ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΠΣ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΜΕΘΟΔΩΝ ΚΑΙ ΤΕΧΝΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ ΥΠΗΡΕΣΙΕΣ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Σαμουέλ Νιγκάτου

Μεσολόγγι 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΠΣ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΜΕΘΟΔΩΝ ΚΑΙ ΤΕΧΝΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ ΥΠΗΡΕΣΙΕΣ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Σαμουέλ Νιγκάτου

Επιβλέπων καθηγητής

Βασίλης Βασιλειάδης

Μεσολόγγι 2020

UNIVERSITY OF PATRAS

SCHOOL OF ECONOMICS & BUSINESS

DEPARTMENT OF MANAGEMENT SCIENCE AND TECHNOLOGY

FORMER DEPARTMENT OF BUSINESS ADMINISTRATION AT MESSOLONGHI

THESIS

CLOUD COMPUTING SERVICES' METHODS' STUDIES AND SECURITY TECHNIQUES

Samuel Nigatu

Messolonghi 2020

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Πανεπιστημίου Πατρών δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Η αλήθεια μπορεί να είναι ότι ο όρος «cloud computing» είναι άγνωστος, αλλά τα διαγράμματα και οι γραφικές παραστάσεις υπολογιστών χρησιμοποιούν γραφικά, ιδίως τα διαγράμματα νέφους, για να αναφέρονται σε δίκτυα. σύστημα επικοινωνίας.

Στον κόσμο του διαδικτύου, ο όρος «cloud» χρησιμοποιήθηκε αρχικά μεταφορικά για να περιγράψει γραφικά ένα τηλεφωνικό δίκτυο. Στη συνέχεια χρησιμοποίησε την υποδομή για να αναπαραστήσει το Διαδίκτυο ως αφηρημένη έννοια σε διαγράμματα δικτύων υπολογιστών. Το πείραμα αυτό ανακαλύφθηκε γύρω στο 1994..

Για παράδειγμα, στη δεκαετία του 1990, οι εταιρείες τηλεπικοινωνιών που είχαν προηγουμένως ειδικευτεί σε κυκλώματα δεδομένων από σημείο σε σημείο άρχισαν να παρέχουν υψηλής ποιότητας αλλά σε λογικές τιμές υπηρεσίες εικονικών ιδιωτικών δικτύων (VPN). Το έμβλημα του σύννεφου χρησιμοποιήθηκε για να σηματοδοτήσει το όριο μεταξύ των δυνατοτήτων του παρόχου και των δυνατοτήτων των χρηστών.

Η έννοια του νέφους χρονολογείται από τη δεκαετία του 1950. Τότε ήταν που τα κεντρικά κομπιούτερ ξεκινήσανε να είναι διαθέσιμα σε εκπαιδευτικά ιδρύματα και επιχειρήσεις και η πρόσβαση σε αυτούς γινόταν μέσω μεμονωμένων τερματικών. Εκείνη την εποχή, η αγορά ενός κεντρικού υπολογιστή ήταν αρκετά ακριβή, οπότε έπρεπε να βρεθεί τρόπος να μεγιστοποιήσει την απόδοση της επένδυσης αγοράς ενός υπολογιστή. Ως εκ τούτου, ήρθε το γεγονός ότι πολλοί χρήστες μοιράζονταν ταυτόχρονα τη παρουσία στον κεντρικό υπολογιστή από πολλά τερματικά, καθώς και την κατανομή του χρόνου του επεξεργαστή, εξαλείφοντας τον χρόνο διακοπής λειτουργίας, κάτι που στη βιομηχανία δικτύων έγινε γνωστό ως κατανομή χρόνου (timesharing).

Με την εξάπλωση των υπολογιστών, οι επιστήμονες και οι μηχανικοί άρχισαν να αναζητούν τρόπους να μοιράζονται την υπολογιστική ισχύ σε μεγάλη κλίμακα. Τα περισσότερα από τα τελευταία γνωρίσματα του υπολογιστικού νέφους (ελαστική τακτοποίηση, άμεση σύνδεση, αυταπάτη του άπειρου χώρου) ανακαλύφθηκαν από τον Douglas Parkhill το 1966, σε σύγκριση με τη χρήση δημόσιων υπηρεσιών στη βιομηχανία ηλεκτρικής ενέργειας και την κοινότητα. Computer Utility Challenge.

Για άλλους ερευνητές, οι βάσεις του Υπολογιστικού Νέφους πάνε πιο πίσω, στη δεκαετία του 1950. Στη συνέχεια, ο Herb Grosh (γνωστός και ως Grosh Law) υποστήριξε ότι ολόκληρος ο κόσμος θα μπορούσε να λειτουργεί με διακομιστές με τη χρήση 15 μεγάλων κέντρων δεδομένων. Εξαιτίας των δυνατοτήτων αυτών των υπολογιστικών μονάδων, πολλές επιχειρήσεις και οργανισμοί θα μπορούσαν να επωφεληθούν από αυτούς τους υπολογιστές διαθέτοντας χρόνο, ανάλογα με τις ανάγκες τους.

Στη δεκαετία του 1970, η διαθεσιμότητα δικτύων υψηλής χωρητικότητας, υπολογιστών και συσκευών αποθήκευσης χαμηλού κόστους και η ευρεία υιοθέτηση δομών προσανατολισμένων στις υπηρεσίες οδήγησαν στη μεγάλη ανάγκη για την ανάπτυξη του υπολογιστικού νέφους.

Αυτή που έπαιξε σημαντικό ρόλο στην ανάπτυξη και εδραίωση του Υπολογιστικού Νέφους ήταν η Amazon, η οποία εκσυγχρόνισε τα κέντρα δεδομένων της. Μέχρι τότε χρησιμοποιούνταν μόλις το 10% της χωρητικότητάς τους για να υπάρχει χώρος για περιστασιακές αιχμές χρήσης του δικτύου. Η εν λόγω εταιρεία διαπίστωσε ότι η νέα αρχιτεκτονική τύπου cloud βελτιώνει σημαντικά την εσωτερική αποτελεσματικότητά της, με την προσθήκη συγκεκριμένων εσωτερικών διαδικασιών. Έτσι άρχισαν να παρουσιάζουν ένα νέο προϊόν στους πελάτες της εταιρείας: «Cloud Computing». Από το 2006, αυτή η προσπάθεια οδήγησε στην Amazon Web Services (AWS) με τη βοήθεια της πληροφορικής.(Μπαμπάνη Ε., 2018).

Δύο χρόνια αργότερα, το 2008, η Eucalyptus εγκαινίασε την πρώτη συμβατή με το AWS πλατφόρμα ανοιχτού κώδικα για ιδιωτικές εφαρμογές cloud. Στις αρχές του 2008, η Fog άνοιξε εκ νέου με την υποστήριξη της Ευρωπαϊκής Ένωσης. (Kumar R. et.al., 2014). Πρόκειται για το πρώτο λογισμικό ανάπτυξης cloud ανοικτού κώδικα. Την ίδια χρονιά, επικεντρωθήκαμε στην παροχή υπηρεσιών υψηλής ποιότητας στην υποδομή μας που βασίζεται στο cloud. Το έργο αυτό στηρίζεται οικονομικά από την Ευρωπαϊκή Επιτροπή με την ονομασία «Ermos». (Cucinotta et al., 2011). Είχε σαν αποτέλεσμα τη δημιουργία ενός περιβάλλοντος cloud σε πραγματικό χρόνο (Hoff C et. al., 2011). Το 2008, η Gartner χώρισε πολύ γρήγορα τους καταναλωτές υπηρεσιών πληροφορικής σε χρήστες και παρόχους, που χρησιμοποιούσαν το cloud computing.

Την 01/03/2011, η IBM ανήγγειλε τη χρήση του πλαισίου Smarter Computing για την υποστήριξη εξυπνότερων σχεδίων. Λίγο αργότερα, το 2012, οι Dr. John Bijou και Dr. Sohail Khaddaj περιέγραψαν το νέφος ως μια υποθετική παροχή σημασιολογικών πληροφοριών: "Το

υπολογιστικό νέφος είναι μια παγκόσμια σειρά πληροφοριών σε όλο το Διαδίκτυο, στη δομή των περιουσιακών στοιχείων (όπως εξοπλισμός δεδομένων, μοναδικές πλατφόρμες, υπηρεσίες κ.λπ.). Διαμορφώνουν μια αμερόληπτη μονάδα σε ένα εικονικό περιβάλλον"

Το cloud computing βασίζεται στην ιδέα του McCarthy για το utility computing. Το "νέφος" περιγράφεται ως ένα σύνολο απομακρυσμένων υπηρεσιών που χρησιμοποιεί ένας οργανισμός χωρίς να παρεμβαίνει στις εσωτερικές του υποθέσεις, όπως προαναφέρθηκε. Αυτή η ιδέα του "αυτόνομου υπολογιστή" είναι που θέτει τις βάσεις για την εξάπλωση των ανωτέρω τεχνολογιών. Η "ανεξάρτητη πληροφορική" αναφέρεται στην αυτοδιαχείριση των ιδιοτήτων των διανεμόμενων πηγών πληροφορικής μέσω της προσαρμογής σε ξαφνικές αλλαγές, με στόχο την συγκάλυψη της πολυπλοκότητας των διαδικασιών για τους χειριστές και τους πελάτες.

Η IBM, που ιδρύθηκε το 2001, διαθέτει συστήματα αυτοεξυπηρετούμενων υπολογιστών που αναπτύχθηκαν για να αντιμετωπίσουν την πολυπλοκότητα και άλλα εμπόδια ανάπτυξης των συστημάτων διαχείρισης ΤΠ. Τα αυτόνομα συστήματα μπορούν να προσαρμόζονται αυτόματα στις μεταβαλλόμενες συνθήκες, παρακολουθώντας και βελτιώνοντας συνεχώς την κατάστασή τους και λαμβάνοντας αποφάσεις με βάση καθοδήγηση υψηλού επιπέδου. «Αυτόνομα προσανατολισμένος υπολογισμός», είναι το μοντέλο που προτάθηκε από τον Jimming Liu το 2001. «Τα δίκτυα υπολογιστών» δημιουργήθηκαν για την ανάπτυξη τεχνολογιών που βασίζονται σε «αυτόματους υπολογισμούς». Ο όρος ημερομηνία αποθηκεύτηκε στις αρχές της δεκαετίας του 1990 και χρησιμοποιείται ως μεταφορά για την εύκολη πρόσβαση στο δίκτυο και την παραγωγή υπολογιστικής ισχύος. Η μεταφορά αυτή χρησιμοποιήθηκε από τους Ian Foster και Karl Kesselmann όταν δημοσίευσαν το άρθρο τους. "The Grid: (2004) (Foster I. Kesselman C., 2003). Στο "grid computing", υπολογιστές από τομείς που δεν είναι όμοιοι, χρησιμοποιούνται από κοινού για την επίτευξη ενός κοινού στόχου. Για παράδειγμα, μπορείτε να επιλύσετε ένα συνεχές έργο. Ταυτόχρονα, οι υπολογιστές μπορούν να διατεθούν πολύ γρήγορα στην αγορά.

Μια από τις βασικές στρατηγικές στη δικτύωση υπολογιστών είναι η κοινή χρήση και η διανομή τμημάτων ενός προγράμματος μεταξύ διαφορετικών υπολογιστών. Το μεγαλύτερο προσόν του μοιρασμένου υπολογισμού είναι ότι κάθε κόμβος μπορεί να αγοραστεί ως ένα ενιαίο κομμάτι υλικού. Έτσι, στο σύνολό τους, οι υπολογιστικές συσκευές μπορούν να παραχθούν με χαμηλότερο κόστος από τους super computers.

Το 2007, εισήχθη ο όρος «Ωφέλιμος Υπολογιστής» (Utility computing). Ο όρος αυτός αναφέρεται στη διαδικασία δημιουργίας υποδομών υπολογιστών, όπως η απογραφή, η αποθήκευση και η εξυπηρέτηση. Τα μοντέλα αυτά έχουν το πλεονέκτημα του χαμηλού κόστους ή της έλλειψης αρχικών πόρων για την αγορά.

Η International Business Machines (IBM), η Hewlett Packard (HP) και η Microsoft ήταν οι πρώτες μεγάλες εταιρείες που ασχολήθηκαν με το νέο αυτό τομέα της πληροφορικής. Η Google, η Amazon αναλαμβάνουν τα ηνία το 2008, ενώ ιδρύουν τις δικές τους υπηρεσίες για την φύλαξη και για τα λογισμικά.

1 Βασικές έννοιες Υπολογιστικού Νέφους

1.1 Ορισμός του Υπολογιστικού Νέφους

Το υπολογιστικό νέφος είναι ένας νέος όρος στον κόσμο των υπολογιστών (Buyya R. et. al., 2009; Vaquero L et.al., 2009) και σηματοδοτεί την εμφάνιση ενός νέου υπολογιστικού προτύπου (Vaquero L et.al., 2009). Αυτό το νέο πρότυπο αναπτύσσεται γρήγορα και προσελκύει τόσο τους πελάτες όσο και τους προμηθευτές. Η γρήγορη ανάπτυξη του υπολογιστικού νέφους τροφοδοτείται από τις αναδυόμενες τεχνολογίες πληροφορικής που επιτρέπουν τη χρήση υπολογιστικών υποδομών σε λογικές τιμές και δυνατότητες μαζικής αποθήκευσης δεδομένων. Αίρει επίσης την ανάγκη για μεγάλες προκαταβολικές επενδύσεις σε υποδομές πληροφορικής (IT). Το υπολογιστικό νέφος είναι ένα υπολογιστικό πρότυπο που περιλαμβάνει την εξωτερική ανάθεση υπολογιστικών πόρων-παροχών με δυνατότητες επεκτασιμότητας, κατ' απαίτηση παροχή (με ελάχιστο ή καθόλου κόστος) επένδυσης σε υποδομές πληροφορικής ((Chow R. et. al., 2009; GNI, 2009). Το υπολογιστικό νέφος προσφέρει τα οφέλη του μέσω τριών τύπων μοντέλων υπηρεσιών ή παράδοσης, δηλαδή υποδομής ως υπηρεσίας (IaaS), πλατφόρμας ως υπηρεσίας (PaaS) και λογισμικού ως υπηρεσίας (SaaS). Παρέχει επίσης την υπηρεσία του μέσω τεσσάρων μοντέλων ανάπτυξης, δηλαδή, δημόσιου νέφους, ιδιωτικού νέφους, σύννεφο κοινότητας και υβριδικό σύννεφο (Shimba F., 2010). Η υιοθέτηση του υπολογιστικού νέφους αντιμετωπίζει μια σειρά προκλήσεων, οι προκλήσεις αυτές είναι: προκλήσεις ασφάλειας, νομικές προκλήσεις και προκλήσεις συμμόρφωσης και οργανωτικές προκλήσεις (Andrei, 2009; Buyya R. et. al., 2009). Συνδεδεμένο με όλες αυτές τις προκλήσεις είναι το ζήτημα της εμπιστοσύνης μεταξύ πελατών και προμηθευτών, επειδή το cloud computing καλεί τους οργανισμούς να εμπιστεύονται τους προμηθευτές με τη διαχείριση των πόρων πληροφορικής και των δεδομένων τους. Η εμπιστοσύνη είναι ένας κρίσιμος παράγοντας για την υιοθέτηση του υπολογιστικού νέφους. Από όλες τις προκλήσεις, η ασφάλεια έχει τις περισσότερες αναφορές. Αυτό συμβαίνει επειδή *"security is both a feeling and a reality. And they are not the same."* (Schneir, 2008).

Με άλλα λόγια, το cloud αφήνει τους χρήστες την πρόσβαση στα ίδια αρχεία δεδομένων και λογισμικά από σχεδόν οποιαδήποτε συσκευή, επειδή όλοι οι υπολογισμοί που γίνονται αλλά και η αποθήκευση των δεδομένων, γίνονται σε διακομιστές σε ένα κέντρο δεδομένων, αντί για επιτόπια στη συσκευή χρήστη. Αυτή είναι η αιτία για τον οποίο ένας χρήστης μπορεί να

συνδεθεί στον λογαριασμό του Instagram σε ένα νέο τηλέφωνο μετά το σπάσιμο του παλιού τηλεφώνου του και να εξακολουθεί να βρίσκει τον παλιό του λογαριασμό στη θέση του, με όλες τις φωτογραφίες, τα βίντεο και το ιστορικό συνομιλιών του. Λειτουργεί με τον ίδιο τρόπο με τους παρόχους email cloud όπως το Gmail ή το Microsoft Office 365 και με τους παρόχους αποθήκευσης cloud, όπως το Dropbox ή το Google Drive.

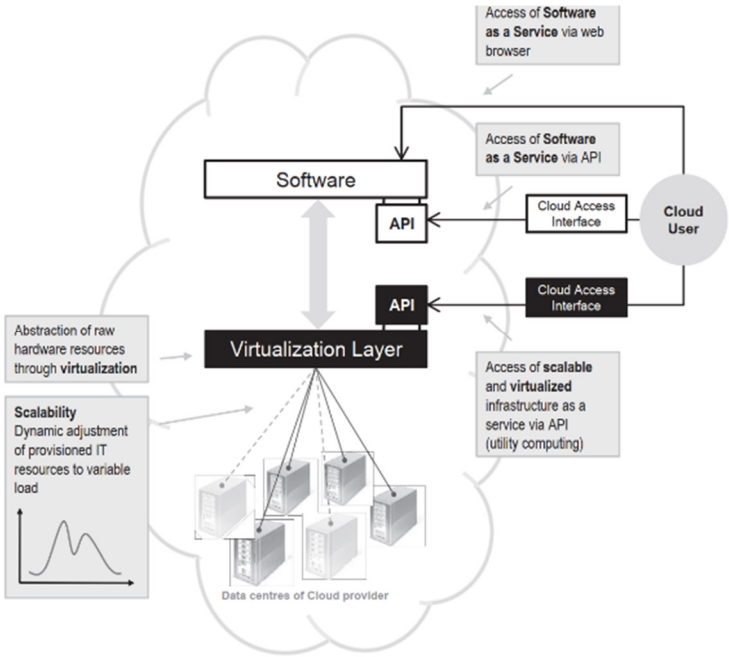
Το "σύννεφο" αναφέρεται σε διακομιστές στους οποίους υπάρχει πρόσβαση μέσω Διαδικτύου και στο λογισμικό και τις βάσεις δεδομένων που λειτουργούν σε αυτούς τους διακομιστές. Οι διακομιστές cloud βρίσκονται σε κέντρα δεδομένων σε όλο τον κόσμο. Με τη χρήση του cloud computing, οι χρήστες και οι εταιρείες δεν χρειάζεται να διαχειρίζονται οι ίδιοι φυσικούς διακομιστές ή να τρέχουν εφαρμογές λογισμικού στα δικά τους μηχανήματα.

Για τις επιχειρήσεις, η μετάβαση στο cloud computing αφαιρεί ορισμένα έξοδα πληροφορικής και γενικά έξοδα: για παράδειγμα, δεν χρειάζεται πλέον να ενημερώνουν και να διατηρούν τους δικούς τους διακομιστές, καθώς ο προμηθευτής cloud που χρησιμοποιεί θα το κάνει αυτό. Αυτό έχει ιδιαίτερα αντίκτυπο για τις μικρές επιχειρήσεις που μπορεί να μην ήταν σε θέση να αντέξουν οικονομικά τη δική τους εσωτερική υποδομή, αλλά μπορούν να αναθέσουν οικονομικά τις ανάγκες υποδομής τους μέσω του cloud. Το cloud μπορεί επίσης να διευκολύνει τις εταιρείες να λειτουργούν διεθνώς, επειδή οι εργαζόμενοι και οι πελάτες μπορούν να έχουν πρόσβαση στα ίδια αρχεία και εφαρμογές από οποιαδήποτε τοποθεσία.

Επιπλέον, οι Stanoevska-Slabeva και Wozniak μνημονεύουν συνοπτικά κάποιους ορισμούς και γνωρίσματα του Cloud Computing (Stanoevska-Slabeva & Wozniak, 2010):

Πηγή (Stanoevska-Slabeva & Wozniak, 2010)	Ορισμός
Gartner	«"Using Internet technology for multiple remote clients" as a "processing style that provides a wide range of scalable processing capabilities" as a service»
IDC	«Development, implementation, information technology dissemination model, real-time distribution of products, services, and solutions through the Internet (cloud service activation, etc.)»
The 451 Group	«“A service model that combines information technology, infrastructure components, architectural

	approaches, and general organizational principles to provide an economic model: essentially network computing as a service (SaaS), virtualization, utility computing. ing, the interface between hosting and software." »
Merrill Lynch	«The concept of providing personal applications (messaging, word processing, presentations, etc.) and business efficiency functions (sales automation, customer service, accounting, etc.) from a central server».



Εικόνα: 1-1: Ορισμός δυνατοτήτων υπολογιστικού νέφους (Stanoevska-Slabeva & Wozniak, 2010)

- Πρόκειται για μια μέθοδο υπολογισμών.
- Το υλικό, η αποθήκευση και το λογισμικό παρέχονται ως πόροι ως υπηρεσία. Όταν αυτές οι λειτουργικές υπηρεσίες προσφέρονται από τρίτους προμηθευτές ή τρίτους πελάτες, μετατρέπεται σε επιχειρηματικό μοντέλο ενοικίασης, ανάλογα με το επίπεδο χρήσης.
- Βασικό χαρακτηριστικό του είναι η χρησιμοποίηση virtual περιβαλλόντων και η δυναμική επέκτασή τους όταν κριθεί απαραίτητο.

- Το Utility Processing και το SaaS παρέχονται σε ένα ενιαίο πακέτο.

1.2 Πώς λειτουργεί το cloud computing

Ο υπολογισμός νέφους είναι δυνατός λόγω μιας τεχνολογίας που ονομάζεται εικονικοποίηση. Η εικονικοποίηση επιτρέπει τη δημιουργία ενός προσομοιωμένου, μόνο ψηφιακού «εικονικού» υπολογιστή που συμπεριφέρεται σαν να ήταν ένας φυσικός υπολογιστής με το δικό του υλικό. Ο τεχνικός όρος για έναν τέτοιο υπολογιστή είναι εικονική μηχανή . Όταν εφαρμοστούν σωστά, οι εικονικές μηχανές στον ίδιο κεντρικό υπολογιστή απομακρύνονται μεταξύ τους, έτσι δεν αλληλεπιδρούν μεταξύ τους καθόλου και τα αρχεία και οι εφαρμογές μιας εικονικής μηχανής δεν είναι ορατά στις άλλες εικονικές μηχανές, παρόλο που είναι ενεργοποιημένες την ίδια φυσική μηχανή.

Οι εικονικές μηχανές κάνουν επίσης πιο αποτελεσματική χρήση του υλικού που τα φιλοξενεί. Με την εκτέλεση πολλών εικονικών μηχανών ταυτόχρονα, ένας διακομιστής μετατρέπεται σε πολλούς διακομιστές και ένα κέντρο δεδομένων γίνεται ένας ολόκληρος αριθμός κεντρικών δεδομένων, ικανών να εξυπηρετήσουν πολλούς οργανισμούς. Έτσι, οι πάροχοι cloud μπορούν να προσφέρουν τη χρήση των διακομιστών τους σε πολύ περισσότερους πελάτες ταυτόχρονα από ό, τι θα μπορούσαν να κάνουν διαφορετικά, και μπορούν να το κάνουν με χαμηλό κόστος.

Ακόμα κι αν οι μεμονωμένοι διακομιστές μειωθούν, οι διακομιστές cloud γενικά θα πρέπει να είναι πάντα συνδεδεμένοι και πάντα διαθέσιμοι. Οι προμηθευτές cloud συνήθως δημιουργούν αντίγραφα ασφαλείας των υπηρεσιών τους σε πολλά μηχανήματα και σε πολλές περιοχές.

Οι χρήστες έχουν πρόσβαση σε υπηρεσίες cloud είτε μέσω προγράμματος περιήγησης είτε μέσω εφαρμογής, που συνδέονται στο cloud μέσω Διαδικτύου - δηλαδή μέσω πολλών διασυνδεδεμένων δικτύων - ανεξάρτητα από τη συσκευή που χρησιμοποιούν.

1.3 Αρχιτεκτονική των Συστημάτων Cloud Computing

Ο πρωταρχικός στόχος του Cloud Computing είναι να παρέχει υπηρεσίες πληροφορικής κατά παραγγελία με υψηλή αξιοπιστία, επεκτασιμότητα και διαθεσιμότητα σε κατανεμημένα περιβάλλοντα. Παρά αυτόν τον κοινό στόχο, το Cloud Computing (Carr N., 2008) έχει περιγραφεί με πολλούς διαφορετικούς τρόπους (Vaquero L et.al., 2009) και δεν έχει υιοθετηθεί κανένας τυπικός ορισμός μέχρι σήμερα. Ακολουθούν δύο παραδείγματα. Η Cisco Systems (Kapil Bakshi K., 2009) όρισε το Cloud Computing ως πόρους και υπηρεσίες πληροφορικής

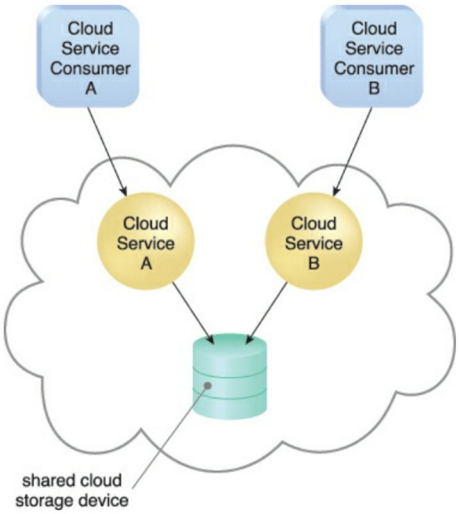
που αφαιρούνται από την υποκείμενη υποδομή και παρέχονται «κατ' απαίτηση» και «σε κλίμακα» σε ένα πολυδύναμο περιβάλλον.» Πρόσφατα, το Εργαστήριο Τεχνολογίας Πληροφοριών στο Εθνικό Ινστιτούτο Πρότυπα και τεχνολογία (NIST) (Mell P., 2011) έχει δημοσιεύσει έναν λειτουργικό ορισμό του υπολογιστικού νέφους: "Το υπολογιστικό νέφος είναι ένα μοντέλο που παρέχει στους παρόχους υπηρεσιών ολοκληρωμένη, οικονομικά αποδοτική και απαιτητική δικτυακή πρόσβαση σε μια ποικιλία προσαρμόσιμων υπολογιστικών πόρων (δίκτυα, διακομιστές, αποθήκευση, εφαρμογές, υπηρεσίες κ.λπ.) που είναι χρονοβόρες και ταχύτερες. (Rimal et al., 2010).

1.3.1 Γνωρίσματα ενός συστήματος Cloud Computing System

Η αρχιτεκτονική αυτή απαρτίζεται από πέντε κύρια γνωρίσματα. Αυτά είναι (Gong et al., 2010):

1. Αυτό-εξυπηρέτηση κατά αξίωση (on-demand-self-service). Η υποδομή cloud SaaS εκτελεί μόνο εφαρμογές που αναπτύσσονται από τον πάροχο υπηρεσιών. Ένα ευρύ φάσμα σταθερών και κινητών συσκευών επιτρέπει σε μεγάλο πληθυσμό πελατών να έχουν πρόσβαση στις υπηρεσίες που παρέχονται από αυτές τις εφαρμογές χρησιμοποιώντας μια διεπαφή thin client, όπως ένα πρόγραμμα περιήγησης ιστού (π.χ. ηλεκτρονικό ταχυδρομείο μέσω Διαδικτύου). Οι χρήστες των υπηρεσιών δεν διευθύνουν ή ελέγχουν την υποκείμενη υποδομή cloud, συμπεριλαμβανομένου του δικτύου, διακομιστές, λειτουργικά συστήματα, αποθήκευση, ή ακόμη και μόνες δυνατότητες λογισμικού, με την ενδεχομένη εξαίρεση καθορισμένων ρυθμίσεων διαμόρφωσης εφαρμογών για συγκεκριμένους χρήστες.
2. Ευρεία πρόσβαση στο δίκτυο (Ubiquitous Access). Ubiquitous πρόσβαση αντιπροσωπεύει την ικανότητα μιας υπηρεσίας cloud να είναι ευρέως προσβάσιμη. Η δημιουργία ελεύθερης ευρείας πρόσβασης για μια υπηρεσία cloud μπορεί να απαιτήσει υποστήριξη για μια σειρά συσκευών, πρωτοκόλλων μεταφοράς, διεπαφών και τεχνολογιών ασφαλείας. Για να καταστεί δυνατή αυτή η πρόσβαση, απαιτείται γενικά η αρχιτεκτονική υπηρεσιών cloud να είναι προσαρμοσμένη στις ιδιαίτερες ανάγκες των διαφόρων καταναλωτών υπηρεσιών cloud. Παρέχεται κάλυψη δικτύου και προσέγγιση μέσω τυποποιημένων μηχανισμών (Mahmood Z., 2013).
3. Πολυσύνθετη Διάθεση Πόρων (Multitenancy - Recource pooling). Το χαρακτηριστικό ενός προγράμματος λογισμικού που μπορεί να εξυπηρετεί με διαφορετικά τμήματα του

(απομονωμένα το ένα με το άλλο), ταυτόχρονα διαφορετικούς χρήστες, αναφέρεται ως πολυσύνθετο. Ένας πάροχος cloud συγκεντρώνει τους πόρους πληροφορικής του για να εξυπηρετήσει πολλούς καταναλωτές υπηρεσιών cloud χρησιμοποιώντας μοντέλα πολλαπλών λειτουργιών που συχνά βασίζονται στη χρήση τεχνολογιών εικονικής διαμόρφωσης. Χρησιμοποιώντας τεχνολογία πολλαπλών λειτουργιών, οι πόροι πληροφορικής μπορούν να εκχωρηθούν δυναμικά και να ανατεθούν εκ νέου, σύμφωνα με τις απαιτήσεις των καταναλωτών υπηρεσιών cloud. Οι πόροι του παρόχου χρησιμοποιούνται για την εξυπηρέτηση πολλαπλών χρηστών. Συνδυάζουν εικονικούς και φυσικούς πόρους για να ικανοποιήσουν τη ζήτηση των καταναλωτών. Μια *αρχιτεκτονική συγκέντρωσης πόρων* βασίζεται στη χρήση ενός ή περισσότερων ομάδων πόρων, στα οποία οι ίδιοι πόροι πληροφορικής ομαδοποιούνται και διατηρούνται από ένα σύστημα που διασφαλίζει αυτόματα ότι παραμένουν συγχρονισμένοι. Τα φυσικά σύνολα διακομιστών αποτελούνται από δικτυωμένους διακομιστές που έχουν εγκατασταθεί με λειτουργικά συστήματα και άλλα απαραίτητα προγράμματα ή/και εφαρμογές και είναι έτοιμοι για άμεση χρήση. Τα εικονικά σύνολα διακομιστών συνήθως ρυθμίζονται χρησιμοποιώντας ένα από τα πολλά διαθέσιμα πρότυπα που επιλέγονται από τον καταναλωτή cloud κατά την παροχή. Για παράδειγμα, ένας καταναλωτής cloud μπορεί να δημιουργήσει ένα σύνολο διακομιστών Windows μεσαίας βαθμίδας με μνήμη RAM 4 GB ή μια ομάδα διακομιστών Ubuntu χαμηλού επιπέδου με μνήμη RAM 2 GB. (Mahmood Z., 2013).



Εικόνα: 1-2: Μεμονωμένη συσκευή αποθήκευσης στο cloud με πολλούς καταναλωτές (Mahmood Z., 2013)

4. Ταχεία Ελαστικότητα. Οι εργασίες προσφέρονται στον τελικό χρήστη γοργά και δραστικά. Η ευελιξία είναι μια αυτοματοποιημένη ικανότητα cloud που διαβαθμίζει με διαφανείς διαδικασίες, τους πόρους πληροφορικής όπως απαιτείται για να καλύψει τις ανάγκες των καταναλωτών ή των παρόχων cloud με την πάροδο του χρόνου ή υπό συγκεκριμένες συνθήκες. Η ευελιξία αναφέρεται συχνά ως ο κύριος λόγος για την υιοθέτηση του cloud computing, κυρίως επειδή σχετίζεται στενά με μια χαμηλή απόδοση επένδυσης και το σχετικό κόστος. Ο πάροχος υπηρεσιών cloud με τους περισσότερους πόρους πληροφορικής μπορεί να προσφέρει τη μεγαλύτερη ευελιξία. (Mahmood Z., 2013).
5. Μετρήσιμες Υπηρεσίες. Το σύστημα διαχειρίζεται και βελτιστοποιεί αυτόματα τη χρήση πόρων προσφέροντας ένα μετρήσιμο σύστημα υπηρεσιών για storage, απόδοση, εύρος ζώνης και άλλα. Ο βαθμός χρησιμοποίησης του συστήματος, αξιοποιεί τις δυνατότητες της πλατφόρμας cloud για να παρακολουθεί συγκεκριμένα τη χρήση των υπολογιστικών πόρων των χρηστών του cloud. Ανάλογα με το τι μετρούν, οι πάροχοι cloud μπορούν να λαμβάνουν μόνο κατανομές πόρων cloud και πληροφορικής που χρησιμοποιούνται στην πραγματικότητα από τους καταναλωτές cloud. Η μετρημένη χρήση σχετίζεται στενά με την απαιτούμενη λειτουργικότητα. Η υπολογισμένη χρήση στατιστικών παρακολούθησης δεν περιορίζεται στους σκοπούς χρέωσης. Παρέχει επίσης μια επισκόπηση των αναφορών σχετικά με τους πόρους και τη χρήση πληροφορικής (τόσο οι πάροχοι cloud όσο και οι καταναλωτές cloud). Έτσι, η μετρούμενη ποσότητα είναι επίσης για χρήση στο cloud. (Refan S., 2011).

1.3.2 Πρότυπα υπηρεσιών

Υπάρχουν τρία πρότυπα υπηρεσίας νέφους, τα οποία συνήθως είναι γνωστά και ως «μοντέλο SPI» (Software, Platform or Infrastructure as a service – Λογισμικό, Πλατφόρμα ή Δομή ως μια υπηρεσία). Αυτά είναι:

- Λογισμικό Νέφους ως υπηρεσία (SaaS). Software as a Service (or application as a service) is a multi-tenant platform. Εκμεταλλεύεται κοινούς πόρους και μία παρουσία τόσο του κώδικα του λογισμικού, όσο και της υποκείμενης βάσης δεδομένων για την ταυτόχρονη υποστήριξη πολλών πελατών. SaaS (Choudhary V., 2007; Staff, 2001; Turner M. et. al., 2003), ενώ κοινώς αναφέρεται ως Application Service Provider (ASP) μοντέλο. Προαναγγέλλεται δε από πολλούς ως το νέο κύμα στη διανομή λογισμικού

εφαρμογών. Παραδείγματα βασικών υπηρεσιών παροχής είναι η Διαχείριση Σχέσεων Πελατών (σύστημα CRM), NetSuite, και Google Office Productivity. Οι κύριοι προβληματισμοί στο SaaS είναι οι απαιτήσεις ενσωμάτωσης με άλλες εφαρμογές. Ένα άλλο κρίσιμο συστατικό είναι η σύνθεση διαφορετικών τύπων τεχνολογίας όπως J2EE, .Net, Hibernate, Spring, Scalable Infrastructure και Services. Σε επίπεδο εφαρμογής, οι σημαντικές πτυχές της επεκτασιμότητας, της απόδοσης, της πολυ-μίσθωσης, της δυνατότητας διαμόρφωσης και της ανοχής σε σφάλματα αποτελούν πρωταρχικά ζητήματα για την αρχιτεκτονική. Πρόκειται για μια δυνατότητα που προσφέρεται στους πελάτες, ώστε να χρησιμοποιήσουν τις δυνατότητες που προσφέρονται στο «Υπολογιστικό Νέφος» (Rimal et al., 2010).

- Πλατφόρμα Νέφους ως υπηρεσία (PaaS). Το υπόβαθρο πίσω από το PaaS είναι να παρέχει στους προγραμματιστές μια πλατφόρμα που καλύπτει όλα τα συστήματα και τα περιβάλλοντα κατά την ανάπτυξη, τον έλεγχο και τη φιλοξενία προηγμένων εφαρμογών ιστού ως υπηρεσία που παρέχεται μέσω πλατφόρμας που βασίζεται σε σύννεφο. Με την υπηρεσία αυτή, οι χρήστες μπορούν να χρησιμοποιούν λογισμικό που έχουν αναπτύξει οι ίδιοι ή να χρησιμοποιούν τα εργαλεία που τους παρέχει ο πάροχος. Βασικά παραδείγματα είναι:
    - Ολοκληρωμένη πλατφόρμα, π.χ., μια πλατφόρμα για την πραγματοποίηση ηλεκτρονικών επιχειρήσεων αλλά και εφαρμογών που παρέχουν ένα ευρύ φάσμα αλληλεπίδρασης μεταξύ πλατφορμών, γλωσσών που χρησιμοποιούνται ή χρηστών, όπως Facebook F8, Sales forge App Exchange.
    - Πλατφόρμα προσανατολισμένη στην ανάπτυξη, π.χ., a πλατφόρμα που παρέχει ένα περιβάλλον για τους προγραμματιστές να αναπτύξουν, να δοκιμάσουν και να αναπτύξουν την εφαρμογή τους εύκολα, όπως Google App Engine, Bunzee connect, και SF force.com κ.λπ.
    - Infra-oriented πλατφόρμα, π.χ. μια πλατφόρμα που παρέχει στους προγραμματιστές μια επεκτάσιμη υποδομή και χώρο αποθήκευσης, όπως Amazon EC2, Simple Storage, Simple DB κ.λπ (Hoff C et. al., 2011; Rimal et al., 2010).

Σε σύγκριση με τη συμβατική ανάπτυξη εφαρμογών, η PaaS μπορεί να μειώσει σημαντικά το χρόνο ανάπτυξης και προσφέρει εκατοντάδες άμεσα διαθέσιμες υπηρεσίες.

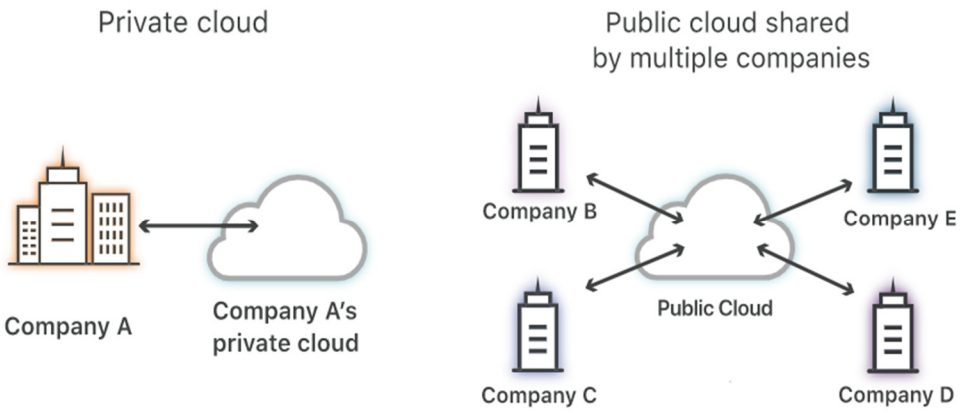
Η PaaS παρέχει μια λύση για την προσφορά πολλαπλών εφαρμογών στην ίδια πλατφόρμα, αυξάνοντας έτσι την οικονομία κλίμακας και μειώνοντας την πολυπλοκότητα. Η PaaS εξαρτάται πλήρως από τον πάροχο για τον χρόνο και τρόπο λειτουργίας της. Υπάρχει μεγάλη πιθανότητα "κλειδώματος" εάν το PaaS πρέπει να προσφέρει ιδιόκτητες διεπαφές υπηρεσιών ή γλώσσες ανάπτυξης. Επομένως, οι πάροχοι PaaS θα πρέπει να κατέχουν αυτά τα χαρακτηριστικά, ενώ πρέπει να είναι σε θέση να επαναπροσδιορίσουν την ή τις υπηρεσίες του συστήματος όταν αυτό χρειαστεί. Η πλατφόρμα ανοικτού κώδικα, ως Υπηρεσία (OPaaS or Open PaaS) είναι ένα ακόμη βήμα στην εξέλιξη του PaaS. Το OPaaS παρέχει ένα ευρύ φάσμα εγκαταστάσεων στους προγραμματιστές, όπως οποιοδήποτε γλωσσικό περιβάλλον προγραμματισμού, εργαλεία ανάπτυξης, διακομιστές, βάση δεδομένων κλπ.

Υποδομή Νέφους ως υπηρεσία (IaaS). Πρόκειται για ένα χαρακτηριστικό που παρέχει στο χρήστη ορισμένες λειτουργίες, όπως επεξεργασία, αποθήκευση, χρήση δικτύου, το οποίο επιτρέπει στο χρήστη να αναπτύσσει και να εκτελεί το λογισμικό που επιθυμεί (π.χ. υπηρεσίες λειτουργικού συστήματος). Η IaaS ονομάζεται επίσης μερικές φορές Hardware as a Service (HaaS). Σύμφωνα με τον Nicholas Carr [10], είναι η ιδέα της αγοράς υλικού πληροφορικής—ή ακόμα και ενός κέντρου δεδομένων—με συνδρομή του τύπου pay as you go που κλιμακώνει ανοδικά ή πτωτικά την χρέωση, ανάλογα με τις ανάγκες. Αυτό το μοντέλο είναι επωφελές για τους εταιρικούς χρήστες, καθώς δεν χρειάζεται να επενδύσουν στην κατασκευή και τη διαχείριση του υλικού των συστημάτων πληροφορικής. Εκτός από την υψηλότερη ευελιξία, ένα βασικό όφελος του IaaS είναι το σύστημα πληρωμών που βασίζεται στη χρήση. Αυτό επιτρέπει στους πελάτες να πληρώνουν καθώς μεγαλώνουν. Ένα άλλο σημαντικό πλεονέκτημα είναι η αγορά και η χρήση της τελευταίας τεχνολογίας. GoGrid,7 Mosso/Rackspace,8 MSP On Demand,9 masterIT,10 NewServers Inc11 είναι μερικοί IaaS πάροχοι. Η δυναμική διαμόρφωση και διαχείριση των πόρων δικτύου, αποθήκευσης και πληροφορικής σε μια ολιστική προσέγγιση είναι οι σημαντικές προκλήσεις (Rimal et al., 2010; Turner M. et. al., 2003) .

1.3.3 Τα Μοντέλα ανάπτυξης

Τα μοντέλα ανάπτυξης νέφους χωρίζονται σε τέσσερις κατηγορίες:

- «Δημόσιο Νέφος» (Public cloud) – είναι διαθέσιμο σε όλο το κοινό. Η έννοια της ανταλλαγής των υπηρεσιών και της υποδομής που παρέχονται από τρίτους παρόχους υπηρεσιών εκτός των εγκαταστάσεων (να κατέχει και να διαχειρίζεται τις φυσικές υποδομές) σε ένα περιβάλλον πολλών μισθωτών-χρηστών, που συνήθως ονομάζεται δημόσιο σύννεφο. Περιγράφει το Υπολογιστικό Νέφος με την πατροπαράδοτη κυρίαρχη έννοια, με τους οποίους οι πόροι παρέχονται δυναμικά σε βάση αυτοεξυπηρέτησης μέσω του Διαδικτύου, μέσω διαδικτυακών εφαρμογών/διαδικτυακών υπηρεσιών. Γενικά, οι επιχειρήσεις δεν θέλουν να μεταφέρουν τις κρίσιμες και βασικές επιχειρηματικές εφαρμογές τους στο δημόσιο cloud λόγω μειωμένης ασφάλειας και ελέγχου.

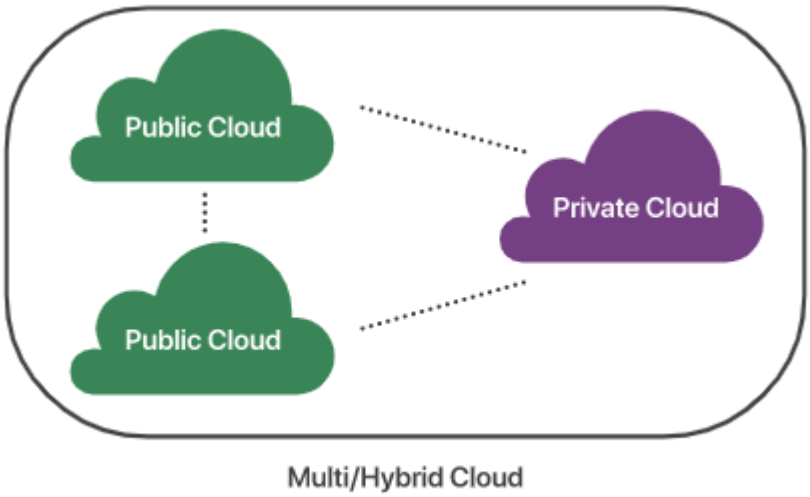


Εικόνα 1-1: Ιδιωτικό και δημόσιο νέφος (ΠΗΓΗ)

- «Ιδιωτικό Νέφος» (Private cloud) – διαθέσιμο αποκλειστικά σε έναν οργανισμό – εταιρεία. Η ιδέα πίσω από το ιδιωτικό cloud είναι η κοινή χρήση υπηρεσιών και υποδομών που παρέχονται από έναν οργανισμό ή τον καθορισμένο πάροχο υπηρεσιών του σε περιβάλλον ενός μισθωτή. Δεν είναι τόσο οικονομικό όσο το δημόσιο σύννεφο, αλλά είναι φθηνότερο από την αγορά και τη διατήρηση ενός κέντρου δεδομένων. Ομοίως, παρέχει στις εταιρείες υψηλό επίπεδο ελέγχου της χρήσης πόρων cloud. Τα δημόσια σύννεφα μπορούν να έχουν πρόσβαση στα δεδομένα στο ιδιωτικό cloud με υπηρεσίες δεδομένων. Οι υπηρεσίες στο δημόσιο cloud επικοινωνούν με ένα επίπεδο

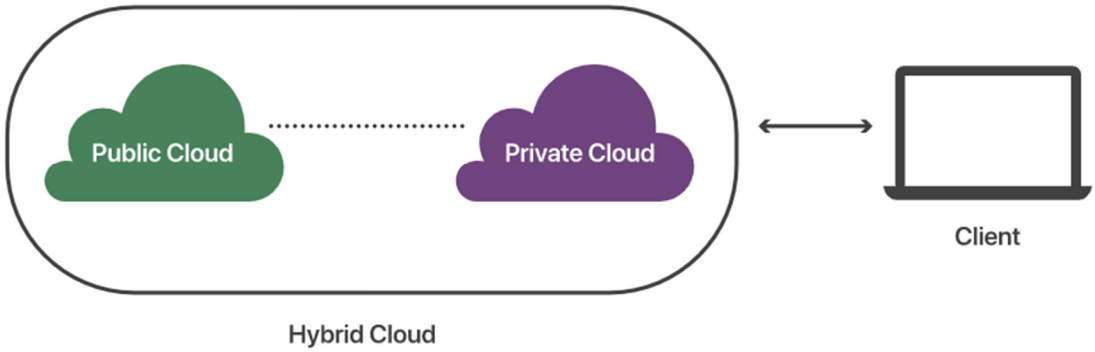
υπηρεσίας δεδομένων. Το τελευταίο υπολογίζει τον τρόπο ανάκτησης των φυσικών δεδομένων από την κατάλληλη θέση μέσω ασφαλούς πρωτοκόλλου.

- «Νέφος Κοινότητας» (Community cloud) – διαθέσιμο σε αρκετούς οργανισμούς με κοινά ενδιαφέροντα. Σύμφωνα με NIST (Mell P., 2011), το cloud κοινότητας μοιράζεται από διάφορους οργανισμούς και υποστηρίζεται από μια καθορισμένη κοινότητα που έχει κοινές έγνοιες (π.χ. προορισμός, αξιώσεις ασφαλείας, πολιτική και θέματα συμμόρφωσης).



Εικόνα 1-2: Νέφος κοινότητας(ΠΗΓΗ)

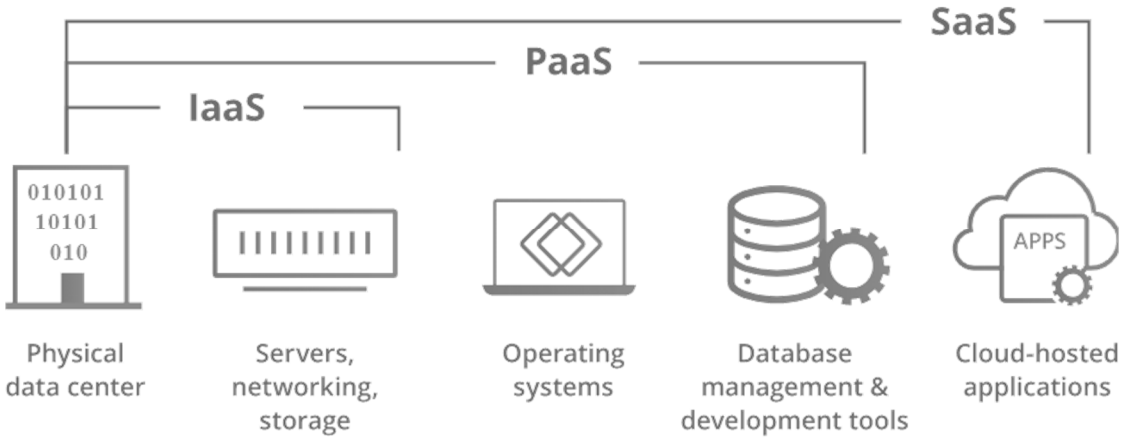
- «Υβριδικό Νέφος» (Hybrid cloud) – κοινή δομή που υποστηρίζει αλλιώτικες μορφές (πχ. συνταίριασμα ιδιωτικού νέφους με νέφος κοινότητας). Αποτελείται από πολλούς εσωτερικούς ή εξωτερικούς παρόχους. Μπορεί να παρέχει εξοικονόμηση κόστους, κλιμακούμενη κατά παραγγελία υποδομή και ασφάλεια. Ο συνδυασμός υβριδικού cloud με παραδοσιακές υποδομές μπορεί να είναι μια βιώσιμη λύση για τις περισσότερες εταιρείες. Ωστόσο, τα υβριδικά σύννεφα εισάγουν την πολυπλοκότητα του καθορισμού του τρόπου διανομής εφαρμογών τόσο σε δημόσιο όσο και σε ιδιωτικό cloud. Εάν η ποσότητα δεδομένων είναι μικρή ή η εφαρμογή είναι απάτριδα, ένα υβριδικό σύννεφο είναι δυνατόν να είναι πολύ πιο επιτυχημένο από ό, τι εάν ένας μεγάλος όγκος δεδομένων ενδείκνυται να μεταφερθεί σε ένα δημόσιο σύννεφο για μια μικρή ποσότητα επεξεργασίας (Mell P., 2011).



Εικόνα 1-3: Υβριδικό Νέφος (ΠΗΓΗ)

Μια ανάπτυξη πολλών σύννεφων συνδυάζει πολλά δημόσια σύννεφα, ενώ ένα υβριδικό σύννεφο συνδυάζει ένα δημόσιο σύννεφο με έναν άλλο τύπο περιβάλλοντος. Ένα πολυσύνθετο μπορεί επίσης να είναι ένα υβριδικό σύννεφο εάν αναμειγνύει πολλούς τύπους περιβαλλόντων σύννεφων, εκτός από τη χρήση πολλών δημόσιων σύννεφων - όπως ένα ορθογώνιο μπορεί να είναι ένα τετράγωνο, αλλά δεν είναι όλα τα ορθογώνια τετράγωνα. Αντιστρόφως, μια υβριδική ανάπτυξη cloud μπορεί επίσης να είναι πολυσύνθετη εάν χρησιμοποιεί πολλά δημόσια cloud.

1.4 Μοντέλα υπηρεσιών (SPI)



Εικόνα 1-4: Μοντέλα υπηρεσιών (ΠΗΓΗ)

1.4.1 Software as a Service (SaaS)

Με τον όρο αυτόν εννοούμε το πατροπαράδοτο μοντέλο καταμερισμού του λογισμικού, στο οποίο αυτό αγοράζεται για να εγκατασταθεί σε προσωπικούς υπολογιστές. Σε αυτό το μοντέλο,

τα λογισμικά φιλοξενούνται από μια υπηρεσία εξυπηρέτησης πελατών και διατίθενται ηλεκτρονικά στους πελάτες. Οι εφαρμογές SaaS πρέπει να μπορούν να αλληλεπιδρούν με άλλα δεδομένα και εφαρμογές σε διάφορες πλατφόρμες. Χρησιμοποιείται για την παροχή υπηρεσιών επιχειρηματικού λογισμικού σε εταιρείες με χαμηλό κόστος. Πολλοί τύποι λογισμικού αντιμετωπίζονται με το παράδειγμα SaaS, Β. Λογιστική, CRM, λογισμικό ηλεκτρονικού ταχυδρομείου, ασφάλεια, διαχείριση υπηρεσιών πληροφορικής, κλήσεις συνδιάσκεψης, ανάπτυξη ιστοσελίδων και διαχείριση δεδομένων δικτύου. Σύμφωνα με τη Microsoft, οι λύσεις SaaS μπορούν να χωριστούν σε 4 επίπεδα όσον αφορά τη διαμόρφωση, την απόδοση και την επεκτασιμότητα εφαρμογών. Τα επίπεδα είναι τα εξής:

- Επίπεδο 1 - Ad - Hoc/Custom

Κάθε αγοραστής έχει μια αποκλειστική έκδοση της εφαρμογής που φιλοξενείται. Αυτή «τρέχει» κανονικά. Η μετάβαση από λογισμικό πελάτη-διακομιστή σε αυτό το επίπεδο μοντέλου SaaS συνήθως απαιτεί ελάχιστη προσπάθεια και κόστος. Κάθε πελάτης έχει τη δική του προσαρμοσμένη έκδοση του προγράμματος φιλοξενίας. Αυτό το πρόγραμμα διαχειρίζεται τη δική του παρουσία στον κεντρικό διακομιστή. Η μετακίνηση ενός υπάρχοντος διακομιστή ή εφαρμογής δικτύου σε αυτό το επίπεδο ωριμότητας SaaS μειώνει συνήθως το κόστος ανάπτυξης και λειτουργίας, ενοποιώντας το υλικό και τη διαχείριση του διακομιστή.

- Επίπεδο 2 - Παραμετροποίηση

Σε αυτό το επίπεδο, πολλοί αγοραστές μπορούν να εκμεταλλεύονται τις διαφορετικές λειτουργίες της ίδιας εφαρμογής. Αυτό αφήνει έναν προμηθευτή να καλύψει τις διαφορετικές ανάγκες του κάθε αγοραστή, χρησιμοποιώντας ρυθμίσεις προσαρμοσμένες στον κάθε έναν ξεχωριστά. Ακόμα ένα θετικό είναι ότι ο πωλητής μπορεί να συντηρήσει την εφαρμογή ενημερώνοντας τον κοινό για όλους κώδικα.

- Επίπεδο 3 - Πολλαπλή Απόδοση

Το επόμενο, 3ο επίπεδο επεκτείνει την πολλαπλή απόδοση που έχει το 2ο επίπεδο. Πρόκειται για ένα πρόγραμμα που έχει την επιτηδειότητα να ωφελήσει όλους τους πελάτες του ίδιου προμηθευτή. Ο τελικός χρήστης δεν καταλαβαίνει κάποια διαφορά, όσοι και να μοιράζονται την ίδια υπηρεσία. Το 3ο επίπεδο ωριμότητας προσθέτει πολυδιάστατη θέση στο 2ο επίπεδο. Αυτό έχει ως αποτέλεσμα μια μεμονωμένη παρουσία προγράμματος που έχει τη δυνατότητα να εξυπηρετεί όλους τους πελάτες του προμηθευτή. Αυτή η προσέγγιση επιτρέπει την

αποτελεσματικότερη χρήση των πόρων διακομιστή χωρίς εμφανή διαφορά για τον τελικό χρήστη, αλλά τελικά αυτό το επίπεδο περιορίζεται στην ικανότητά του να κλιμακώνεται μαζικά.

- Επίπεδο 4 - Επεκτασιμότητα

Στο τέταρτο επίπεδο ωριμότητας SaaS, η επεκτασιμότητα προστίθεται με τη χρήση μιας πολυεπίπεδης αρχιτεκτονικής. Αυτή η αρχιτεκτονική είναι σε θέση να υποστηρίξει μία ισορροπημένη παρουσία πανομοιότυπων εφαρμογών που εκτελούνται σε έναν μεταβλητό αριθμό διακομιστών, κάποιες φορές σε εκατοντάδες ή ακόμη και χιλιάδες. Το μέγεθος του συστήματος μπορεί να αυξηθεί ή να μειωθεί δυναμικά για να ταιριάζει με τη ζήτηση φορτίου προσθέτοντας ή αφαιρώντας διακομιστές, χωρίς να απαιτείται περαιτέρω αλλαγή της αρχιτεκτονικής λογισμικού εφαρμογών.

Πλεονεκτήματα του μοντέλου Software as a Service

Σε μια αρχιτεκτονική προσανατολισμένη στις υπηρεσίες, η ανάπτυξη λογισμικού είναι ένα πιο πολύπλοκο πρόβλημα από το παραδοσιακό μοντέλο ανάπτυξης λογισμικού. Επομένως, οι εφαρμογές SaaS συνήθως τιμολογούνται ανάλογα με τον αριθμό των χρηστών που μπορούν να έχουν πρόσβαση στην υπηρεσία. Η χρήση ενός γραφείου βοήθειας συνεπάγεται συχνά επιπλέον εύρος ζώνης και κόστος αποθήκευσης. Οι ροές εσόδων SaaS προς τον προμηθευτή είναι συνήθως χαμηλότερες αρχικά από τα παραδοσιακά τέλη άδειας χρήσης λογισμικού. Ωστόσο, ο συμβιβασμός για χαμηλότερα τέλη άδειας χρήσης είναι μια μηνιαία επαναλαμβανόμενη ροή εσόδων, η οποία θεωρείται από τους περισσότερους εταιρικούς CFOs ως ένας πιο προβλέψιμος δείκτης για το πώς η επιχείρηση τα πάει από τρίμηνο σε τρίμηνο. Αυτές οι μηνιαίες επαναλαμβανόμενες χρεώσεις προβάλλονται όπως τα τέλη συντήρησης για λογισμικό με άδεια χρήσης (Rittinghouse J. Ransome J. et al., 2010). Τα βασικά χαρακτηριστικά του λογισμικού SaaS είναι τα ακόλουθα

Τα βασικά γνωρίσματα του μοντέλου SaaS είναι τα εξής:

- Η διαχείριση μέσω δικτύου και η πρόσβαση στο λογισμικό που διατίθεται στην αγορά από κεντρικό σημείο και όχι από οποιαδήποτε τοποθεσία του πελάτη, αφήνει τους πελάτες να έχουν πρόσβαση σε απομακρυσμένες εφαρμογές από το Διαδίκτυο.
- Η Εφαρμογή διανέμεται από ένα -προς-πολλά μοντέλα.

- Κεντρική ενίσχυση και γνώση του κώδικα που δεν καθιστά απαραίτητη τη λήψη και την εγκατάσταση από τη μεριά του χρήστη.

Τα οφέλη του SaaS για τον πελάτη είναι σαφή (Rittinghouse J. Ransome J. et al., 2010).

Ενισχύει τις εταιρείες, ώστε να κατοχυρώνουν ότι όλοι οι χώροι χρησιμοποιούν τη τελευταία, λειτουργική έκδοση του λογισμικού και, άρα, η μορφή των στοιχείων που χρησιμοποιούνται και μεταφέρονται είναι συνεπής και ακριβής. Ακόμα παρέχεται:

- Εγγύηση σε τεχνολογία cloud computing και πραγμάτωση τεχνικών ασφαλείας
- Αναβαθμισμένη χρήση
- Άμεση ενημέρωση στον κώδικα
- Τα δεδομένα είναι χρησιμοποιήσιμα και αναγνώσιμα σε ολόκληρη την επιχείρηση - Διευκόλυνση συνεργασίας
- Παγκόσμια πρόσβαση.

1.4.2 Platform as a Service (PaaS)

Το μοντέλο PaaS παρέχει όλες δυνατότητες που είναι κρίσιμες για την ορθή λειτουργία των εφαρμογών του διαδικτύου και την υποστήριξη των υπηρεσιών. Πλήρως διαθέσιμες υπηρεσίες στο Διαδίκτυο. Αντίθετα με το IaaS, όπου οι προγραμματιστές έχουν τη δυνατότητα να φτιάξουν μια συγκεκριμένη έκδοση του λειτουργικού συστήματος, στο μοντέλο PaaS οι προγραμματιστές εστιάζονται μόνο για στην ανάπτυξη εφαρμογών ιστού και δεν ενδιαφέρονται καθόλου για το λειτουργικό σύστημα.

Το PaaS επιτρέπει στους χρήστες να επικεντρώσουν την καινοτομία σε πολύπλοκες υποδομές. Αυτό δίνει στους προγραμματιστές σε όλο τον κόσμο απεριόριστη πρόσβαση στην υπολογιστική ισχύ. Έτσι, μπορείτε να δημιουργήσετε εφαρμογές για χρήστες σε όλο τον κόσμο με μια απλή σύνδεση στο Διαδίκτυο.

Το παραδοσιακό και σύγχρονο μοντέλο εγκατάστασης

Κάθε λύση προϋποθέτει ένα συγκεκριμένο υλικού που αποτελείται από το λειτουργικό σύστημα, τη βάση δεδομένων, τα e-mail, τους web servers κλπ. Μόλις αυτό αλλά και το λογισμικό περιβάλλον είναι λειτουργικά, οι προγραμματιστές μπορούν να πλοηγηθούν σε ένα

σύνολο πλατφόρμων προγραμματισμού για τη δημιουργία των εφαρμογών τους. Επιπλέον, απαιτείται για τη σωστή λειτουργία μια ομάδα διαχείρισης δικτύου, της database καθώς και ένα σύστημα διαχείρισης εμπειρογνωμόνων. Πριν τη διάθεσή του στην αγορά, απαιτούνται δοκιμές. Επιπλέον, οι μεγάλες επιχειρήσεις επιθυμούν συνήθως εξειδικευμένες υπηρεσίες για την παραμονή των κέντρων πληροφοριών τους. Τεράστιες ποσότητες ηλεκτρικής ενέργειας είναι επιπλέον αναπόσπαστο στοιχείο για την αντοχή των διακομιστών καθώς και για τη διατήρηση των δομών στη σωστή θερμοκρασία..

Βασικά χαρακτηριστικά του μοντέλου PaaS

Το μοντέλο PaaS παρέχει ταχύτερη και φθηνότερη ανάπτυξη εφαρμογών. Παρέχει μια κρίσιμη υποδομή για διαδικτυακούς προορισμούς. Το μοντέλο αυτό έχει εφαρμοστεί από μεγάλες εταιρείες όπως η Amazon, το eBay, η Google, η Apple και το YouTube. Το PaaS βασίζεται σε ένα μετρικό ή συνδρομητικό μοντέλο. Με άλλα λόγια, οι χρήστες πληρώνουν μόνο για ό,τι καταναλώνουν..

Τα εργαλεία Ιστού βασίζονται σε κοινά πρότυπα όπως HTML και JavaScript. Οι πάροχοι PaaS συχνά παρέχουν ταυτόχρονα υπηρεσίες διαχείρισης ζήτησης, επεκτασιμότητας, διατάραξης και ασφάλειας. Ένα άλλο πλεονέκτημα είναι η ενοποίηση με υπηρεσίες ιστού και βάσεων δεδομένων. Επιπλέον, η ικανότητα εγγραφής και κοινής χρήσης κώδικα σε κατανεμημένα συμπλέγματα βελτιώνει σημαντικά την απόδοση του μοντέλου PaaS.

1.4.3 Infrastructure as a Service (IaaS)

Το IaaS έχει τη δυνατότητα να παρέχει επεξεργασία, αποθήκευση, δίκτυα και άλλους θεμελιώδεις υπολογιστικούς πόρους. Ο χρήστης, είναι σε θέση να αναπτύξει και να εκτελέσει ελεύθερο λογισμικό, το οποίο μπορεί να αποτελείται από λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή cloud, αλλά έχει τον έλεγχο των λειτουργικών συστημάτων, την αποθήκευση, τις αναπτυγμένες εφαρμογές και ενδεχομένως τον περιορισμένο έλεγχο ορισμένων στοιχείων δικτύωσης, π.χ. τείχη προστασίας κεντρικού υπολογιστή (Marinescu D., 2018). Οι υπηρεσίες που προσφέρονται από αυτό το μοντέλο παράδοσης περιλαμβάνουν: φιλοξενία διακομιστών, διακομιστές ιστού, αποθήκευση, υπολογιστικό υλικό, λειτουργικά συστήματα, εικονικές παρουσίες, εξισορρόπηση φορτίου, πρόσβαση στο Διαδίκτυο και παροχή εύρους ζώνης Ως μοντέλο IaaS είναι η προσφορά ενός πακέτου υποδομών πληροφορικής ως υπηρεσία. Το μοντέλο IaaS

χρησιμοποιεί την τεχνολογία, τις υπηρεσίες, τις επενδύσεις και τα δεδομένα για να παρέχει ποικίλες υπηρεσίες στους πελάτες. Οι πάροχοι IaaS μπορούν να διαχειριστούν τη μετάβαση και τη φιλοξενία επιλεγμένων εφαρμογών εντός της υποδομής τους. Ο πελάτης διατηρεί την κυριότητα και τον έλεγχο της εφαρμογής.

Αντί να αγοράζουν δεδομένα, διακομιστές, λογισμικό, συσκευές δικτύου κ.λπ. οι πελάτες IaaS μισθώνουν αυτούς τους πόρους σε εξωτερικές υπηρεσίες. Έτσι, ο πελάτης πληρώνει μόνο για τα αναλώσιμα. Τα πλεονεκτήματα αυτής της εργασίας είναι τα εξής:

- Χρήση της νεότερης τεχνολογίας για τον εξοπλισμό των υποδομών.
- Υπολογιστικές πλατφόρμες που συνήθως παρακολουθούνται για παραβάσεις ασφαλείας.
- Χαμηλότερο κόστος των υπηρεσιών αφού δεν αγοράζουμε εμείς οι ίδιοι τον εξοπλισμό
- Μείωση του χρόνου επέκτασης από την προσθήκη νέων χαρακτηριστικών ή δυνατότητες.

On-Demand χρήση των Infrastructure υπηρεσιών

Το μοντέλο On-demand γίνεται με την παρέλευση του χρόνου ολοένα και πιο δημοφιλές αφού οι υπολογιστικοί πόροι, διατίθενται στον χρήστη σύμφωνα με τις ανάγκες του ανάλογα με τη χρονική στιγμή που τις ζητάει. Έννοιες όπως το «Σύμπλεγμα Υπολογιστών», το «Δίκτυο Υπολογιστών» (grid computing), η «Χρηστικότητα Υπολογιστών» (utility computing) κ.ά. μπορεί να δείχνουν ίδιες με την έννοια της on-demand Υπολογιστικής Χρήσης, αλλά έχουν τη δυνατότητα να γίνουν καλύτερα κατανοητές αν σκεφτεί κανείς πως τα δομικά στοιχεία ξεκίνησαν και πως κατέληξαν στο πέρασμα του χρόνου, έτσι ώστε σήμερα να έχουμε αυτό που ονομάζουμε «Υπολογιστικό Νέφος».

2 Ρίσκα και Κίνδυνοι

2.1 Συμβόλαια ασφαλείας και ρίσκα οργανισμού

Ο Οργανισμός Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) διερεύνησε παραβιάσεις ασφαλείας και εντόπισε τους σοβαρότερους κινδύνους ασφαλείας που σχετίζονται με το cloud computing. Ανήκουν στις ακόλουθες κατηγορίες:

- Συμφωνίες ασφαλείας και επιχειρηματικοί κίνδυνοι, όπως κλείδωμα προμηθευτών, απώλεια κυριαρχίας, ζητήματα συμμόρφωσης και εξαγορές παρόχων υπηρεσιών cloud.
- Μετριασμός των τρωτών σημείων του νέφους και του λειτουργικού συστήματος μέσω τεχνικών κινδύνων, όπως η απώλεια δεδομένων, η απώλεια κλειδιών κρυπτογράφησης και η ταυτόχρονη λειτουργία μεταξύ των λειτουργιών του πελάτη.
- Νομικά ρίσκα, όπως είναι η προστασία δεδομένων και η αδειοδότηση λογισμικού.
- Ρίσκα όπως προβλήματα δικτύου, μη εξουσιοδοτημένη πρόσβαση στα κέντρα πληροφοριών και φυσικές καταστροφές (Betcher T., 2010).

Αναλύοντας τα ρίσκα ασφαλείας που υπάρχουν κατά την μετάβαση των επιχειρήσεων σε υπηρεσίες υπολογιστικού νέφους θα πρέπει να γίνει μια σύγκριση σχετικά με τις περιγραφές του κινδύνου που αναφέρονται παρακάτω:

- Οι κίνδυνοι για τις επιχειρηματικές ευκαιρίες πρέπει πάντα να είναι πλήρως κατανοητοί. Οι υπηρεσίες νέφους περιλαμβάνουν βασικά πλεονεκτήματα όπως η βολική αποθήκευση και η πρόσβαση από πολλές συσκευές, καθώς και η εύκολη συνδεσιμότητα και τα πολλαπλά σημεία άμεσης συνεργασίας. Ως εκ τούτου, η ανάλυση κινδύνου θα πρέπει να συγκρίνεται και με τα δεδομένα που είναι αποθηκευμένα στο νέφος..
- Οι κίνδυνοι συχνά διαφέρουν σημαντικά ανάλογα με τον τύπο της αρχιτεκτονικής του νέφους.
- Ο κίνδυνος αυτός θα πρέπει να συγκρίνεται με το κόστος της υπηρεσίας, καθώς ο πελάτης του νέφους μπορεί να μεταφέρει τον κίνδυνο στον πάροχο του νέφους.

2.2 Απώλεια διακυβέρνησης

Με μια υποδομή cloud, οι πελάτες δεν χρειάζεται να εμπιστεύονται στους προμηθευτές τους ορισμένα πράγματα που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια. Οι πάροχοι υπηρεσιών διαδικτύου συνήθως περιλαμβάνουν μια συμφωνία επιπέδου υπηρεσιών (SLA) στους όρους της συμφωνίας με τους πελάτες τους για τον καθορισμό του επιπέδου υπηρεσιών (SLA) που πωλείται. Είναι σαφές ότι υπήρξε παραβίαση της ασφάλειας.

Είναι σύνηθες για τους παρόχους υπηρεσιών νέφους να αναθέτουν τις υπηρεσίες τους σε τρίτους. Παρόμοια με τους όρους παροχής υπηρεσιών, οι έλεγχοι του παρόχου νέφους αλλάζουν. Αυτό μπορεί να έχει καταστροφικές συνέπειες για την εταιρεία.

2.3 Lock-in

Εικόνα 2-1: Κλείδωμα εταιρειών

2.3.1 Κλείδωμα προμηθευτή πολλαπλών cloud[1]

Η μετάβαση στο cloud μπορεί να αποφέρει πολλά οφέλη στην εταιρεία, όπως αυξημένη ευελιξία, ευελιξία και εξοικονόμηση κόστους. Παρά όλα αυτά τα θετικά, πολλές εταιρείες που σκέφτονται να μετακινηθούν στο cloud έχουν ανησυχίες. Και ένα από τα πρωταρχικά ζητήματα είναι το κλείδωμα του προμηθευτή. Όταν η βάση της πληροφορικής της εταιρείας βρίσκεται στα χέρια ενός εξωτερικού προμηθευτή, αυτές οι ανησυχίες είναι έγκυρες.

Τι γίνεται αν οι προσφορές του παρόχου υπηρεσιών cloud (CSP) δεν ικανοποιούν τις ανάγκες μου; Τι γίνεται αν το CSP κάνει μια σημαντική αλλαγή προϊόντος που δεν λειτουργεί για την επιχείρησή; Τι θα συμβεί εάν ο πάροχος κλείσει; Οι περισσότερες μετακινήσεις στο cloud, αν σχεδιαστούν και εκτελεστούν σωστά, γίνονται αρκετά ομαλά. Αλλά αν κάτι πάει στραβά με τον πάροχο μετά τη μετεγκατάσταση, η μετακίνηση σε άλλον προμηθευτή cloud μπορεί να προκαλέσει σημαντικό κόστος, τεχνικά προβλήματα και πολλά άλλα. Τι μπορεί να γίνει για

[1] https://www.thorntech.com/avoidingcloudvendorlockin/

να αποφευχθεί ο αποκλεισμός προμηθευτών cloud ή τουλάχιστον να ελαχιστοποιηθούν οι αρνητικές επιπτώσεις;

2.3.2 Αιτίες φόβων κλειδώματος προμηθευτών cloud

Ο φόβος του κλειδώματος προμηθευτή cloud έχει πολλές αιτίες. Πρώτον, είναι η απώλεια ελέγχου στα δεδομένα και την υποδομή που τροφοδοτούν τις εφαρμογές των επιχειρήσεων. Το να μην έχεις πλήρη έλεγχο σε πτυχές όπως η ασφάλεια, ο χρόνος λειτουργίας και η συνολική διαχείριση της υποδομής μπορεί να είναι τρομακτικό. Στη συνέχεια, είναι η εξάρτηση από έναν προμηθευτή για τόσες κρίσιμες ανάγκες. Οι διακομιστές, τα δεδομένα, η δικτύωση, η διαχείριση χρηστών και πολλά άλλα βρίσκονται στα χέρια μιας εταιρείας, επομένως η εξάρτηση από τον πάροχο είναι τεράστια. Και αν κάτι πάει στραβά, μπορεί να είναι πολύ επιζήμιο για την επιχείρηση. Επίσης, μπορεί να υπάρχει φόβος ότι ένας πάροχος cloud δεν μπορεί να καλύψει τις τρέχουσες ή μελλοντικές ανάγκες του πελάτη. Ο πάροχος υπηρεσιών νέφους - CSP ενδέχεται να μην πληροί συμφωνίες επιπέδου υπηρεσιών ή να προκαλέσει κάποια στιγμή παραβίαση δεδομένων. Ακόμα χειρότερα, ο κίνδυνος να φύγει ο σταματήσει τις εργασίες του ο προμηθευτής είναι κάτι που θα πρέπει να υπάρχει πάντα στα υπόψη των πελατών. Η δυσκολία και το κόστος της μετάβασης σε έναν νέο προμηθευτή είναι μεγάλα στο μυαλό κάθε διαχειριστή πληροφορικής όταν αποφασίζει να μετακινηθεί στο cloud και επιλέγει έναν νέο πάροχο υπηρεσιών cloud.

2.3.3 Τύποι κινδύνων κλειδώματος προμηθευτή

Το πρόβλημα με το κλείδωμα του προμηθευτή είναι η δυσκολία της μετακίνησης σε άλλο πάροχο υπηρεσιών cloud. Υπάρχουν τέσσερις κύριοι κίνδυνοι κλειδώματος που θα αναλάβει μία εταιρεία που έχει σχέση με ένα πάροχο υπηρεσιών νέφους. Αυτοί είναι::

- Κίνδυνος μεταφοράς δεδομένων
- Κίνδυνος μεταφοράς εφαρμογών
- Κίνδυνος μεταφοράς υποδομής
- Κίνδυνος γνώσης ανθρώπινου δυναμικού

2.3.3.1 Κίνδυνος μεταφοράς δεδομένων

Δεν είναι εύκολο να μεταφέρετε τα δεδομένα μία εταιρεία ή γενικότερα, ένας πελάτης, από τον ένα πάροχο στον άλλο. Πολλοί προβληματισμοί θα προκύψουν κατά τη διάρκεια μιας διαδικασίας μετεγκατάστασης δεδομένων, όπως:

- Ποιος είναι υπεύθυνος για την εξαγωγή των δεδομένων από τις βάσεις δεδομένων cloud και τις αποθήκες δεδομένων;
- Σε ποια μορφή θα είναι τα δεδομένα; Θα λειτουργήσει αυτή η μορφή με τον νέο πάροχο cloud ή θα πρέπει να γίνουν σημαντικές αλλαγές στα δεδομένα;
- Πώς μπορούν να μεταφερθούν τα δεδομένα χωρίς απώλεια της λειτουργικότητας της εφαρμογής;
- Πόσο καιρό θα πάρει και πόσο θα κοστίσει η μεταφορά όλων αυτών των δεδομένων;
- Ενώ ορισμένοι βιομηχανικοί όμιλοι έχουν προσπαθήσει να δημιουργήσουν πρότυπα για την ανταλλαγή δεδομένων, μερικές φορές είναι δύσκολο για τις εταιρείες να τα εφαρμόσουν λόγω των μοναδικών επιχειρηματικών τους απαιτήσεων.

2.3.3.2 Κίνδυνος μεταφοράς εφαρμογών

Εάν δημιουργηθεί μια εφαρμογή σε έναν πάροχο, που αξιοποιεί πολλές από τις προσφορές της, η αναδιαμόρφωση αυτής της εφαρμογής ώστε να λειτουργεί εγγενώς σε άλλο πάροχο μπορεί να είναι μια εξαιρετικά δαπανηρή και δύσκολη διαδικασία. Για παράδειγμα, ας υποτεθεί ότι μία εταιρεία έχει αναπτύξει μια πλατφόρμα επιχειρηματικής ευφυΐας στο Microsoft Azure. Μπορεί να αξιοποιήσει βασικές υπηρεσίες cloud όπως υπολογισμό, αποθήκευση, βάσεις δεδομένων και δικτύωση. Αλλά η εφαρμογή περιλαμβάνει επίσης μηχανική εκμάθηση του Azure, ανάλυση δεδομένων και υπηρεσίες bot. Οι αλλαγές που πρέπει να γίνουν σε αυτό ακριβώς το σημείο για την μετάβαση σε ένα νέο πάροχο, είναι δραματικά πολλές. Ένας λόγος για αυτήν τη δυσκολία είναι η έλλειψη τυπικών διεπαφών και ανοιχτών API. Κάθε CSP έχει τις δικές του προδιαγραφές και πρότυπα, τα οποία καθιστούν πολύ δύσκολη τη μετάβαση από το ένα στο άλλο.

Ένας άλλος λόγος είναι ότι η τεχνολογία και οι ανάγκες των πελατών αλλάζουν τόσο γρήγορα. Οι πελάτες των παρόχων, και οι συνεργάτες απαιτούν συνεχώς αλλαγές και βελτιώσεις στο προϊόν. Όσο γρηγορότερα προστεθούν και επεξεργαστούν οι λειτουργίες μίας εφαρμογής στο

cloud, τόσο μεγαλύτερη σχέση θα υπάρξει με τον πάροχο και η δυσκολία μετάβασης σε νέο θα είναι μεγαλύτερη.

2.3.3.3 Κίνδυνος μεταφοράς υποδομής

Κάθε σημαντικός πάροχος κάνει τα ίδια πράγματα διαφορετικά. Αυτή είναι άλλωστε μία διαφορά ανάμεσα σε εταιρείες που ασχολούνται στο ίδιο πεδίο. Οι μορφές εικονικών μηχανών (virtual machines) και οι σχετικές κοστολογήσεις τους διαφέρουν από προμηθευτή σε προμηθευτή, καθιστώντας δύσκολο να διασφαλιστεί ότι ο πελάτης έχει την κατάλληλη χρήση πόρων και την απαραίτητη εξοικονόμηση κόστους εάν αλλάξει πάροχο. Οι προσφορές και οι μορφές βάσεων δεδομένων μπορεί επίσης να διαφέρουν. Και ένας πάροχος cloud μπορεί να έχει πιο ελκυστικές προσφορές σε ορισμένα στοιχεία υποδομής, ενώ δεν διαθέτει άλλες υπηρεσίες που μπορεί να χρειαστούν. Αυτές οι διαφορές στην υποκείμενη υποδομή έχουν ως αποτέλεσμα δυσκολίες στη μετάβαση από έναν πάροχο υπηρεσιών cloud σε άλλον.

2.3.3.4 Κίνδυνος γνώσης ανθρώπινου δυναμικού

Εάν υπάρχει συνεργασία με ένα μόνο πάροχο, ο πελάτης έχει αποκτήσει πιθανώς πολλές θεσμικές γνώσεις σχετικά με τα εργαλεία και τις διαμορφώσεις του παρόχου αυτού. Εάν πρέπει να μεταφερθούν οι εφαρμογές σε άλλο CSP, θα χρειαστεί χρόνος για να βελτιωθούν οι μηχανισμοί, η λειτουργικότητα μίας εφαρμογής, αλλά και η εμβάθυνση στα νέα δεδομένα και απαιτήσεις, που μπορεί να έχει ο νέος πάροχος. Η ανάγκη για μία νέα γνώση από τον πελάτη μτά την μεταφορά σε νέο πάροχο αποτελεί ένα εξίσου σημαντικό κίνδυνο..

2.3.4 Αποφυγή αποκλεισμού προμηθευτή.

Οι κίνδυνοι που αναλαμβάνει μία επιχείρηση, στην περίπτωση που χρειαστεί να αλλάξει πάροχο, είναι δυσοίωνοι. Υπάρχουν όμως μερικά πράγματα που μπορείτε να γίνουν για να διασφαλιστεί ότι ο κίνδυνος κλειδώματος του προμηθευτή ελαχιστοποιείται.

Πριν γίνει η επιλογή του παρόχου, πρέπει να ελεγχθεί σχολαστικά εάν αυτός μπορεί να παράσχει όλα τα εφόδια, προκειμένου να γίνεται απρόσκοπτα η λειτουργία ων διαφόρων εφαρμογών.

Η διαδικασία επιλογής ενός παρόχου, πρέπει να περιλαμβάνει:

a. Καθορισμό τον στόχων που επιβάλλουν την μετάβαση των υπηρεσιών μίας εταιρείας, στο νέφος.

b. Αξιολόγησης της τρέχουσας κατάστασης των υπολογιστικών αναγκών μίας επιχείρησης, αλλά και των υπαρχουσών υποδομών. Είναι σημαντικό επίσης να είναι γνωστό το κόστος της μετάβασης και διατήρησης του κύκλου εργασιών, μίας επιχείρησης, στο νέφος.

c. Επιλογή ενός από τους τρεις τύπου νέφους, που υπάρχουν (δημόσιο, ιδιωτικό ή υβριδικό) τον τύπο του περιβάλλοντος cloud που απαιτείται - δημόσιο, ιδιωτικό ή υβριδικό;

d. Την γνώση για το τι χρειάζεται η επιχείρηση και τι προσδοκά από την μεταφορά της στο cloud.

e. Επιλογή, τέλος, του κατάλληλου, κατά περίπτωση παρόχου.

Πρέπει να ληφθεί υπόψη το σύνολο των προσφορών για τις υπηρεσίες από τους παρόχους (ο νόμος αγοράς αναφέρει ότι είναι απαραίτητη η λήψη προσφορών από πολλούς παρόχους), σύγκριση αυτών (διαφορετική τιμολογιακή πολιτική, διαφορετικά επίπεδα υπηρεσιών, διαφορετικό κόστος υπηρεσιών).

Πρέπει εξαρχής ο πελάτης να έχει προγραμματίσει και σχεδιάσει πιθανή μεταφορά σε νέο πάροχο κάποια στιγμή. Είναι ένα ρίσκο (και οικονομικό κόστος) το οποίο πρέπει να υπολογίζεται από την αρχή της σχέσης με ένα πάροχο. Ο σχεδιασμός και ο υπολογισμός του κόστους μετάβασης σε νέο πάροχο, πρέπει να γίνεται σε βάθος ορίζοντα διετίας.

Για να ελαχιστοποιηθούν οι κίνδυνοι εγκλωβισμού σε ένα πάροχο, θα πρέπει οι εφαρμογές μία επιχείρησης, να δημιουργηθούν ή να μεταφερθούν ώστε να είναι όσο το δυνατόν πιο ευέλικτες και χαλαρά συνδεδεμένες. Τα στοιχεία των εφαρμογών του cloud θα πρέπει να συνδέονται χαλαρά με τα στοιχεία των εφαρμογών του πελάτη που αλληλοεπιδρούν με αυτά. Αυτό μπορεί να γίνει με την ενσωμάτωση REST APIs με δημοφιλή πρότυπα όπως το HTTP, JSON και OAuth για να υπάρχει η δυνατότητα αποδέσμευσης των εφαρμογών από την υποκείμενη ιδιοκτησιακή υποδομή του cloud. Επίσης, οποιαδήποτε επιχειρηματική λογική θα πρέπει όχι μόνο να διαχωρίζεται από τη λογική της εφαρμογής, αλλά και να ορίζεται και να

τεκμηριώνεται με σαφήνεια. Με τον τρόπο αυτό θα αποφευχθεί η ανάγκη αποκρυπτογράφησης των επιχειρηματικών κανόνων σε περίπτωση μετάβασης σε νέο CSP. Αυτό όχι μόνο μειώνει το επίπεδο εγκλωβισμού σε έναν μόνο προμηθευτή, αλλά δίνει επίσης στην εφαρμογή διαλειτουργικότητα που απαιτείται για τη γρήγορη μετάβαση των φόρτων εργασίας και των περιβαλλόντων πολλαπλών υπολογιστικών νεφών.

2.3.4.1 Μεγιστοποίηση της φορητότητας των δεδομένων.

Τα δεδομένα είναι ένα από τα μεγαλύτερα σημεία που κολλάνε στις μεταναστεύσεις στο νέφος, καθώς οι διαφορετικές μορφές και μοντέλα μπορούν να προκαλέσουν προβλήματα φορητότητας. Το Open Data Element Framework[2] δημιουργήθηκε για να βοηθήσει στην τυποποίηση της τεκμηρίωσης, της κατηγοριοποίησης και της ευρετηρίασης των δεδομένων, ενώ το Cloud Data Management Interface βοηθά στον καθορισμό του τρόπου δημιουργίας, ανάκτησης, ενημέρωσης και διαγραφής στοιχείων δεδομένων από το cloud. Αυτά τα πρότυπα δεν είναι πάντα κατανοητά, αποδεκτά ούτε εφαρμόζονται. Για να μεγιστοποιηθεί η φορητότητα των δεδομένων, πρέπει να αποφεύγεται η ιδιόκτητη μορφοποίηση. Πρέπει να υπάρχει σαφή περιγραφή των μοντέλων δεδομένων με όσο το δυνατόν μεγαλύτερη σαφήνεια, χρησιμοποιώντας τα ισχύοντα πρότυπα σχημάτων για τη δημιουργία λεπτομερούς τεκμηρίωσης που διαβάζεται από υπολογιστή και άνθρωπο. Επιπλέον, θα πρέπει να υπάρχει διαβεβαίωση ότι ο πάροχος του νέφους παρέχει έναν τρόπο για να εξάγονται τα δεδομένα εύκολα και οικονομικά. Ο εγκλωβισμός δεδομένων είναι ίσως ο πιο δύσκολος κίνδυνος που μπορεί να μετριαστεί, οπότε η λήψη αυτών των μέτρων θα διευκολύνει σε μεγάλο βαθμό τη μετάβαση των δεδομένων από τον έναν CSP στον άλλο.

2.3.4.2 Στρατηγική πολλαπλών υπολογιστικών νεφών

Όλο και περισσότερες επιχειρήσεις προχωρούν σε ένα περιβάλλον πολλαπλών υπολογιστικών νεφών, όπου μπορεί να αξιοποιηθούν πολλαπλοί CSPs για την τροφοδοσία των εφαρμογών. Για παράδειγμα, μπορεί να χρησιμοποιηθεί το Amazon EC2 για την υπολογιστική ισχύ και το Redshift για την αποθήκη δεδομένων, ενώ παράλληλα το Watson του IBM Bluemix ως

---

[2] https://www.google.com/search?q=Open+Data+Element+Framework&rlz=1C1GCEA_enGR966GR966&oq=Open+Data+Element+Framework+&aqs=chrome..69i57.1804j0j15&sourceid=chrome&ie=UTF-8

πλατφόρμα τεχνητής νοημοσύνης. Με τη χρήση πολλαπλών υπολογιστικών νεφών, εξαρτάται μία επιχείρηση, λιγότερο από έναν CSP για όλες τις ανάγκες της. Ένα άλλο πλεονέκτημα είναι ότι μπορεί να επιλέγονται προσφορές από κάθε πάροχο cloud, ώστε να μπορεί να εφαρμόζονται οι βέλτιστες υπηρεσίες στις εφαρμογές. Υπάρχουν και κάποια μειονεκτήματα στην προσέγγιση του multi-cloud, όπως η αυξημένη επιβάρυνση των ομάδων ανάπτυξης, ο μεγαλύτερος κίνδυνος ασφάλειας και άλλα.

2.3.4.3 Εφαρμογή εργαλείων και διαδικασιών DevOps.

Τα εργαλεία DevOps εφαρμόζονται όλο και περισσότερο για τη μεγιστοποίηση της φορητότητας του κώδικα. Η τεχνολογία που παρέχεται από εταιρείες όπως η Docker και η CoreOS συμβάλλει στην απομόνωση του λογισμικού από το περιβάλλον του και στην αφαίρεση των εξαρτήσεων από τον πάροχο cloud. Και δεδομένου ότι οι περισσότεροι CSPs υποστηρίζουν τυποποιημένες μορφές container, θα πρέπει να είναι εύκολη η μεταφορά της εφαρμογής σας σε έναν νέο πάροχο cloud, αν χρειαστεί. Επιπλέον, εργαλεία διαχείρισης ρυθμίσεων όπως το Chef και το Puppet βοηθούν στην αυτοματοποίηση της διαμόρφωση της υποδομής στην οποία εκτελούνται οι εφαρμογές. Αυτό επιτρέπει την ανάπτυξη των εφαρμογών σε διαφορετικά περιβάλλοντα πληροφορικής, γεγονός που μπορεί να μειώσει τη δυσκολία της μετάβασης σε έναν νέο CSP. Αυτές οι τεχνολογίες μειώνουν τους κινδύνους εγκλωβισμού που απορρέουν από ιδιόκτητες διαμορφώσεις και μπορούν να διευκολύνουν τη μετάβαση από έναν CSP σε έναν άλλο.

2.4 Τεχνικά ρίσκα[3]

Οι οργανισμοί συνεχίζουν να αναπτύσσουν νέες εφαρμογές ή να μετεγκαθίστανται υπάρχουσες εφαρμογές σε υπηρεσίες που βασίζονται στο cloud. Η ομοσπονδιακή κυβέρνηση πρόσφατα κατέστησε την υιοθέτηση του cloud κεντρικό δόγμα της στρατηγικής εκσυγχρονισμού της πληροφορικής. Ένας οργανισμός που υιοθετεί τεχνολογίες cloud ή/και επιλέγει παρόχους υπηρεσιών cloud (CSP) και υπηρεσίες ή εφαρμογές χωρίς να ενημερώνεται πλήρως για τους κινδύνους που ενέχονται εκτίθεται σε μυριάδες εμπορικούς, οικονομικούς, τεχνικούς, νομικούς και κινδύνους συμμόρφωσης. Σε αυτήν την ανάρτηση ιστολογίου,

[3] https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/

περιγράφουμε 12 κινδύνους, απειλές και ευπάθειες που αντιμετωπίζουν οι οργανισμοί κατά τη μετακίνηση εφαρμογών ή δεδομένων στο cloud. Στην ανάρτησή μας, Βέλτιστες πρακτικές για την ασφάλεια στο cloud, διερευνούμε μια σειρά βέλτιστων πρακτικών που αποσκοπούν στο να βοηθήσουν τους οργανισμούς να μεταφέρουν με ασφάλεια δεδομένα και εφαρμογές στο cloud.

Θα θέλαμε να σημειώσουμε ότι οι απειλές και τα τρωτά σημεία που εμπλέκονται στη μετανάστευση στο cloud εξελίσσονται συνεχώς και αυτά που αναφέρονται εδώ δεν είναι σε καμία σημείο εξαντλητικά. Είναι σημαντικό να εξετάσουμε άλλες προκλήσεις και κινδύνους που σχετίζονται με την υιοθέτηση στο cloud ειδικά για τις αποστολές, τα συστήματα και τα δεδομένα τους.

Το μοντέλο cloud του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) παρέχει έναν ορισμό του υπολογιστικού νέφους και του τρόπου με τον οποίο μπορεί να χρησιμοποιηθεί και να αναπτυχθεί.

Το NIST προσδιορίζει τα ακόλουθα χαρακτηριστικά και μοντέλα για το υπολογιστικό νέφος:

Βασικά χαρακτηριστικά: αυτοεξυπηρέτηση κατ' απαίτηση, ευρεία πρόσβαση στο δίκτυο, συγκέντρωση πόρων, ταχεία ελαστικότητα και μετρημένη εξυπηρέτηση

Μοντέλα υπηρεσιών: λογισμικό ως υπηρεσία (SaaS), πλατφόρμα ως υπηρεσία (PaaS) και υποδομή ως υπηρεσία (IaaS)

Μοντέλα ανάπτυξης: ιδιωτικό σύννεφο, σύννεφο κοινότητας, δημόσιο σύννεφο και υβριδικό σύννεφο

Απειλές, κίνδυνοι και ευπάθειες υπολογιστικού νέφους

Εμπειρία περιβάλλοντος cloud -σε υψηλό επίπεδο- τις ίδιες απειλές με τα παραδοσιακά περιβάλλοντα κέντρων δεδομένων. η εικόνα της απειλής είναι η ίδια. Δηλαδή, το υπολογιστικό νέφος τρέχει λογισμικό, το λογισμικό έχει ευπάθειες και οι αντίπαλοι προσπαθούν να

εκμεταλλευτούν αυτές τις ευπάθειες. Ωστόσο, σε αντίθεση με τα συστήματα τεχνολογίας πληροφοριών σε ένα παραδοσιακό κέντρο δεδομένων, στο υπολογιστικό νέφος, η ευθύνη για τον μετριασμό των κινδύνων που προκύπτουν από αυτές τις ευπάθειες λογισμικού μοιράζεται μεταξύ του CSP και του καταναλωτή cloud. Ως εκ τούτου, οι καταναλωτές πρέπει να κατανοήσουν τον καταμερισμό των ευθυνών και να εμπιστευτούν ότι ο CSP ανταποκρίνεται στις ευθύνες του. Με βάση τις αναζητήσεις βιβλιογραφίας και τις προσπάθειες ανάλυσης, εντοπίστηκε η ακόλουθη λίστα με μοναδικά στο cloud και κοινόχρηστα τρωτά σημεία και απειλές cloud/on-premise. Ο παρακάτω αριθμός περιγράφει επίσης λεπτομερώς την εικόνα απειλής για πλατφόρμες υπολογιστικού νέφους.

Μοναδικές απειλές και κίνδυνοι για το cloud

Οι ακόλουθες ευπάθειες είναι αποτέλεσμα της εφαρμογής από το CSP των πέντε χαρακτηριστικών υπολογιστικού νέφους. Αυτά τα θέματα ευπάθειας δεν υπάρχουν σε κλασικά κέντρα δεδομένων πληροφορικής.

1. Οι καταναλωτές έχουν μειωμένη ορατότητα και έλεγχο. Κατά τη μετάβαση στοιχείων/λειτουργιών στο cloud, οι οργανισμοί χάνουν κάποια ορατότητα και έλεγχο σε αυτά τα περιουσιακά στοιχεία/λειτουργίες. Κατά τη χρήση εξωτερικών υπηρεσιών υπολογιστικού νέφους, η ευθύνη για ορισμένες από τις πολιτικές και τις υποδομές μεταφέρεται στο CSP.

Η πραγματική μετατόπιση της ευθύνης εξαρτάται από τα μοντέλα υπηρεσιών cloud που χρησιμοποιούνται, οδηγώντας σε αλλαγή παραδείγματος για τους οργανισμούς σε σχέση με την παρακολούθηση και την καταγραφή της ασφάλειας. Οι οργανισμοί πρέπει να εκτελούν παρακολούθηση και ανάλυση πληροφοριών σχετικά με εφαρμογές, υπηρεσίες, δεδομένα και χρήστες, χωρίς να χρησιμοποιούν παρακολούθηση και καταγραφή βάσει δικτύου, η οποία είναι διαθέσιμη για εσωτερική πληροφορική.

2. Αυτοεξυπηρέτηση κατ ' απαίτηση απλοποιεί τη μη εξουσιοδοτημένη χρήση. Οι CKΠ καθιστούν πολύ εύκολη την παροχή νέων υπηρεσιών. Οι κατά παραγγελία

δυνατότητες παροχής αυτοεξυπηρέτησης του cloud επιτρέπουν στο προσωπικό ενός οργανισμού να προσφέρει πρόσθετες υπηρεσίες από το CSP του οργανισμού χωρίς τη συγκατάθεση πληροφορικής. Η πρακτική της χρήσης λογισμικού σε έναν οργανισμό που δεν υποστηρίζεται από το τμήμα IT του οργανισμού αναφέρεται συνήθως ως σκιώδης it.

Λόγω του χαμηλότερου κόστους και της ευκολίας εφαρμογής των προϊόντων PaaS και SaaS, αυξάνεται η πιθανότητα μη εξουσιοδοτημένης χρήσης υπηρεσιών cloud. Ωστόσο, οι υπηρεσίες που παρέχονται ή χρησιμοποιούνται εν αγνοία της πληροφορικής ενέχουν κινδύνους για έναν οργανισμό. Η χρήση μη εξουσιοδοτημένων υπηρεσιών cloud θα μπορούσε να οδηγήσει σε αύξηση των λοιμώξεων από κακόβουλο λογισμικό ή της εξαγωγής δεδομένων, καθώς ο οργανισμός δεν είναι σε θέση να προστατεύσει πόρους που δεν γνωρίζει. Η χρήση μη εξουσιοδοτημένων υπηρεσιών cloud μειώνει επίσης την προβολή και τον έλεγχο του δικτύου και των δεδομένων ενός οργανισμού.

3. API διαχείρισης προσβάσιμα στο Διαδίκτυο μπορούν να διακυβευτούν. Οι CSPs εκθέτουν ένα σύνολο διεπαφών προγραμματισμού εφαρμογών (API) που χρησιμοποιούν οι πελάτες για τη διαχείριση και την αλληλεπίδραση με υπηρεσίες cloud (επίσης γνωστές ως επίπεδο διαχείρισης). Οι οργανισμοί χρησιμοποιούν αυτά τα API για την παροχή, τη διαχείριση, την ενορχήστρωση και την παρακολούθηση των περιουσιακών στοιχείων και των χρηστών τους. Αυτά τα API μπορούν να περιέχουν τα ίδια θέματα ευπάθειας λογισμικού με ένα API για ένα λειτουργικό σύστημα, βιβλιοθήκη κ.λπ. Σε αντίθεση με τα API διαχείρισης για υπολογιστές εσωτερικής εγκατάστασης, τα API CSP είναι προσβάσιμα μέσω του Διαδικτύου, εκθέτοντάς τα ευρύτερα σε πιθανή εκμετάλλευση.

Οι παράγοντες απειλής αναζητούν ευπάθειες στα API διαχείρισης. Εάν ανακαλυφθεί, αυτές οι ευπάθειες μπορούν να μετατραπούν σε επιτυχημένες επιθέσεις και τα στοιχεία cloud του οργανισμού μπορούν να διακυβευτούν. Από εκεί, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τα περιουσιακά στοιχεία του οργανισμού για να διαπράξουν περαιτέρω επιθέσεις εναντίον άλλων πελατών CSP.

4. Διαχωρισμός μεταξύ πολλαπλών ενοικιαστών αποτυγχάνει. Η εκμετάλλευση τρωτών σημείων συστήματος και λογισμικού εντός της υποδομής, των πλατφορμών ή των εφαρμογών ενός CSP που υποστηρίζουν την πολυκατοικία μπορεί να οδηγήσει σε αποτυχία διατήρησης του διαχωρισμού μεταξύ των ενοίκων. Αυτή η αποτυχία μπορεί να χρησιμοποιηθεί από έναν εισβολέα για να αποκτήσει πρόσβαση από τον πόρο ενός οργανισμού στα περιουσιακά στοιχεία ή τα δεδομένα ενός άλλου χρήστη ή οργανισμού. Η πολυ-μίσθωση αυξάνει την επιφάνεια επίθεσης, οδηγώντας σε αυξημένη πιθανότητα διαρροής δεδομένων σε περίπτωση αποτυχίας των ελέγχων διαχωρισμού.

Αυτή η επίθεση μπορεί να επιτευχθεί με την εκμετάλλευση ευπαθειών στις εφαρμογές, τον υπερ-έλεγχο ή το υλικό του CSP, ανατρέποντας λογικά στοιχεία ελέγχου απομόνωσης ή επιθέσεις στο API διαχείρισης του CSP. Μέχρι σήμερα, δεν έχει υπάρξει τεκμηριωμένη αποτυχία ασφαλείας της πλατφόρμας SaaS ενός CSP που είχε ως αποτέλεσμα ένας εξωτερικός εισβολέας να αποκτήσει πρόσβαση στα δεδομένα των ενοίκων.

Δεν εντοπίστηκαν αναφορές επίθεσης που να βασίζονται σε λογική αποτυχία διαχωρισμού. Ωστόσο, έχουν αποδειχθεί τα κατορθώματα απόδειξης της έννοιας.

5. Διαγραφή δεδομένων είναι ελλιπής. Απειλές που σχετίζονται με τη διαγραφή δεδομένων υπάρχουν επειδή ο καταναλωτής έχει μειώσει την ορατότητα στο πού αποθηκεύονται τα δεδομένα του στο cloud και μειωμένη ικανότητα επαλήθευσης της ασφαλούς διαγραφής των δεδομένων του. Ο κίνδυνος αυτός είναι ανησυχητικός, διότι τα δεδομένα κατανέμονται σε διάφορες συσκευές αποθήκευσης εντός της υποδομής του CSP σε περιβάλλον πολλαπλών μίσθωσης. Επιπλέον, οι διαδικασίες διαγραφής ενδέχεται να διαφέρουν από πάροχο σε πάροχο. Οι οργανισμοί ενδέχεται να μην είναι σε θέση να επαληθεύσουν ότι τα δεδομένα τους διαγράφηκαν με ασφάλεια και ότι τα υπολείμματα των δεδομένων

δεν είναι διαθέσιμα στους επιτιθέμενους. Αυτή η απειλή αυξάνεται καθώς ένας οργανισμός χρησιμοποιεί περισσότερες υπηρεσίες CSP.

Απειλές και κίνδυνοι cloud και on-premise

Ακολουθούν κίνδυνοι που ισχύουν τόσο για τα κέντρα δεδομένων cloud όσο και για τα κέντρα δεδομένων πληροφορικής που πρέπει να αντιμετωπίσουν οι οργανισμοί.

6. Διαπιστευτήρια εκλάπησαν. Εάν ένας εισβολέας αποκτήσει πρόσβαση στα διαπιστευτήρια cloud ενός χρήστη, ο εισβολέας μπορεί να έχει πρόσβαση στις υπηρεσίες του CSP για την παροχή πρόσθετων πόρων (εάν τα διαπιστευτήρια επέτρεπαν την πρόσβαση στην παροχή), καθώς και να στοχεύσει τα περιουσιακά στοιχεία του οργανισμού. Ο εισβολέας θα μπορούσε να αξιοποιήσει πόρους υπολογιστικού νέφους για να στοχεύσει τους χρήστες διαχείρισης του οργανισμού, άλλους οργανισμούς που χρησιμοποιούν το ίδιο CSP ή τους διαχειριστές του CSP. Ένας εισβολέας που αποκτά πρόσβαση στα διαπιστευτήρια cloud ενός διαχειριστή CSP ενδέχεται να μπορεί να χρησιμοποιήσει αυτά τα διαπιστευτήρια για να αποκτήσει πρόσβαση στα συστήματα και τα δεδομένα του οργανισμού.

Οι ρόλοι διαχειριστή διαφέρουν μεταξύ ενός CSP και ενός οργανισμού. Ο διαχειριστής του CSP έχει πρόσβαση στο δίκτυο, τα συστήματα και τις εφαρμογές CSP (ανάλογα με την υπηρεσία) της υποδομής του CSP, ενώ οι διαχειριστές του καταναλωτή έχουν πρόσβαση μόνο στις υλοποιήσεις cloud του οργανισμού. Στην ουσία, ο διαχειριστής CSP έχει δικαιώματα διαχείρισης σε περισσότερους από έναν πελάτες και υποστηρίζει πολλαπλές υπηρεσίες.

7. Κλείδωμα προμηθευτή περιπλέκει τη μετακίνηση σε άλλα CSPs. Το κλείδωμα προμηθευτή γίνεται πρόβλημα όταν ένας οργανισμός εξετάζει το ενδεχόμενο να μετακινήσει τα περιουσιακά στοιχεία/τις λειτουργίες του από ένα CSP σε ένα άλλο. Ο οργανισμός ανακαλύπτει ότι ο χρόνος

κόστους/προσπάθειας/χρονοδιαγράμματος που απαιτείται για τη μετακίνηση είναι πολύ υψηλότερος από ό, τι αρχικά λαμβάνεται υπόψη λόγω παραγόντων όπως οι μη τυπικές μορφές δεδομένων, τα μη τυποποιημένα API και η εξάρτηση από τα ιδιόκτητα εργαλεία ενός CSP και τα μοναδικά API.

Αυτό το ζήτημα αυξάνεται στα μοντέλα υπηρεσιών όπου το CSP αναλαμβάνει περισσότερες ευθύνες. Καθώς ένας οργανισμός χρησιμοποιεί περισσότερες δυνατότητες, υπηρεσίες ή API, η έκθεση στις μοναδικές υλοποιήσεις ενός CSP αυξάνεται. Αυτές οι μοναδικές υλοποιήσεις απαιτούν αλλαγές όταν μια δυνατότητα μετακινείται σε διαφορετικό CSP. Εάν ένα επιλεγμένο CSP κλείσει, καθίσταται μείζον πρόβλημα, καθώς τα δεδομένα μπορούν να χαθούν ή δεν μπορούν να μεταφερθούν εγκαίρως σε άλλο CSP.

8. Αυξημένη πολυπλοκότητα επιβαρύνει το προσωπικό πληροφορικής. Η μετεγκατάσταση στο cloud μπορεί να εισαγάγει πολυπλοκότητα στις λειτουργίες πληροφορικής. Η διαχείριση, η ενσωμάτωση και η λειτουργία στο cloud μπορεί να απαιτήσει από το υπάρχον προσωπικό πληροφορικής του οργανισμού να μάθει ένα νέο μοντέλο. Το προσωπικό πληροφορικής πρέπει να διαθέτει την ικανότητα και το επίπεδο δεξιοτήτων για τη διαχείριση, την ενσωμάτωση και τη διατήρηση της μετανάστευσης περιουσιακών στοιχείων και δεδομένων στο cloud, πέραν των υφιστάμενων αρμοδιοτήτων του για την εσωτερική it.

Οι βασικές υπηρεσίες διαχείρισης και κρυπτογράφησης γίνονται πιο περίπλοκες στο cloud. Οι υπηρεσίες, οι τεχνικές και τα εργαλεία που είναι διαθέσιμα για την καταγραφή και την παρακολούθηση υπηρεσιών cloud συνήθως διαφέρουν μεταξύ των CSPs, αυξάνοντας περαιτέρω την πολυπλοκότητα. Ενδέχεται επίσης να υπάρχουν αναδυόμενες απειλές/κίνδυνοι στις υβριδικές υλοποιήσεις cloud λόγω της τεχνολογίας, των πολιτικών και των μεθόδων εφαρμογής, οι οποίες προσθέτουν πολυπλοκότητα. Αυτή η πρόσθετη πολυπλοκότητα οδηγεί σε αυξημένες δυνατότητες για κενά ασφαλείας στις υλοποιήσεις cloud και εσωτερικής εγκατάστασης ενός οργανισμού.

9. Εξουσιοδοτημένη πρόσβαση κατάχρησης εμπιστευτικών πληροφοριών. Οι εμπιστευτικές πληροφορίες, όπως το προσωπικό και οι διαχειριστές τόσο για οργανισμούς όσο και για CSPs, οι οποίοι καταχρώνται την εξουσιοδοτημένη πρόσβασή τους στα δίκτυα, τα συστήματα και τα δεδομένα του οργανισμού ή του CSP είναι μοναδικά τοποθετημένα για να προκαλέσουν ζημιά ή να αποπνέουν πληροφορίες.

Ο αντίκτυπος είναι πιθανότατα χειρότερος κατά τη χρήση του IaaS λόγω της ικανότητας ενός εκ των έσω να παρέχει πόρους ή να εκτελεί κακόβουλες δραστηριότητες που απαιτούν εγκληματολογία για ανίχνευση. Αυτές οι εγκληματολογικές δυνατότητες μπορεί να μην είναι διαθέσιμες με πόρους cloud.

10. Αποθηκευμένα δεδομένα χάνονται. Τα δεδομένα που είναι αποθηκευμένα στο cloud μπορούν να χαθούν για λόγους άλλους από κακόβουλες επιθέσεις. Η τυχαία διαγραφή δεδομένων από τον πάροχο υπηρεσιών cloud ή μια φυσική καταστροφή, όπως πυρκαγιά ή σεισμός, μπορεί να οδηγήσει σε μόνιμη απώλεια δεδομένων πελατών. Το βάρος της αποφυγής απώλειας δεδομένων δεν βαρύνει αποκλειστικά τους ώμους του παρόχου. Εάν ένας πελάτης κρυπτογραφήσει τα δεδομένα του πριν τα ανεβάσει στο cloud, αλλά χάσει το κλειδί κρυπτογράφησης, τα δεδομένα θα χαθούν. Επιπλέον, η ανεπαρκής κατανόηση του μοντέλου αποθήκευσης ενός CSP μπορεί να οδηγήσει σε απώλεια δεδομένων. Οι οργανισμοί πρέπει να εξετάσουν την ανάκτηση δεδομένων και να είναι προετοιμασμένοι για τη δυνατότητα απόκτησης του CSP τους, αλλαγής προσφορών υπηρεσιών ή πτώχευσης.

Αυτή η απειλή αυξάνεται καθώς ένας οργανισμός χρησιμοποιεί περισσότερες υπηρεσίες CSP. Η ανάκτηση δεδομένων σε ένα CSP μπορεί να είναι ευκολότερη από την ανάκτημά τους σε έναν οργανισμό, επειδή μια SLA ορίζει ποσοστά διαθεσιμότητας/χρόνου λειτουργίας. Τα ποσοστά αυτά θα πρέπει να διερευνώνται όταν ο οργανισμός επιλέγει CSP.

11. Εφοδιαστική αλυσίδα CSP τίθεται σε κίνδυνο. Εάν το CSP αναθέσει σε τρίτους τμήματα της υποδομής, των λειτουργιών ή της συντήρησής του, αυτά τα τρίτα μέρη ενδέχεται να μην πληρούν/υποστηρίξουν τις απαιτήσεις που έχει συνάψει ο CSP για την παροχή ενός οργανισμού. Ένας οργανισμός πρέπει να αξιολογήσει τον τρόπο με τον οποίο το CSP επιβάλλει τη συμμόρφωση και να ελέγξει αν το CSP ρέει τις δικές του απαιτήσεις σε τρίτους. Εάν οι απαιτήσεις δεν επιβάλλονται στην αλυσίδα εφοδιασμού, τότε η απειλή για τον οργανισμό αυξάνεται.

Αυτή η απειλή αυξάνεται καθώς ένας οργανισμός χρησιμοποιεί περισσότερες υπηρεσίες CSP και εξαρτάται από μεμονωμένα CSPs και τις πολιτικές εφοδιαστικής αλυσίδας.

12. Ανεπαρκής δέουσα επιμέλεια αυξάνει τον κίνδυνο κυβερνοασφάλειας. Οι οργανισμοί που μεταναστεύουν στο cloud συχνά εκτελούν ανεπαρκή δέουσα επιμέλεια. Μεταφέρουν δεδομένα στο cloud χωρίς να κατανοούν το πλήρες πεδίο εφαρμογής τους, τα μέτρα ασφαλείας που χρησιμοποιούνται από το CSP και τη δική τους ευθύνη για την παροχή μέτρων ασφαλείας. Λαμβάνουν αποφάσεις για τη χρήση υπηρεσιών cloud χωρίς να κατανοούν πλήρως τον τρόπο με τον οποίο πρέπει να διασφαλίζονται αυτές οι υπηρεσίες.

Αναδίπλωση και κοιτάζοντας μπροστά

Είναι σημαντικό να θυμόμαστε ότι οι CSPs χρησιμοποιούν ένα μοντέλο κοινής ευθύνης για την ασφάλεια. Το CSP αναλαμβάνει την ευθύνη για ορισμένες πτυχές της ασφάλειας. Άλλες πτυχές της ασφάλειας μοιράζονται μεταξύ του CSP και του καταναλωτή. Τέλος, ορισμένες πτυχές της ασφάλειας παραμένουν αποκλειστική ευθύνη του καταναλωτή. Η αποτελεσματική ασφάλεια στο cloud εξαρτάται από τη γνώση και την εκπλήρωση όλων των ευθυνών των καταναλωτών. Η αδυναμία των καταναλωτών να κατανοήσουν ή να ανταποκριθούν στις ευθύνες τους αποτελεί κύρια αιτία συμβάντων ασφάλειας σε συστήματα που βασίζονται στο cloud.

Σε αυτήν την ανάρτηση ιστολογίου, έχουμε εντοπίσει πέντε μοναδικές στο cloud και επτά απειλές cloud και εσωτερικής εγκατάστασης που αντιμετωπίζουν οι οργανισμοί καθώς εξετάζουν το ενδεχόμενο μετεγκατάστασης των δεδομένων και των περιουσιακών στοιχείων τους στο cloud. Στην επόμενη ανάρτηση αυτής της σειράς,θα διερευνήσουμε μια σειρά βέλτιστων πρακτικών που αποσκοπούν στο να βοηθήσουν τους οργανισμούς να μεταφέρουν με ασφάλεια δεδομένα και εφαρμογές στο cloud.

3 Ιδιωτικότητα και προσωπικά δεδομένα στο Cloud Computing

3.1 Η έννοια της ιδιωτικότητας

Οι χρήστες των δικτυακών υπηρεσιών συχνά θεωρούν την προστασία των δεδομένων ως μέρος των υπηρεσιών ασφάλειας των πληροφοριακών συστημάτων. Η προσέγγιση αυτή είναι εντελώς εσφαλμένη, διότι οι έννοιες της ιδιωτικής ζωής και της ασφάλειας των πληροφοριών είναι πολύ στενά συνυφασμένες.

Πρέπει να ληφθεί υπόψη, ότι η ιδιωτική ζωή είναι μια άλλη σφαίρα και, όπως και κάθε άλλη έννοια, απαιτεί ειδική μεταχείριση με βάση την πολιτιστική, εθνική, εθιμική και ηθική προέλευση του θεατή. Βασίζεται στις δημόσιες και νομικές προσδοκίες και δεν διαθέτει έναν γενικά αποδεκτό ορισμό. Η προστασία των δεδομένων είναι αυτό που ονομάζουμε ιδιωτικότητα.

Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), ο όρος ορίζεται ως «κάθε πληροφορία που αφορά ένα αναγνωρίσιμο ή προσδιορίσιμο άτομο (υποκείμενο των δεδομένων)». Η προστασία σας αφορά τα δικαιώματα ή τις υποχρεώσεις σας σε σχέση με τη συλλογή, την επεξεργασία, τη γνωστοποίηση, την αποθήκευση και την καταστροφή των προσωπικών σας δεδομένων..

Με απλά λόγια, όταν μιλάμε για τη διασφάλιση της εμπιστευτικότητας των επικοινωνιών και την προστασία των προσωπικών δεδομένων στο νέφος, μιλάμε για την εταιρική ευθύνη απέναντι στους τελικούς χρήστες. Επίσης, ελέγξτε το επίπεδο διαφάνειας που

χαρακτηρίζει τις πολιτικές του οργανισμού σας'όσον αφορά τη διαχείριση των προσωπικών πληροφοριών.

Αυτός είναι ο ορισμός του Αμερικανικού Ινστιτούτου Ορκωτών Λογιστών (AICPA) και του Καναδικού Ινστιτούτου Ορκωτών Λογιστών (CICA). Σύμφωνα με τα αποδεκτά γενικά πρότυπα προστασίας της ιδιωτικής ζωής, αυτό περιγράφεται ως GAPP και Προσωπικά Δεδομένα. "Συλλογή, χρήση, διατήρηση και αποκάλυψη προσωπικών δεδομένων και τα δικαιώματα και οι υποχρεώσεις των ατόμων και των οργανισμών". (Mather T.; Kumaraswamy S.;Latif S, 2009)

3.2 Το Data Life Cycle Management

Για να γίνει κατανοητό το DLM, είναι απαραίτητο να γνωρίζει κάποιος, τις φάσεις του κύκλου ζωής των δεδομένων. Παρόλο που δεν υπάρχει βιομηχανικό πρότυπο για DLM επιχειρήσεων, οι περισσότεροι ειδικοί συμφωνούν ότι ο κύκλος ζωής των δεδομένων περιλαμβάνει αυτά τα έξι στάδια: δημιουργία, αποθήκευση, χρήση, κοινή χρήση, αρχειοθέτηση και καταστροφή.

3.2.1 Στάδιο 1: Δημιουργία δεδομένων

Η απόκτηση και η καταγραφή δεδομένων πραγματοποιείται στην αρχή του κύκλου, όταν ένας επιχειρηματικός οργανισμός αποκτά νέες, ελεγμένες πληροφορίες, συμπεριλαμβανομένης της εσωτερικής δημιουργίας δεδομένων, της αγοράς δεδομένων τρίτων και τη συλλογή δεδομένων καθώς ρέει από εφαρμογές. Τα δεδομένα δημιουργούνται σε πολλές μορφές, συμπεριλαμβανομένων εγγράφων του Word, υπολογιστικών φύλλων Excel, PDF, email, κειμένων, εικόνων και άλλων.

3.2.2 Στάδιο 2: Αποθήκευση δεδομένων

Η αποθήκευση δεδομένων στο DLM αναφέρεται στην εφαρμογή πλεονασμάτων και στρατηγικών ασφάλειας σε ενεργά δεδομένα (έναντι ανενεργών δεδομένων που αρχειοθετούνται), καθώς και στην αποθήκευση δεδομένων με τέτοιο τρόπο ώστε να μην μπορεί να τροποποιηθεί κατά λάθος. Η αποθήκευση δεδομένων πρέπει να συμμορφώνεται με τις συμβάσεις και την κανονιστική νομοθεσία. Αυτό μπορεί να σημαίνει μόνο αποθήκευση σε διακομιστές ή μόνο αποθήκευση αντιγράφων ασφαλείας σε κρυπτογραφημένους δίσκους.

Σε αυτό το στάδιο, τα αποθηκευμένα δεδομένα είναι προσβάσιμα μόνο στο εκχωρημένο προσωπικό. Είναι συνηθισμένο να καθορίζεται η ευαισθησία των δεδομένων,

συμπεριλαμβανομένων ιδιωτικών, ευαίσθητων, περιορισμένων ή δημόσιων. Αυτό προστατεύει την πνευματική ιδιοκτησία του οργανισμού καθώς και τις σχέσεις με τους πελάτες.

Αυτό το στάδιο διαχειρίζεται επίσης σχέδια ανάκτησης δεδομένων. Σε περίπτωση αποτυχίας, οι οργανισμοί θα πρέπει να έχουν ένα σχέδιο για τη συνέχιση της πρόσβασης στα δεδομένα, όπως ένα προσωρινό αντίγραφο ασφαλείας σε ένα ιεραρχικό σύστημα διαχείρισης αποθήκευσης.

3.2.2.1 Ιεραρχική Διαχείριση Αποθήκευσης (HSM)

Το HSM είναι ένας τύπος προϊόντος DLM. Η ιεραρχία αντιπροσωπεύει διαφορετικούς τύπους μέσων αποθήκευσης, όπως συστήματα RAID (περιττή σειρά ανεξάρτητων δίσκων), οπτική αποθήκευση ή ταινία, κάθε τύπος αντιπροσωπεύει ένα διαφορετικό επίπεδο κόστους και ταχύτητας ανάκτησης όταν απαιτείται πρόσβαση. Χρησιμοποιώντας ένα προϊόν HSM, ένας διαχειριστής μπορεί να καθορίσει οδηγίες για το πόσο συχνά πρέπει να αντιγραφούν διαφορετικά είδη αρχείων σε εφεδρική συσκευή αποθήκευσης. Μόλις οριστεί η κατευθυντήρια γραμμή, το λογισμικό HSM διαχειρίζεται τα πάντα αυτόματα. Συνήθως, οι εφαρμογές HSM μεταφέρουν δεδομένα με βάση το χρονικό διάστημα από την τελευταία πρόσβαση, ενώ οι εφαρμογές DLM επιτρέπουν πολιτικές που βασίζονται σε πιο πολύπλοκα κριτήρια.

3.2.3 Στάδιο 3: Χρήση δεδομένων

Σε αυτό το στάδιο, η χρήση δεδομένων διασφαλίζει ότι η εγγραφή πληροί ορισμένες επικυρώσεις για να είναι προσβάσιμη για τους χρήστες. Όσον αφορά τη χρήση δεδομένων, το DLM καθορίζει ποιος μπορεί να χρησιμοποιήσει τα δεδομένα και για ποιους σκοπούς.

3.2.4 Στάδιο 4: Κοινή χρήση δεδομένων

Όταν δημοσιεύονται δεδομένα, μπορούν να διατίθενται σε άτομα εκτός του συστήματος ενός οργανισμού, όπως ένα τιμολόγιο που χρησιμοποιεί δεδομένα πελατών ως αρχείο. Τα δεδομένα μοιράζονται συνεχώς. Εργαζόμενοι, χρήστες, πελάτες, φίλοι, στελέχη και μέλη του διοικητικού συμβουλίου είτε μοιράζονται δεδομένα στις πλατφόρμες που παρέχονται είτε με άλλες μεθόδους. Όσο περισσότερα άτομα μοιράζονται δεδομένα μέσω ανεπίσημων μεθόδων, τόσο μεγαλύτερος είναι ο κίνδυνος να μην συμμορφώνονται με τους κανόνες διακυβέρνησης και νομικούς ή πολιτικούς.

3.2.5 Στάδιο 5: Αρχειοθέτηση δεδομένων

Σε αυτό το στάδιο, τα δεδομένα υποβάλλονται σε αρχειακή διαδικασία που διασφαλίζει τον πλεονασμό. Τα ενεργά αρχεία είναι μια ιδανική μέθοδος αποθήκευσης για οργανισμούς που τείνουν να αποθηκεύουν μεγάλο όγκο δεδομένων και που χρειάζονται πρόσβαση στις πληροφορίες κατά καιρούς. Τα αρχειοθετημένα δεδομένα δεν είναι ενεργά. Έτσι, μπορεί να αποθηκευτεί σε μονάδες δίσκου που δεν βρίσκονται στο δίκτυο, αλλά είναι προσβάσιμες για ad hoc αναφορές και αναλύσεις. Οι στρατηγικές DLM καθορίζουν πότε, πού και για πόσο χρονικό διάστημα μπορούν να αρχειοθετηθούν τα δεδομένα. Αυτό θα διαφέρει ανάλογα με το ποια είναι τα δεδομένα. Μπορεί να είναι κάτι που έχει νομικούς κανονισμούς, όπως προσωπικά, ερευνητικά ή ιατρικά δεδομένα, ή μπορεί να είναι απλά εσωτερικά έγγραφα της εταιρείας.

3.2.6 Στάδιο 6: Καταστροφή δεδομένων

Στο τελικό στάδιο του κύκλου ζωής, τα δεδομένα καθαρίζονται από τα αρχεία και καταστρέφονται.(Xiaojun Yu. , 2010).

3.3 Προβληματισμοί σχετικά με την ιδιωτικότητα στις υπηρεσίες υπολογιστικού νέφους

Η αλήθεια είναι ότι εγείρονται πολλά και διαφορά ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων, όταν αυτά εκτίθενται σε περιβάλλον υπολογιστικού νέφους. Οι προβληματισμοί αυτοί σχετίζονται και διαμορφώνονται κατά κάποιο τρόπο από των συνδυασμό θεμάτων ασφάλειας των πληροφοριακών συστημάτων και της ιδιωτικότητας. Παρακάτω, γίνεται προσπάθεια να αναφερούμε σε κάποιους από αυτούς τους προβληματισμούς

Πρόσβαση: Ο κάτοχος των δεδομένων έχει το δικαίωμα να γνωρίζει προσωπικά στοιχεία και σε ορισμένες περιπτώσεις να ζητήσει παραίτηση. Αυτό εξηγείται ξεκάθαρα από το νόμο. 3471/2006 και το νόμο 2472/97. Πρέπει να σημειωθεί ότι αυτοί οι κανόνες παίζουν σημαντικό ρόλο στην ανάπτυξη της διαφήμισης και άλλων επιχειρηματικών δραστηριοτήτων, κατά κανόνα, οι κανόνες ενσωματώνονται πλήρως στην πολιτική απορρήτου που παρέχει ο καθένας. Ειδικότερα, σε σχέση με το περιβάλλον Cloud, δημιουργείται η ανησυχία σχετικά με την

ικανότητα του οργανισμού να παρέχει όλες τις απαραίτητες πληροφορίες στον πελάτη της – ιδιοκτήτη των δεδομένων σχετικά με τα μέτρα του οργανισμού για τη συμμόρφωσή του με τις νομικές του δεσμεύσεις.

Δημιουργείται, λοιπόν, το ερώτημα αναφορικά με το τι γίνεται σχετικά με το δικαίωμα του ενδιαφερόμενου να ζητήσει από τον οργανισμό να καταστρέψει τα προσωπικά του στοιχεία του και πως μπορεί αυτός να εξασφαλίσει ότι όλες οι πληροφορίες του υποκειμένου έχουν διαγραφεί από το Cloud.

Συμμόρφωση: Μια σειρά προβληματισμών δημιουργείται με αυτό που ονομάζουμε συμμόρφωση προς τη νομοθεσία του ιδιωτικού απορρήτου. Συγκεκριμένα, αυτά συνοψίζονται στα παρακάτω:

- Ποιες είναι οι απαιτήσεις συμμόρφωσης αναφορικά με την εξασφάλιση ιδιωτικού απορρήτου σε περιβάλλον cloud;
- Ποια είναι η ισχύουσα νομοθεσία, οι κανονισμοί, τα πρότυπα και οι συμβατικές δεσμεύσεις που ρυθμίζουν το κύκλο ζωής των πληροφοριών αυτών;
- Ποιος είναι υπεύθυνος για τη τήρηση και την εφαρμογή των νομικών και άλλων δεσμεύσεων;
- Πώς η υφιστάμενη δομή εξασφαλίζει την τήρηση του απορρήτου;
- Πως ενσωματώνεται στην πολιτική των εταιριών, το γεγονός ότι οι υποδομές cloud, είναι αντικείμενα πολλών, και κάποιες φορές αντικρουόμενων, εθνικών και υπερεθνικών ρυθμίσεων δεδομένης μάλιστα και της γεωγραφικής διασποράς τους σε διαφορετικές χώρες; Για παράδειγμα, ποιο δικαστήριο είναι αρμόδιο και ποια νομοθεσία θα πρέπει να εφαρμοστεί στην περίπτωση που τα δεδομένα χρησιμοποιούνται στην Ελλάδα αλλά αποθηκεύονται στις ΗΠΑ;

Αποθήκευση: Οι ερωτήσεις αποθήκευσης δεδομένων αφορούν το πού αποθηκεύονται, ποιος "αποθηκεύεται" στο κέντρο δεδομένων και σε άλλες χώρες και αν τα δεδομένα διαφορετικών μερών που είναι αποθηκευμένα στο ίδιο σύννεφο είναι "μπερδεμένα". Τι γίνεται με την ελληνική νομοθεσία για τη διασφάλιση του απορρήτου των επικοινωνιών; Οι πράξεις L.3674 / 2008, L.3471 / 2006, L.3431 / 2006 και L.3115 / 2003 επιβάλλουν περιορισμούς στη μεταφορά προσωπικών δεδομένων σε οργανισμούς άλλων χωρών; Αυτό το ερώτημα προκύπτει επειδή υπάρχει η πιθανότητα τα δεδομένα που είναι αποθηκευμένα στο cloud να

μεταφερθούν σε άλλες χώρες χωρίς να είναι γνωστά στον χρήστη. Σε αυτήν την περίπτωση, πρόκειται για παραβίαση της εθνικής νομοθεσίας.

Διατήρηση : Μια παράμετρος που πρέπει να λάβετε υπόψη είναι το πόσο καιρό πρέπει να αποθηκευτούν τα προσωπικά δεδομένα που πρόκειται να μεταφερθούν για να διαγραφούν. Ειδικότερα, πρέπει να εξεταστεί η πολιτική αποθήκευσης που διέπει αυτά τα δεδομένα. Ποιος κατέχει τα πραγματικά δεδομένα, ποιος είναι ο οργανισμός πελατών ή ο πάροχος cloud, ποιος είναι υπεύθυνος για τις πολιτικές αποθήκευσης δεδομένων και ποιες εγγυήσεις δίνονται για την προστασία των δικαιωμάτων των ατόμων;

Καταστροφή: Στην έννοια αυτή, οι προβληματισμοί έγκειται στο με ποια μέθοδο ο πάροχος του cloud οδηγεί τα προσωπικά δεδομένα στην καταστροφή, μετά το πέρας της περιόδου υποχρεωτικής διακράτησης και στον τρόπο που αυτά όντως θα καταστραφούν και δεν θα πέσουν στα χέρια τρίτων προς εκμετάλλευση. Στο σημείο αυτό να αναφερεί ότι πρέπει να εξασφαλιστεί ότι δεν διατηρούνται κρυφά αντίγραφα ασφαλείας που θα διατεθούν προς εμπορικούς σκοπούς.

Να σημειωθεί, ότι για την επίτευξης της μεγίστης διαθεσιμότητας πολλοί πάροχοι του cloud παρέχουν την υπηρεσία replication, η οποία συνιστάται στην αυτόματη αναπαραγωγή/αποθήκευση της πληροφορίας σε πολλαπλά συστήματα ή και τοποθεσίες. Το Replication μετατρέπεται σε πρόκληση, όταν ο οργανισμός προσπαθεί να καταστρέψει τα δεδομένα. Δημιουργείται λοιπόν το ερώτημα αν μπορούμε να καταστρέψουμε αποτελεσματικά το σύνολο των δεδομένων όταν αυτά μεταναστεύσουν στο Cloud. Ο πάροχος του cloud πραγματικά καταστρέφει τα δεδομένα η απλά τα κάνει απροσπέλαστα για τον πελάτη του;

3.4 Η ευθύνη για τη προστασία του απορρήτου

Υπάρχουν αντικρουόμενες απόψεις σχετικά με το ποιος φορέας είναι υπεύθυνος για την ασφάλεια και το ιδιωτικό απόρρητο. Η νομική και αλλά και η επιστημονική κοινότητα θεωρούν πως η ευθύνη αυτή ανήκει στους παρόχους των υποδομών Cloud.

Δυστυχώς, είναι νομικά αδυνατή η μεταβίβαση της αστικής ευθύνης μέσω συμβατικών συμφωνιών, επομένως αδύνατη είναι και η μεταφορά της απαίτησης για λογοδοσία.

Η ασφάλεια των δεδομένων ανήκει στις υποχρεώσεις της οργάνωσης που συλλέγει τα δεδομένα. Η κλοπή των στοιχείων της ταυτότητας και της χρήσης της σε μη εξουσιοδοτημένες

ενέργειες (χαρακτηριστικό παράδειγμα που όλοι γνωρίζουμε η έκδοση Πιστωτικής Κάρτας) είναι μόνο ένα παράδειγμα του τι μπορεί να συμβεί σε περίπτωση διάρρηξης της ιδιωτικότητας. Αν κάτι τέτοιο συμβεί σε περιβάλλον Cloud, τότε οι ευθύνες θα αναζητηθούν από αυτόν που πήρε την απόφαση για την επιλογή του παρόχου του cloud και την μεταφορά των δεδομένων σε αυτό. Συμπερασματικά, καταλήγουμε στο ότι είναι ευθύνη του οργανισμού να λαμβάνει όλες της απαραίτητες μέριμνες για την διασφάλιση των δεδομένων των χρηστών. Στην πραγματικότητα η αποτελεσματική διαχείριση των προσωπικών δεδομένων απαιτεί την ύπαρξη μια ομάδας νομικών και τεχνικών, με ειδίκευση στις ιδιαιτερότητες των δομών Cloud Computing (Xiaojun Yu. , 2010).

4 Ασφάλεια στο Cloud Computing

4.1 Γενικά για την ασφάλεια Cloud

Η ασφάλεια στο cloud είναι το σύνολο στρατηγικών και πρακτικών για την προστασία δεδομένων και εφαρμογών που φιλοξενούνται στο cloud. Όπως η ασφάλεια στον κυβερνοχώρο, η ασφάλεια στο cloud είναι μια πολύ ευρεία περιοχή και δεν είναι ποτέ δυνατό να αποτραπεί κάθε ποικιλία επιθέσεων. Ωστόσο, μια καλά σχεδιασμένη στρατηγική ασφάλειας στο cloud μειώνει σημαντικά τον κίνδυνο επιθέσεων στον κυβερνοχώρο.

Ακόμα και με αυτούς τους κινδύνους, το cloud computing είναι συχνά πιο ασφαλές από τον υπολογισμό επί τόπου. Οι περισσότεροι πάροχοι cloud διαθέτουν περισσότερους πόρους για τη διατήρηση των δεδομένων με ασφάλεια από τις μεμονωμένες επιχειρήσεις, πράγμα που επιτρέπει στους παρόχους cloud να διατηρούν ενημερωμένη την υποδομή και να επιδιορθώνουν τα τρωτά σημεία το συντομότερο δυνατό. Μια μεμονωμένη επιχείρηση, από την άλλη πλευρά, μπορεί να μην έχει αρκετούς πόρους για να εκτελεί με συνέπεια αυτές τις εργασίες. Οι περισσότεροι κίνδυνοι ασφάλειας στο cloud εντάσσονται σε μία από αυτές τις γενικές κατηγορίες:

- Τα δεδομένα εκτίθενται ή διαρρέουν
- Ένας μη εξουσιοδοτημένος χρήστης εκτός του οργανισμού έχει πρόσβαση σε εσωτερικά δεδομένα

- Ένας εσωτερικός, εξουσιοδοτημένος χρήστης έχει υπερβολική πρόσβαση σε εσωτερικά δεδομένα
- Μια κακόβουλη επίθεση, όπως μια επίθεση DDoS ή μια μόλυνση από κακόβουλο λογισμικό , ακρωτηριάζει ή καταστρέφει την υποδομή του cloud

Ο στόχος μιας στρατηγικής ασφάλειας cloud είναι να μειώσει όσο το δυνατόν περισσότερο την απειλή από αυτούς τους κινδύνους, προστατεύοντας τα δεδομένα, διαχειριζόμενος τον έλεγχο ταυτότητας και την πρόσβαση των χρηστών και παραμένοντας σε λειτουργία ενάντια σε μια επίθεση.

4.2 Τεχνολογίες ασφάλειας πληροφοριών

Μια στρατηγική ασφάλειας cloud θα πρέπει να περιλαμβάνει όλες τις ακόλουθες τεχνολογίες:

4.2.1 Κρυπτογράφηση (Encryption)

Η κρυπτογράφηση είναι ένας τρόπος ανακατεύθυνσης δεδομένων, έτσι ώστε μόνο τα εξουσιοδοτημένα μέρη να μπορούν να κατανοήσουν τις πληροφορίες. Εάν ένας εισβολέας εισβάλει στο σύννεφο μιας εταιρείας και εντοπίσει μη κρυπτογραφημένα δεδομένα, είναι σε θέση να κάνει οποιαδήποτε κακόβουλη ενέργεια με τα δεδομένα: να τα διαρρεύσει, να τα πουλήσει, να τα χρησιμοποιήσει για να πραγματοποιήσει περαιτέρω επιθέσεις κ.λπ. Ωστόσο, εάν τα δεδομένα της εταιρείας είναι κρυπτογραφημένο, ο εισβολέας θα βρει μόνο ανακατεμένα δεδομένα που δεν μπορούν να χρησιμοποιηθούν εκτός εάν ανακαλύψουν με κάποιο τρόπο το κλειδί αποκρυπτογράφησης (κάτι που θα πρέπει να είναι σχεδόν αδύνατο). Με αυτόν τον τρόπο, η κρυπτογράφηση βοηθά στην αποφυγή διαρροής και έκθεσης δεδομένων, ακόμη και όταν αποτυγχάνουν άλλα μέτρα ασφαλείας.

Τα δεδομένα μπορούν να κρυπτογραφηθούν τόσο σε κατάσταση ηρεμίας (όταν αποθηκεύονται) όσο και σε μεταφορά (ενώ αποστέλλονται από το ένα μέρος στο άλλο). Τα δεδομένα του νέφους θα πρέπει να κρυπτογραφούνται τόσο σε ηρεμία όσο και κατά τη μεταφορά, έτσι ώστε οι επιτιθέμενοι να μην μπορούν να τα υποκλέψουν και να τα διαβάσουν. Η κρυπτογράφηση δεδομένων κατά τη μεταφορά θα πρέπει να αφορά τόσο τα δεδομένα που ταξιδεύουν μεταξύ ενός σύννεφου και ενός χρήστη, όσο και τα δεδομένα που ταξιδεύουν από το ένα σύννεφο στο άλλο, όπως σε περιβάλλον πολλαπλών σύννεφων ή υβριδικών σύννεφων.

Επιπλέον, τα δεδομένα πρέπει να κρυπτογραφούνται όταν αποθηκεύονται σε βάση δεδομένων ή μέσω υπηρεσίας αποθήκευσης cloud.

Εάν τα σύννεφα σε περιβάλλον πολλαπλών σύννεφων ή υβριδικών σύννεφων είναι συνδεδεμένα στο επίπεδο δικτύου, ένα VPN μπορεί να κρυπτογραφήσει την κίνηση μεταξύ τους. Εάν είναι συνδεδεμένα στο επίπεδο εφαρμογής, θα πρέπει να χρησιμοποιηθεί κρυπτογράφηση SSL/TLS. Το SSL / TLS θα πρέπει επίσης να κρυπτογραφεί την κίνηση μεταξύ ενός χρήστη και ενός σύννεφου (δείτε Τι είναι το HTTPS;).

4.2.2 Διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management):

Τα προϊόντα ταυτότητας και διαχείρισης πρόσβασης (IAM) παρακολουθούν ποιος είναι ο χρήστης και τι επιτρέπεται να κάνουν και εξουσιοδοτούν τους χρήστες και αρνούνται την πρόσβαση σε μη εξουσιοδοτημένους χρήστες, όπως απαιτείται. Το IAM είναι εξαιρετικά σημαντικό στο cloud computing επειδή η ταυτότητα και τα δικαιώματα πρόσβασης ενός χρήστη καθορίζουν εάν μπορούν να έχουν πρόσβαση σε δεδομένα και όχι στη συσκευή ή την τοποθεσία του χρήστη.

Το IAM βοηθά στη μείωση των απειλών μη εξουσιοδοτημένων χρηστών που αποκτούν πρόσβαση σε εσωτερικά περιουσιακά στοιχεία και εξουσιοδοτημένων χρηστών που υπερβαίνουν τα προνόμιά τους. Η σωστή λύση IAM θα βοηθήσει στον μετριασμό πολλών ειδών επιθέσεων, συμπεριλαμβανομένης της εξαγοράς λογαριασμού και της επίθεσης εσωτερικών πληροφοριών (όταν ένας χρήστης ή υπάλληλος καταχραστεί την πρόσβασή του προκειμένου να εκθέσει δεδομένα).

Το IAM μπορεί να περιλαμβάνει πολλές διαφορετικές υπηρεσίες ή μπορεί να είναι μια ενιαία υπηρεσία που συνδυάζει όλες τις ακόλουθες δυνατότητες:

- Οι πάροχοι ταυτότητας (IdP) πιστοποιούν την ταυτότητα χρήστη
- Οι υπηρεσίες μεμονωμένης σύνδεσης (SSO) βοηθούν στον έλεγχο ταυτότητας χρηστών για πολλές εφαρμογές, έτσι ώστε οι χρήστες να πρέπει να συνδεθούν μόνο μία φορά για πρόσβαση σε όλες τις υπηρεσίες cloud τους

- Οι υπηρεσίες ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) ενισχύουν τη διαδικασία ελέγχου ταυτότητας χρήστη
- Οι υπηρεσίες ελέγχου πρόσβασης επιτρέπουν και περιορίζουν την πρόσβαση των χρηστών

4.2.3 Τείχος προστασίας (Firewall)

Ένα τείχος προστασίας cloud παρέχει ένα επίπεδο προστασίας γύρω από τα περιουσιακά στοιχεία του cloud, αποκλείοντας την κακόβουλη κυκλοφορία ιστού. Σε αντίθεση με τα παραδοσιακά τείχη προστασίας , τα οποία φιλοξενούνται επί τόπου και προστατεύουν την περίμετρο του δικτύου, τα τείχη προστασίας σύννεφων φιλοξενούνται στο σύννεφο και αποτελούν ένα εικονικό εμπόδιο ασφαλείας γύρω από την υποδομή του νέφους. Τα περισσότερα τείχη προστασίας εφαρμογών ιστού ανήκουν σε αυτήν την κατηγορία.

Τα τείχη προστασίας νέφους αποκλείουν επιθέσεις DDoS, κακόβουλη δραστηριότητα bot και εκμεταλλεύσεις ευπάθειας. Αυτό μειώνει τις πιθανότητες μιας κυβερνοεπίθεσης να καταστρέψει την υποδομή cloud ενός οργανισμού.

4.3 Ασφάλεια πληροφοριών

Αναφέρθηκε παραπάνω ότι οι περισσότερες επιχειρήσεις χρησιμοποιούν το Cloud Computing, τις περισσότερες φορές με τη μέθοδο της χρονικής μίσθωσης, για να έχουν μειωμένα κόστη όταν θέλουν να αποκτήσουν χώρο για την αποθήκευση πληροφοριών. Έχει αποδειχτεί ότι αυτή η μέθοδος είναι όντως η φθηνότερη, είναι όμως και η ασφαλέστερη; Γίνεται εύκολα αντιληπτό, ότι η ασφάλεια θεωρείται μείζον ζήτημα για την κάθε εταιρεία και τους υπαλλήλους της. Για γίνει κατανοητό το ζήτημα της ασφάλειας στα συστήματα υπολογιστικού νέφους πρέπει να γίνει κατανοητή η δομή του συστήματος.

Τα περισσότερα ζητήματα ασφάλειας που προκύπτουν στο Cloud Computing είναι αποτέλεσμα της έλλειψης ελέγχου πάνω στη δομή από τη μεριά του χρήστη ή της επιχείρησης. Και αυτό συμβαίνει γιατί οι πιο πολλές επιχειρήσεις δε ξέρουν που αποθηκεύονται τα δεδομένα τους και τι είδους μηχανισμοί ενεργοποιούνται για να τα προστατέψουν.

Σε σχετική μελέτη που διενεργήθηκε (Jensen et al) παρουσιάστηκαν μεν τα τεχνικά ζητήματα ασφαλείας στο Cloud Computing, ωστόσο διαπιστώθηκε πως τα προβλήματα παρουσιάζονται περισσότερο στις υπηρεσίες δικτύου και των προγραμμάτων περιήγησης στο

δίκτυο παρά με το Νέφος και τον τρόπο που αυτό λειτουργεί. Τα ζητήματα αυτά είναι εξίσου πολύ σημαντικά, μιας και το χρησιμοποιεί εκτεταμένα τις υπηρεσίες δικτύου ενώ οι χρήστες του κάνουν χρήση των προγραμμάτων περιήγησης (Jensen et al., 2009). Η ασφάλεια των προγραμμάτων αυτών είναι σημαντικό ζήτημα στο Cloud Computing γιατί οι υπολογισμοί γίνονται σε απομακρυσμένους servers και ο περιφερειακός υπολογιστής client χρησιμοποιείται μόνο για τις μεταβιβάσεις των πληροφοριών (I/O) και να πιστοποιεί τις εντολές στο Νέφος. Η χρήση τω προγραμμάτων περιήγησης δημιούργησε την αμφιβολία της ασφάλειας.

Το TLS (Transport Layer Security – Ασφάλεια Μεταφοράς σε Επίπεδα) είναι σημαντικό σε αυτό το επίπεδο αφού χρησιμοποιείται για τη πιστοποίηση και τη κρυπτογράφηση δεδομένων. Ειδικότερα, η κωδικοποίηση XML δε μπορεί να χρησιμοποιηθεί αμέσως από το πρόγραμμα περιήγησης καθώς η κωδικοποίηση μπορεί να επιτευχθεί μόνο μέσω του TLS. Άρα συμπεραίνουμε ότι τα προγράμματα περιήγησης λειτουργούν ως «παθητικές αποθήκες δεδομένων» (Jensen et al., 2009).

Επιπλέον, είναι σημαντικό να γίνει κατανοητή η εξάρτηση μεταξύ των μοντέλων Νέφους. Οι έλεγχοι ασφαλείας στο Cloud Computing δεν διαφέρουν από αυτούς σε ένα περιβάλλον πληροφοριακού συστήματος. Ωστόσο, χρησιμοποιεί διαφορετικά μοντέλα υπηρεσίας, λειτουργικά μοντέλα και τεχνολογίες, παρουσιάζει διαφορετικά ρίσκα για μια επιχείρηση. Επομένως, μπορούμε να μιλήσουμε για ασφάλεια στις εγκαταστάσεις (φυσική ασφάλεια), με τη δομή του δικτύου της (ασφάλεια δικτύου), με το πληροφοριακό σύστημα της και με τις υπόλοιπες εφαρμογές που χρησιμοποιεί. Από αυτό καταλήγουμε ότι ο χρήστης είναι τελικά αυτός που έχει μεγαλύτερη ευθύνη.

Στο σημείο αυτό, είναι πολύ σημαντικό να γίνουν κατανοητές οι διαφορές μεταξύ των μοντέλων υπηρεσιών για τη στάση διαχείρισης ρίσκου των επιχειρήσεων. Σύμφωνα με τη Cloud Computer Alliance (2009), πέρα από την αρχιτεκτονική, υπάρχουν κάποιοι ακόμη παράγοντες που πρέπει να ληφθούν υπόψη όταν γίνεται αναφορά στην ασφάλεια ενός Νέφους. Αυτοί οι παράγοντες χωρίζονται σε δύο τομείς: τον Τομέα Διακυβέρνησης και τον Επιχειρησιακό Τομέα.

Ο τομέας Διακυβέρνησης αντιμετωπίζει τα στρατηγικά ζητήματα εντός του περιβάλλοντος Νέφους, ενώ ο Επιχειρησιακός Τομέας ασχολείται με πιο βραχυπρόθεσμα ζητήματα ασφαλείας και ζητήματα εφαρμογής των ποικιλιών αρχιτεκτονικής.

Ειδικότερα, ο Τομέας Διακυβέρνησης περιλαμβάνει:

1. Διακυβέρνηση και διαχείριση επιχειρηματικού ρίσκου: Ασχολείται με την ικανότητα του οργανισμού να μετράει το επιχειρηματικό ρίσκο που δημιουργείται από το Cloud Computing. Αντιμετωπίζει ζητήματα νομικά όπως την ευθύνη να προστατεύει ευαίσθητα δεδομένα.

2. Νομική και ηλεκτρονική κάλυψη: Ασχολείται με τα νομικά ζητήματα που προκύπτουν όταν μια επιχείρηση κάνη χρήση υπηρεσιών Νέφους.

3. Συμβατότητα και λογιστικός έλεγχος: Αφορά τη διατήρηση και παροχή συμβατότητας.

4. Διαχείριση κύκλου ζωής των πληροφοριών: Ασχολείται με τη διαχείριση των δεδομένων που παραμένουν στο Νέφος

5. Φορητότητα και διαλειτουργικότητα: Αφορά τη μεταφορά δεδομένων από έναν πάροχο σε έναν άλλο.

Ο Επιχειρησιακός Τομέας περιλαμβάνει:

- Παραδοσιακή ασφάλεια, επιχειρησιακή συνοχή και ανάκτηση πληροφοριών: Επικεντρώνεται στα ρίσκα που λαμβάνονται από τις υπηρεσίες Νέφους αναλογικά πάντα με τις προσδοκίες της επιχείρησης για καλύτερη διαχείριση του ρίσκου.
- Λειτουργίες του κέντρου πληροφοριών: Ασχολείται με την αξιολόγηση του κέντρου πληροφοριών του παρόχου.
- Αντιμετώπιση περιστατικών, ειδοποιήσεις και αποκατάσταση. Εξετάζει τα συστήματα τόσο του παρόχου όσο και του χρήστη ώστε να εξασφαλίζεται σωστή αντιμετώπιση ενός αναπάντεχου περιστατικού.
- Ασφάλεια εφαρμογών: Ασχολείται με την επιλογή αν μια επιχείρηση θα μεταβεί σε υπηρεσίες Νέφους και, αν ναι, το πιο μοντέλο να υιοθετήσει (IaaS, PaaS ή SaaS).
- Κωδικοποίηση και διαχείριση κλειδιών: Αναγνωρίζει τη σωστή χρήση κωδικοποίησης και την επεκτασιμότητα της διαχείρισης κλειδιών.
- Διαχείριση ταυτότητας και πρόσβασης: Αφορά τη διαχείριση των ταυτοτήτων.
- Δημιουργία εικονικών πόρων: Το κομμάτι αυτό ασχολείται με τη χρήση του virtualization στο Cloud Computing.

Ο Ευρωπαϊκός Οργανισμός Δικτύου και Ασφάλειας Πληροφοριών, με τη σειρά του, έχει ασχοληθεί με ζητήματα ασφαλείας και τα ρίσκα που μπορούν να προκύψουν από την υιοθέτηση του Cloud Computing. Έχει παρουσιάσει, λοιπόν, έναν κατάλογο 35 ρίσκων, τα οποία μπορούν να κατηγοριοποιηθούν ως εξής:

1. Συμβόλαιο ασφαλείας και ρίσκα οργανισμού, όπως το «lock-in» του παρόχου, η απώλεια διακυβέρνησης, οι δυσκολίες συμβατότητας και η απόκτηση παρόχου υπηρεσιών Νέφους.
2. Τεχνικά ρίσκα, όπως διαρροή πληροφοριών, απώλεια κλειδιών κωδικοποίησης
3. Νομικά ρίσκα, όπως είναι η προστασία δεδομένων και η αδειοδότηση λογισμικού.
4. Ρίσκα που δεν είναι προέρχονται απαραίτητα από τις υπηρεσίες Νέφους, όπως τα προβλήματα δικτύου.

4.4 Κέρδη προστασίας από το Cloud Computing

Είναι αλήθεια πως η μέχρι τώρα συζήτηση έχει επικεντρωθεί στα προβλήματα που εγείρονται γύρω από την αποθήκευση δεδομένων στο Cloud Computing. Είναι σημαντικό, παρ' όλα αυτά, να γίνει αναφορά και στα οφέλη αυτής της διαδικασίας. Ο Ευρωπαϊκός Οργανισμός Δικτύου και Ασφάλειας Πληροφοριών (ENISA – European Network and Information Security Agency) έχει ερευνήσει μεταξύ άλλων και τα πλεονεκτήματα που έχουν οι επιχειρήσεις που υιοθετούν το Cloud Computing. Τα σημαντικότερα από αυτά είναι:

1. **Οικονομικά ωφέλη:** Οι επιχειρήσεις λαμβάνουν καλύτερη προστασία στην ίδια τιμή. Στην προστασία περιλαμβάνονται όλα τα είδη αμυντικών μέτρων, όπως φίλτρα μεταφοράς πληροφοριών, ελαττώματα υλικού και λογισμικού, ισχυρός έλεγχος ταυτότητας και λύσεις διαχείρισης ταυτότητας με κεντρική υποστήριξη. Όλες οι προαναφερθείσες μορφές προστασίας βελτιώνουν επίσης τις σχέσεις μεταξύ των εταίρων σύμφωνα με τις ακόλουθες παραμέτρους:

- Πολλαπλές τοποθεσίες: Οι πάροχοι υπηρεσιών cloud πρέπει να διατηρούν διαθέσιμους οικονομικούς πόρους για την αναπαραγωγή περιεχομένου.
- Δίκτυα αιχμής: Το Cloud Computing παρέχει αξιοπιστία, βελτίωση της ποιότητας και λιγότερα προβλήματα δικτύου για τις επιχειρήσεις.
- Διαχείριση απειλών: Με τις υπηρεσίες νέφους, οι μικρές επιχειρήσεις που δεν μπορούν να διαθέσουν πόρους για να αντιμετωπίσουν συγκεκριμένα ζητήματα ασφαλείας, δεν

αντιμετωπίζουν τέτοιου είδους προβλήματα αφού το χρέος αυτό αναλαμβάνουν να επιλύσουν οι πάροχοι cloud.

2. **Οφέλη σε ζητήματα ασφάλειας**: Όπως αναφέρθηκε προηγουμένως, η ασφάλεια είναι ζωτικής σημασίας για όλες τις επιχειρήσεις. Ως εκ τούτου, οι αποφάσεις τους επηρεάζονται από την ποιότητα των υπηρεσιών που παρέχει ο πάροχος νέφους σε αυτόν τον τομέα. Ως αποτέλεσμα του ανταγωνισμού στην αγορά, οι πάροχοι υπηρεσιών νέφους αναγκάζονται να βελτιώσουν την ασφάλεια που παρέχουν.

3. **Τυποποιημένα περιβάλλοντα για τις υπηρεσίες ασφάλειας**: Οι περισσότεροι πάροχοι υπηρεσιών ασφαλείας παρέχουν ανοικτές, τυποποιημένες πλατφόρμες για τη διαχείριση των υπηρεσιών ασφαλείας. Με τον τρόπο αυτό δημιουργείται μια ανοικτή αγορά υπηρεσιών στην οποία οι πελάτες μπορούν αρχικά να επιλέξουν ή αργότερα να αλλάξουν πάροχο με βάση τις προσφερόμενες υπηρεσίες και το κόστος.

4. **Γρήγορη επέκταση των πόρων**: Οι υπηρεσίες νέφους παρέχουν πόρους όπως αποθήκευση, χρόνο επεξεργασίας δεδομένων, μνήμη, υπηρεσίες δικτύου και χρήση εικονικών μηχανών. Οι πόροι αυτοί δεν παραμένουν σταθεροί, αλλά επεκτείνονται και προσαρμόζονται ανάλογα με τη ζήτηση και τις τεχνολογικές απαιτήσεις. Οι εταιρείες παροχής υπηρεσιών cloud έχουν πρόσβαση σε παρόμοιους πόρους. Φιλτράρισμα πληροφοριών για λόγους ασφαλείας, κωδικοποίηση κ.ο.κ. όταν αναμένεται να εκδηλωθεί επίθεση, προκειμένου να ενισχυθούν τα μέτρα ασφαλείας κ.ο.κ. Οι πάροχοι μπορούν έτσι να επεκτείνουν αυτούς τους πόρους κατά περίπτωση, χρησιμοποιώντας την κατάλληλη στρατηγική και τα κατάλληλα εργαλεία, για να βελτιστοποιήσουν τις υπηρεσίες που προσφέρουν..

5. **Έλεγχος και συλλογή στοιχείων**: Το Cloud Computing αποτελεί μια οικονομικά συμφέρουσα μέθοδο για την αποθήκευση καταγραφών.

6. **Καλύτερη διαχείριση κινδύνου** : Οι πάροχοι υπηρεσιών Νέφους είναι υποχρεωμένοι να πραγματοποιούν εσωτερικού ελέγχους και να αξιολογούν κινδύνους για να είναι προετοιμασμένη σε ενδεχόμενη απειλή.

7. **Συγκέντρωση πόρων**: Η συγκέντρωση πόρων έχει ως αποτέλεσμα χαμηλότερο έλεγχο πρόσβασης ανά μονάδα πόρου, γεγονός που οδηγεί σε χαμηλότερη εφαρμογή μιας ολοκληρωμένης πολιτικής ασφάλειας και ελέγχου των δεδομένων, των περιστατικών και, τελικά, σε χαμηλότερες διαδικασίες συντήρησης.

8. **Αποτελεσματικότερες αναβαθμίσεις και προεπιλογές**: Όλες οι αναβαθμίσεις γίνονται σε μικρότερο χρόνο (Dupre L., 2012).

4.5 Τα τεχνικά οφέλη του Cloud Computing

Ο Balding (2008) παρουσιάζει εφτά τεχνικά οφέλη σχετικά με την ασφάλεια των επιχειρήσεων. Κάποια από αυτά έχουν βραχυχρόνιες και άλλα μακροχρόνιες επιπτώσεις.

Τα τεχνικά αυτά χαρακτηριστικά είναι:

1. **Κεντρική διαχείριση δεδομένων**: Μέσω της κεντρικής διαχείρισης δεδομένων επιτυγχάνεται η μειωμένη διαρροή πληροφοριών και, φυσικά, ο καλύτερος έλεγχος. Η μειωμένη διαρροή δεδομένων είναι το μεγαλύτερο κέρδος του Cloud Computing που παρέχεται στις επιχειρήσεις. Οι περισσότερες επιχειρήσεις αποθηκεύουν τα δεδομένα τους σε φορητές συσκευές αποθήκευσης, αλλά αυτό δεν εξασφαλίζει την ασφάλειά τους. Επίσης, σπάνια χρησιμοποιούν τεχνικές κρυπτογράφησης.

Συνεπώς, οι τεχνολογίες υπολογιστικού νέφους μπορούν να διασφαλίσουν την ασφάλεια των δεδομένων. Εκτός από όλα τα παραπάνω, έχει αποδειχθεί ότι τα δεδομένα που συγκεντρώνονται μπορούν να ελέγχονται και να παρακολουθούνται ευκολότερα. Υπάρχει, ωστόσο, μια πιθανότητα ληστείας για πολλούς, όπου όλα τα δεδομένα θα καταστραφούν αν συμβεί αυτό. Ο Baldingen (2008) αναφέρει ότι η κεντρική διαχείριση από πολλές απόψεις είναι προτιμότερη, δεδομένου ότι ο σχεδιασμός ενός ασφαλούς συστήματος κεντρικής αποθήκευσης είναι καλύτερος και πιο αποδοτικός από τα μεμονωμένα συστήματα (Marinescu C., 2012).

2. **Αντιμετώπιση παραβίασης ασφαλείας**: Όπως αναλύθηκε παραπάνω στην χρήση του IaaS, ένας ξεχωριστός διακομιστής Νέφους βρίσκεται σε κατάσταση offline, έτοιμος ανά πάσα στιγμή να αντιμετωπίσει περιστατικά παραβίασης στην ασφάλεια. Ο χρήστης σε αυτήν την περίπτωση πληρώνει μόνο τις υπηρεσίες αποθήκευσης. Αν συμβεί κάποιο περιστατικό παραβίασης, τότε ο διακομιστής μπαίνει σε λειτουργία online μειώνοντας με αυτόν τον τρόπο τον χρόνο απόκτησης στοιχείων.

Ο χρόνος εντοπισμού διαρροής και αντιμετώπισης των «περίεργων» περιστατικών περιορίζεται από το Cloud Computing για τις επιχειρήσεις. Αυτό συμβαίνει γιατί το hardware

του χρήστη είναι σε ηλεκτρονική μορφή με αποτέλεσμα να γίνεται πολύ πιο γρήγορα ο έλεγχος και ο εντοπισμός του προβλήματος.

3. **Έλεγχος αξιοπιστίας κωδικού (cracking)**: Οι επιχειρήσεις συχνά τσεκάρουν τη δύναμη και την ισχύ ενός κωδικού με ειδικά προγράμματα, διαδικασία ομολογουμένως αρκετά χρονοβόρα. Με τη χρήση του Cloud Computing, η διαδικασία αυτή γίνεται αυτόματα από τον πάροχο της υπηρεσίας.

4. **Καταγραφή αρχείων** : Ένα σημαντικό κέρδος για τις επιχειρήσεις με τα υπολογιστικά νέφη είναι η δυνατότητα απεριόριστης αποθήκευσης αρχείων. Οι επιχειρήσεις, με αυτόν τον τρόπο, μπορούν να αναζητήσουν πολύ πιο γρήγορα όποιο αρχείο επιθυμούν.

5. **Βελτίωση στις επιδόσεις**: Οι πάροχοι Cloud Computing λόγω του ανταγωνισμού, κατασκευάζουν πιο όλο και πιο αποδοτικά λογισμικά ασφαλείας.

6. **Δομές και δοκιμές ασφαλείας**: Οι επιχειρήσεις είναι σε θέση να δοκιμάζουν τις μεταβολές στις δομές ασφαλείας. Το μόνο που έχουν να κάνουν είναι μία κόπια του παραγωγικού περιβάλλοντος τους, να κάνουν τις μετατροπές στην ασφάλεια και να τεστάρουν τις επιρροές με χαμηλό κόστος και σε ελάχιστο χρόνο. Το κόστος αυτών των δοκιμών είναι ιδιαιτέρως χαμηλό. Με τη χρήση του SaaS, οι πάροχοι ζητούν μόνο ένα μέρος του συνολικού κόστους ελέγχου της ασφάλειας καθώς οι επιχειρήσεις μοιράζονται τις ίδιες εφαρμογές σαν υπηρεσίες. Έτσι μειώνουν το κόστος αυτής της υπηρεσίας (Marinescu C., 2012).

4.6 Η προσφορά δεδομένων και η ασφάλεια τους

Χώρια από την ασφάλεια των δεδομένων των πελατών, αυτοί θα πρέπει να αγωνιούν σχετικά με τα δεδομένα που συλλέγει ο πάροχος (τα λεγόμενα μετα-δεδομένα) και πώς αυτά προστατεύονται. Είναι αλήθεια ότι ο προμηθευτής cloud έχει την υποχρέωση να συλλέγει και κυρίως να προστατεύει τα δεδομένα. Για τη συνέχεια της ανάλυσης, πρέπει να ξεκαθαρίσουμε ότι για τα στοιχεία που είναι αποθηκευμένα στο «Υπολογιστικό Νέφος», αναφερόμαστε στο μοντέλο IaaS. 3 είναι τα βασικά στοιχεία

Τα τρία στοιχεία που εμφανίζουν ενδιαφέρον αναφορικά με την αποθήκευση των δεδομένων: η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

4.6.1 Εμπιστευτικότητα

Όταν αναφερόμαστε στην προάσπιση του απορρήτου των στοιχείων που είναι αποθηκευμένα σε ένα δημόσιο σύννεφο, δύο είναι τα θέματα που εγείρονται. Το πρώτο έχει να κάνει με τον έλεγχο πρόσβασης. Αυτός συνίσταται από δύο στοιχεία, την επιβεβαίωση ταυτότητας και την αδειοδότηση. Τις περισσότερες φορές, το μοναδικό επίπεδο ασφάλειας που παρέχεται είναι η άδεια διαχειριστή και η άδεια χρήσης. Το δεύτερο ζήτημα σχετίζεται με τον τρόπο που προστατεύονται τα δεδομένα που είναι αποθηκευμένα στο cloud.

Σίγουρα αυτά θα πρέπει να είναι κρυπτογραφημένα, όμως σε ποιο βαθμό έχει γίνει η κρυπτογράφηση και με ποιον αλγόριθμο και αν το κλειδί αυτί είναι αρκετά ισχυρό πρέπει να απασχολούν τις επιχειρήσεις – χρήστες. Είναι γεγονός, πώς δεν είναι το ίδιο ισχυροί όλοι οι αλγόριθμοι κρυπτογράφησης. Μια άλλη παράμετρος για έλεγχο είναι το μέγεθος του κλειδιού που χρησιμοποιείται. Με συμμετρική κρυπτογράφηση, όσο μεγαλύτερο είναι το κλειδί (δηλ. όσο μεγαλύτερος είναι δηλαδή ο συνδυασμός του 0 και του 1), τόσο πιο ασφαλής είναι η κρυπτογράφηση. Ένα άλλο ζήτημα τίθεται και με τον τρόπο διαχείρισης αυτών των κλειδιών. (Mather T.; Kumaraswamy S.;Latif S, 2009).

4.6.2 Αρτιότητα

Οι οργανισμοί που κάνουν χρήση των clouds θα πρέπει επίσης να ανησυχούν για την αρτιότητα του τα δεδομένα σας. Η εμπιστευτικότητα που αναλύσαμε παραπάνω, δεν πρέπει να ταυτίζεται και δεν οδηγεί απαραίτητα στην ακεραιότητα των δεδομένων. Τα δεδομένα ναι μεν κρυπτογραφούνται για λόγους εμπιστευτικότητας, ωστόσο δεν υπάρχει τρόπος να επαληθευτεί η ακεραιότητά τους. Η αλήθεια είναι ότι η ακεραιότητα απαιτεί συγκεκριμένες διεργασίες.

Ο πιο απλός τρόπος για να χρησιμοποιήσουμε τα κρυπτογραφημένα δεδομένα είναι με τη χρήση ενός συμμετρικού αλγορίθμου και μιας συνάρτησης hash. Αξίζει να σημειωθεί, σε αυτό το σημείο, πως με τον τρόπο που μόλις περιεγράφηκε, παρέχονται πληροφορίες σχετικά με το πόσο προηγμένο σχέδιο ασφάλειας χρησιμοποίει ο πάροχος. Για τον πελάτη – οργανισμό βασικό ζητούμενο είναι να μπορεί να επαληθεύει την ακεραιότητα των δεδομένων του, δίχως να είναι ανάγκη κάθε φορά να κατεβάζει και να ανεβάζει τα δεδομένα από το σύννεφο. Η διαδικασία αυτή είναι δύσκολη μα συνάμα και περίπλοκη γιατί ο χρήστης πρέπει για να το κάνει να γνωρίζει που ακριβώς είναι αποθηκευμένα τα δεδομένα του (Mather T.; Kumaraswamy S.;Latif S, 2009).

4.6.3 Διαθεσιμότητα

Αν ένας πελάτης του cloud είναι ικανοποιημένος με την εμπιστευτικότητα και την ακεραιότητά στα δεδομένα του, θα πρέπει να εξετάσει την παράμετρο διαθεσιμότητα. Για την ώρα, τρία είναι τα βασικά προβλήματα που σχετίζονται με αυτήν την παράμετρο.

Στην πρώτη περίπτωση η απειλή έχει σχέση με τις επιθέσεις ασφάλειας. Στη δεύτερη απειλή, έχουμε απώλεια δεδομένων, από το νέφος, λόγω πιθανολογούμενης διακοπής της χρήσης-λειτουργίας του νέφους. Στην τρίτη περίπτωση εγκυμονεί ο κίνδυνος της συνεχούς παρουσίας του παρόχου στον επαγγελματικό στίβο. Τον Φεβρουάριο του 2009, ο πάροχος Coghead έκλεισε αιφνιδίως, παραχωρώντας στους πελάτες εννέα εβδομάδες να κατεβάσουν δεδομένα από τους διακομιστές τους. Αρκετοί πάροχοι αποθήκευσης cloud δεν δημιουργούν αντίγραφα ασφαλείας των δεδομένων πελατών ή το κάνουν μόνο ως πρόσθετη υπηρεσία με επιπλέον χρέωση. (Mather T.; Kumaraswamy S.;Latif S, 2009)

5 Μελέτη μεθόδων και τεχνικών ασφάλειας σε υπηρεσίες υπολογιστικού νέφους

Σε αυτό το κεφάλαιο παρουσιάζονται κάποιες εφαρμογές, τόσο για την κάλυψη ιδιωτικών όσο και επαγγελματικών εφαρμογών για την εξυπηρέτηση του χρήστη που βασίζονται στα υπολογιστικά νέφη. Αυτά τις περισσότερες φορές είναι ταξινομημένα σε μια ιεραρχία..

Η υποδομή ως υπηρεσία (IaaS) παρέχει τους γενικούς πόρους κατόπιν παραγγελίας όπως οι virtualized κεντρικοί υπολογιστές(servers) ή διάφορες μορφές αποθήκευσης (block, key/value, βάση δεδομένων κτλ.). Μερικές φορές αποκαλείται και ως υλικό ως υπηρεσία (Hardware as a Service). Η πλατφόρμα ως υπηρεσία (PaaS) παρέχει υποδομή λογισμικού υψηλού επιπέδου για την οικοδόμηση των ιδιαίτερων κατηγοριών εφαρμογών και υπηρεσιών. Το λογισμικό ως υπηρεσία (SaaS) παρέχει συγκεκριμένες προκατασκευασμένες εφαρμογές που προσφέρουν εξ αποστάσεως πλήρεις ή τμηματικές υπηρεσίες. Μερικές φορές έχει τη μορφή διαδικτυακών εφαρμογών και άλλες φορές αποτελείται από τυπικές μη απομακρυσμένες εφαρμογές με αποθήκευση στον ιστό ή άλλες αλληλεπιδράσεις δικτύου. Παρακάτω θα επιχειρήσουμε μια μικρή ανάλυση σε μελέτη περιπτώσεων εφαρμογών που βασίζονται στο cloud computing.

5.1 Το Dropbox

Μπορεί να μην το έχουμε αντιληφθεί όμως τα τελευταία χρόνια, όλοι μας κάνουμε χρήση των υπηρεσιών του cloud computing. Με ποιον τρόπο; Μα φυσικά με τη χρήση των mails και της ηλεκτρονικής αλληλογραφίας εν γένει. Παράλληλα, πολλές από τις δημόσιες υπηρεσίες με τις υποίες συνδιαλεγόμαστε καθημερινά χρησιμοποιούν τέτοιες τεχνολογίες. Χαρακτηριστική περίπτωση ο ΟΑΕΔ, το ΙΚΑ, η εφορία με την υπηρεσία του taxis ακόμα και οι τράπεζες με τα e- banking, υπηρεσίες που χωρίς να το έχουμε καταλάβει μας έχουν εξοικειώσει με το cloud computing. Ωστόσο, πρέπει να αναφερθεί ότι οι εφαρμογές που μόλις αναφέρθηκαν ανήκουν στην κατηγορία του λογισμικού ως υπηρεσία, άρα δεν μπορούν να καταταχτούν στις εφαρμογές υπολογιστικού νέφους, αν και έχουν πολλά από τα χαρακτηριστικά του.

Αντίθετα ως εφαρμογές νέφους μπορεί να είναι ιστοσελίδες μέσων κοινωνικής δικτύωσης γιατί ο χρήστης, εμείς με λίγα λόγια, χρησιμοποιούμε πόρους που δεν μας ανήκουν.

Το Dropbox είναι μια εφαρμογή cloud computing ή με άλλα λόγια μια υπηρεσία που επιτρέπει την αποθήκευση, τον συγχρονισμό και την κοινή χρήση αρχείων μεταξύ διαφορετικών συσκευών που ο χρήστης έχει επιλέξει να συνδέσει στο λογαριασμό του (F., G. «There's room yet in the cloud». The Economist. Προσφέρεται με χωρητικότητα αποθηκευτικού χώρου από 2GB έως 16GB δωρεάν, ενώ διατίθεται σε Windows, Mac, Linux, iPhone, iPad, Android και BlackBerry[4].

Η εταιρεία ιδρύθηκε στο Σαν Φρανσίσκο το 2007 από τους φοιτητές του MIT Drew Houston και Arash Ferdowsi (Dropbox / about). Η εφαρμογή παρουσιάστηκε για πρώτη φορά τον Σεπτέμβριο του 2008 και κυκλοφόρησε στην αγορά τον Οκτώβριο του 2011. Η υπηρεσία παρέχει διαχειριστικό έλεγχο του περιβάλλοντος εργασίας και χώρο για τη συνεργασία των εργαζομένων. Σήμερα, περισσότεροι από 200 εκατομμύρια χρήστες παγκοσμίως χρησιμοποιούν την υπηρεσία και εκτιμάται ότι κάθε μέρα αποθηκεύονται 1 δισεκατομμύριο αρχεία.

Εύκολο στη χρήση. Οι νέοι χρήστες μπορούν να εγκαταστήσουν το Dropbox στον υπολογιστή τους αφού δημιουργήσουν λογαριασμό στον ιστότοπο της υπηρεσίας. Αφού ολοκληρωθεί η εγκατάσταση, θα δημιουργηθεί στον υπολογιστή σας ένας ειδικός φάκελος με

[4] Dropbox/company info

την ονομασία Dropbox. Αυτός ο φάκελος επιτρέπει στους χρήστες να μεταφέρουν αρχεία σε άλλο φάκελο, να δημιουργούν νέους φακέλους και να ανοίγουν και να επεξεργάζονται αρχεία. Εν τω μεταξύ, το λογισμικό παρακολούθησης του Dropbox αναπαράγει αυτές τις λειτουργίες σε άλλους συνδεδεμένους υπολογιστές. Το Dropbox είναι διαθέσιμο σε υπολογιστή και κινητές συσκευές, ώστε οι χρήστες να έχουν πρόσβαση στα αρχεία τους οποιαδήποτε στιγμή και οπουδήποτε.

Ταυτόχρονα, οι παραπάνω λειτουργίες μπορούν να εκτελούνται μεταξύ μιας ή περισσότερων συσκευών χρηστών μόνο εάν όλοι οι χρήστες είναι μέλη του κοινόχρηστου φακέλου. Ένα αντίγραφο του αρχείου αποθηκεύεται επίσης στον διακομιστή υπηρεσιών διαδικτύου, οπότε σε περίπτωση βλάβης ή απώλειας της συσκευής, το αρχείο μπορεί να αποκατασταθεί και ο χρήστης έχει στη διάθεσή του 30 ημέρες για να διαγράψει την προηγούμενη έκδοση του αρχείου ή το τροποποιημένο αρχείο. (Drobox, 2021).

Οι πιο δημοφιλείς εφαρμογές που έχουν δημιουργηθεί μέσα στην εν λόγω υπηρεσία σήμερα είναι οι:

DropItToMe: Το Dropbox επιτρέπει στους χρήστες να ανεβάζουν αρχεία και να τα μοιράζονται με άλλους, αλλά δυσκολεύει τη μεταφόρτωση αρχείων άλλων χρηστών στο λογαριασμό τους. Το DropItToMe επιτρέπει τις παραπάνω λειτουργίες και παρέχει επίσης έναν εύκολο τρόπο για τους χρήστες να ανεβάζουν αρχεία στο λογαριασμό τους στο Dropbox.

Box Cryptor: Η υπηρεσία χρησιμοποιεί κρυπτογράφηση 256-bit AES για την αυτόματη κρυπτογράφηση των αρχείων πριν από τη μεταφόρτωσή τους στο λογαριασμό στο Dropbox.

Droptunes: Το Dropbox δεν μπορεί να αναπαράγει αρχεία ήχου που είναι αποθηκευμένα στους διακομιστές της υπηρεσίας, οπότε οι χρήστες πρέπει να τα μεταφορτώσουν στη συσκευή τους για αναπαραγωγή. Το DropTunes μεταφέρει αρχεία ήχου μέσω του Διαδικτύου χωρίς αυτή την κουραστική διαδικασία..

IFTTT: Οι χρήστες δημιουργούν συνδέσμους μεταξύ υπηρεσιών ιστού για την απλούστευση και την αυτοματοποίηση εργασιών. Δηλαδή, αποθηκεύει την εντολή ακολουθούμενη από την ενέργεια ακολουθούμενη από μια αυτόματη απάντηση. Για παράδειγμα, οι χρήστες μπορούν να ζητήσουν να αποθηκεύονται αυτόματα όλα τα συνημμένα αρχεία του Gmail που λαμβάνουν στο Dropbox.

Send to Dropbox : Δημιουργεί μια διεύθυνση ηλεκτρονικού ταχυδρομείου , στην οποία ότι συνημμένο αποστέλλεται αποθηκεύεται αυτόματα στο Dropbox (Cassavoy L., 2013).

Το Dropbox είναι υπηρεσία αποθήκευσης cloud που επιτρέπει στους χρήστες να αποθηκεύουν αρχεία σε απομακρυσμένους διακομιστές cloud και τη δυνατότητα κοινής χρήσης αρχείων σε συγχρονισμένη μορφή. Το Dropbox παρέχει μια διαδικτυακή λύση αποθήκευσης που υποστηρίζεται από το μοντέλο υποδομής cloud computing service ως υπηρεσία (IaaS). Το Dropbox προσφέρει διάφορες επιλογές αποθήκευσης στο cloud. Είτε πρόκειται για μια μεμονωμένη, μικρή επιχείρηση ή μεγάλη εταιρεία, η χρήση του Dropbox για αποθήκευση στο cloud επιτρέπει να αποθηκεύονται τα πάντα με ασφάλεια στο cloud και να υπάρχει πρόσβαση σε μεταφορτώσεις αρχείων από πολλές συσκευές.

Το Dropbox καθιστά την προστασία δεδομένων cloud κορυφαία προτεραιότητά του – χρησιμοποιώντας πολλαπλά επίπεδα προστασίας σε μια κατανεμημένη, αξιόπιστη υποδομή cloud (dropbox.com/features). Αυτό σημαίνει ότι τα άτομα μπορούν με βεβαιότητα να χρησιμοποιήσουν το ασφαλές σύννεφο μας για να αποθηκεύουν αρχεία, να μοιράζονται έγγραφα και να ζητούν πρόσβαση. Επιπλέον, οι οργανισμοί μπορούν να αισθάνονται ασφαλείς ότι το κρυπτογραφημένο cloud storage εταιρικού επιπέδου υποστηρίζει τις απαιτήσεις συμμόρφωσης των πελατών και ακολουθεί τις πολιτικές ασφάλειας δεδομένων των επιχειρηματικών και διεθνών κανονισμών, όπως το GDPR και το HIPAA.

5.2 Το Amazon Cloud

Η Amazon έχει αναπτύξει μια σειρά από διαδικτυακές υπηρεσίες, γνωστές και ως "Amazon Web Services (Ma S., 2012), δίνοντας τα παρακάτω, ως βασική υποδομή για επίπεδο υπηρεσιών:

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Simple DB
- Amazon Elastic Block Store (EBS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Cloud Front

- Amazon Simple Queue Service (Amazon SQS)
- AWS Premium Support

Πρώτον, αξίζει να αναφέρουμε ότι το Elastic Cloud Computing (EC2) είναι η ναυαρχίδα του cloud της Amazon, το οποίο επιτρέπει στις εικονικές μηχανές να χρεώνονται βάσει των αναγκών χρήσης τους. Αυτό γίνεται με τη μίσθωση μιας μονάδας που ονομάζεται instances. Κάθε ενότητα αντιπροσωπεύει έναν εικονικό διακομιστή με συγκεκριμένες προδιαγραφές υλικού. Για τους χρήστες, είναι σημαντικό να νοικιάζουν έναν φυσικό διακομιστή κάθε ώρα. Υπάρχουν πέντε τύποι μισθώσεων με διαφορετικές επιδόσεις CPU, χώρο στο δίσκο και επιδόσεις I/O. Οι εφαρμογές που χρησιμοποιούν μεγάλες ποσότητες μνήμης RAM ή ισχύος CPU μπορούν να νοικιάσουν πιο ακριβά και πιο ισχυρά στοιχεία, ενώ τα δίκτυα που εξαρτώνται από την εφαρμογή, όπως οι διακομιστές ιστού, μπορούν να χρησιμοποιήσουν φθηνότερα και πιο ισχυρά στοιχεία. Το EC2 γενικότερα παρέχει μετρημένες υπολογιστικές εγκαταστάσεις προσωρινής τοπικής αποθήκευσης (Mather T.; Kumaraswamy S.;Latif S, 2009). Τα υπόλοιπα τρία προϊόντα του Amazon, το Elastic Block Store (EBS), το Simple Storage Service (S3) και το Simple DB, παρέχουν δοσομετρικές μόνιμες εγκαταστάσεις αποθήκευσης.

Το Elastic Block Store (EBS) συνεργάζεται με το EC2 για να παρέχει πρόσθετες επιδόσεις και μόνιμο αποθηκευτικό χώρο. Τα δείγματα EC2 διαθέτουν τοπικό αποθηκευτικό χώρο, αλλά αυτός ο αποθηκευτικός χώρος είναι προσωρινός και μπορεί να χρησιμοποιηθεί μόνο όταν η δειγματοληψία εξακολουθεί να εκτελείται.

Το EBS αποθηκεύει σαν έναν πλασματικό σκληρό δίσκο (αποθήκευση block), και μπορεί να σχετισθεί με ένα συγκεκριμένο instance EC2. Σε αυτό το ενδεχόμενο, τα στοιχεία υπάρχουν έτοιμα προς χρήση, χωρίς να είναι απαραίτητο να τρέχουν τα EC2 instances (Velte A. et.al., 2010).

Το Simple Storage Service[5](S3) ήταν η αρχική βάση σε επίπεδο web υπηρεσιών της Amazon, που άρχισε να λειτουργεί τους πρώτους μήνες του 2006. Το S3 προσφέρει δυνατότητα ισχυρής αποθήκευσης αντικείμενων υπολογισμένη σε gigabyte ανά μήνα. Το EBS προσφέρει έναν virtual δίσκο, όπως τη δυνατότητα αφαιρετικής δέσμευσης σε block για να

[5] aws.amazon.com/s3/

δίνει στο EC2 εικονικής μηχανής, ταυτόχρονα δε S3 προσφέρει συνθήκες δίνοντας τη δυνατότητα να υπάρχει πρόσβαση χωρίς την απαραίτητη παρουσία των EC2 instances. Υπάρχει δηλαδή η δυνατότητα να χρησιμοποιηθεί το S3, ως δηλαδή ένας χώρο αποθήκευσης χωρίς τη χρήση του EC2. Επίσης είναι δυνατόν κάποιος να έχει πολλά instances EC2 και να φέρει πρόσβαση στα ίδια δεδομένα από το S3.

Η Simple Data Base[6] είναι μια ψευδό-σχεσιακή υπηρεσία για την διατήρηση των δεδομένων του χρήστη. Κρατάει - φυλάσσει τα δεδομένα με τη μορφή μίας σχέσης βάσης δεδομένων (Relational DataBase Management System) και μπορεί να είναι προσβάσιμη, μακριά από τα EC2 instances παρουσιάζοντας ταυτόχρονα σημαντικότερο επίπεδο υπηρεσιών ως βάση δεδομένων.

Το Cloud Front[7] είναι μία νέα δυνατότητα που προσφέρει η Amazon, με την δημιουργία της να ξεκινά τον Νοέμβριο του 2008. Πρόκειται για μία δαιδαλώδες κατανομή περιεχομένων σε δίκτυο (Content Delivery Network), το οποίο χρησιμοποιεί το S3, για την άντληση των αποθηκευμένων δεδομένων του. Η παράδοση των δεδομένων (περιεχόμενο) έως τους καταναλωτές τους (πελάτες / τελικούς χρήστες), γίνεται με την CDN που έχει σχεδιαστεί για την ενίσχυση της παράδοσης, προφέροντας πιο κοντινές τοποθεσίες για τη διανομή τους. Με την παροχή αυτή, μια υπηρεσία παροχής περιεχομένου μπορεί να παρέχει στους τελικούς χρήστες του μικρότερο χρόνο παράδοσης και καλύτερη απόδοση.

Η Simple Queue Service[8] (SQS) της Amazon παρέχει αξιόπιστη ανταλλαγή μηνυμάτων μεταξύ στοιχειών διανεμημένου λογισμικού. Χρησιμοποιείται συχνά σε συνδυασμό με την EC2 για να διευθύνει τις δράσεις σε αλλιώτικα instances ή σε διαφορετικές συνιστώσες μιας μείζονας εφαρμογής που τρέχει στο EC2.

Τέλος, αξίζει να αναφέρουμε πως η AWS Premium Support[9] δεν είναι ένα τεχνικό προϊόν. Πρόκειται για μία δυνατότητα που προσφέρεται για την υποστήριξη των υπηρεσιών cloud της Amazon. Αυτό σημαίνει ότι η εταιρεία – κολοσσός είναι σε θέση να προσφέρει

---

[6] https://aws.amazon.com/simpledb/

[7] https://aws.amazon.com/cloudfront/

[8] https://aws.amazon.com/sqs/

[9] https://aws.amazon.com/premiumsupport/

λειτουργική υποστήριξη και υποστήριξη για τεχνικά ζητήματα που σχετίζονται με την ανάπτυξη λογισμικού μέσω της υπηρεσίας cloud..

5.3 Το iCloud

Το iCloud βασίζεται στην τελευταία τεχνολογία υπολογιστικού νέφους. Έτσι, πρόκειται για μια υπηρεσία cloud που διατηρεί τη μουσική, τις φωτογραφίες, τις εφαρμογές, τις επαφές, τα ημερολόγια, τα έγγραφα των χρηστών και πολλά άλλα, μαζί. Αποθηκεύει και συγχρονίζει με όλα τα λειτουργικά συστήματα σε πολλαπλές συσκευές και υπολογιστές και ταυτόχρονα δημιουργεί αντίγραφα ασφαλείας των συσκευών Apple. Οι χρήστες μπορούν να έχουν δωρεάν πρόσβαση στο iCloud σε συσκευές που τρέχουν την βασική, τρέχουσα έκδοση του λειτουργικού συστήματος.

Αντί να βασίζεται σε χειροκίνητα αντίγραφα ασφαλείας, το iCloud παρέχει έναν τρόπο για να δημιουργείτε ασύρματα αντίγραφα ασφαλείας της συσκευής iOS στον Mac ή τον υπολογιστή με Windows χρησιμοποιώντας το λογισμικό iTunes. Οι χρήστες αυτής της υπηρεσίας έχουν την δυνατότητα να ανταλλάσσουν γρήγορα, φωτογραφίες, μουσική και παιχνίδια συνδέοντας τους λογαριασμούς τους μέσω της άλλης υπηρεσίας της εταιρείας, του AirDrop..

Η δημιουργία λογαριασμού iCloud προϋποθέτει χρήση συσκευών που λειτουργούν σε σε περιβάλλον με λειτουργικό iOS 5 ή νεότερο, προσφέρεται επίσης για χρήση σε υπολογιστές Mac που λειτουργούν σε περιβάλλον OS X Lion v10.7.5 ή πιο πρόσφατο, απαιτώντας ταυτόχρονα ένα συμβατό, με τις συσκευές αυτές, πρόγραμμα περιήγησης. Ο συγχρονισμός με έναν υπολογιστή προϋποθέτει λειτουργικό περιβάλλον Windows 7 ή νεότερη έκδοση και χρησιμοποιώντας τον Πίνακα Ελέγχου iCloud και προαιρετικά το Outlook 2007 ή νεότερη έκδοση ή τις ενσωματωμένες εφαρμογές Windows Mail και Ημερολόγιο για συγχρονισμό Ημερολογίου, Επαφών και Υπενθυμίσεων. Οι χρήστες πρέπει να είναι κύριοι μιας συσκευής Apple για να ρυθμίσουν το iCloud για Windows.

Ο συγχρονισμός των σελιδοδεικτών προϋποθέτει λειτουργία συγκεκριμένων προγραμμάτων περιήγησης στο διαδίκτυο και συγκεκριμένα, Safari 5.1.1 ή νεότερη έκδοση για Mac OS και Internet Explorer 9, Firefox 22 ή Google Chrome 28 ή νεότερη έκδοση για περιβάλλοντα Windows. Οι χρήστες του λογαριασμού MobileMe έχουν τη δυνατότητα να

περάσουν τους λογαριασμούς τους σε έναν λογαριασμό iCloud με τη ταυτόχρονη διατήρηση των στοιχείων-χαρακτηριστικών του προηγούμενού τους λογαριασμού.

Με λίγα λόγια, το iCloud προσφέρεται με την αγορά κάθε νέας συσκευής Apple. Αυτό εξασφαλίζει ότι όλα τα δεδομένα του αγοραστή-χρήστη όπως, φωτογραφίες, αρχεία, σημειώσεις κ.ά.– είναι ασφαλή, ενημερωμένα ως προς την τελευταία έκδοσή τους είναι ταυτόχρονα διαθέσιμα όπου κι αν βρίσκεται ο χρήστης. Προφέρει, έναν αρχικό, δωρεάν χώρο αποθήκευσης μεγέθους 5 GB στο περιβάλλον iCloud για να μπορεί ο χρήστης να δοκιμάσει την λειτουργία του, αλλά και για τις πρώτες ανάγκες του, ενώ προσφέρει και τη δυνατότητα αγοράς επιπλέον αποθηκευτικού χώρου, ανάλογα τις ανάγκες, ανά πάσα στιγμή.

Αναφορικά με την ενσωματωμένη εφαρμογή "photos" του iCloud, ο χρήστης μπορεί να περιηγηθεί, να αναζητήσει και να μοιραστεί όλες τις φωτογραφίες και τα βίντεο από οποιαδήποτε συσκευή, χωρίς να έχει σημασία πότε έχουν τραβηχτεί[10].

Η υπηρεσία, για να εξοικονομήσει αποθηκευτικό χώρο στις συσκευές, στέλνει τις αρχικές φωτογραφίες που έχει τραβήξει ο χρήστης και είναι σε κανονική, μέγιστη ανάλυση στο iCloud δίνοντας παράλληλα στην χρήστη την δυνατότητα να βλέπει "υποβαθμισμένες" εικόνες, ως προς το μέγεθός τους (όχι όμως λιγότερο ποιοτικές και με χαμηλότερη ανάλυση). Παράλληλα, μπορεί να κατεβάσει τις πρωτότυπες όποτε τις χρειαστεί. Αντίστοιχα, μπορεί να οργανώσει κοινόχρηστα allbum με τις φωτογραφίες αυτές που μπορούν να έχουν πρόσβαση χρήστες που αυτός μπορεί να επιλέξει, μέσα από τη δυνατότητα διαμοιρασμού που προσφέρεται.

Άλλωστε, τα αρχεία που διατηρούνται ασφαλή στο iCloud Drive είναι εύκολο για το χρήστη να τα ανακτήσει, ανεξάρτητα από τη συσκευή που χρησιμοποιεί. Μπορεί, με λίγα λόγια, να έχει πρόσβαση σε όλα τα αρχεία του από το app Αρχεία στο iOS και το iPadOS, το Finder στον Mac, την Εξερεύνηση αρχείων σε Windows PC ή από το iCloud.com, ανάλογα πιο έχει πιο εύκολη πρόσβαση κάθε στιγμή.

Παράλληλα, μια ακόμα υπηρεσία, το iCloud Drive, επιτρέπει στο κάθε χρήστη να οργανώσει τα αρχεία του με φακέλους, να τα μετονομάσει και γενικότερα να τα διαχειριστεί όπως ο καθένας θέλει. Εξυπακούεται, πώς όταν γίνεται μια αλλαγή, η ενημέρωση γίνεται σε

[10] apple.com/gr/icloud

όλες τις συσκευές που διαθέτει ο χρήστης. Για παράδειγμα, μπορεί να έχει όλα τα δεδομένα του κάποιος από την επιφάνεια εργασίας του Mac και τους φακέλους εγγράφων αυτόματα διαθέσιμα στο iCloud Drive.

Το iCloud Drive δίνει τη δυνατότητα εύκολης και γρήγορης συνεργασίας με άλλους, από οποιαδήποτε τοποθεσία. Πώς λειτουργεί; Ο χρήστης απλά στέλνει τον ιδιωτικό σύνδεσμο, ο οποίος θα τους δώσει άμεση πρόσβαση στους φακέλους και στα αρχεία που έχουν επιλεγεί. Μάλιστα, ο χρήστης μπορεί να δώσει σε αυτά τα αρχείο περιορισμένη πρόσβαση.

Πρέπει να αναφερεθείστο σημείο αυτό, ότι το iCloud διατηρεί αυτόματα τα apps, συμπεριλαμβανομένων των apps Mail, Ημερολόγιο, Επαφές, Υπομνήσεις, Safari ενημερωμένα σε όλες τις συσκευές σου. Έτσι, όταν ο χρήστης προσθέσει ή αφαιρέσει έναν αριθμό τηλεφώνου, ορίσει έναν σελιδοδείκτη σε έναν ιστότοπο ή ενημερώσει μια διαφάνεια σε μια παρουσίαση, η αλλαγή εμφανίζεται παντού.

Παράλληλα, το iCloud αποθηκεύει αυτόματα όλα τα μηνύματα ενώ δίνει τη δυνατότητα στον χρήστη να επιστρέψει στο σημείο που ήταν σε οποιαδήποτε συζήτηση. Ακόμη και αν χρησιμοποιείς άλλο τηλέφωνο ή υπολογιστή.

Ως προς τα αντίγραφα ασφαλείας, το iCloud δημιουργεί αυτόματα εφεδρικά αντίγραφα από τις συσκευές iOS και iPad OS, όταν αυτές είναι συνδεδεμένες στην πρίζα και σε δίκτυο Wi-Fi. Έτσι, αν «χάσεις» μια συσκευή ή αποκτήσεις μια νέα, θα έχεις διαθέσιμα όλα τα σημαντικά δεδομένα σου, άμεσα.

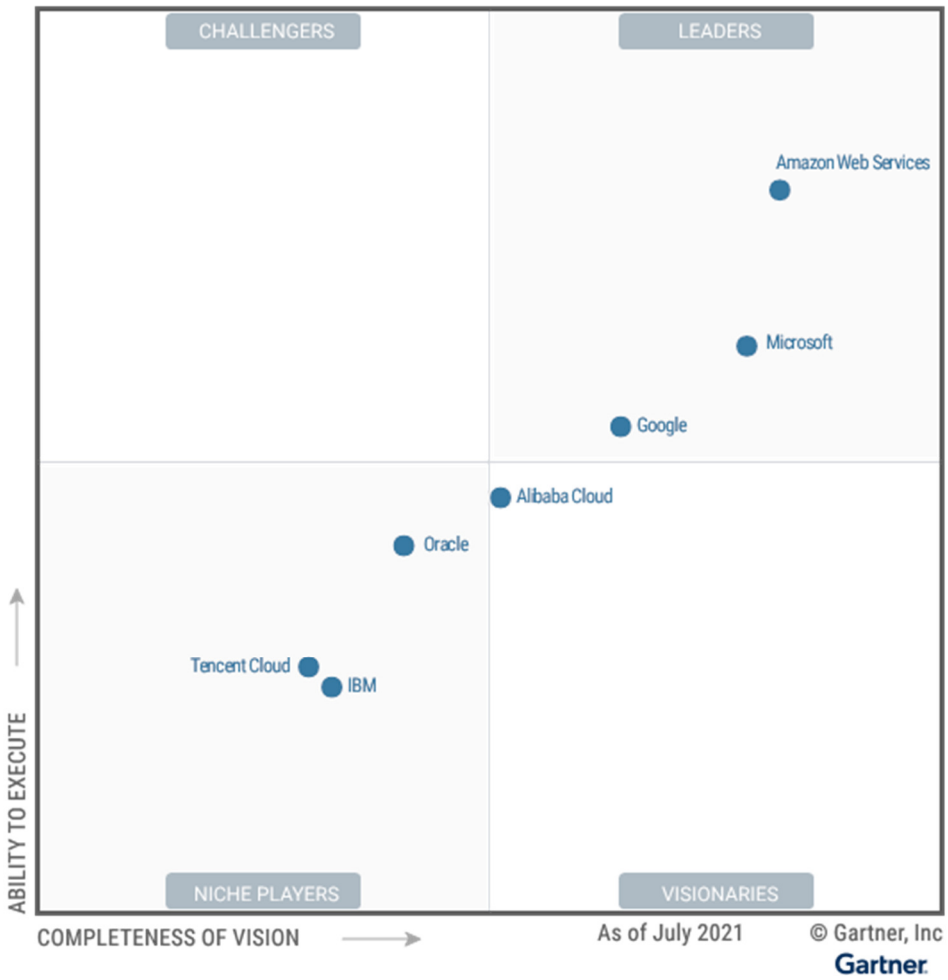
5.4 Σύγκριση υπηρεσιών νέφους

Ο ανταγωνισμός για την ηγετική θέση στο δημόσιο υπολογιστικό νέφος είναι ένας σκληρός αγώνας τριών δρόμων: Amazon Web Services (AWS) εναντίον Microsoft Azure εναντίον Google Cloud Platform (GCP). Είναι σαφές ότι αυτές οι τρεις κορυφαίες εταιρείες cloud κατέχουν ηγετική θέση στις αγορές υποδομής ως υπηρεσία (IaaS) και πλατφόρμας ως υπηρεσία (PaaS).

Η AWS είναι ιδιαίτερα δυναμική. Σύμφωνα με έκθεση του 2020 της Synergy Research Group (Group, 2021), "η ανάπτυξη της Amazon συνέχισε να αντικατοπτρίζει στενά τη συνολική

ανάπτυξη της αγοράς, ώστε να διατηρήσει το 33% του μεριδίου της στην παγκόσμια αγορά [cloud]. Η δεύτερη στην κατάταξη Microsoft αναπτύχθηκε και πάλι ταχύτερα από την αγορά και το μερίδιο αγοράς της αυξήθηκε κατά σχεδόν τρεις ποσοστιαίες μονάδες τα τελευταία τέσσερα τρίμηνα, φθάνοντας το 18%". Εν τω μεταξύ, η Microsoft είναι ιδιαίτερα ισχυρή στο SaaS, ενώ η Google Cloud, με τη δύναμή της στην τεχνητή νοημοσύνη, είναι τοποθετημένη για επιθετική ανάπτυξη καθώς η αγορά τεχνητής νοημοσύνης αναπτύσσεται - και είναι γνωστή για την προσφορά εκπτώσεων.

Με ένα τεράστιο σύνολο εργαλείων που συνεχίζει να αναπτύσσεται εκθετικά, οι δυνατότητες της Amazon είναι απαράμιλλες. Ωστόσο, η δομή του κόστους της μπορεί να προκαλέσει σύγχυση και η εστίασή της στο δημόσιο cloud και όχι στο υβριδικό cloud ή στο ιδιωτικό cloud σημαίνει ότι η διαλειτουργικότητα με το κέντρο δεδομένων δεν είναι η κορυφαία προτεραιότητα της AWS. Ένας στενός ανταγωνιστής του AWS με μια εξαιρετικά ικανή υποδομή cloud είναι το Microsoft Azure. Το Azure μιλάει τη γλώσσα των πελατών του, αφού λίγες είναι οι εταιρείες που έχουν το επιχειρηματικό υπόβαθρο (και την υποστήριξη των Windows) όπως η Microsoft. Η Azure γνωρίζει ότι εξακολουθεί ο πελάτης να διαχειρίζεται ένα κέντρο δεδομένων και η πλατφόρμα Azure εργάζεται σκληρά για να διαλειτουργεί με κέντρα δεδομένων- το υβριδικό cloud είναι ένα πραγματικό πλεονέκτημα. Η Google προσφέρει στην αγορά το Google Cloud, ένα καλά χρηματοδοτημένο αουτσάιντερ στον ανταγωνισμό. Η Google κατάφερε έτσι και ενώ εισήλθε στην αγορά cloud αργότερα, δεν έχει τόσο μεγάλη εστίαση στις επιχειρήσεις που βοηθά στην προσέλκυση εταιρικών πελατών. Όμως η τεχνογνωσία της είναι βαθιά και τα κορυφαία εργαλεία της στον τομέα της βαθιάς μάθησης και της τεχνητής νοημοσύνης, της μηχανικής μάθησης και της ανάλυσης δεδομένων αποτελούν σημαντικά πλεονεκτήματα.



Εικόνα 5-1: Μαγικό τεταρτημόριο για υποδομές cloud και υπηρεσίες πλατφόρμας (ΠΗΓΗ)

Αυτό το μαγικό τεταρτημόριο της Gartner δείχνει την κυρίαρχη θέση του AWS έναντι του Microsoft Azure έναντι του Google Cloud Platform. Αναμένετε ότι αυτό θα αλλάξει σημαντικά με την πάροδο του χρόνου, καθώς το Alibaba Cloud, το Oracle Cloud και το IBM Cloud συνεχίζουν να εξελίσσονται. Κάθε ένας από τους κορυφαίους προμηθευτές έχει συγκεκριμένα πλεονεκτήματα και αδυναμίες που τον καθιστούν καλή επιλογή για ορισμένα έργα - δεν υπάρχει λύση cloud "ένας κάνει τα πάντα".

Το μεγαλύτερο πλεονέκτημα της Amazon είναι η κυριαρχία της στην αγορά του δημόσιου cloud. Στο Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, η Gartner σημείωσε: "Η AWS είναι ο ηγέτης του μεριδίου αγοράς στο cloud IaaS για πάνω από 10 χρόνια". Μέρος του λόγου της δημοτικότητάς του είναι αναμφίβολα το τεράστιο εύρος των δραστηριοτήτων της. Η AWS διαθέτει ένα τεράστιο και αυξανόμενο φάσμα διαθέσιμων υπηρεσιών, καθώς και το πιο ολοκληρωμένο δίκτυο παγκόσμιων κέντρων δεδομένων. Η έκθεση της Gartner το συνόψισε λέγοντας: "Η AWS είναι ο πιο ώριμος, έτοιμος για

επιχειρήσεις πάροχος, με τις βαθύτερες δυνατότητες για τη διαχείριση μεγάλου αριθμού χρηστών και πόρων". Οι μεγάλες αδυναμίες της Amazon σχετίζονται με το κόστος. Ενώ η AWS μειώνει τακτικά τις τιμές της, πολλές επιχειρήσεις δυσκολεύονται να κατανοήσουν τη δομή του κόστους της εταιρείας και να διαχειριστούν αποτελεσματικά το κόστος αυτό όταν εκτελούν μεγάλο όγκο φορτίων εργασίας στην υπηρεσία. Σε γενικές γραμμές, ωστόσο, αυτά τα μειονεκτήματα υπερκαλύπτονται από τα δυνατά σημεία της Amazon και οργανισμοί όλων των μεγεθών συνεχίζουν να χρησιμοποιούν την AWS για μια μεγάλη ποικιλία φόρτων εργασίας.

Η Microsoft ήρθε αργότερα στην αγορά του cloud, αλλά έδωσε στον εαυτό της ένα προβάδισμα, παίρνοντας ουσιαστικά το λογισμικό της στις εγκαταστάσεις της - Windows Server, Office, SQL Server, Sharepoint, Dynamics Active Directory, .Net και άλλα - και επαναπροσδιορίζοντάς το για το cloud. Ένας σημαντικός λόγος για την επιτυχία του Azure: τόσες πολλές επιχειρήσεις αναπτύσσουν τα Windows και άλλο λογισμικό της Microsoft. Επειδή το Azure είναι στενά ενσωματωμένο με αυτές τις άλλες εφαρμογές, οι επιχειρήσεις που χρησιμοποιούν πολύ λογισμικό της Microsoft συχνά διαπιστώνουν ότι είναι]λογικό να χρησιμοποιούν το Azure. Αυτό ενισχύει την αφοσίωση των υφιστάμενων πελατών της Microsoft. Επίσης, εάν είστε ήδη υφιστάμενος επιχειρηματικός πελάτης της Microsoft, αναμένετε σημαντικές εκπτώσεις στα συμβόλαια παροχής υπηρεσιών. Από την πλευρά των μειονεκτημάτων, η Gartner βρίσκει λάθη σε ορισμένες από τις ατέλειες της πλατφόρμας. "Ενώ το Microsoft Azure είναι μια πλατφόρμα έτοιμη για επιχειρήσεις, οι πελάτες της Gartner αναφέρουν ότι η εμπειρία των υπηρεσιών μοιάζει λιγότερο έτοιμη για επιχειρήσεις από ό,τι περίμεναν, δεδομένης της μακράς ιστορίας της Microsoft ως προμηθευτή επιχειρήσεων", αναφέρεται. "Οι πελάτες αναφέρουν προβλήματα με την τεχνική υποστήριξη, την τεκμηρίωση, την εκπαίδευση και το εύρος του οικοσυστήματος συνεργατών ISV".

Η Google έχει μια ισχυρή προσφορά στα κοντέινερ, καθώς η Google ανέπτυξε το πρότυπο Kubernetes που προσφέρουν τώρα οι AWS και Azure. Η GCP ειδικεύεται σε προσφορές υψηλού υπολογιστικού δυναμικού, όπως Big Data, analytics και machine learning. Προσφέρει επίσης σημαντική κλίμακα και εξισορρόπηση φορτίου - η Google γνωρίζει τα κέντρα δεδομένων και τον γρήγορο χρόνο απόκρισης. Στα αρνητικά, η Google είναι μακράν τρίτη σε μερίδιο αγοράς, ίσως επειδή δεν έχει την παραδοσιακή σχέση με τους πελάτες των επιχειρήσεων. Ωστόσο, επεκτείνει γρήγορα τόσο τις προσφορές της όσο και το αποτύπωμα των παγκόσμιων κέντρων δεδομένων της. Η Gartner δήλωσε ότι "οι πελάτες της επιλέγουν

συνήθως το GCP ως δευτερεύοντα πάροχο και όχι ως στρατηγικό πάροχο, αν και το GCP επιλέγεται όλο και περισσότερο ως στρατηγική εναλλακτική λύση για το AWS από πελάτες των οποίων οι επιχειρήσεις ανταγωνίζονται την Amazon και οι οποίες είναι περισσότερο επικεντρωμένες στον ανοικτό κώδικα ή στο DevOps και, ως εκ τούτου, είναι λιγότερο καλά προσαρμοσμένες στο Microsoft Azure".

ΣΥΜΠΕΡΑΣΜΑΤΑ - ΕΠΙΛΟΓΟΣ

Συνοψίζοντας, σε αυτό το τελευταίο κομμάτι της παρούσας εργασίας θα επικεντρωθούμε στα πιο σημαντικά στοιχεία του «Υπολογιστικού Νέφους», όπως αυτά αναφέρθηκαν παραπάνω. Υπενθυμίζουμε πως όταν αναφερόμαστε στον όρο «Υπολογιστικό Νέφος» κάνουμε λόγο για υπολογιστικούς πόρους (υλικό και λογισμικό) που χρησιμοποιούμε χρησιμοποιούνται ως υπηρεσία μέσω δικτύου και κυρίως του Internet.

Με το «Υπολογιστικό Νέφος» είναι δυνατή η εξ αποστάσεως διαχείριση υπηρεσιών, δεδομένων, λογισμικού και υπολογιστικού μέρους από τον κάθε χρήστη. Το κέρδος που έφερε η εν λόγω υπηρεσία σχετίζεται όπως κάθε ανακάλυψη με την μείωση του κέρδους. Ειδικότερα με την εφαρμογή των υπηρεσιών του υπολογιστικού νέφους τα πολυδάπανα συστήματα υπολογιστών ανήκουν πλέον στο παρελθόν.

Η αρχιτεκτονική αποτελείται από πέντε ουσιώδη χαρακτηριστικά. Αυτά είναι:

- Αυτό- εξυπηρέτηση κατά απαίτηση (on-demand-self-service).
- Ευρεία πρόσβαση στο δίκτυο.
- Διάθεση Πόρων (Recource pooling).
- Ταχεία Ελαστικότητα.
- Μετρίσιμες Υπηρεσίες.

Το μοντέλο IaaS χρησιμοποιεί τεχνολογία, υπηρεσίες, επενδύσεις και δεδομένα για την παροχή ποικίλων υπηρεσιών στους πελάτες. Τα κύρια πλεονεκτήματα της χρήσης του είναι τα εξής:

- Χρήση της πιο πρόσφατης τεχνολογίας επεξεργασίας υποδομών.

- Ασφαλής υπολογιστική πλατφόρμα
- Ελαχιστοποιεί τον κίνδυνο ιδιοκτησίας των πόρων του ιστότοπου από τρίτους. Δυνατότητα διαχείρισης των υπηρεσιών σε περιόδους υψηλής και χαμηλής ζήτησης.
- Μείωση του κόστους των υπηρεσιών.

Οι υπηρεσίες PaaS επιτρέπουν στους χρήστες να επικεντρωθούν στην καινοτομία και όχι στην πολύπλοκη υποδομή. Οι οργανισμοί μπορούν να δαπανήσουν σημαντικά τμήματα του προϋπολογισμού τους για την ανάπτυξη προγραμμάτων που παρέχουν πραγματική επιχειρηματική αξία αντί να δημιουργούν προβλήματα υποδομής. Έτσι, το μοντέλο "λογισμικό ως υπηρεσία" είναι μια διανομή λογισμικού στην οποία οι εφαρμογές φιλοξενούνται από έναν προμηθευτή ή πάροχο υπηρεσιών και διατίθενται στους πελάτες στο Διαδίκτυο. Τα οφέλη του SaaS για τους πελάτες περιλαμβάνουν:

- Ενισχυμένη διαχείριση
- Υπηρεσία αυτόματης ενημέρωσης και διαχείρισης κώδικα
- Τα δεδομένα είναι B2B (όλοι οι χρήστες χρησιμοποιούν την ίδια έκδοση λογισμικού)
- Όλα τα δεδομένα είναι κοινά σε όλη την επιχείρηση.
- Όλα τα δεδομένα είναι εταιρικά - συλλέγονται ευρέως - όλα τα δεδομένα μοιράζονται σε όλη την επιχείρηση
- ευρεία παγκόσμια εμβέλεια

Αναφορικά με το μείζον θέμα που προκύπτει από τη χρήση συστημάτων υπολογιστικού νέφους, τα επίπεδα ασφαλείας δηλαδή, από τη μελέτη που πραγματοποιήσαμε διαπιστώθηκε ότι τα περισσότερα ζητήματα έχουν να κάνουν με προβλήματα που προκύπτουν από τις υπηρεσίες δικτύου και από τα προγράμματα περιήγησης παρά με τη φιλοσοφία που έχει στηθεί το cloud computing και τον τρόπο λειτουργίας του.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Andrei, T. (2009). Cloud Computing Challenges and Related Security Issues.

Betcher T. (2010). *Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners* University of Oregon].

Buyya R. et. al. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6), 599-616. https://doi.org/10.1016/j.future.2008.12.001

Carr N. (2008). *The Big Switch Rewiring the World, from Edison to Google*.

Cassavoy L. (2013). *Five free Dropbox tools you're not using (but should be)*. https://www.pcworld.com/article/2046475/five-free-dropbox-tools-youre-not-using-but-should-be-.html

Choudhary V. (2007). Software as a Service: Implications for Investment in Software Development. 40th Hawaii International Conference on System Sciences, Hawaii

Chow R. et. al. (2009). *Controlling data in the cloud* Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09,

Cucinotta, T., Checconi, F., Kousiouris, G., Konstanteli, K., Gogouvitis, S., Kyriazis, D., Varvarigou, T., Mazzetti, A., Zlatev, Z., Papay, J., Boniface, M., Berger, S., Lamp, D., Voith, T., & Stein, M. (2011). Virtualised e-Learning on the IRMOS real-time Cloud. *Service Oriented Computing and Applications*, *6*(2), 151-166. https://doi.org/10.1007/s11761-011-0089-4

Drobox. (2021). *Do the costs of the cloud outweigh the benefits?* https://www.economist.com/business/2021/07/03/do-the-costs-of-the-cloud-outweigh-the-benefits

Dupre L. (2012). *Cloud Computing Security Risk Assessment*.

Foster I. Kesselman C. (2003). *The Grid 2. Blueprint for a New Computing Infrastructure* (2nd ed.). Morgan Kaufmann.

GNI. (2009). Demystifying the cloud: Important opportunities, crucial choices.

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). *The Characteristics of Cloud Computing* 2010 39th International Conference on Parallel Processing Workshops,

Group, S. R. (2021). *2020 – The Year that Cloud Service Revenues Finally Dwarfed Enterprise Spending on Data Centers*.

Hoff C et. al. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing*.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). *On Technical Security Issues in Cloud Computing* 2009 IEEE International Conference on Cloud Computing,

Kapil Bakshi K. (2009). *Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions*.

Kumar R. et.al. (2014). *OpenNebula: Open Source IaaS Cloud Computing Software Platforms* National Conference on Computational and Mathematical Sciences, Jaipur.

Ma S. (2012). A Review on Cloud Computing Development. https://doi.org/10.4304/jnw.7.2.305-310

Mahmood Z. (2013). *Cloud Computing Concepts, Technology Architecture* ServiceTech Press.

Marinescu C. (2012). Cloud Computing and Computer Clouds. *Journal of Technology Research*.

Marinescu D. (2018). *Cloud Computing Theory and Practice* (Second ed.). Morgan Kaufmann publications.

Mather T.; Kumaraswamy S.;Latif S. (2009). *Cloud Security and Privacy*. O'Reilly Media, Inc., .

Mell P., G. T. (2011). *The NIST Definition of Cloud Computing* (Recommendations of the National Institute of Standards and Technology, Issue.

Refan S. (2011). *Cloud Computing's effect on Enterprises* LUND UNIVERSITY].

Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y. (2010). Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing*, *9*(1), 3-26. https://doi.org/10.1007/s10723-010-9171-y

Rittinghouse J. Ransome J., I., Management, & Security, a. (2010). *Cloud Computing*.

Shimba F. (2010). *Cloud Computing:Strategies for Cloud Computing Adoption* Technological University Dublin]. Dublin.

Staff, S. (2001). *Software as a Service: Strategic Backgrounder*.

Stanoevska-Slabeva, K., & Wozniak, T. (2010). Cloud Basics – An Introduction to Cloud Computing. In *Grid and Cloud Computing* (pp. 47-61). https://doi.org/10.1007/978-3-642-05193-7_4

Turner M. et. al. (2003). Turning Software into a Service. *IEEE Computer Society*.

Vaquero L et.al. (2009). A Break in the Clouds: Towards a Cloud Definition. *ACM SIGCOMM Computer Communication Review*, *39*, 50-56.

Velte A. et.al. (2010). *Cloud Computing_A Practical Approach* McGraw-Hill.

Xiaojun Yu. , Q. W. (2010). *A View about Cloud Data Security from Data Life Cycle*

Μπαμπάνη Ε. (2018). *ΔΙΚΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ* [ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ, ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ].

ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ