργία της Αρχής για το σύστημα προστασίας των προσωπικών δεδομένων, καταδεικνύεται από το ότι η Αρχή αυτή κατοχυρώθηκε μετά την πρόσφατη συνταγματική αναθεώρηση και σε συνταγματικό επίπεδο. Συγκεκριμένα στη διάταξη του άρθρου 9Α εδάφιο β, ορίζεται ότι: «Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Παράλληλα στη διάταξη του άρθρου 101Α του Συντάγματος προβλέπεται η διαδικασία συγκρότησης των ανεξάρτητων διοικητικών αρχών. Η Αρχή Προστασίας Προσωπικών Δεδομένων αποτελεί, όπως αναφέραμε ανεξάρτητη δημόσια αρχή, η οποία δεν υπόκειται σε οιονδήποτε διοικητικό έλεγχο και εδρεύει στην Αθήνα.

Σύμφωνα δε με τη διάταξη του άρθρου 15 παρ. 1 Ν. 2742/1997 η Αρχή έχει ως αποστολή την εποπτεία της εφαρμογής του νόμου και άλλων ρυθμίσεων που αφορούν στην προστασία του πολίτη από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.

Η Αρχή δε αυτή συγκροτείται από ένα δικαστικό λειτουργό βαθμού Συμβούλου της Επικρατείας, ως Πρόεδρο και έξι μέλη. Από τα μέλη οι τρεις είναι Καθηγητές Πανεπιστημίου με γνωστικό αντικείμενο το δίκαιο και το

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αντικείμενο της πληροφορικής και τα λοιπά τρία μέλη είναι πρόσωπα με εμπειρία στον τομέα της προστασίας δεδομένων προσωπικού χαρακτήρα.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει σύμφωνα με τις κείμενες διατάξεις, ένα ευρύτατο πεδίο αρμοδιοτήτων. Πρέπει να αναφερθεί ότι στο πλέγμα των αρμοδιοτήτων περιλαμβάνεται, εκτός των άλλων:

1. η διενέργεια διοικητικών ελέγχων και αρχείων και επεξεργασιών,
2. η κατάρτιση κανονιστικών πράξεων και συστάσεων,
3. η εξέταση προσφυγών,
4. η εξέταση αιτήσεων και η χορήγηση αδειών τήρησης αρχείων ή επεξεργασιών ευαίσθητων δεδομένων,
5. η ενημέρωση και ευαισθητοποίηση του κοινού σε θέματα προστασίας προσωπικών δεδομένων,
6. η κατάρτιση υποδειγμάτων και σχετικών τεχνικών οδηγιών για την υποστήριξη των υπεύθυνων επεξεργασίας,
7. η επιβολή διοικητικών κυρώσεων.

5.3.4 Το δικαίωμα προστασίας των προσωπικών δεδομένων σε διεθνές επίπεδο

Σε ευρωπαϊκό επίπεδο η τάση για τη θέσπιση ενός κατάλληλου και ορθολογιστικού δικαιϊκού πλαισίου που θα απέβλεπε στην αποτελεσματική κατοχύρωση του δικαιώματος προστασίας των προσωπικών δεδομένων είχε αρχίσει να διαφαίνεται ήδη από το 1970 με τον πρωτοποριακό νόμο του Ομοσπονδιακού Κρατιδίου της Έσσης. Ακολούθησαν, οι εθνικές νομοθεσίες των Βορείων Χωρών, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, της Αυστρίας, της Ελβετίας και στη συνέχεια όλες οι ευρωπαϊκές χώρες.[41]

Σε επίπεδο συνταγματικής ρύθμισης πρωτοπορεί σε σχέση με τα λοιπά ευρωπαϊκά συντάγματα, το Σουηδικό Σύνταγμα του 1975/1980, το οποίο περιλαμβάνει ειδικές διατάξεις για την προστασία των προσωπικών δεδομένων. Στη συνέχεια τα περισσότερα συνταγματικά κείμενα χωρών της Ευρωπαϊκής Ένωσης προέβλεψαν την κατοχύρωση του συγκεκριμένου δικαιώματος. Ειδικότερα, τα Συντάγματα της Αυστρίας, της Ολλανδίας, της Πορτογαλίας και της Ισπανίας περιέχουν αντίστοιχες ρυθμίσεις.[41]

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Σε διεθνές επίπεδο αξίζει να αναφερθεί, ότι ήδη από το Σεπτέμβριο του 1980 ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α.) υιοθέτησε ένα κείμενο με τίτλο: «Αρχές διέπουσες την προστασία της προσωπικής σφαίρας του ανθρώπου από και τις διασυνοριακές ροές προσωπικών στοιχείων».

Σε επίπεδο νομοθεσίας της Ευρωπαϊκής Ένωσης, το Συμβούλιο της Ευρώπης με τη Σύμβαση 108/1981 «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα» κωδικοποίησε τις θεμελιώδεις αρχές που αποτελούσαν τον «σκληρό πυρήνα» της προστασίας δεδομένων προσωπικού χαρακτήρα. Η Σύμβαση αυτή αποτέλεσε το έναυσμα για αρκετές χώρες να προβούν στη ψήφιση ειδικών νόμων, ενώ άλλες να τροποποιήσουν τη νομοθεσίας τους προκειμένου να θεσπίσουν ένα άρτιο και κατάλληλο νομοθετικό πλαίσιο προστασίας του ανθρώπου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η Ελλάδα κύρωσε τη Σύμβαση 108/1981 με το ν. 2068/1992.

Ειδική μνεία πρέπει να γίνει και για τη «Σύμβαση Εφαρμογής της Συμφωνίας του Schengen», η οποία υπογράφθηκε στη πόλη Schengen του Λουξεμβούργου την 19η Ιουνίου 1990, αφού περιέχει ειδικές διατάξεις για την προστασία δεδομένων προσωπικού χαρακτήρα και ασφάλειας δεδομένων στο πλαίσιο αυτού του συστήματος πληροφοριών. Η Ελλάδα με το Ν. 2514/1997 κύρωσε τη Συμφωνία Σύμβαση Εφαρμογής καθώς και τα σχετικά πρωτόκολλα.

Το 1995 και μετά από μακροχρόνιες διαπραγματεύσεις, η Ευρωπαϊκή Ένωση υιοθετεί την Οδηγία για την «Προστασία των δεδομένων». Είναι η Οδηγία 95/46 του Ευρωπαϊκού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Η Οδηγία αυτή περιέχει τις γενικές αρχές (γνωστές και ως «Οκτώ Αρχές»), οι οποίες αποτυπώθηκαν αρχικά στις κατευθυντήριες αρχές του ΟΟΣΑ και κωδικοποιήθηκαν στη Σύμβαση του Συμβουλίου της Ευρώπης του 1981. Οι αρχές αυτές θα υπομνησθούν στη συνέχεια με αφορμή την ανάλυση του

ελληνικού νόμου 2472/1997, που αποτέλεσε το νομοθετικό πλαίσιο προσαρμογής της ως άνω Οδηγίας στα ελληνικά δεδομένα.

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

Στη συνέχεια, εκτός των άλλων, εκδίδεται η οδηγία 97/66 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997, «περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα». Η οδηγία αυτή αντικαταστάθηκε με την πρόσφατη οδηγία 58/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 «σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών»[41].

5.3.5 Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) είναι ένας νέος φορέας που λειτουργεί με βάσει το Ν. 3115/2003 με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών[42].

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

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις Συναφείς Υπηρεσίες και Εφαρμογές

Σκοπός του συγκεκριμένου Κανονισμού είναι:

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

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

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

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

5.4 Προστασία Προσωπικών Δεδομένων στο πλαίσιο του Cloud Computing

5.4.1 Επεξεργασία Προσωπικών Δεδομένων

Τα κράτη μέλη της Ε.Ε. καθορίζουν τις προϋποθέσεις υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα συμφωνεί με το νόμο. Προβλέπεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται νόμιμη και θεμιτή επεξεργασία και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Θα πρέπει εξάλλου τα δεδομένα αυτά

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

να είναι ακριβή και, αν χρειάζεται, να ενημερώνονται. Τα παραπάνω πρέπει να τα λάβει υπόψη του ο πάροχος υπηρεσιών Cloud Computing έτσι ώστε να εξασφαλίζει την νομιμότητα των ενεργειών του.

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

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

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

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

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

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια.

Τα κράτη μέλη προβλέπουν ότι κάθε πρόσωπο θα πρέπει να έχει τη δυνατότητα νομικής προσφυγής στην περίπτωση παραβίασης των δικαιωμάτων που ορίζουν οι εθνικές διατάξεις οι οποίες ισχύουν για τη σχετική επεξεργασία δεδομένων.

Επιτρέπονται οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι η εν λόγω τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Ως γνωστόν, όλα τα Κράτη-Μέλη της ΕΕ εφαρμόζουν την Κοινοτική Οδηγία 2002/58 (ενσωματωμένη στο εσωτερικό τους δίκαιο) που περιέχει αυστηρούς κανόνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Βασική αρχή της είναι ότι απαγορεύεται η εξαγωγή δεδομένων σε τρίτες (εκτός ΕΕ) χώρες, οι οποίες δεν εξασφαλίζουν αντίστοιχο (adequate) επίπεδο προστασίας. Οι χώρες εκτός ΕΕ που πράγματι έχει κριθεί κεντρικά (από την ΕΕ) ότι εξασφαλίζουν ένα τέτοιο επίπεδο είναι συγκεκριμένες και παρατίθενται σε λίστα. Προφανώς αποτελούν μειοψηφία, σε σχέση με τις χώρες όλου του κόσμου. Ειδικά και συγκεκριμένα στις ΗΠΑ μόνο υπό όρους επιτρέπεται εξαγωγή δεδομένων προσωπικού χαρακτήρα.

Παρακάτω σας παραθέτουμε την πιο πρόσφατη λίστα με τις τρίτες χώρες που διαθέτουν το κατάλληλο επίπεδο προστασίας, έτσι ώστε να επιτρέπονται οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα:

1. **Ανδόρα**
2. **Αργεντινή**
3. **Αυστραλία**
4. **Καναδάς**
5. **Ελβετία**
6. **Νησιά Φερόες**
7. **Γκέρνσεϊ**
8. **Ισραήλ**
9. **Νήσος Μάν**
10. **Τζέρσεϊ**
11. **Η.Π.Α.**

Σχετικά με την τοποθεσία του παρόχου και τις διατάξεις που εφαρμόζονται θα αναφερθούμε αναλυτικότερα παρακάτω στο κεφάλαιο 5.4.3.[51]

5.4.2 Δεδομένα Κίνησης

Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τους φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να απαλείφονται όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας. Ο φορέας παροχής υπηρεσιών πρέπει να ενημερώνει το χρήστη σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασίας αυτής, προτού ο χρήστης δώσει τη συγκατάθεση του για αυτή την επεξεργασία.

Διασφαλίζεται η προστασία της ιδιωτικής ζωής για τους χρήστες όσον αφορά τις υπηρεσίες πληροφοριών θέσης κινητών συσκευών. Η επεξεργασία των συναφών δεδομένων επιτρέπεται μόνο με τη ρητή συγκατάθεση του χρήστη, ο οποίος πρέπει να ενημερώνεται για το είδος, τους σκοπούς και τη διάρκεια της επεξεργασίας.[51]

5.4.3 Τοποθεσία Παρόχου Υπηρεσιών Cloud Computing

Στην περίπτωση του παρόχου μιας υπηρεσίας μέσω διαδικτύου, που είναι εγκατεστημένος σε ένα ή περισσότερα κράτη μέλη και παρέχει όλες τις υπηρεσίες του από τα κράτη αυτά, δεν υπάρχει αμφιβολία ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αυτόν εμπίπτει στο πεδίο εφαρμογής της οδηγίας 58/2002, για την προστασία των δεδομένων που αναφέραμε στο κεφάλαιο της διεθνής νομοθεσίας. Πρέπει να σημειωθεί ότι σ' αυτή την περίπτωση, οι κανόνες για την προστασία των δεδομένων δεν περιορίζονται στα πρόσωπα στα οποία αναφέρονται τα δεδομένα και τα οποία ευρίσκονται στο έδαφος ή έχουν την ιθαγένεια ενός από τα κράτη μέλη.

Όταν ο πάροχος είναι υπεύθυνος της επεξεργασίας και δεν είναι εγκατεστημένος στον ΕΟΧ (Ευρωπαικός Οικονομικός Χώρος), η κοινοτική νομοθεσία προστασίας των δεδομένων εξακολουθεί να εφαρμόζεται σε δύο περιπτώσεις. Πρώτον, όταν ο πάροχος έχει έδρα σε κράτος μέλος, όπως ορίζεται στο άρθρο 4 παράγραφος 1 στοιχείο α). Δεύτερον, όταν η υπηρεσία προσφεύγει σε μέσα ευρισκόμενα στο έδαφος κράτους μέλους, όπως ορίζεται στο άρθρο 4 παράγραφος 1 στοιχείο γ). Στη δεύτερη περίπτωση, η υπηρεσία,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

σύμφωνα με το άρθρο 4 παράγραφος 2, πρέπει να υποδείξει έναν αντιπρόσωπο εγκατεστημένο στο έδαφος του εν λόγω κράτους μέλους.

Για να καθοριστεί ποια εθνική νομοθεσία εφαρμόζεται σε μια συγκεκριμένη περίπτωση, απαιτείται εμπεριστατωμένη ανάλυση των πραγματικών περιστατικών. Οι πάροχοι πρέπει να συνεισφέρουν στην ανάλυση αυτή δίνοντας τις κατάλληλες διευκρινίσεις σχετικά με τον ρόλο και τις δραστηριότητές τους στον ΕΟΧ. Στην περίπτωση παρόχων υπηρεσιών πολυεθνικού χαρακτήρα:

- το κράτος μέλος στο οποίο είναι εγκατεστημένος ο πάροχος εφαρμόζει στην επεξεργασία των δεδομένων την εθνική του νομοθεσία για την προστασία των δεδομένων, σύμφωνα με το άρθρο 4 παράγραφος 1 στοιχείο α)·

- εάν ο πάροχος δεν είναι εγκατεστημένος σε κανένα κράτος μέλος, το κράτος εφαρμόζει στην επεξεργασία των δεδομένων την εθνική του νομοθεσία για την προστασία των δεδομένων, σύμφωνα με το άρθρο 4 παράγραφος 1 στοιχείο γ), εάν η εταιρεία προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, στο έδαφος του εν λόγω κράτους μέλους14, για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (παραδείγματος χάριν, στη χρήση ενός «cookie»).

Σε ορισμένες περιπτώσεις, ένας πάροχος πολυεθνικού χαρακτήρα θα πρέπει να συμμορφώνεται με πολλές νομοθεσίες για την προστασία των δεδομένων λόγω των κανόνων σχετικά με το εφαρμοστέο δίκαιο και του διακρατικού χαρακτήρα της επεξεργασίας των προσωπικών του δεδομένων:

- ένα κράτος μέλος εφαρμόζει την εθνική του νομοθεσία σε μία υπηρεσία εγκατεστημένη εκτός του ΕΟΧ εάν αυτή προσφεύγει σε μέσα ευρισκόμενα στο κράτος μέλος

- ένα κράτος μέλος δεν μπορεί να εφαρμόζει την εθνική του νομοθεσία σε υπηρεσία εγκατεστημένη στον ΕΟΧ, σε άλλο δικαιοδοτικό σύστημα, ακόμη και εάν αυτή προσφεύγει σε μέσα ευρισκόμενα στο κράτο μέλος. Σε

αυτές τις περιπτώσεις, εφαρμόζεται η εθνική νομοθεσία του κράτους μέλους στο οποίο είναι εγκατεστημένη η υπηρεσία.

5.5 Νομοθετικό Πλαίσιο στην Ελλάδα

Από όσα έχουν αναφερθεί γίνεται προφανές ότι η αναμενόμενη έκρηξη στη χρήση του Internet για την πραγματοποίηση εμπορικών συναλλαγών, που αναπόφευκτα θα συμβεί και στη χώρα μας, καθιστά το ζήτημα της ασφάλειας πολύ σημαντικό. Θα μπορούσαμε να πούμε ότι μόνο τα τελευταία χρόνια έχει αρχίσει μια προσπάθεια ενημέρωσης και ευαισθητοποίησης των πολιτών και των εταιρειών σχετικά με ζητήματα ασφάλειας. Επιπλέον, έχει γίνει μια σημαντική εκστρατεία ενημέρωσης του κοινού σχετικά με ζητήματα προστασίας προσωπικών δεδομένων [48].

Εξετάζοντας το νομοθετικό πλαίσιο που ισχύει στην Ελλάδα, εκτός από τον Ν. 2472/1997, υπάρχουν και άλλοι σημαντικοί νόμοι που ενισχύουν το νομοθετικό πλαίσιο που σχετίζεται με ζητήματα τηλεπικοινωνιακών δικτύων και της ασφάλειας που παρέχεται σε αυτά. Έχουμε λοιπόν τους εξής νόμους και προεδρικά διατάγματα:

- Ο νόμος 2867/19-12-2000, που σχετίζεται με την οργάνωση και λειτουργία των τηλεπικοινωνιακών φορέων.
- Ο νόμος 2225/20-07-1994 περί προστασίας του απορρήτου των τηλεπικοινωνιών, ο οποίος όμως καθορίζει και τις περιπτώσεις άρσης του απορρήτου αυτού.
- Ο νόμος 3979/11, σχετικά με την αναγνώριση του δικαιώματος των φυσικών προσώπων και των νομικών προσώπων ιδιωτικού δικαίου να επικοινωνούν και να συναλλάσσονται με τους φορείς του δημόσιου τομέα με χρήση τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) και τημ 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.
- Νόμος 3471/2006 [28.06.06]. Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/1997. Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002). Σκοπός των διατάξεων των άρθρων 1 έως 17 του παρόντος νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

- Το προεδρικό διάταγμα 150/2001, σχετικά με τις ηλεκτρονικές υπογραφές το οποίο προσαρμόζει την ελληνική νομοθεσία στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης στις 13/12/1999 "Σχετικά με το Κοινοτικό Πλαίσιο για τις Ηλεκτρονικές Υπογραφές". Στην οδηγία 99/93/ΕΚ διαμορφώνεται ένα ενιαίο για τον Κοινοτικό χώρο πλαίσιο αντιμετώπισης νομικών ζητημάτων, που προκύπτουν από τη χρήση της ηλεκτρονικής υπογραφής ως μεθόδου ηλεκτρονικής πιστοποίησης στοιχείων.
- Νόμος 3115/2003. Με το άρθρο 1 του συγκεκριμένου νόμου συστάθηκε, σύμφωνα με την παράγραφο 2 του άρθρου 19 του Συντάγματος, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Το γεγονός ότι οι νόμοι αυτοί ψηφίσθηκαν τα τελευταία χρόνια δείχνει πόσο ραγδαίες είναι οι εξελίξεις και η ανάγκη προσαρμογής της νομοθεσίας σε αυτές. Εκτός από την ενίσχυση του νομοθετικού πλαισίου, το γεγονός ότι στο ζήτημα της ασφάλειας των δικτύων και των προσωπικών δεδομένων έχει υπάρξει τα τελευταία χρόνια μια σημαντική πρόοδος γίνεται εμφανές και από τη δραστηριοποίηση πολλών Ελληνικών εταιριών που παρέχουν σε εταιρίες και οργανισμούς υπηρεσίες και προϊόντα για την ασφάλεια των δικτύων τους και των δικτυακών τους τόπων στο Internet. Η ανάπτυξη των εταιριών αυτών τα τελευταία χρόνια είναι ραγδαία, κάτι που δείχνει τη συνεχή αύξηση εταιριών και οργανισμών για θέματα ασφάλειας. Παρακάτω συγκεντρώσαμε τους σχετικούς νόμους και διατάξεις που

αφορούν την νομιμότητα της επεξεργασίας των δεδομένων στο Cloud Computing σε διεθνές αλλά και σε τοπικό επίπεδο.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Νομοθετικές Ρυθμίσεις στην Ελλάδα	
Νόμος 2472/1997	Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα
Νόμος 2867/19-12-2000	Οργάνωση και λειτουργία των τηλεπικοινωνιακών φορέων
Νόμος 2225/20-07-1994	Προστασία του απορρήτου των τηλεπικοινωνιών
Νόμος 3979/11	Διακίνηση εγγράφων με ηλεκτρονικά μέσα στα πλαίσια του δημοσίου τομέα
Νόμος 3471/2006	Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
Προεδρικό Διάταγμα 150/2001	Ηλεκτρονικές υπογραφές
Νόμος 3115/2003	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Νομοθετικές Ρυθμίσεις στην Ευρωπαϊκή Ένωση	
Σύμβαση 108/1981	Προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα
Σύμβαση Εφαρμογής της Συμφωνίας του Schengen	Ειδικές διατάξεις για την προστασία δεδομένων προσωπικού χαρακτήρα και ασφάλειας δεδομένων στο πλαίσιο αυτού του συστήματος πληροφοριών
Οδηγία 95/46 του Ευρωπαϊκού Κοινοβουλίου	Προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
Οδηγία 58/2002	Επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

5.6 Κατανομή Ρόλων και Ευθύνης

Στα πλαίσια εφαρμογής της τεχνολογίας Cloud Computing και στην παροχή των εν λόγω υπηρεσιών τα δεδομένα προσωπικού αλλά και επαγγελματικού χαρακτήρα, γίνονται άμεσα διαθέσιμα στον πάροχο υπηρεσιών Cloud Computing για επεξεργασία και αποθήκευση. Γίνεται λοιπόν σαφές ότι στους κόλπους του παρόχου Cloud υπηρεσιών θα πρέπει να οριστούν οι ρόλοι των εργαζομένων και οι θέσεις ευθύνης που αναλαμβάνει ο κάθε εργαζόμενος που έρχεται σε άμεση επαφή με τα δεδομένα κάποιου πελάτη Cloud Computing υπηρεσιών. Γι'αυτό τον λόγο θα πρέπει να ορίσουμε με σαφήνεια τον υπεύθυνο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα αλλά και αυτόν που εκτελεί την επεξεργασία πάνω στα δεδομένα.

5.6.1 Ορισμός Υπευθύνου και του Εκτελούντος την Επεξεργασία

Η οδηγία 95/46/ΕΚ και ο ελληνικός νόμος 2472/1997 στο άρθρο 2, αναφέρονται ρητά στην έννοια του υπευθύνου της επεξεργασίας σε αρκετές διατάξεις. Οι ορισμοί του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», οι οποίοι παρέχονται στο άρθρο 2 στοιχεία δ) και ε) της οδηγίας έχουν ως ακολούθως:

> ***«Υπεύθυνος της επεξεργασίας»,*** *το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Όταν οι στόχοι και ο τρόπος της επεξεργασίας καθορίζονται από νομοθετικές ή κανονιστικές διατάξεις, εθνικές ή κοινοτικές, ο υπεύθυνος της επεξεργασίας ή τα ειδικά κριτήρια για τον ορισμό του μπορούν να καθορίζονται από το εθνικό ή το κοινοτικό δίκαιο.*
>
> ***«Εκτελών την επεξεργασία»,*** *το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.*

Οι ορισμοί αυτοί διαμορφώθηκαν κατά τις διαπραγματεύσεις σχετικά με το σχέδιο πρότασης της οδηγίας στις αρχές της δεκαετίας του 1990, και η έννοια του «υπευθύνου της επεξεργασίας» προήλθε ουσιαστικά από τη Σύμβαση αριθ. 108 του Συμβουλίου της Ευρώπης, η οποία συνάφθηκε το 1981. Κατά τις διαπραγματεύσεις αυτές επήλθαν ορισμένες σημαντικές αλλαγές.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Καταρχάς, ο «κύριος του αρχείου» που αναφέρεται στη Σύμβαση αριθ. 108 αντικαταστάθηκε με τον «υπεύθυνο της επεξεργασίας» σε σχέση με την «επεξεργασία δεδομένων προσωπικού χαρακτήρα». Πρόκειται για μια ευρεία έννοια, η οποία ορίζεται στο άρθρο 2 στοιχείο β) της οδηγίας ως «κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η εναρμόνιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή». Έτσι, η έννοια του «υπευθύνου» δεν χρησιμοποιείται πλέον για ένα στατικό αντικείμενο (το αρχείο), αλλά συνδέεται με δραστηριότητες που αντικατοπτρίζουν τον κύκλο ζωής των πληροφοριών από τη συλλογή έως την καταστροφή τους, και πρέπει να εξετάζεται τόσο αναλυτικά όσο και στο σύνολό της («εργασία ή σειρά εργασιών»). Παρότι το αποτέλεσμα μπορεί να είναι το ίδιο σε πολλές περιπτώσεις, η έννοια απέκτησε με τον τρόπο αυτό πολύ πιο ευρεία και δυναμική σημασία και πεδίο εφαρμογής.

Άλλες αλλαγές αφορούν τη θέσπιση της δυνατότητας «πολλαπλού ελέγχου» («μόνος ή από κοινού με άλλους»), την απαίτηση ο υπεύθυνος της επεξεργασίας να «καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα», και την ιδέα ότι ο καθορισμός αυτός πρέπει να γίνει από την εθνική ή την κοινοτική νομοθεσία ή με άλλον τρόπο. Η οδηγία θέσπισε επίσης την έννοια του «εκτελούντος την επεξεργασία», η οποία δεν αναφέρεται στη Σύμβαση αριθ. 108[43].

Στο συγκεκριμένο κεφάλαιο διαχωρίσαμε τον «Υπεύθυνο της επεξεργασίας» και τον «Εκτελών την επεξεργασία» διότι στο περιβάλλον του Cloud Computing τα δεδομένα πρέπει να είναι ξεκάθαρο ποιος έχει την ευθύνη επεξεργασίας τους και ποιος τα επεξεργάζεται με στόχο την ορθή εφαρμογή του νομοθετικού πλαισίου.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κεφάλαιο 6ο - Προτάσεις/Συστάσεις

Ύστερα από την ανάλυση του Cloud Computing θεωρήσαμε αναγκαίο να παραθέσουμε κάποιες προτάσεις/συστάσεις όσον αφορά την ορθή εφαρμογή της νέα τεχνολογίας, χωρισμένες σε τρείς κατηγορίες. Συγκεκριμένα, συνοψίζοντας και αναλύοντας προτάσεις που έχουν διατυπωθεί κατά τα τελευταία χρόνια [34][35][36] προτείνουμε τα εξής:

Σχέση Παρόχου – Πελάτη

1. Η διαχείριση του κινδύνου και οι νομικές δικλείδες ασφαλείας πρέπει να αποσαφηνιστούν με σαφήνεια μεταξύ του παρόχου και του πελάτη με τρόπο διαφανή και σε σχέση με την αποθήκευση και την πρόσβαση των δεδομένων (π.χ. η φυσική θέση αποθήκευσης των δεδομένων). Με αυτό τον τρόπο μπορούν να αναπτυχθούν σχέσεις εμπιστοσύνης μεταξύ των δύο πλευρών.
2. Η επικοινωνία μεταξύ του πελάτη και του παρόχου πρέπει να προστατεύεται κατάλληλα και να διασφαλίζει την εμπιστοσύνη, την ακεραιότητα, τον πιστοποιημένο έλεγχο καθώς και να ελαχιστοποιεί το ρίσκο επιθέσεων denial-of-service. Ένας σαφής προσδιορισμός των μέτρων που πρέπει να ληφθούν για την ασφάλεια της επικοινωνίας είναι απαραίτητο να υιοθετείται από τον πάροχο και να βασίζεται σε ανοιχτά και διαφανή πρότυπα (standards) και τεχνολογίες. (Το παρόν εντάσσεται και στην Τρίτη κατηγορία – Υποχρεώσεις Ασφάλειας)
3. Η υποχρεωτική διαγραφή των δεδομένων πρέπει να συμπεριληφθεί στην επικείμενη νομοθετική ρύθμιση σχετικά με τις υπηρεσίες Cloud Computing αλλά δεν πρέπει να βασιζόμαστε σ' αυτήν σε μεγάλο βαθμό, κάτι που σημαίνει ότι και ο πελάτης θα πρέπει να παρέχει στον εαυτό του προστασία όσον αφορά τα προσωπικά του δεδομένα και να μην στηρίζεται εξ' ολοκλήρου στον πάροχο Cloud Computing υπηρεσιών. Δεν υπάρχει κάποια εγγυημένη διαγραφή δεδομένων και αυτό πρέπει να ληφθεί σοβαρά υπόψη στην περίπτωση που τα δεδομένα συλλέγονται και αποθηκεύονται.
4. Πρέπει να παρέχεται κατάλληλη καταγραφή και έλεγχος πρόσβασης των δεδομένων. Ένας εξωτερικός έλεγχος μπορεί να είναι ευεργετικός για την

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

φήμη των παρόχων Cloud Computing όπως επίσης και για την ενδυνάμωση της εμπιστοσύνης με τον πελάτη.

Υποχρεώσεις Παρόχου για την Τήρηση της Νομοθεσίας

1. Η παρεχόμενη υπηρεσία πρέπει να είναι συμβατή με το κανονιστικό πλαίσιο, ενώ επίσης ο πελάτης και ο πάροχος πρέπει να έχουν την δυνατότητα να συμμορφώνονται με αυτήν.
2. Οι πάροχοι θα πρέπει να είναι υποχρεωμένοι να διασφαλίζουν την εμπιστευτικότητα των δεδομένων με συμβάσεις οι οποίες θα προβλέπουν ποινικές ρήτρες και κυρώσεις σε περίπτωση παραβίασης τους.
3. Με τη λογική ότι στο μέλλον θα χρειαστεί κάποιος κανονισμός σε οικονομικό αλλά και νομικό επίπεδο (π.χ. η εξισορρόπηση της δύναμης μεταξύ πελατών και παρόχων υπηρεσιών Cloud Computing) θα ήταν συνετό να αναλογιστούμε τις αδυναμίες και τα θέματα πριν το Cloud Computing γίνει μια κρίσιμη υπηρεσία ή υποδομή. Χρειάζεται να εξεταστεί ποιές από τις διαστάσεις των συγκρούσεων και των ρυθμιστικών προοπτικών είναι σχετικές (για παράδειγμα η εγγύηση και η αξιοπιστία σε συνδυασμό με την εμπιστευτικότητα και την ακεραιότητα των δεδομένων). Πιο συγκεκριμένα όταν ο πάροχος υπηρεσιών Cloud Computing αποτελεί τμήμα μιας σημαντικής υποδομής πληροφοριών κρίνονται απαραίτητοι μερικοί κανονισμοί ή περιορισμοί σχετικά με την πιθανή εξαγορά του από κάποιον τρίτο ή ανταγωνιστή.

Υποχρεώσεις Ασφάλειας

1. Τα προβλήματα και οι κίνδυνοι που επηρεάζουν την προστασία και την ασφάλεια των δεδομένων στην Ευρώπη θα πρέπει να λαμβάνονται υπόψην κατάλληλα όταν ο πάροχος των υπηρεσιών Cloud Computing βρίσκεται εκτός Ευρώπης.
2. Πρέπει να ενθαρρυνθεί η ανάπτυξη και η καλύτερη προώθηση του λογισμικού που επιτρέπει την τοπική μεταφορά δεδομένων μεταξύ συσκευών. Με αποτέλεσμα η μεταφορά να είναι ασφαλέστερη και εγγυρότερη όσον αφορά την ταχύτητα αλλά και την πληρότητα των δεδομένων.
3. Το τηλεπικοινωνιακό δίκτυο το οποίο υποστηρίζει τις υπηρεσίες Cloud Computing πρέπει να προστατεύεται ενάντια σε ιούς και σε επιθέσεις DoS (Denial-of-Service).
4. Οι απλοί χρήστες πρέπει να εκπαιδεύονται με βάση τις εξελίξεις της τεχνολογίας και τα νέα μοντέλα που προκύπτουν. Η εκπαίδευση πρέπει να τους προετοιμάζει να παίρνουν πιο υπεύθυνες αποφάσεις ως προς τον τρόπο που χρησιμοποιούν τις υπηρεσίες Cloud Computing καθώς και ως προς τον τρόπο που μεταφέρονται οι πληροφορίες στις υποδομές του Cloud.
5. Οι επαγγελματίες πρέπει να αναπτύσσουν τις δεξιότητες τους στη διαχείριση νέων ειδών κινδύνων. Όπως και με την αρχική εφαρμογή του διαδικτύου έτσι και τώρα η εφαρμογή της νέας τεχνολογίας Cloud Computing γεννά νέους κινδύνους και νέες τεχνικές κακόβουλης επίθεσης στα πληροφοριακά συστήματα των Cloud υπηρεσιών. Γι' αυτό τον λόγο οι επαγγελματίες θα πρέπει να είναι ενημερωμένοι και πολύ καλά εκπαιδευμένοι στην αντιμετώπιση οποιουδήποτε κινδύνου.
6. Αντίγραφα Ασφαλείας και Ανάκτηση τους. Η επιχείρηση πρέπει να εξετάσει τις δυνατότητες του παρόχου για δημιουργία αντιγράφων ασφαλείας (backup) των δεδομένων της καθώς και τον τρόπο με τον οποίο αυτά δημιουργούνται. Ο προμηθευτής θα πρέπει να διαθέτει όσο το δυνατόν πιο σύγχρονα και αποτελεσματικά εργαλεία, τόσο υλικό (hardware) όσο και λογισμικό (software), που θα επιτρέπουν τη δημιουργία των αντιγράφων ασφαλείας και την ανάκτησή τους εύκολα, γρήγορα και αξιόπιστα. Το σύστημα δημιουργίας αντιγράφων ασφαλείας θα πρέπει να

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

είναι συμβατό με όλες τις εφαρμογές από τις οποίες σας ενδιαφέρει να διατηρείτε backup (π.χ. SQL server, Exchange server etc). Ακόμη είναι σημαντικό να καταγράφει λεπτομερώς όλες τις ενέργειες που συμβαίνουν κατά τη διαδικασία του backup και της ανάκτησης σε σχετικά αρχεία (logs) έτσι ώστε να είναι δυνατός ο έλεγχος για πιθανά σφάλματα και απώλειες δεδομένων κατά τη διάρκεια της διαδικασίας. Τα εφεδρικά αρχεία είναι προτιμότερο να αποθηκεύονται σε σκληρούς δίσκους και όχι σε κασέτες αποθηκευτικού χώρου, έτσι ώστε να είναι δυνατή η γρήγορη ανάκτησή τους. Ιδιαίτερη αξία έχει και η δυνατότητα για incremental backup, δηλαδή για ενημέρωση των ήδη υπαρχόντων αντιγράφων ασφαλείας με τις νέες αλλαγές, χωρίς να χρειάζεται να δημιουργηθούν τα αντίγραφα ασφαλείας ξανά από την αρχή. Με αυτό τον τρόπο δεν απαιτείται να τεθεί το σύστημα εκτός λειτουργίας για να δημιουργηθούν τα αντίγραφα ασφαλείας και έτσι αυτό είναι διαθέσιμο 24 ώρες το 24ωρο. Τέλος, επιθυμητή είναι η μεγάλη συμπίεση και μείωση του μεγέθους των εφεδρικών αρχείων, έτσι ώστε αυτά να καταλαμβάνουν μικρότερο αποθηκευτικό χώρο και να μπορούν να ανακτηθούν πολύ πιο γρήγορα[26].

7. Πιστοποίηση με Διεθνώς Αναγνωρισμένα Πρότυπα ασφαλείας. Τα data centers του προμηθευτή είναι σημαντικό να βρίσκονται σε μία συνεχή διαδικασία ελέγχου και αξιολόγησης, που επαναλαμβάνεται σε τακτά χρονικά διαστήματα (π.χ. κάθε χρόνο), από κάποιους διεθνείς οργανισμούς πιστοποίησης σχετικά με τη συμμόρφωσή τους σε διεθνή πρότυπα και τυποποιήσεις ασφαλείας. Μερικά από τα πιο γνωστά και ευρείας αποδοχής πρότυπα είναι τα ISO/IEC 27000 και SAS 70 Type I & II[26].
8. Η έρευνα σε βασικές αρχές στην Πληροφορική, στην ασφάλεια, στην ιδιωτικότητα και στις συνέπειες σχετικά με το Cloud Computing πρέπει να ενθαρρύνεται. Επίσης ζητήματα σχετικά με το πιθανό αποτέλεσμα των υπηρεσιών Cloud Computing στην επαλήθευση των πιστοποιητικών των εφαρμογών καθώς και την καταλληλότητα τους πρέπει να διευρηθούν περαιτέρω.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Επίλογος

Το Cloud Computing αποτελεί μια καινούρια, καινοτομική και πρωτοποριακή τεχνολογία που τα τελευταία χρόνια έχει κάνει την εμφάνιση της και στην χώρα μας. Είναι μια τεχνολογία πολλά υποσχόμενη η οποία με το πέρασμα του χρόνου θα γίνει δέκτης της προτίμησης του ευρύτερου κοινού και θα αποκαταστήσει τις καθιερωμένες in house υποδομές. Προφανώς, εξαιτίας της δομής και του τρόπου λειτουργίας της εν λόγω τεχνολογίας πολλοί είναι οι κίνδυνοι που ελλοχεύουν, γι' αυτό και είναι απαραίτητη η θέσπιση νόμων για την κατάλληλη προστασία απέναντι σε φαινόμενα παραβίασης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των υπηρεσιών.

Θέλουμε να πιστεύουμε ότι η διστακτικότητα που υπάρχει ακόμα απέναντι στην τεχνολογία του Cloud Computing θα μειωθεί με το πέρασμα του χρόνου και αυτή η νέα και πρωτοποριακή τεχνολογία θα εδραιωθεί στον τομέα των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Εικόνες	
Εικόνα 1	Software as a service diagram http://mikelloydtech.wordpress.com/2011/02/23/cloud-watching-1-cloud-101/
Εικόνα 2	Infrastructure as a service diagram http://mikelloydtech.wordpress.com/2011/02/23/cloud-watching-1-cloud-101/
Εικόνα 3	Platform as a service diagram http://mikelloydtech.wordpress.com/2011/02/23/cloud-watching-1-cloud-101/
Εικόνα 4	Private – Community – Public Cloud Computing http://howcrmworks.com/tag/cloud/
Εικόνα 5	Hybrid Cloud Computing http://howcrmworks.com/tag/cloud/

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Εικόνα 6	Τεχνικά χαρακτηριστικά Βασικών υλοποιήσεων Cloud Computing [47]
Εικόνα 7	Ο κύκλος ζωής των δεδομένων
Εικόνα 8	Έκταση του ελέγχου και της προστασίας σε κάθε υπηρεσία.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Βιβλιογραφία

1. Assuncao, M.D.d., A.d. Costanzo, and R. Buyya, Evaluating the cost-benefit of using cloud computing to extend the capacity of clusters, in Proceedings of the 18th ACM international symposium on High performance distributed computing2009, ACM: Garching, Germany. p. 141-150.
2. Chowdhury, N.M.M.K. and R. Boutaba, A survey of network virtualization. Computer Networks, 2010. 54(5): p. 862-876.
3. Buyya, R., S. Pandey, and C. Vecchiola, Cloudbus Toolkit for Market-Oriented Cloud Computing, in Cloud Computing, M. Jaatun, G. Zhao, and C. Rong, Editors. 2009, Springer Berlin / Heidelberg. p. 24-44.
4. Weiss, A., Computing in the clouds. netWorker, 2007. 11(4): p. 16-25.
5. Nurmi, D., et al. The Eucalyptus Open-Source Cloud-Computing System. in 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09). 2009. Washington: IEEE Computer Society.
6. Buyya, R., Y. Chee Shin, and S. Venugopal. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. in High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on. 2008.
7. Velte, A.T., T.J. Velte, and R. Elsenpeter, Cloud Computing Practical Approach2010, USA: The McGraw-Hill Companies.
8. Hintzbergen, K., et al., Foundations of Information Security Based on Iso27001 and Iso270022010: Van Heren Publishing, Zaltbommel, www.vanharen.net.
9. Πλεονεκτήματα και μειονεκτήματα του Cloud Computing. Από Beth Schultz - freelance IT writer in Chicago http://www.itworld.com/saas/68088/cloud-computing-pros-and-cons
10. Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. http://aws.amazon.com/ec2/
11. Google App Engine enables you to build and host web apps on the same systems that power Google applications http://code.google.com/intl/el-GR/appengine/

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

12. Windows Azure and SQL Azure enable you to build, host and scale applications in Microsoft datacenters http://www.microsoft.com/windowsazure/
13. McGraw Hill.-.Cloud Computing A Practical Approach, p. 34-35
14. Wiley.-.Cloud Computing Principles and Paradigms, p. 45-47
15. Wikipedia. Cloud Computing, Wikipedia – the free encyclopedia http://en.wikipedia.org/wiki/Cloud_Computing
16. University of Cambridge Computer Laboratory. Xen User's Manual http://www.cl.cam.ac.uk/research/srg/netos/xen/readmes/user/user.html
17. Armbrust, Michael,et al. Above the Clouds: A Berkeley View of Cloud Computing. UC Berkeley RAD Systems Laboratory, Technical Report No. UCB/EECS---2009---28, February 10, 2009.
18. Wikimedia. Azure Services Platform. Wikipedia. http://en.wikipedia.org/wiki/Azure_Services_Platform.
19. Cloud Computing Strategist. Demystifying the cloud, an introduction to Cloud Computing, Version 1.1 – August 2010 p. 16-18 www.janakiramm.net
20. National Institute of Standards and Technology Draft-SP-800-145_cloud-definition www.nist.gov
21. Mateen Greenway, chief Technologist της Hewllett Packard EMEA. στον τομέα Enterprise Services. Publication of his interview – Benefits of the new technology www.tovima.gr
22. AMD's global research highlights the growing acceptance of cloud computing. The hole research can be found at http://www.slideshare.net/AMDUnprocessed/amd-cloud-adoption-approaches-and-attitudes-research-report
23. Ελληνική Δημοκρατία Υπουργείο Παιδείας Δια Βιου Μαθησης και Θρησκευμάτων. Παρουσίαση – Συνέντευξη Τύπου για την υιοθέτηση νέας τεχνολογίας (Cloud Computing), 20/09/2010 www.minedu.gov.gr
24. Hellenic Internet Defence Force. Άρθρο για τα οφέλη του Cloud Computing στην προσπάθεια της Ελλάδος για έξοδο από την κρίση. http://internet-defence.blogspot.com/2011/02/cloud-computing.html
25. Publication by Δημήτρης Γαγανέλης - Η αξία του cloud για τη σύγχρονη επιχείρηση. July 12, 2011. http://blog.softone.gr/archives/category/cloud-services/

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

26. Publication by Κωνσταντίνος Πιστόλας – Η ασφάλεια μέσα στο σύννεφο. June 20, 2011. http://blog.softone.gr/archives/category/cloud-services/
27. Publication by Gartner – Seven cloud computing security risks. July 2, 2008 http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
28. Publication by Peter Laudenslager – Six Cloud Computing Benefits For Small and Midsize businesses. June 02, 2010. http://www.informationweek.com/news/225200751
29. J.Staten, S.Y., F.Gillett, W.Saleh, R. A. Dines, Is Cloud Computing Ready For The Enterprise?, Forrester, Editor 2008.
30. Buyya, R., et al., Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 2009. 25(6): p. 599-616.
31. Mathon, V. and H. Laurent, Life cycle of Sahelian mesoscale convective cloud systems. Quarterly Journal of the Royal Meteorological Society, 2001. 127(572): p. 377-406.
32. Publications by PUNKT – Cloud Computing Pay as you go (υπηρεσίες). http://www.punkt.gr/cms/gr/content/Pay_as_you_go_Services.aspx
33. CEPIS Statement, Social Networks – Problems of Security and Data Privacy, 2008, www.cepis.org/index.jsp?p=942&n=963#Social%20Networks
34. J. Brodkin, Gartner: Seven cloud-computing security risks, available at: www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.
35. Cloud Computing: Benefits, Risks and Recommendations for Information Security, ENISA Report, 2009, available at: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
36. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance (CSA) Report, 2009, available at: www.cloudsecurityalliance.org/csaguide.pdf.
37. Vic (J.R.) Winkle, ”Securing the Cloud”.
38. Φραγκάκης. Ν, 2008 Τα όρια μεταξύ ελευθερίας και ασφάλειας, δημόσιου και ιδιωτικού, Διαθέσιμο στην ιστοσελίδα της εφημερίδας «ΤΟ ΒΗΜΑ»:

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

http://www.vimaideon.gr//Article.aspx?d=20080201&nid=7342365&sn=%CA%D5% D1%C9%CF%20%D4%C5%D5%D7°/oCF°/oD3&spid= 1478&cs=1

39. Information Privacy Διαθέσιμο στον δικτυακό τόπο: http://en.wikipedia.org/wiki/Information_privacy
40. Υπόθεση παραβίασης της ιδιωτικής ζωής στη Γερμανία (07/07/2010) από γνωστή ιστιοσελίδα κοινωνικής δικτύωσης. Διαθέσιμη στην ιστοσελίδα της εφημερίδας «ΤΟ ΒΗΜΑ»: http://www.tovima.gr/relatedarticles/article/?aid=341985
41. Το δικαίωμα προστασίας των προσωπικών δεδομένων στην ελληνική έννομη τάξη. Διονύσιος Φιλίππου - Επίκουρος καθηγητής Νομικής Σχολής. http://www.infolaw.gr/articles.asp?ArticleID=578
42. Άρθρο 6 – Αρμοδιότητες της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών. http://www.drindrin.gr/index.php/home/145
43. Ομάδα εργασίας του άρθρου 29 για την προστασία δεδομένων. Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία» της 16ης Φεβρουαρίου 2010. Ο πρόεδρος Jacob KOHNSTAMM. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_el.pdf
44. Έρευνα της CSA και της HP για τις απειλές που προκύπτουν στο Cloud Computing. Η πλήρης αναφορά είναι διαθέσιμη στην ιστοσελίδα της CSA, στη διεύθυνση : http://cloudsecurityalliance.org/pr20100301a.html
45. Για τις θεωρίες περί ιδιωτικότητας και την εξέλιξη της έννοιας από το right to be left alone στο δικαίωμα άσκησης ελέγχου επί των πληροφοριών. Βλ. Κ. Μαυριά, Το δικαίωμα του ιδιωτικού βίου, Αθήνα-Κομοτήνη 1980, σελ. 59 επ., Β. Βουτσάκη, Το δικαίωμα στην ιδιωτική ζωή: υποκειμενικές και αντικειμενικές πτυχές, σε Γ. Παπαδημητρίου (επιμ.), Νέες τεχνολογίες και συνταγματικά δικαιώματα, Αθήνα-Θεσσαλονίκη 2004, σελ. 87 επ.. Αναλυτικότερα D. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154 (2006), No 3, σελ. 479-564.
46. Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνιες - Η νομική διάσταση. Επίκουρη Καθηγήτρια Λίλιαν Μήτρου - Τμήμα Μηχανικών & Πληροφοριακών Συστημάτων - Πανεπιστήμιο Αιγαίου.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

47. Above the Clouds: A Berkeley View of Cloud Computing Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia (Comments should be addressed to abovetheclouds@cs.berkeley.edu) UC Berkeley Reliable Adaptive Distributed Systems Laboratory http://radlab.cs.berkeley.edu/ February 10, 2009.
48. Κ. Μουλινός, Κ. Καμπουράκη, "Ε¬Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή", Αρχή Δεδομένων Προσωπικού Χαρακτήρα www.dpa.gr/Documents/Gre/Com/article.doc
49. Terasvirta, T. and H.M. Anderson, Characterizing nonlinearities in business cycles using smooth transition autoregressive models. Journal of Applied Econometrics, 1992. 7(S1): p. S119-S136.
50. Cloud Computing: A Primer on Legal Issues, Including Privacy and Data Security Concerns. Privacy and Information Management Practice / Washington, DC. http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/docs/CloudPrimer.pdf
51. Data Protection in Cloud Computing – Κωνσταντίνου Ευάγγελος. Μεταπτυχιακή Εργασία - Πανεπιστήμιο Αιγαίου Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων σελ. 18 Βασικές Αρχές Επεξεργασίας Δεδομένων.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ