Πτυχιακή εργασία

Ασφάλεια και εφαρμογές Cloud Computing

Όνομα: ΤΣΕΣΜΕΛΗΣ ΒΑΣΙΛΕΙΟΣ

Τμήμα: Η/Υ ΣΥΣΤΗΜΑΤΩΝ

Ημερομηνία: Μάρτιος 2018

Επιβλέπων καθηγητής: ΓΙΑΝΝΑΚΟΠΟΥΛΟΣ Π.

Περιεχόμενα

Περίληψη

Η παρούσα πτυχιακή εργασία ¨Ασφάλεια και εφαρμογές του Cloud Computing¨ εκπονήθηκε βάση του προγράμματος σπουδών του τμήματος μηχανικών Ηλεκτρονικών Υπολογιστικών Συστημάτων του πανεπιστήμιου Πειραιά Τ.Τ..

Επιλέγοντας την ανάλυση αυτού του ζητήματος, γίνεται λόγος για την κατανόηση της έννοιας της ορολογίας "Cloud Computing" ξεκινώντας από την ιστορική αναδρομή της ενότητας καθώς επίσης και μια πιο αναλυτική περιγραφή των ενοτήτων και των υπηρεσιών οι οποίες την αποτελούν αντίστοιχα. Εν συνεχεία, γίνεται ανάλυση της ασφάλειας η οποία παρέχεται στο πλαίσιο της παροχής των υπηρεσιών του Cloud Computing όπως επίσης και ανάλυση των σχετικών εφαρμογών του Nimbus, OpenNebula, OpenStack, CloudStack και Eucalyptus Cloud.

Το Cloud Computing είναι το σύνολο μηχανημάτων (hardware), δικτύων, αποθηκευτικών χώρων, υπηρεσιών καθώς και διεπαφών που διανέμουν από κοινού τον κάθε επιθυμητό υπολογισμό ως ανάλογη υπηρεσία. Οι υπηρεσίες «νέφους» περιλαμβάνουν την παροχή λογισμικού, υποδομών και αποθήκευσης μέσω του διαδικτύου, είτε ως απομονωμένα δεδομένα, είτε ως ολοκληρωμένη πλατφόρμα βασισμένη σε αυτό που έχει ζητήσει ο χρήστης.

Το Cloud Computing έχει ιδιαίτερα πλεονεκτήματα όχι μόνο για τους προμηθευτές του αλλά και για τους χρήστες του. Ορισμένα από τα χαρακτηριστικά του, όπως το «κατά απαίτηση» και το "self provisioning" σημαίνουν ότι, όταν οι οργανισμοί χρειάζονται υπολογιστικούς πόρους, αυτοί μπορούν να ανατεθούν, ενώ η γρήγορη ευελιξία τους σημαίνει ότι οι πόροι μπορούν να προσφερθούν ανάλογα με το πόσο υψηλές είναι οι απαιτήσεις του χρήστη και ακόμα πιο σημαντικά, όταν δεν χρησιμοποιούνται επαναφέρονται είτε απελευθερώνονται. Παρόλα αυτά, όπως οτιδήποτε καινούριο, έτσι και το cloud computing είχε αντιδράσεις δυσπιστίας και αυτό λόγω προβληματισμών που προέκυψαν κατά την εφαρμογή του.

Abstract

The presented dissertation “Security and technologies of cloud Computing” has been created based on the graduate program of studies in sector of Computer Systems of Piraeus University.

Analyzing this subject matter, it is mentioned the meaning of “Cloud Computing” starting from the historic background of the term as well a detailed description of the units and services which apart it accordingly. In continuation, there is an analysis regarding to the security which is provided from Cloud Computing as well as an analysis of its technologies, Nimbus, OpenNebula, OpenStack, CloudStack and Eucalyptus Cloud. Cloud Computing is a combination of hardware, networks, storage facilities, services and interfaces that distribute together each desired calculation as a service accordingly. Cloud services include the provision of software, infrastructure, and storage through the Internet, as separated components or as a completed platform based on what the user is requiring.

The Cloud Computing has assets of great concern, not only for suppliers but also for users too. Some of its features, such as "on demand" and "self provisioning" means that when organizations need computing resources, they can be assigned. Moreover, fast flexibility means that resources can be offered depending on, how high the requirements of the user can be and also important, when are not in use can be reset or released. Despite that, as any new service in the market, cloud computing has also caused controversy and disbelief caused by natural problems which had been arisen due to its implementation.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαιτέρως τον επιβλέποντα καθηγητή μου Κ^{ο} Γιαννακόπουλο ο όποιος με βοήθησε παρά πολύ κατά τη διάρκεια της εκπόνησης της εργασίας μου. Του οφείλω τις θερμότατες ευχαριστίες γιατί με τις ουσιώδεις υποδείξεις του και την καθοδήγησή του, συνέβαλε αποφασιστικά στην ολοκλήρωση και στην ομαλή διεκπεραίωση της συγγραφής αυτής της πτυχιακής εργασίας. Αφιέρωσε τον πολύτιμο χρόνο του, για αυτό και τον ευχαριστώ θερμά για την στήριξη και το ενδιαφέρον του και την εξολοκλήρου καθοδήγησή του για την εκπόνηση της εργασίας μου.

ΚΕΦΑΛΑΙΟ 1ο

1.1. Περιγραφή του Cloud Computing

Το Cloud Computing εμφανίστηκε στα μέσα της δεκαετίας του 1990 για να καλύψει τις ανάγκες των χρηστών σε λίγο χρόνο και με τη μεγαλύτερη απόδοση, από τις εταιρείες παροχής Ιντερνέτ όταν το κόστος των υπέρ-υπολογιστών ήταν υπέρογκο, οι εταιρείες τηλεπικοινωνιών που ενδιαφέρονταν παλαιότερα κατά βάση με point-to-point κυκλώματα δεδομένων, ξεκίνησαν να παρέχουν εικονικού ιδιωτικού δικτύου (VPN) υπηρεσίες υψηλής ποιότητας, αλλά σε πολύ χαμηλότερο κόστος.

Με την διαφοροποίηση της κυκλοφορίας δικτύου για να εξισσοροπηθεί η ζήτηση σε αυτό, κατά βούληση, θα ήταν σε θέση να λάβουν το συνολικό εύρος ζώνης του δικτύου τους πιο αποτελεσματικά. Το σύμβολο του σύννεφου χρησιμοποιήθηκε για να υποδηλώσει το σημείο αναφοράς μεταξύ των δυνατοτήτων του παρόχου και των δυνατοτήτων των χρηστών. Το «Υπολογιστικό Νέφος» διευρύνει το όριο αυτό αναφορικά με την χρήση των διακομιστών, όπως και την υποδομή του δικτύου.

Η κύρια ιδέα του «Υπολογιστικού Νέφους» χρονολογείται από τη δεκαετία του 1950, όταν μεγάλης κλίμακας κεντρικών υπολογιστών, άρχισαν να διατίθενται σε πανεπιστήμια και επιχειρήσεις, προσβάσιμα μέσω ατομικών τερματικών. Επειδή ήταν πολύ ακριβή η απόκτηση τέτοιου είδους κεντρικού υπολογιστή, ήταν αναγκαίο να βρεθούν τρόποι να έχουμε τη μέγιστη απόδοση της επένδυσης σε αυτά, επιτρέποντας σε πολλούς χρήστες να μοιράζονται ταυτόχρονα την φυσική πρόσβαση στον κεντρικό υπολογιστή από ξεχωριστά τερματικά, καθώς και να μοιράζονται το χρόνο της CPU, ελαττώνοντας τις περιόδους αδράνειας, γνωστή στη βιομηχανία των δικτύων ως time sharing.

Ενώ οι υπολογιστές έγιναν ευρέως διαδεδομένοι, οι επιστήμονες και οι τεχνολόγοι ήθελαν να διερευνήσουν τρόπους ώστε να διατίθεται μεγάλου βεληνεκούς υπολογιστική δύναμη σε πιο πολλούς χρήστες μέσω του καταμερισμού του χρόνου. Αυτό θα γινόταν με τη χρήση αλγορίθμων, ώστε τόσο η υποδομή όσο και οι εφαρμογές να παρέχουν την αποδοτικότερη χρήση τους, με προτεραιότητα στην πρόσβαση της CPU για την καλύτερη εξυπηρέτηση των τελικών χρηστών. Σχεδόν όλα τα σύγχρονα στοιχεία του «Υπολογιστικού Νέφους», η ελαστική διάταξη, η

απευθείας σύνδεση, η ψευδαίσθηση του άπειρου χώρου, σε σύγκριση με τη βιομηχανία ηλεκτρικής ενέργειας και τη χρήση των δημόσιων υπηρεσιών μιας κοινότητας, είχαν διερευνηθεί το 1966 στο βιβλίο του Douglas Parkhill, «The Challenge of the Computer Utility». Άλλοι μελετητές έχουν σημειώσει ότι οι ρίζες του «Υπολογιστικού Νέφους» εμφανίστηκαν στη δεκαετία του 1950, όταν ο επιστήμονας Herb Grosch (ο συντάκτης του νόμου Grosch), θεωρούσε ότι ολόκληρος ο κόσμος θα μπορούσε να λειτουργήσει με τερματικά που θα χρησιμοποιούσαν 15 μεγάλα κέντρα δεδομένων. Λόγω της αξίας αυτών των υπολογιστών, πολλές εταιρείες και φορείς θα μπορούσαν να επωφεληθούν από την αποδοτικότητα τους μέσω του καταμερισμού του χρόνου, όπως η GEISCO της GE, η IBM, η Tymshare (ιδρύθηκε το 1966). Ήδη από το 1970 ένα ήταν κοινό αποδεκτό: η παγκοσμίως παρούσα διαθεσιμότητα των δικτύων υψηλής χωρητικότητας, οι υπολογιστές και συσκευές αποθήκευσης χαμηλού κόστους, καθώς και η γενικότερη υιοθέτηση της service oriented αρχιτεκτονικής έχουν οδηγήσει σε τεράστια ανάγκη εξέλιξης του Cloud Computing. Εν συνεχεία, η Amazon είχε έδραιωτικό ρόλο στην ανάπτυξη του «Υπολογιστικού Νέφους» με τον εκσυγχρονισμό των κέντρων δεδομένων της, η οποία, όπως και τα περισσότερα δίκτυα υπολογιστών, χρησιμοποιούσαν μόλις το 10% της χωρητικότητάς τους ανά πάσα στιγμή, για να αφήσει χώρο για περιστασιακές αιχμές χρήσης του δικτύου. Αφού διαπίστωσε ότι η νέα αρχιτεκτονική τύπου σύννεφο οδήγησε σε σημαντικές εσωτερικές βελτιώσεις της αποτελεσματικότητας προσθέτοντας νέες λειτουργίες, η Amazon άρχισε μια προσπάθεια εξέλιξης για να παρέχει ένα καινούργιο προϊόν, το «Υπολογιστικό Νέφος» σε εξωτερικούς πελάτες.

Το αποτέλεσμα αυτής της προσπάθειας ήταν το Amazon Web Service (AWS) με υπολογιστική χρησιμότητα (Utility computing) από το 2006. Στις αρχές του 2008, το Eucalyptus Cloud έγινε η πρώτη ανοιχτού τύπου, AWS API συμβατή πλατφόρμα για την ανάπτυξη των ιδιωτικών σύννεφων. Στις αρχές του 2008, η OpenNebula, ενισχύεται με το πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή «RESERVOIR», και έγινε έτσι το πρώτο λογισμικό ανοιχτού κώδικα για την ανάπτυξη των ιδιωτικών και υβριδικών σύννεφων, για την ομοσπονδία των σύννεφων.

Κατά το ίδιο έτος, οι προσπάθειες επικεντρώθηκαν στην παροχή υψηλής ποιότητας υπηρεσιών για υποδομές βασισμένες στα σύννεφα, στο πλαίσιο προγράμματος που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή με το όνομα

«IRMOS», με αποτέλεσμα να δημιουργηθεί ένα περιβάλλον σύννεφου σε πραγματικό χρόνο. Έως τα μέσα του 2008, η εταιρία Gartner θεώρησε ευκαιρία για το «Υπολογιστικό Νέφος», να διαμορφώσει τη σχέση μεταξύ των καταναλωτών των υπηρεσιών πληροφορικής, σε εκείνους που χρησιμοποιούν τις υπηρεσίες πληροφορικής και εκείνους που τις πωλούν ξεχωριστά, αρχίζοντας να στρέφεται στην αξιοποίηση του Cloud Computing. Το 2011, η IBM ανακοίνωσε τη χρήση του Smarter Computing framework για την υποστήριξη του Smarter Planet. Το 2012, ο Δρ. John Biju και ο Δρ. Souheil Khaddaj χαρακτηρίζουν το σύννεφο ως μια εικονική και σημασιολογική πηγή πληροφοριών, αναφέροντας ότι το «Υπολογιστικό Νέφος» είναι μια καθολική συλλογή των δεδομένων που εκτείνεται πάνω από το διαδίκτυο, με τη μορφή των πόρων όπως το υλικό πληροφοριών, διάφορες πλατφόρμες, υπηρεσίες και διαμορφώνει επιμέρους μονάδες στο εικονικό περιβάλλον.

Η τεχνολογία αυτή είχε ραγδαία ανάπτυξή, κατάφερε από απλό εσωτερικό σύστημα για τα τμήματα των IT να εξελιχθεί σε δημόσια υπηρεσία, από απλό εργαλείο εξοικονόμησης κόστους σε κερδοφόρα τεχνολογία. Το Cloud Computing θεωρείται ότι αποτελείται από μεγάλα κέντρα δεδομένων, τα οποία προσφέρουν οικονομίες κλίμακας, φθηνότερη υπολογιστική ισχύ και κυρίως, την ευελιξία να πληρώνει κανείς μόνο για οτιδήποτε χρησιμοποιεί. Υπηρεσίες πληροφορικής για ιδιώτες και οργανισμούς φιλοξενούνται στο Διαδίκτυο και έτσι δεν υπάρχει ανάγκη για τοπικούς διακομιστές στο χώρο τους. Οι υπολογιστές βρίσκονται σε κέντρα δεδομένων σχεδιασμένα για τη βέλτιστη ενεργειακή αποδοτικότητα (για παράδειγμα, όσο το δυνατόν πιο κοντά σε σταθμούς παραγωγής ενέργειας). Επιπλέον, επιχειρήσεις και οργανισμοί αποφεύγουν την επένδυση και τη χρήση επιπλέον εξοπλισμού για να καλύψουν εποχιακές ανάγκες τους προβαίνοντας απλώς στη χρήση του συννέφου αντιστοίχως χωρίς να θεωρείται αναγκαία η αγορά σχετικού επιπλέον εξοπλισμού.

Cloud Computing

Το Cloud Computing υπηρεσία σύννεφου αναφέρεται τόσο στις εφαρμογές που παρέχονται ως υπηρεσίες μέσω του διαδικτύου όπως και στο υλικό και τα συστήματα λογισμικού στα ποικίλα κέντρα δεδομένων που παρέχουν αυτές τις υπηρεσίες. Ο όρος του Cloud Computing στηρίζεται σε κάποια βασικά χαρακτηριστικά, όπως οι κοινόχρηστοι πόροι (multitenancy), οι τεράστιες δυνατότητες κλιμάκωσης, η ελαστικότητα, το pay as you go, και η προμήθεια (self-provisioning) των πόρων.

- **Multitenancy (κοινόχρηστοι πόροι)**

Εν αντιθέσει με έτερα μοντέλα υπολογιστών, τα οποία ανέλαβαν αποκλειστικούς πόρους όπως οι υπολογιστικές εγκαταστάσεις που είναι για ένα μόνο χρήστη είτε ιδιοκτήτη, το Cloud Computing στηρίζεται σε ένα επιχειρηματικό μοντέλο στο οποίο οι πόροι διαμοιράζονται, δηλαδή, διάφοροι χρήστες χρησιμοποιούν τον ίδιο πόρο, στα επίπεδα δικτύου, φιλοξενίας και στο επίπεδο εφαρμογής.

- **Massive scalability (δυνατότητες κλιμάκωσης)**

Ενώ οι οργανισμοί μπορεί να έχουν εκατοντάδες είτε χιλιάδες συστήματα, το Cloud Computing δίνει τη δυνατότητα να κλιμακωθούν σε δεκάδες χιλιάδες συστήματα, καθώς επίσης και την δυνατότητα να κλιμακώνει μαζικά το εύρος ζώνης και το χώρο αποθήκευσης.

- **Ελαστικότητα**

Οι χρήστες του Cloud Computing έχουν τη δυνατότητα να αυξάνουν και να μειώνουν άμεσα τους υπολογιστικούς τους πόρους, ανάλογα με τις απαιτήσεις τους, καθώς και να απελευθερώνουν πόρους για άλλες χρήσεις, όταν δεν είναι πλέον απαραίτητοι.

- **Pay as you go**

Οι χρήστες πληρώνουν μόνο για τους πόρους που αποκλειστικά έχουν χρησιμοποιήσει και μόνο για το χρόνο που τα χρειάζονται.

- **Self - provisioning των πόρων (αυτοεξυπηρέτηση)**

Οι χρήστες αυτοεξυπηρετούνται με τους πόρους, όπως πρόσθετα συστήματα για δυνατότητα επεξεργασίας του λογισμικού και αποθήκευσης καθώς επίσης και τους πόρους δικτύου. Ένα από τα βασικά χαρακτηριστικά του Cloud Computing είναι η ελαστικότητα των πόρων. Αυτή η δυνατότητα του δίνει τη δυνατότητα στους χρήστες να αυξήσουν είτε να μειώσουν τους διάφορους υπολογιστικούς τους πόρους.

Υπάρχει φυσικά μια επίγνωση της αναφοράς των διαφόρων υπολογιστικών πόρων, αλλά η πρόβλεψη ποικίλων αναγκών είναι δύσκολη, ιδίως όταν οι απαιτήσεις αλλάζουν συνεχώς. Το Cloud Computing αποτελεί ένα τρόπο ο οποίος προσφέρει πόρους κατά απαίτηση (on demand) στο IT και address spikes σε χρήση.

Το ενδιαφέρον για το cloud μεγαλώνει καθώς οι λύσεις cloud δίνουν στους χρήστες πρόσβαση σε δυνατότητες υπερυπολογιστών (supercomputer) σε μικρό κόστος για την αγορά μια τέτοιας ολοκληρωτικής λύσης. Το πιο σημαντικό είναι ότι αυτές οι λύσεις μπορούν να αποκτηθούν κατά απαίτηση (on demand).

Το δίκτυο γίνεται υπερυπολογιστής (supercomputer) στο cloud στο οποίο οι χρήστες έχουν τη δυνατότητα να αγοράσουν αυτό που χρειάζονται, τη στιγμή όπου το χρειάζονται. Το Cloud Computing καταλαβαίνει πού παρέχονται οι κλιμακούμενες IT-enabled δυνατότητες ως υπηρεσία στους χρήστες που χρησιμοποιούν τεχνολογίες διαδικτύου.

Το Cloud Computing έχει δημιουργήσει τεράστιο ενδιαφέρον στην αγορά και πρόκειται να αναπτυχθεί πολύ, σύμφωνα με το πρόσφατο αξιοσημείωτο cloud και τα τρέχοντα έσοδα για τις cloud-based υπηρεσίες. Το Cloud Computing πρόκειται να εξελιχθεί σε μια ιδιαίτερη κινητήρια δύναμη στην ανάπτυξη των παγκόσμιων υπολογιστικών δαπανών.

Η ποικιλία των συσκευών για την πρόσβαση στο cloud έχει εξελιχθεί τα τελευταία χρόνια. Υπολογιστές στο σπίτι, υπολογιστές επιχειρήσεων, υπολογιστές δικτύου, συσκευές κινητής τηλεφωνίας, προσαρμοσμένες συσκευές χειρός, και στατικές συσκευές (συμπεριλαμβανομένων των ψυγείων) είναι όλα σε άμεση σύνδεση. Είναι ιδιαίτερο ότι, η ανάπτυξη του iPhone και ο πολλαπλασιασμός των διαθέσιμων εφαρμογών από το App Store της Apple, παρουσιάζει μια αύξηση από την άποψη πρόσβασης στο cloud. Για παράδειγμα μπορούμε πια να χρησιμοποιήσουμε το Skype μέσω του iPhone, φέρνοντας έτσι το peer-to-peer δίκτυο πολύ πιο κοντά στους χρήστες, και η Salesforce.com έφτιαξε μια εφαρμογή που δίνει τη δυνατότητα στους χρήστες να έχουν πρόσβαση στις υπηρεσίες μέσω iPhone, καθώς και μέσω smartphone άλλων εταιρειών εκτός της Apple.

- **Browsers και thin clients**

Οι χρήστες πολλαπλών τύπων συσκευών έχουν τη δυνατότητα για πρόσβαση σε εφαρμογές και πληροφορίες από οπουδήποτε μπορούν να φορτώσουν πρόγραμμα περιήγησης (browser). Στην ουσία, τα προγράμματα περιήγησης (browsers) εξελίσσονται. Σε εφαρμογές επιχειρήσεων, όπως η SAP και η Oracle, οι χρήστες έχουν πρόσβαση μέσω ενός browser interface. Οι χρήστες έχουν εξοικειωθεί με τη λειτουργία του προγράμματος περιήγησης και χρησιμοποιούν μια διακριτή εφαρμογή, όπου το πλαίσιο είναι έξυπνο, χωρίς να απαιτείται εξειδίκευση είτε άλλοι οδηγοί χρήσης.

- **High speed broadband access (ευρυζωνική πρόσβαση)**

Ένα ιδιαίτερο στοιχείο του cloud είναι το ευρυζωνικό δίκτυο, το οποίο δίνει τη δυνατότητα στα μέσα να συνδεθούν με εξαρτήματα και παρέχει μία από τις πιο ιδιαίτερες διαφορές στον όρο του Cloud Computing 30 χρόνια πρίν. Η ευρυζωνική πρόσβαση είναι πλέον διαθέσιμη παγκόσμια, ιδιαίτερα σε μητροπόλεις. Υπάρχει ασύρματη πρόσβαση όπως σε WiFi, κινητά, είτε αναδυόμενες WiMAX, η οποία έχει εφαρμόσει κινητές συσκευές ως σημεία εισόδου σε τεχνολογικούς πόρους του cloud.

- **Data centers and server farms**

Τα datacenters και τα server farms χρειάζονται Cloud-based υπηρεσίες καθώς και ιδιαίτερη υπολογιστική ικανότητα. Αυτά τα κατανεμημένα data centers και τα server farms εκτείνονται σε διάφορες τοποθεσίες και συνδέονται μέσω Internet παρέχοντας κατανεμημένα υπολογιστικά συστήματα και δυνατότητες παροχής υπηρεσιών. Μια σειρά από παραδείγματα σήμερα παρουσιάζουν την ευελιξία και την επεκτασιμότητα της δυναμικότητας του Cloud Computing. Για παράδειγμα η Salesforce.com παρέχει SaaS στην τεράστια πελατειακή βάση της, με την κατηγοριοποίηση των πελατών της σε ομάδες για να ενεργοποιήσει την επεκτασιμότητα και την ευελιξία. Από την άλλη η Google έχει συνδεθεί με ποικίλους ακριβούς servers για να παρέχει τεράστια ευελιξία και ισχύ. Επιπλέον το Amazon’s Elastic Compute Cloud (EC2), παρέχει πρόγραμμα εικονοποίησης (virtualization) στο data center για τη δημιουργία τεράστιου αριθμού από εικονικές περιπτώσεις για υπηρεσίες που έχουν ζητηθεί.

- **Storage Devices (υπηρεσίες αποθήκευσης)**

Με τη μείωση του κόστους αποθήκευσης και την ευελιξία με την οποία μπορεί να αναπτυχθεί η αποθήκευση, έχει τροποποιηθεί ο τρόπος της αποθήκευσης. Η σταθερή συσκευή αποθήκευσης άμεσης πρόσβασης (DASD – direct access storage device) έχει αντικατασταθεί με τα δίκτυα περιοχής αποθήκευσης (SAN), τα οποία έχουν ελαττώσει το κόστος και δίνουν περισσότερη ευελιξία στην αποθήκευση. Το λογισμικό SAN διαχειρίζεται την ενσωμάτωση των συσκευών αποθήκευσης και μπορεί να δίνει ανεξάρτητα χώρο αποθήκευσης κατά απαίτηση (on demand) σε διάφορες συσκευές, έκαστη εφαρμογή χρειάζεται ένα υπολογιστικό μοντέλο για αποθήκευση σε περίπτωση που υποτεθεί ότι η εφαρμογή είναι ακόμα trivially distributed, ένα μοντέλο επικοινωνίας. Η στατιστική πολυπλεξία που είναι σημαντική για να γίνει η ελαστικότητα και η ψευδαίσθηση της άπειρης χωρητικότητας απαιτεί πόρους για να είναι εικονική. Ποικίλες utility computing προσφορές θα πρέπει να ξεχωρίζονται με βάση το επίπεδο αφαίρεσης που παρουσιάζεται στον προγραμματιστή και το επίπεδο διαχείρισης των πόρων.

1.2. Τι είναι το Cloud Computing ;

Η τεχνολογία Cloud Computing (Σύννεφο) είναι εφαρμογή του διαδικτύου και αποτελείται από την απεικόνιση του διαδικτύου με διαγράμματα-παρουσιάσεις. Ποικίλα είδη πληροφοριών και υπηρεσιών διατίθενται και αλληλεπιδρούν μεταξύ τους έχοντας ως βάση τους μία κοινή πλατφόρμα. Είναι ένα σετ λογισμικών, δικτύων, αποθηκευτικών χώρων, υπηρεσιών και διεπαφών που μοιράζουν από κοινού τον κάθε υπολογισμό ως υπηρεσία. Οι υπηρεσίες «νέφους» αποτελούνται από την παροχή λογισμικού, υποδομών και αποθήκευσης μέσω του διαδικτύου (είτε ως ξεχωριστά στοιχεία, είτε ως ολοκληρωμένη πλατφόρμα) βασισμένη σε αυτό που έχει ζητήσει ο χρήστης αντιστοίχως.

Το Cloud Computing έχει ιδιαίτερα πλεονεκτήματα για τους προμηθευτές του αλλά και για τους χρήστες του. Κάποια από τα χαρακτηριστικά του, όπως το «κατά απαίτηση» και το “self provisioning” σημαίνουν ότι, όταν οι οργανισμοί χρειάζονται υπολογιστικούς πόρους, ενώ η γρήγορη ευελιξία σημαίνει ότι οι πόροι μπορούν να

διατεθούν ανάλογα με τις απαιτήσεις του χρήστη και ακόμα πιο σημαντικά, όταν δεν χρησιμοποιούνται επαναφέρονται είτε απελευθερώνονται .

Το Cloud Computing συγκρίνεται με τις παρακάτω τεχνολογίες, με τις οποίες έχει κοινά χαρακτηριστικά.

- **Utility computing (Υπολογιστική χρησιμότητα)**

Είναι σύστημα πληροφορικής με πολύ ιδιαίτερη ιστορία, το οποίο επίσης διαθέτει υπολογιστικούς πόρους, με τη διαφορά ότι γίνεται τιμολόγηση βάση της χρήσης και όχι τη σταθερή χρέωση πελατών. Το Cloud Computing μπορεί να κατανοηθεί ως η ιδανικότερη υλοποίηση του utility computing. Με τη κατανομή των πόρων της ζήτησης και της χρησιμότητας βάση των παρόχων υπηρεσιών τιμολόγησης, αυξάνει την αξιοποίηση των πόρων και ελαχιστοποιεί το κόστος λειτουργίας τους.

- **Grid computing (Τεχνολογία πλέγματος)**

Είναι διαμοιραζόμενο σύστημα πληροφορικής, το οποίο οργανώνει τους διάφορους διαδικτυακούς πόρους. Κύρια λειτουργία του είναι η διεκπεραίωση υπολογιστικών εργασιών μεγάλου όγκου που συνήθως χρειάζονται μεγάλη υπολογιστική ισχύ.

Το Cloud Computing είναι παρόμοιο με το Grid computing αναφορικά με τους κατανεμημένους πόρους για την ολοκλήρωση εφαρμογής.

- **Virtualization (Εικονικό περιβάλλον)**

Είναι τεχνολογία που ξεπερνά τους περιορισμούς του φυσικού υλικού και διαθέτει εικονικούς πόρους για ιδιαίτερου τύπου επιστημονικές εφαρμογές. Παρέχει ένα οικονομικά αποδοτικό και ευέλικτο τρόπο χρήσης και διαχείρισης των υπολογιστικών πόρων. Αυτή η τεχνική αντίστοιχα χρησιμοποιείται και στο Grid computing και στο Cloud Computing για τη καλύτερη διανομή των υπολογιστικών παροχών σύμφωνα με τη ζήτηση. Δίνει τη δυνατότητα στους πιο χαμηλούς υπολογιστικούς πόρους να τροφοδοτηθούν κατά την εκτέλεση τους από τους χρήστες σύμφωνα με τις απαιτήσεις των εφαρμογών.

1.3. Εννοιολογική Προσέγγιση της έννοιας Cloud Services (Υπηρεσίες Cloud)

Το «νέφος υπολογιστών» είναι ένα μοντέλο το οποίο επιτρέπει την απεριόριστη ζήτηση πρόσβασης σε ένα σύνολο παραμετροποιημένων υπολογιστικών πόρων (δίκτυο, διακομιστές, αποθήκευση, εφαρμογές και υπηρεσίες) οι οποίοι μπορούν να δεσμευτούν και να απελευθερωθούν γρήγορα με ελάχιστη προσπάθεια και αλληλεπίδραση.

Οι χρήστες του Cloud ζητούν την πρόσβαση από αντίστοιχη ομάδα υπηρεσιών διαδικτύου, οι οποίες διαχειρίζονται τους υπολογιστικούς πόρους (υπολογιστές, δίκτυο, αποθηκευτικός χώρος, λειτουργικά συστήματα, περιβάλλοντα ανάπτυξης εφαρμογών αλλά και εφαρμογές) οι οποίοι είναι διαθέσιμοι. Όταν δοθεί ένα τμήμα πόρων σε κάποιον χρήστη Cloud, το τμήμα αυτό είναι αποκλειστικά αφιερωμένο σε αυτόν το χρήστη μέχρι αυτός να το αποδεσμεύσει από τη χρήση του.

Ονομάζεται Cloud Computing γιατί ο χρήστης δεν μπορεί στην πραγματικότητα να καθορίσει και να αντιληφθεί το που βρίσκονται ακριβώς οι υποδομές που χρησιμοποιεί είτε τον εξοπλισμό που φιλοξενεί τις υπηρεσίες που έχει ζητήσει και έχει λάβει την άδεια να τις χρησιμοποιήσει. Σχηματικά θα μπορούσαμε να πούμε ότι οι πόροι λαμβάνονται από ένα Cloud πόρων όταν δοθούν σε κάποιο χρήστη και αυτές επιστρέφουν πίσω σε αυτό όταν αποδεσμευτούν.

1.4. Σημαντικά σημεία στην ιστορία του Cloud Computing

- Ιούλιος 2002.

Τον Ιούλιο του 2002 ξεκίνησαν οι υπηρεσίες των Amazon Web Services. Η αρχική έκδοση του AWS το 2002 ήταν στηριγμένη στη διάθεση ποικίλων πληροφοριών από την Amazon σε διάφορους συνεργάτες μέσω ενός τύπου διαδικτυακών υπηρεσιών μέσω προγραμμάτων και ανάπτυξης εφαρμογών και πιο ιδιαίτερα είχε στόχο ως μεταπράτης. Ενώ αυτό το γεγονός ορίζει το σκηνικό, στην βάση η έναρξη του S3 ήταν το πραγματικά αρχικό βήμα προς τη δημιουργία μιας πλατφόρμας Cloud.

- Μάρτιος 2006.

Το Μάρτιο του 2006 ξεκίνησε το S3 (Simple Storage Service). Η ιδιαίτερη καινοτομία που εισήγαγε το Amazon S3 ήταν το τιμολογιακό μοντέλο που δημιούργησε. Αυτό στηρίχτηκε σε μια λογική "pay-per use" (πληρωμή ανά χρήση) η οποία και έχει γίνει πλέον δεδομένο για την τιμολόγηση υπηρεσιών Cloud. Επίσης, με την εκκίνηση του S3 τοποθέτησε την Amazon από έναν απλό μεταπράτη στην θέση ενός πολύ δυνατού συμβαλλόμενου στοιχείου στον χώρο της τεχνολογίας. Ιδιαίτερες είναι οι σημαντικές κριτικές που είχε από το οικονομικό και το τεχνολογικό τύπο, αυτή η καινοτομία της Amazon.

- Αύγουστος 2006.

Τον Αύγουστο του 2006 ξεκίνησε το EC2 (Elastic Compute Cloud). Το EC2 ξεκίνησε πολύ πιο ομαλά από το S3 αλλά θεωρήθηκε ότι θα είχε μεγαλύτερη επίπτωση, κάνοντας διαθέσιμη την υποδομή υπολογιστικής ισχύος. Αυτό έκανε πιο λειτουργική και πολύ πιο συμπαγή και ολοκληρωμένη την υποδομή Cloud. Κατά βάση εκείνη η περίοδος είχε να καταπολεμήσει πολλές δυσκολίες, να γίνει κατανοητό πόσο μεγάλο θέμα ήταν, και πολύ περισσότερο θεώρησε αυτή την καινοτομία σαν μια ακόμα υπηρεσία που μπορούσε να φιλοξενήσει υπηρεσίες online απλά με ένα διαφορετικό μοντέλο τιμολόγησης.

- Απρίλιος 2008.

Τον Απρίλιο του 2008 ξεκίνησε το Google App Engine. Η έναρξη του Google App Engine ήταν η είσοδος της πρώτης εταιρίας του είδους της Google στην αγορά του Cloud Computing. Η είσοδος μιας επικρατούσας εταιρίας, στο χώρο του Internet όπως η Google, σε αυτή την αυξανόμενη αγορά ήταν ιδιαίτερα ένα πολύ μεγάλο βήμα προς την ευρεία αποδοχή και υιοθέτηση του Cloud Computing. Όπως και με όλα τα σχετικά προϊόντα έγιναν σημαντικές τιμολογιακές πολιτικές, με ένα πλάνο για δωρεάν εισαγωγικό στάδιο και με πολύ χαμηλές υπηρεσίες υπολογιστικής ισχύος και αποθηκευτικού χώρου.

- Νοέμβριος 2009.

Το Νοέμβριο του 2009 ξεκίνησε το Windows Azure Beta. Η είσοδος της Microsoft στο Cloud Computing είναι μια ιδιαίτερη ένδειξη της εξέλιξης αυτού του χώρου. Η Microsoft για πολύ καιρό δεν θεωρούσε το Διαδίκτυο σαν μια ιδιαίτερη και υποσχόμενη αγορά και συνέχιζε να δίνει σημασία στην αγορά του προσωπικού desktop υπολογιστή επί χρόνια. Έπειτα όταν αντιλήφθηκε ότι το Διαδίκτυο ήταν πολύ ιδιαίτερης σημασίας άλλαξε στάση επί του ζητήματος και έτσι συνέβαλε σε αυτό. Η έναρξη του Azure είναι ένα κλειδί στην ιστορία του Cloud Computing καθώς η μεγαλύτερη εταιρία λογισμικού πήρε μια μικρή αλλά πάρα πολύ ιδιαίτερη στροφή προς το Διαδίκτυο.

1.5. Σημαντικά λειτουργικά χαρακτηριστικά του Cloud Computing

- **Rapid elasticity**.

(Ταχεία ελαστικότητα). Αυτοί οι πόροι μπορούν να δεσμευτούν αυτομάτως, έτσι να εμφανίζουν άμεσα την ένδειξη ως μη διαθέσιμοι και να αποδεσμεύονται και επαναδεσμεύονται αμέσως. Στον καταναλωτή – τελικό χρήστη οι δυνατότητες αυτές που είναι διαθέσιμες είναι αναρίθμητες και μπορούν να αποκτηθούν σε οποιαδήποτε ποσότητα, οποιαδήποτε στιγμή .

- **Measured Service**.

(Μετρήσιμα επίπεδα παροχής υπηρεσιών). Τα συστήματα Cloud ελέγχουν και μεγιστοποιούν αυτόματα τη χρήση των υπολογιστικών πόρων, λαμβάνοντας τη χρήση συγκεκριμένων μετρητικών συστημάτων σε κάποιο από τα επίπεδα αφαίρεσης που εισάγουν, το οποίο και είναι απαραίτητο για την σχετική παρεχόμενη υπηρεσία όπως αποθηκευτικό χώρο, υπολογιστική ισχύς, εύρος ζώνης, ενεργός αριθμός χρηστών. Η χρήση των πόρων μπορεί να ελεγχθεί και να αναφερθεί ότι παρέχει διαφάνεια και για τις δύο πλευρές, τελικού χρήστη – καταναλωτή και παρόχου της χρησιμοποιούμενης υπηρεσίας .

- **On-demand self-service**.

(Αυτοεξυπηρέτηση κατά απαίτηση). Ο καταναλωτής μπορεί να χρησιμοποιήσει τους υπολογιστικούς πόρους που θέλει (όπως ο χρόνος που θα

χρησιμοποιήσει στον διακομιστή και το μέγεθος του αποθηκευτικού χώρου που θα χρησιμοποιήσει μέσω δικτύου αυτόματα) χωρίς τη διαμεσιτική συμβολή ανθρώπου με τον πάροχο της αντίστοιχης υπηρεσίας .

- **Ubiquitous network access**.

(Ευρεία δικτυακή πρόσβαση). Η δυνατότητα αυτή είναι άμεσα διαθέσιμη μέσω δικτύου και η πρόσβαση σε αυτή μπορεί να γίνει μέσω μηχανισμών και ετερόκλητων πλατφόρμων χρηστών όπως τα κινητά τηλέφωνα.

- **Location independent resource pooling**.

(Κοινή διάθεση των πόρων). Οι υπολογιστικοί πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν ποικίλους και διάφορους καταναλωτές με τη χρήση του μοντέλου πολλαπλών μισθωτών (multitenant), με τους ποικίλους φυσικούς και εικονικούς πόρους να θέτονται δυναμικά και εκ νέου σύμφωνα με τη ζήτηση των καταναλωτών. Ο καταναλωτής γενικά δεν έχει κανένα έλεγχο και γνώση για την ακριβή τοποθέτηση του παρεχόμενου πόρου, αλλά μπορεί να κατατοπίσει σε ένα πιο γενικευμένο επίπεδο την τοποθεσία όπως η χώρα η πόλη ή το συγκεκριμένο data-center. Παραδείγματα τέτοιων πόρων είναι αποθηκευτικός χώρος, επεξεργασία, μνήμη, εύρος ζώνης δικτύου, και εικονικές μηχανές.

1.6. Μοντέλα παροχής υπηρεσιών

Στη τεχνολογία του Cloud Computing χρησιμοποιούνται τρία κύρια μοντέλα παροχής υπηρεσιών, τα οποία λειτουργούν για την εξυπηρέτηση διάφορων αναγκών και υπηρεσιών. Αυτά τα μοντέλα είναι: το Software as a Service, Cloud Platform as a Service, Infrastructure as a Service.

- **Software as a Service (SaaS)**

Η λογική στην οποία στηρίζεται το Software as a Service δεν παρουσιάζεται στην αγορά της άδειας χρήσης ενός λογισμικού, αλλά στην υπενοικίασή του από έναν πάροχο υπηρεσιών. Το λογισμικό λειτουργεί σε κεντρικό δίκτυο διακομιστή και διατίθεται από το διαδίκτυο ως υπηρεσία. Είναι γνωστό και ως «software on demand»

και αποτελεί τον πιο γνωστό τύπο Cloud Computing για διαφόρους λόγους όπως ελάχιστη συντήρηση από τη μεριά του χρήστη, ποιότητα υπηρεσιών, μέγιστη ευελιξία. Στον πάροχο της υπηρεσίας διατηρούνται και τα δεδομένα και η εφαρμογή, δίνοντας τη ικανότητα στους χρήστες της να χρησιμοποιούν τις υπηρεσίες παντού. Στο μοντέλο αυτό (SaaS) ο χρήστης δεν έχει καμία υποχρέωση για συντήρηση είτε αναβάθμιση, από τη στιγμή που ο ίδιος δεν χρειάζεται να προνοήσει για τη χωρητικότητα, τη διαθεσιμότητα, και την κλιμάκωση της πλατφόρμας η της υπηρεσίας.

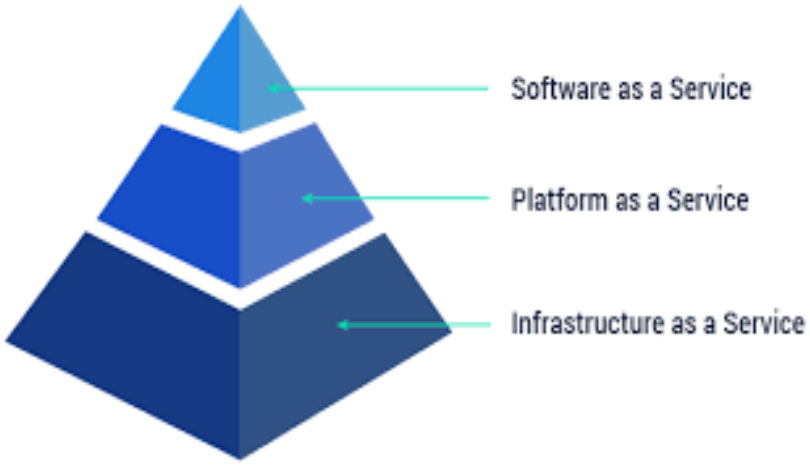
- **Platform as a Service (PaaS)**

Αυτό το μοντέλο δίνει στους χρήστες τις απαραίτητες υπηρεσίες, με στόχο να μπορέσουν να καλυτερεύσουν, να διαθέσουν και να συντηρήσουν εφαρμογές και υπηρεσίες σε ένα κοινό περιβάλλον πλατφόρμας, το οποίο είναι ευέλικτο και διαθέσιμο, δίνοντας τη δυνατότητα αυτό-διαχείρισης, αυτό-συντήρησης και αυτό-κλιμάκωσης του λειτουργικού συστήματος, της υποδομής και της πλατφόρμας εφαρμογών. Το μοντέλο που στηρίζεται το PaaS είναι το «Pay-per-use», το οποίο δίνει τη δυνατότητα να αξιοποιούνται εξολοκλήρου οι υπολογιστικοί πόροι που χρησιμοποιούνται, βάση του κόστους της χρήσης. Σε συνδυασμό με το στοιχείο της αυτό-κλιμάκωσης, μπορεί να γίνει δυνατή η διάθεση υπηρεσιών οι οποίες αντιστοίχως θα μπορούν να ανταποκριθούν σε οποιαδήποτε αλλαγή της χωρητικότητας που θα θεωρηθεί απαραίτητη, χωρίς να δεσμευτεί εκ των προτέρων σχετικά με την αγορά πλατφόρμας λογισμικού είτε υποδομής είτε με ένα συμβόλαιο που να παρέχει υπηρεσίες φιλοξενίας, υποδομής και πλατφόρμας συγκεκριμένης χρονικής διάρκειας και χωρητικότητας.

- **Infrastructure as a Service (IaaS)**

Αυτό το μοντέλο δίνει στο χρήστη τη δυνατότητα να υπενοικιάσει μόνο την υποδομή (χωρίς τη πλατφόρμα όπως αναλύσαμε παραπάνω στο PaaS), με τον ίδιο τρόπο που χρησιμοποιεί το PaaS (Pay-per-use), έναντι του να αποκτήσει εξοπλισμό είτε να κάνει συμβόλαιο παροχής υπηρεσιών φιλοξενίας υποδομής για το συγκεκριμένο χρονικό διάστημα. Ένα μεγάλο όφελος αυτού του μοντέλου είναι ότι

μπορεί να μεταφέρει άμεσα εικονικές μηχανές, από την εταιρία είτε τον ιδιώτη στο cloud, με συνοπτικές διαδικασίες. Η υποδομή του θεωρείται το μέσο αποθήκευσης, παροχής επεξεργασίας, δικτύου και άλλων βασικών υπολογιστικών πόρων.



Εικόνα 1: Pyramid of Cloud Computing

- **Storage as a service (StaaS)**

Σε αυτό το μοντέλο υπάρχει πάροχος αποθηκευτικού χώρου διαδικτυακά ο οποίος κατά κύριο λόγο τον νοικιάζει έναντι κάποιας ανάλογης αμοιβής. Ένα παράδειγμα απλό θα μπορούσε να θεωρηθεί το Dropbox.

- **Hardware as Service a (HaaS)**

Σε αυτό το μοντέλο ο προμηθευτής της υπηρεσίας σύννεφου δίνει στον χρήστη έναντι αμοιβής τον εξοπλισμό που έχει ανάγκη όπως μνήμη CPU, διακομιστές ιστού, αποθηκευτικό χώρο και ότι άλλο χρειάζεται ο χρήστης για να εξοπλιστεί. Τα χρήματα που δίνει κάποιος στο HaaS είναι σύμφωνα της χρήσεως των πόρων του συστήματος που χρησιμοποιεί.

- **Database as Service (DaaS)**

Σε αυτό το μοντέλο υπάρχει υπηρεσία διαδικτυακά η οποία δίνει την βάση δεδομένων την οποία μπορούμε να χρησιμοποιήσουμε με σχετική εφαρμογή ιστού. Το βασικό πλεονέκτημα είναι ότι πληρώνουμε σύμφωνα με την χρήση. Όσο πιο

πολλοί κάνουν χρήση την εφαρμογή μας τόσο περισσότερα πληρώνουμε. Μία τέτοια υπηρεσία είναι η mongoDB.

1.7. Μοντέλα Υπηρεσιών Cloud

Το μοντέλο μπορεί να διαχωριστεί στις παρακάτω κατηγορίες:

- **Private Cloud:**

Το Private Cloud ιδιωτικό σύννεφο: είναι ένα σύνολο υπολογιστικών πόρων που διατίθενται έτσι ώστε να καθορίζονται και να ελέγχονται από έναν αποκλειστικό οργανισμό. Σημαντικό μειονέκτημά του είναι το μεγάλο κόστος απόκτησης και λειτουργίας του. Συνήθως συγχέεται με την εικονοποίηση η οποία ωστόσο αποτελεί μόνο ένα μικρό κομμάτι του. Τα ιδιωτικά σύννεφα ωστόσο, τίθενται σε περιορισμούς ασφαλείας του οργανισμού λόγω της εφαρμογής του στο πλαίσιο ενός ήδη υπάρχοντος κέντρου δεδομένων ενός οργανισμού, παρέχοντας έτσι μεγαλύτερη ασφάλεια για τα ευαίσθητα δεδομένα. Τέλος, τα ιδιωτικά σύννεφα σταθεροποιούν και βελτιστοποιούν την απόδοση ενός υπάρχοντος εξοπλισμού σε ένα συγκεκριμένο κέντρο ελέγχου μέσω των τεχνολογιών εικονοποίησης τις οποίες χρησιμοποιούν, χαμηλώνοντας με αυτό το τρόπο τα λειτουργικά κόστη και αυξάνοντας την αποτελεσματικότητα του κέντρου δεδομένων.

- **Public Cloud:**

Το Public Cloud δημόσιο σύννεφο : είναι ένα σύνολο πόρων από υπολογιστές και δίκτυα υπολογιστών, βάση του πρότυπου Cloud Computing και είναι διαθέσιμοι μέσω διαδικτύου ενώ τις περισσότερες φορές παρέχονται από έναν πάροχο. Αυτό το μοντέλο έχει πολλά πλεονεκτήματα μερικά από τα ποία είναι οι ασφαλείς υπηρεσίες που προσφέρονται στους χρήστες, η μεγάλη ευελιξία λόγω της άμεσης διάθεσης υπηρεσιών, η ελαστικότητα και η συνεχόμενη διαθεσιμότητα, και η χρέωση η οποία αφορά μόνο τις υπηρεσίες που χρησιμοποιούνται.

- **Community Cloud:**

Το Community Cloud κοινοτικό σύννεφο: έχει υποδομή η οποία είναι διαμοιρασμένη από διάφορους οργανισμούς και εξυπηρετεί συγκεκριμένη κοινότητα. Η κοινότητα αυτή έχει συγκεκριμένο στόχο ή ενδιαφέρον. Χαρακτηριστικό αυτού του μοντέλου είναι ότι μπορεί να το διαχειρίζεται ένας οργανισμός είτε τον έλεγχο του να τον έχει ένας άλλος οργανισμός είτε επιχείρηση.

- **Hybrid Cloud**:

Το Hybrid Cloud υβριδικό σύννεφο συνδυάζει τους πόρους που προέρχονται από το Public Cloud δημόσιο σύννεφο, είτε τους πόρους που προέρχονται από ένα ή περισσότερα Private Cloud ιδιωτικά σύννεφα, ακόμα και συνδυασμό αυτών των δύο. Ένα μοντέλο Hybrid Cloud μπορεί να προσφέρει στους χρήστες του τα ακόλουθα: Επεκτασιμότητα: Ενώ τα ιδιωτικά σύννεφα προσφέρουν ένα συγκεκριμένο επίπεδο κλιμάκωσης, ανάλογα με τις ρυθμίσεις τους, τα δημόσια σύννεφα διαθέτουν επεκτασιμότητα με λιγότερα όρια, καθώς οι πόροι αποσπώνται από τη μεγαλύτερη υποδομή σύννεφου. Εξοικονομήσεις κόστους: Τα δημόσια σύννεφα είναι πιθανό να προσφέρουν πιο σημαντικές οικονομίες κλίμακας (όπως η κεντρική διαχείριση), και έτσι μεγαλύτερη αποδοτικότητα του κόστους από τα ιδιωτικά σύννεφα. Με αυτό τον τρόπο, τα υβριδικά σύννεφα επιτρέπουν στους οργανισμούς να έχουν πρόσβαση σε αυτές τις εξοικονομήσεις για όσες επιχειρηματικές λειτουργίες είναι δυνατόν, διατηρώντας ωστόσο ασφαλείς τις ευαίσθητες επιχειρήσεις. Ασφάλεια: Το ιδιωτικό σύννεφο ως στοιχείο του υβριδικού σύννεφου δεν παρέχει μόνο την ασφάλεια, που είναι απαραίτητο για τις ευαίσθητες λειτουργίες, αλλά μπορεί επίσης να εκπληρώσει τις κανονιστικές απαιτήσεις για το χειρισμό και την αποθήκευση όταν μπορεί να εφαρμοστεί. Ευελιξία: Η διαθεσιμότητα των πόρων παρέχει στους οργανισμούς περισσότερες ευκαιρίες για να εξερευνήσουν διάφορες επιχειρησιακές κατευθύνσεις.

1.8. Πλεονεκτήματα και μειονεκτήματα cloud computing.

1.8.1. Πλεονεκτήματα του Cloud Computing

Το Cloud Computing διαθέτει πλεονεκτήματα σημαντικά για το χρήστη.

Πρόσβαση από παντού : Ο χρήστης μπορεί να μπει από το διαδίκτυο στα δεδομένα που έχουν αποθηκευτεί από οποιοδήποτε σημείο του κόσμου με ασφάλεια.

Όταν η σύνδεση με το διαδίκτυο δεν είναι εφικτή, μπορούν να ικανοποιηθούν οι απαιτήσεις και μέσω του mobile internet.

Ευελιξία : Σε περίπτωση που μια εταιρεία χρειαστεί να μετακινηθεί ολόκληρη είτε κάποιο συγκεκριμένο τμήμα της, ο χρόνος που θα παραμείνει χωρίς πληροφορίες είτε ο κίνδυνος απώλειας των στοιχείων είναι μηδενικός καθώς όλα τα συστήματα και το λογισμικό παραμένουν διαθέσιμα.

Συνεργασία: Καθώς υπάρχουν τα δεδομένα αποθηκευμένα και υπάρχει διαθέσιμη πρόσβαση στο διαδίκτυο, οι εργαζόμενοι μιας επιχείρησης μπορούν να συνεργαστούν ακόμα και στη περίπτωση που βρίσκονται και εκτός του χώρου εργασίας.

Αποθηκευτικός χώρος : Ο αποθηκευτικός χώρος είναι απεριόριστος κάτι που είναι πλεονέκτημα για την επιχείρηση καθώς την αποδεσμεύει από συνεχείς αναβαθμίσεις με στόχο την εξοικονόμηση χώρου.

Καλύτερη χρήση πόρων: Παλαιότερα οι επιχειρήσεις σπαταλουσαν χρόνο για την προετοιμασία υπηρεσιών και πολλές φορές χωρίς αποτέλεσμα καθώς δεν ανταποκρίνονταν στις προσδοκίες τους. Με το Cloud Computing μειώνονται οι δαπάνες και αυξάνεται η χωρητικότητα καθώς οι πόροι διατίθενται μόνο όταν είναι απαραίτητοι.

Disaster Recovery: Σε περίπτωση καταστροφής της μηχανοργάνωσης μιας επιχείρησης, μέσω των υπηρεσιών σύννεφων μπορούν να ενεργοποιηθούν οι διαδικασίες αποκατάστασης της ζημιάς και μέσω των αντιγράφων ασφαλείας που υπάρχουν να επέλθει η λύση.

Οικονομικά Οφέλη: Η οικονομία είναι από τα βασικότερα οφέλη του cloud computing. Το κόστος που μπορεί να έχει ένα λογισμικό ίσως να είναι πολύ μεγάλο για μία μικρή εταιρία. Με το «cloud» τα δεδομένα αυτά αλλάζουν καθώς η εταιρία δεν πληρώνει την εφαρμογή αλλά πληρώνει την χρήση της. Συνήθως σε δίκτυα cloud υπάρχουν πολλές δυνατότητες και τρόποι για την πληρωμή της χρήσης κάποιας εφαρμογής.

Λογισμικό: Το λογισμικό που συνδέεται με ένα διακομιστή σύννεφου ο οποίος ενημερώνεται αυτόματα με αποτέλεσμα να βοηθά με τη σειρά του την επιχείρηση να ασχολείται μόνο με τα θέματα που την απασχολούν.

Πολλαπλές τοποθεσίες: Για την αναπαραγωγή περιεχομένου, οι πάροχοι συντηρούν κάποιους οικονομικούς πόρους κάνοντας έτσι δυνατή την αποφυγή αποτυχιών. Με αυτό τον τρόπο απορρίπτεται οποιαδήποτε ζημιά.

Διαχείριση απειλών: Ένας απλός καταναλωτής είτε μια μικρή επιχείρηση δεν έχει τα μέσα και τους τρόπους για να αντιμετωπίσει πιθανές απειλές. Οι πάροχοι των υπηρεσιών Cloud παρόλα αυτά διαθέτουν μπορούν να βρουν τρόπους ακόμα και να αναπτύξουν στρατηγικές διαχείρισης των απειλών.

Άμεση ανταπόκριση σε οποιαδήποτε πρόκληση: Οι πάροχοι των υπηρεσιών Cloud μπορούν να αντιληφθούν άμεσα ένα κακόβουλο λογισμικό λόγω της εφαρμογής συστημάτων που τους επιτρέπουν την άμεση ανταπόκριση.

Δίκτυα αιχμής: Οι υπηρεσίες Cloud διαθέτουν δυνατότητες αποθήκευσης και επεξεργασίας πληροφοριών μέσω εξελιγμένων τεχνολογιών, προσφέροντας στους χρήστες αξιοπιστία, βελτιωμένη ποιότητα και λιγότερα προβλήματα δικτύου.

Γρήγορη επέκταση των πόρων: Οι πόροι που υποστηρίζονται από τις υπηρεσίες Cloud (αποθήκευση, επεξεργασία δεδομένων, μνήμη, χρήση εικονικών μηνυμάτων, υπηρεσίες δικτύου), έχουν τη δυνατότητα να επεκταθούν γρήγορα με τη βοήθεια και από την συνεχόμενη εξέλιξη της τεχνολογίας. Οι πάροχοι διαθέτουν αρκετούς πόρους και δυνατότητα αναδιανομής τους, προκείμενου να μεγιστοποιήσουν τα μέτρα ασφαλείας όταν πρόκειται να πραγματοποιηθεί πιθανή «επίθεση». Με αυτό τον τρόπο μπορούν να περιοριστούν οι επιθέσεις και οι επιπτώσεις που αυτές επιφέρουν, χρησιμοποιώντας συνδυαστικά την ευέλικτη αναδιανομή των πόρων και την κατάλληλη μέθοδο βελτιστοποίησης των πόρων.

Συγκέντρωση των πόρων: Η συγκέντρωση των πόρων έχει αρκετά οφέλη εκτός από κάποια μειονεκτήματα. Θεωρώντας την ύπαρξη ικανοποιητικών μέτρων ασφαλείας δεδομένη, η συγκέντρωση των πόρων πλεονεκτεί στη φθηνότερη

παραμετροποίηση και στο φθηνότερο έλεγχο πρόσβασης ανά μονάδα πόρου, στη φθηνότερη εφαρμογή ολοκληρωμένης πολιτικής ασφάλειας και ελέγχου πάνω στη διαχείριση δεδομένων και στη διαχείριση περιστατικών, όπως επίσης και φθηνότερες διαδικασίες συντήρησης.

Αναβαθμίσεις και προεπιλογές στο Cloud Computing οι εικόνες των εικονικών μηχανών και το λογισμικό που χρησιμοποιείται από τους πελάτες μπορεί να αναβαθμιστεί με τις τελευταίες εκδόσεις και ρυθμίσεις ασφαλείας. Επίσης, οι υπηρεσίες IaaS προσφέρουν περιβάλλοντα προγραμμάτων τα οποία παρέχουν τη δυνατότητα λήψης φωτογραφίας από το εικονικό περιβάλλον και να συγκρίνεται με το αρχικό. Οι αναβαθμίσεις πολλές φορές λαμβάνουν χώρα πιο γρήγορα πάνω στη πλατφόρμα. Αυτά είναι όλα τα οφέλη που αφορούν τη βελτίωση της ασφάλειας

1.8.2. Μειονεκτήματα του Cloud Computing.

Παρόλα τα πλεονεκτήματα που χαρακτηρίζουν το Cloud Computing, προκύπτουν κάποια μειονεκτήματα τα οποία συνδέονται κυρίως με την διαθέσιμη συνδεσιμότητα με το διαδίκτυο και με την λειτουργικότητα του διακομιστή. Η κοινή χρήση δεδομένων μπορεί εύκολα να γίνει μειονέκτημα, καθώς προκύπτουν θέματα νομικής φύσεως και θέματα ασφαλείας.

Ασφάλεια: Αποτελεί ένα από τα κύρια μειονεκτήματα καθώς συχνά ο διακομιστής δέχεται επιθέσεις από Hackers. Πιο συγκεκριμένα, ο χρήστης αποθηκεύει τα δεδομένα του στο διακομιστή ο οποίος σε περίπτωση που δεχτεί την επίθεση μπορεί να χάσει τα δεδομένα.

Πρόσβαση στο διαδίκτυο: Βασικός συντελεστής για την χρήση των υπηρεσιών Cloud είναι η σύνδεση με το διαδίκτυο. Σε περίπτωση που δεν υπάρχει σύνδεση στο διαδίκτυο δεν μπορεί ο χρήστης να κάνει χρήση των υπηρεσιών.

Κόστος: Το χρονικό διάστημα το οποίο απαιτείται για να πραγματοποιηθεί η μετάβαση από τη συμβατική τεχνολογία ίσως δημιουργεί κόστος το οποίο να αποτρέπει το χρήστη να συνεχίσει τη διαδικασία.

Προβληματισμοί Νομικής Φύσεως: Ένας άλλος προβληματισμούς αφορά θέματα νομικού περιεχομένου, αφορά την προστασία προσωπικών δεδομένων όταν ένας χρήστης χρησιμοποιεί περιβάλλον σύννεφου. Οι προβληματισμοί χρήζουν ουσιαστικής προσοχής όταν υπάρχει συνδυασμός θεμάτων ασφάλειας και ιδιωτικότητας. Ο χρήστης θα πρέπει να γνωρίζει πότε προστατεύεται και όταν υπάρχει επεξεργασία δεδομένων, θα πρέπει να γνωρίζει ποια από τα προσωπικά στοιχεία καταγράφηκαν και σε περίπτωση που δεν συμφωνεί με αυτό να ζητήσει διακοπή της διαδικασίας.

Ασφάλεια δεδομένων: Κάποιες φορές υπάρχουν συγκεκριμένα δεδομένα σε δικό μας τοπικό διακομιστή και όχι στο σύννεφο “cloud”.

Αυξημένη πολυπλοκότητα: Όταν έχουμε μία εφαρμογή αποθηκευμένη κάπου τοπικά, σε ένα δικό μας διακομιστή και προσπαθούμε να την κάνουμε να επικοινωνήσει με μία άλλη στο σύννεφο “cloud”.

ΚΕΦΑΛΑΙΟ 2ο

Ασφάλεια στο Cloud Computing

2.1. Ασφάλεια Υποδομών

Ασφάλεια στο επίπεδο δικτύου

Βλέποντας το επίπεδο δικτύου ασφαλείας των υποδομών, είναι απαραίτητο να διαχωρίσουμε τα δημόσια και τα ιδιωτικά cloud αντιστοίχως. Με τα ιδιωτικά clouds, δεν υπάρχουν νέες επιθέσεις, και πρέπει να ελέγχονται τα αδύναμα σημεία, οι διακυμάνσεις του κινδύνου ειδικά για την τοπολογία που το προσωπικό ασφαλείας θα πρέπει να δίνει ιδιαίτερη σημασία. Εν αντιθέσει ότι η αρχιτεκτονική του οργανισμού μας μπορεί να τροποποιηθεί με την εφαρμογή ενός ιδιωτικού cloud, η σημερινή τοπολογία του δικτύου μας πιθανόν να μην αλλάξει ιδιαίτερα. Σε περίπτωση που διατηρούμε μια ιδιωτική extranet στη θέση του όπως για την πριμοδότηση των χρηστών είτε για στρατηγικούς εταίρους, για πρακτικούς λόγους έχουμε την τοπολογία του δικτύου για ένα ιδιωτικό cloud ήδη σε διαθεσιμότητα για χρήση. Οι εκτιμήσεις ασφαλείας που έχουμε ισχύουν σημαντικά για την υποδομή ενός ιδιωτικού cloud. Και τα εργαλεία ασφαλείας που διαθέτουν είτε θα έπρεπε να διαθέτουν είναι επίσης σημαντικά για ένα ιδιωτικό cloud και θα πρέπει να λειτουργούνμε τον ίδιο τρόπο.

Παρόλα αυτά, σε περίπτωση που επιλέξουμε να κάνουμε χρήση τις δημόσιες υπηρεσίες cloud, και να διαφοροποιήσουμε τις απαιτήσεις ασφαλείας θα απαιτούνται μετά σχετικές διαφοροποιήσεις στην τοπολογία του δικτύου μας. Θα πρέπει να αντιμετωπίσουμε το τύπο όπου η υπάρχουσα τοπολογία του δικτύου μας αλληλεπιδρά με την τοπολογία του παροχέα cloud. Υπάρχουν τέσσερις σημαντικοί παράγοντες κινδύνου σε αυτή τη περίπτωση χρήσης

- Η εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας των data-in-transit του οργανισμού μας από και πρός τον δημόσιο πάροχο cloud μας.

- Η εξασφάλιση του σωστού ελέγχου πρόσβασης (έλεγχος ταυτότητας, άδεια, και του λογιστικού ελέγχου), στους όποιους πόρους χρησιμοποιούμε το δημόσιο cloud πάροχό μας.

- Η εξασφάλιση των διαθέσιμων πόρων του Διαδικτύου σε ένα δημόσιο cloud οι οποίοι μπορούν να χρησιμοποιηθούν από τον οργανισμό μας, είτε έχουνε παραχωρηθεί για τον οργανισμό μας από τους παρόχους του δημόσιου cloud μας.

- Η αντικατάσταση του καθιερωμένου μοντέλου των ζωνών δικτύου και των βαθμίδων με domains.

Διασφάλιση εμπιστευτικότητας και ακεραιότητας δεδομένων

Κάποιοι πόροι και δεδομένα αντίστοιχα τα οποία μέχρι σήμερα περιορίζονταν σε ένα ιδιωτικό δίκτυο διατίθενται σήμερα στο Internet, και σε έναν κοινόχρηστο δημόσιο δίκτυο που ανήκει σε έναν third-party cloud πάροχο.

Ένα από τα προβλήματα που συνδέονται με αυτόν το πρώτο παράγοντα κινδύνου είναι η ευπάθεια ασφαλείας του Amazon Web Services (AWS) που ανέφερε τοΔεκέμβριο του 2008. Παρότι η χρήση του HTTPS (αντί του HTTP) θα ελαττώσει τον κίνδυνο ακεραιότητας, το γεγονός ότι οι χρήστες δεν χρησιμοποιούν HTTPS αλλά χρησιμοποιούν το http τους έβαλε να αντιμετωπίζουν αυξημένο κίνδυνο για τα δεδομένα τους τα οποία θα μπορούσαν να έχουνε αλλοιωθεί κατά τη μεταφορά εν αγνοία τους.

Εξασφάλιση σωστού ελέγχου πρόσβασης

Από την στιγμή που ένα υποσύνολο αυτών των πόρων είτε ακόμη και όλοι τους διατίθενται στο Διαδίκτυο, μια οργάνωση η οποία κάνει χρήση κάποιου δημόσιου cloud είναι αντιμέτωπη με ιδιαίτερα αυξημένη επικινδυνότητα αναφορικά για τα δεδομένα της. Η ικανότητα να επιτηρούνται οι διεργασίες του δικτύου του cloud παρόχου μας (πόσο μάλλον για την realtime παρακολούθηση, όπως σε δικό μας δίκτυο), ακόμα και μετά του γεγονότος, είναι μάλλον ανύπαρκτη. Θα έχουμε χαμηλή πρόσβαση στις σχετικές καταγραφές σε επίπεδο δικτύου και δεδομένων, καθώς και μειωμένη ικανότητα για τη διεξαγωγή ερευνών και τη συλλογή δεδομένων.

Ένα παράδειγμα των προβλημάτων που συνδέονται με αυτόν τον δεύτερο παράγοντα κινδύνου είναι το θέμα της επαναχρησιμοποίησης (reassigned) διευθύνσεων IP.

Γενικά, όταν μια διεύθυνση IP δεν είναι απαραίτητη πλέον για έναν πελάτη δεν θεωρείται παλιά από τον cloud πάροχο. Οι διευθύνσεις αυτές συνήθως χρησιμοποιούνται εκ νέου από έτερους πελάτες καθώς είναι διαθέσιμες. Από την πλευρά του cloud παρόχου αυτό έχει νόημα. Οι διευθύνσεις IP έχουνε περιορισμένη ποσότητα και θεωρούνται περιουσιακά στοιχεία. Παρόλα αυτά, από την άποψη ασφάλειας του πελάτη, η διατήρηση των διευθύνσεων IP που δεν χρησιμοποιούνται πλέον μπορεί να παρουσιάσουν πρόβλημα. Ένας πελάτης δεν μπορεί να υποθέσει ότι η πρόσβασή του στους πόρους του δικτύου έχει τερματιστεί μέχρι να απελευθερωθεί η διεύθυνση IP του. Υπάρχει λοιπόν μια χρονική καθυστέρηση ανάμεσα στην αλλαγή της διεύθυνσης IP στο DNS και την εκκαθάριση της εν λόγω διεύθυνσης από τις caches του DNS. Υπάρχει ένα παρόμοιο χρονικό διάστημα που μεσολαβεί όταν οι φυσικές όπως η MAC διευθύνσεις αλλάζουν ARP πίνακες και όταν οι παλιές διευθύνσεις ARP εκκαθαρίζονται από την cache. Τότε μια παλιά διεύθυνση παραμένει στις ARP caches μέχρι να εκκαθαριστούν. Αυτό σημαίνει ότι ακόμα και αν οι διευθύνσεις μπορεί να έχουνε αλλάξει, η (τώρα) παλιά διεύθυνσή μας είναι ακόμα διαθέσιμη στη μνήμη cache, και ως εκ τούτου, εξακολουθεί να επιτρέπει στους χρήστες να χρησιμοποιούν αυτούς τους μη διαθέσιμους πόρους. Πρόσφατα, υπήρξαν πολλές σημειώσεις για αυτό τοπρόβλημα των “non-aged” διευθύνσεων IP σε έναν από τους μεγαλύτερους παρόχους cloud.

Παρόλα αυτά, το θέμα των “non-aged” διευθύνσεων IP και της μη εξουσιοδοτημένης πρόσβασης στους πόρους του δικτύου δεν ισχύει μόνο για routable διευθύνσεις δηλαδή οι πόροι που προορίζονται για να είναι προσβάσιμοι άμεσα από το Internet. Το ζήτημα αυτό αφορά και στα εσωτερικά δίκτυα των cloud παρόχων που προσφέρονται για χρήση από τους πελάτες και τους έχουν δοθεί non-routable διευθύνσεις IP. Παρότι και οι πόροι σας μπορεί να μην είναι άμεσα προσβάσιμοι από το Διαδίκτυο, για διαχειριστικούς λόγους οι πόροι μας πρέπει να είναι προσβάσιμοι εντός του δικτύου του παρόχου του cloud μέσω ιδιωτικής διευθυνσιοδότησης. Αλλοι χρήστες του cloud παρόχου σας μπορεί να μην έχουνε καλές προθέσεις και μπορεί να είναι σε θέση να φτάσουν τους πόρους μας εσωτερικά μέσω του δικτύου του cloud παρόχου μας.

Κάποια προϊόντα που βγαίνουν στην αγορά, θα βοηθήσουν να ελαττωθεί το πρόβλημα της επαναχρησιμοποίησης διευθύνσεων IP, αλλά σε περίπτωση που οι πάροχοι cloud προσφέρουν αυτά τα προϊόντα ως διαχειριστικές υπηρεσίες, οι χρήστες θα πληρώνουν για ένα ακόμη third-party προϊόν για να λυθεί το πρόβλημα που οι ίδιοι οι πάροχοι cloud έκαναν.

Αντικατάσταση του Established Model of Network Zones και Tiers με Domains

Το κύριο μοντέλο των περιοχών του δικτύου και των βαθμίδων δεν δίνεται πλέον στα δημόσια IaaS και τα PaaS clouds. Για πολύ καιρό, η ασφάλεια του δικτύου στηριζόταν σε ζώνες, όπως το intranet έναντι του extranet και της ασφάλειας έναντι της παραγωγής, να διαχωρίζουν την κυκλοφορία του δικτύου για τη βελτίωση της ασφάλειας. Το μοντέλο βασίστηκε μόνο για άτομα και συστήματα σε συγκεκριμένους ρόλους να έχουν πρόσβαση σε συγκεκριμένες ζώνες. Με την ίδια λογική, τα συστήματα μέσα σε μια συγκεκριμένη βαθμίδα συχνά έχουν μόνο συγκεκριμένη πρόσβαση στο εσωτερικό είτε σε μια συγκεκριμένη βαθμίδα. Για παράδειγμα, τα συστήματα με tier παρουσίασης δεν μπορούν να επικοινωνούν άμεσα με τα συστήματα της δεύτερης βαθμίδας της βάσης δεδομένων, αλλά μπορούν να επικοινωνούν μόνο με εγκεκριμένο σύστημα εντός της ζώνης εφαρμογής. Τα SaaS clouds είναι φτιαγμένα σε δημόσια IaaS είτε τα PaaS clouds τα οποία έχουν επίσης τα ίδια χαρακτηριστικά. Παρόλα αυτά, ένα δημόσιο SaaS στηριγμένο σε ένα ιδιωτικό IaaS όπως το Salesforce.com μπορεί να βασιστεί στο κλασσικό τύπο της απομόνωσης, αλλά αυτές οι τοπολογικές πληροφορίες τυπικά δεν μοιράζονται με τους χρήστες.

Το κλασσικό μοντέλο των δικτυακών ζωνών και βαθμίδων έχει αντικατασταθεί στο δημόσιο cloud computing με “security groups”, “security domains”, είτε “virtual data centers” τα οποία έχουν διαχωρισμό μεταξύ των βαθμίδων αλλά είναι πιο ανακριβείς και παρέχουν μικρότερη προστασία από το προηγούμενο μοντέλο. Για παράδειγμα, οι ομάδες ασφαλείας που διατίθενται στην AWS επιτρέπουν στις εικονικές μηχανές (VMs) να έχουν πρόσβαση η μία στην άλλη χρησιμοποιώντας ένα εικονικό τείχος προστασίας το οποίο έχει την ικανότητα να φιλτράρει την κυκλοφορία με βάση τη διεύθυνση IP (μια συγκεκριμένη διεύθυνση είτε ένα δευτερεύον δίκτυο), τα είδη πακέτων (TCP,UDP,ICMP) και τις θύρες.

Τα domain names χρησιμοποιούνται σε ποικίλα περιβάλλοντα δικτύωσης και για application-specific ονοματοδοτικούς και διευθυνσιοδοτικούς σκοπούς που βασίζονται στο DNS. Όπως η Google App Engine έχει μια λογική ομαδοποίηση των εφαρμογών που στηρίζονται σε domain names όπως το mytestapp.test.mydomain.com και το myprodapp.prod.mydomain.com.

Ο βασικός τύπος για το δικτύο ζωνών και βαθμίδων, δεν είναι μόνο τα συστήματα ανάπτυξης που διαχωρίζονται από τα συστήματα παραγωγής σε επίπεδο δικτύου, αλλά αυτές οι ομάδες συστημάτων οι οποίες είναι διαχωρισμένες στο host level δηλαδή λειτουργούν σε φυσικά διαχωρισμένους διακομιστές σε διαχωρισμένες ζώνες του δικτύου. Με το cloud computing, παρόλα αυτά, αυτός ο διαχωρισμός δεν υφίσταται πλέον. Το μοντέλοτου cloud computing διαχωρισμού από τους τομείς παρέχει μόνο διαχωρισμό διευθυνσιοδότησης. Δεν υπάρχει κανένας "required" φυσικός διαχωρισμός, για διαχωρισμό domain και ένα domain παραγωγής μπορεί να είναι στον ίδιο φυσικό διακομιστή. Ακόμη, ο παλιός διαχωρισμός του δικτύου δεν υπάρχει πια. Λογικός διαχωρισμός υπάρχει τώρα στο host level και με τα δύο domain να λειτουργούν μαζί στο ίδιο φυσικό server και διαχωρίζονται μόνο λογικά από VM οθόνες (hypervisors).

2.2. Ασφάλεια υποδομών: Το Host Level

Κατά την επανεξέταση της ασφάλειας υποδοχής και εκτίμησης των κινδύνων, θα πρέπει να ελέγξουμε το πλαίσιο του cloud μοντέλων παροχής υπηρεσιών (SaaS,PaaS,IaaS) και τα μοντέλα ανάπτυξης δημόσιο, ιδιωτικό είτε υβριδικό. Παρότι δεν υπάρχουν καινούργιες γνωστές απειλές σε κεντρικούς υπολογιστές που είναι αποκλειστικά για cloud computing, κάποιοι virtualization security κίνδυνοι, όπως το VM escape, η διαμόρφωση συστήματος drift, και οι εσωτερικές απειλές μέσω του ελέγχου περιορισμένης πρόσβασης στο hypervisor, είναι στο δημόσιο περιβάλλον του cloud computing. Η δυναμική φύση (ελαστικότητα) του cloud computing μπορεί να έχει νέες προκλήσεις από την άποψη της διαχείρισης ασφάλειας. Το επιχειρησιακό μοντέλο παρακινεί την ταχεία παροχή και τις φευγαλέες instances των VMs. Η διαχείριση των τρωτών σημείων και ως εκ τούτου, τα patches είναι πιο δύσκολα από

το να λειτουργείς απλά ένα scan, καθώς ο ρυθμός της αλλαγής είναι τεράστιος από ότι σε ένα παραδοσιακό κέντρο δεδομένων (data center).

Ακόμη, το γεγονός ότι τα Clouds εκμεταλλεύονται τη δύναμη διάφορων υπολογιστικών κόμβων, σε συνδυασμό με την ομογένεια του λειτουργικού συστήματος που χρησιμοποιείται από τους hosts, υποδηλώνει ότι οι απειλές μπορούν να ενισχυθούν γρήγορα και εύκολα "velocity of attack". Ιδιαίτερα σημαντικό είναι ότι πρέπει να κατανοήσουμε τα όρια εμπιστοσύνης και τις ευθύνες που έχουμε για να εξασφαλίσουμε την host υποδομή την οποία διαχειριζόμαστε. Και πρέπει να συγκρίνουμε το ίδιο με τις ευθύνες των παρόχων για την διασφάλιση μέρους της host υποδομής την οποία διαχειρίζεται το CSP.

2.2.1. SaaS και PaaS Host Security

Γενικώς, τα CSPs δεν δίνουν δημόσια στοιχεία που σχετίζονται με τα host λειτουργικά συστήματα, τις πλατφόρμες υποδοχής, και τις διαδικασίες που είναι σε θέση να εξασφαλίσει τους hosts, καθώς οι hackers μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες, όταν προσπαθήσουν να εισβάλλουν στην υπηρεσία cloud. Γι' αυτό το λόγο, στο πλαίσιο των SaaS όπως το Salesforce.com, είτε των PaaS όπως το Google AppEngine, υπηρεσιών cloud, η ασφάλεια υποδοχής είναι αδιαφανή για τους πελάτες και η ευθύνη της εξασφάλισης των hosts υποβιβάζεται σε CSP.

Για να πάρει τη διαβεβαίωση από τον CSP για την ομαλή ασφάλεια από τους hosts, θα πρέπει να ζητήσουμε από τον πάροχο να ανταλλάσσονται πληροφορίες στο πλαίσιο της συμφωνίας εμπιστευτικότητας (NDA) είτε απλώς να ζητείται το CSP να μοιράζεται τις πληροφορίες μέσω ενός πλαισίου αξιολόγησης, όπως το SysTrust είτε το πρότυπο ISO 27002. Από την οπτική ενός ελέγχου διασφάλισης, το CSP θα πρέπει να διασφαλίσει ότι προληπτικοί και κατασταλτικοί έλεγχοι είναι σε ετοιμότητα και θα πρέπει να διασφαλίζεται μέσω ενός τρίτου προσώπου είτε του τύπου ISO 27002 πλαισίου αξιολόγησης.

Λόγω ότι η εικονικότητα (virtualization) είναι μια βασική τεχνολογία που αυξάνει τη χρήση (utilization) του λογισμικού (host hardware), μεταξύ άλλων οφελών, είναι σύνηθες για τους CSP να απασχολούν εικονικές (virtualization)

πλατφόρμες, όπως Xen και VMware hypervisors, στην αρχιτεκτονική πλατφόρμα υποδοχής του host. Θα πρέπει να γίνει κατανοητό ότι ο πάροχος χρησιμοποιεί την τεχνολογία εικονοποίησης (virtualization) και τη διαδικασία που ασφαλίζει ο πάροχος το στρώμα εικονοποίησης (virtualization).

Τόσο οι PaaS και SaaS πλατφόρμες λαμβάνουν και κρύβουν το λειτουργικό σύστημα της υποδοχής από τους τελικούς χρήστες με ένα αφαιρετικό στρώμα host. Μια σημαντική διαφορά μεταξύ των PaaS και SaaS είναι η διαδικασία για τη σχετική προσβασιμότητα των απορροφητικών στρωμάτων τα οποία κρύβουν το λειτουργικό σύστημα υπηρεσιών που κάνουν χρήση οι εφαρμογές. Στη περίπτωση του SaaS, το απορροφητικό στρώμα δεν φαίνεται στους χρήστες και είναι διαθέσιμο μόνο στους προγραμματιστές και το προσωπικό των επιχειρήσεων του CSP, στο οποίο οι χρήστες PaaS έχουν έμμεση πρόσβαση στο host abstraction layer στο τύπο μιας διεπαφής προγραμματισμού PaaS (API), το οποίο έπειτα αλληλεπιδρά με το host abstraction layer.

Οι ευθύνες για την ασφάλεια του host στις SaaS και στις PaaS υπηρεσίες μεταβιβάζονται στο CSP. Το γεγονός ότι δεν χρειάζεται να ανησυχούμε για την προστασία των hosts από host-based απειλές ασφάλειας είναι ένα ιδιαίτερο πλεονέκτημα λόγω της διαχείρισης της ασφάλειας και του κόστους. Παρόλα αυτά, θα συνεχίσουν οι χρήστες να έχουν τον κίνδυνο της διαχείρισης των πληροφοριών που διατηρούνται στις υπηρεσίες του cloud. Είναι λοιπόν ευθύνη των χρηστών να πάρουν το σωστό επίπεδο αξιοπιστίας σχετικά με τον τρόπο με τον οποίο ο CSP διαχειρίζεται την σωστή ασφάλεια.

2.2.2. IaaS Host Security

Εν αντιθέσει με τα PaaS και SaaS, οι πελάτες IaaS είναι βασικά υπεύθυνοι για την διασφάλιση των hosts που τροφοδοτούν το cloud. Επειδή όλες σχεδόν οι διαθέσιμες υπηρεσίες IaaS έχουν εικονοποίηση(virtualization) στο host layer, η ασφάλεια (host security) στο IaaS θα πρέπει να χωρίζεται ως εξής:

Ασφάλεια λογισμικού εικονοποίησης

Είναι το στρώμα του λογισμικού που είναι στη κορυφή του bare metal και δίνει στους χρήστες τη δυνατότητα να φτιάξουν και να καταστρέψουν virtual instances. Η εικονοποίηση (Virtualization) στο host level μπορεί να γίνει χρησιμοποιώντας οποιοδήποτε από τα μοντέλα εικονοποίησης, συμπεριλαμβανομένου του OS-level virtualization (Solaris containers, BSD jails, Linux-VServer), paravirtualization συνδυασμός της hardware έκδοσης και της έκδοσης του Xen και VMware, είτε το λογισμικό που βασίζεται σε εικονοποίηση (Xen,Vmware, Microsoft Hyper-V). Είναι σημαντικό να διασφαλιστεί αυτό το στρώμα του λογισμικού που είναι μεταξύ του hardware και των virtual servers. Σε μια δημόσια υπηρεσία IaaS, οι χρήστες δεν έχουν πρόσβαση σε αυτό το λογισμικό στρώμα, καθώς το διαχειρίζεται μόνο το CSP.

Customer guest OS είτε virtual server security

Μια virtual instance κάποιου λειτουργικού συστήματος που τροφοδοτείται στη κορυφή του virtualization layer φαίνεται από τους χρήστες στο διαδίκτυο, όπως οι διάφορες εκδόσεις Linux, Microsoft και Solaris. Οι χρήστες έχουν γενική πρόσβαση στους virtual servers.

2.2.3. Δεδομένα παρόχου και η ασφάλειά τους

Εκτός από την ασφάλεια των δεδομένων τους οι χρήστες θα πρέπει επίσης να ανησυχούν και για τα δεδομένα που διατηρεί ο πάροχος και τον τρόπο που ο CSP προστατεύει τα συγκεκριμένα δεδομένα. Αναφορικά με τα στοιχεία των χρηστών, τα metadata τα οποία έχει ο πάροχος για τα δεδομένα του, τον τρόπο βάση του οποίου τα έχει ασφαλισμένα, και το τύπο της πρόσβασης την οποία έχουν οι χρήστες σε αυτά τα metadata. Όσο αυξάνεται ο όγκος δεδομένων που μοιραζόμαστε με έναν πάροχο τόσο αυξάνεται και η αξία αυτών των metadata. Ακόμη, ο πάροχός μας διατηρεί και πρέπει να ασφαλίζει ένα όγκο από security-related δεδομένων. Για παράδειγμα, σε επίπεδο δικτύου, ο φορέας θα πρέπει να συλλέγει, να παρακολουθεί, και να ασφαλίζει το firewall, το σύστημα αποτροπής εισβολών (IPS), τα περιστατικά ασφάλειας τα διαχειριστικά instances (SIEM), και τα δεδομένα ροής του router. Στο επίπεδο του host ο πάροχος θα πρέπει να διατηρεί αρχεία καταγραφής του συστήματος, και σε

επίπεδο εφαρμογής SaaS παρόχων θα πρέπει να διατηρεί αρχείο δεδομένων των εφαρμογών, των πληροφοριών πιστοποίησης και εξουσιοδότησης.

Αποθήκευση

Για τα δεδομένα που αποθηκεύονται στο cloud δηλαδή, storage-as-a-service, σε IaaS υπηρεσία και όχι δεδομένα που σχετίζονται με εφαρμογές που τρέχουν σε PaaS είτε SaaS cloud.

Εμπιστευτικότητα

Αναφορικά με την προστασία του απορρήτου των δεδομένων που αποθηκεύονται σε ένα δημόσιο cloud, υπάρχουν δύο πιθανές ανησυχίες. Αφενός, ο τρόπος που ο έλεγχος προστασίας υπάρχει στην πρόσβαση των δεδομένων. Ο έλεγχος πρόσβασης αποτελείται από την ταυτότητα και την αδειοδότηση. Τα CSP έχουν τις πιο πολλές φορές μη ικανούς μηχανισμούς πιστοποίησης όπως το όνομα χρήστη (username) και το κωδικό (password), καθώς και οι έλεγχοι άδειας (“access”) που δίνονται στους χρήστες τείνουν να είναι αρκετά άβολη για μεγάλους οργανισμούς, αυτή η έγκριση παρουσιάζει σημαντικές ανησυχίες για την προσωπική ασφάλεια. Συνήθως, τα μόνα επίπεδα εξουσιοδότησης που παρέχουν οι cloud πάροχοι είναι η άδεια διαχειριστή δηλαδή ο ίδιος ο ιδιοκτήτης του λογαριασμού και την άδεια χρήστη δηλαδή όλοι οι υπόλοιποι εξουσιοδοτημένοι χρήστες, χωρίς επίπεδα στο ενδιάμεσο όπως διαχειριστές επιχειρησιακών μονάδων, δίνουν την άδεια για την πρόσβαση για το ποιοί είναι εξουσιοδοτημένοι για πρόσβαση από το προσωπικό. Και πάλι, αυτά τα ζητήματα ελέγχου πρόσβασης δεν είναι μοναδικά για τα CSPs.
Αφετέρου είναι ο τρόπος με τον οποίο τα δεδομένα που είναι αποθηκευμένα στο cloud προστατεύονται στην πραγματικότητα. Η προστασία των δεδομένων που είναι αποθηκευμένα στο cloud περιλαμβάνει την χρήση κρυπτογράφησης.

Ανάλογα με ποια CSP χρησιμοποιούμε ποικίλει ο τρόπος κρυπτογράφησης των στοιχείων. Η Mozy Enterprise της EMC κάνει κρυπτογράφηση των δεδομένων του χρήστη ενώ το AWS δεν κρυπτογραφεί τα δεδομένα των πελατών. Οι χρήστες μπορούν να κρυπτογραφήσουν τα δεδομένα τους μόνοι τους πρίν από το ανέβασμα στο cloud, όμως το S3 δεν παρέχει κρυπτογράφηση.

Σε περίπτωση που ένας CSP κρυπτογραφεί τα δεδομένα ενός χρήστη, ο επόμενος προβληματισμός μας είναι ο τύπος του αλγόριθμου κρυπτογράφησης τον οποίο χρησιμοποιεί. Δεν είναι όλοι οι αλγόριθμοι κρυπτογράφησης ίδιοι.

Κρυπτογραφικά, πολλοί αλγόριθμοι παρέχουν επαρκή ασφάλεια. Μόνο οι αλγόριθμοι που έχουν ελεγχθεί από έναν επίσημο πρότυπο οργανισμό όπως το NIST είναι ασφαλείς. Θα πρέπει φυσικά να αποφεύγεται οποιοσδήποτε αλγόριθμος είναι ιδιόκτητος. Σε αυτή τη φάση, αναφερόμαστε για συμμετρικούς αλγόριθμους κρυπτογράφησης. Η συμμετρική κρυπτογράφηση περιλαμβάνει τη χρήση ενιαίου μυστικού κλειδιού τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Μόνο η συμμετρική κρυπτογράφηση έχει τη ταχύτητα και την υπολογιστική αποδοτικότητα για να χειριστεί την κρυπτογράφηση μεγάλου όγκου δεδομένων.

Η επόμενή μας ανησυχία είναι το μήκος του κλειδιού που χρησιμοποιείται. Με συμμετρική κρυπτογράφηση, όσο πιο μεγάλο είναι το κλειδί όπως ο μεγαλύτερος αριθμός των bits του κλειδιού, τόσο πιο ισχυρή είναι η κρυπτογράφηση. Παρότι μεγάλα σε μήκος κλειδιά δίνουν μεγαλύτερη προστασία, είναι και πιο υπολογιστικά ευαίσθητα, και μπορούν να καταπονήσουν τις δυνατότητες των επεξεργαστών των ηλεκτρονικών υπολογιστών. Αυτό που πρέπει να αναφέρουμε είναι ότι το μήκος του κλειδιού θα πρέπει να είναι τουλάχιστον 112 bits για Triple DES (Data Encryption Standard) και 128 bits για το AES(Advanced Encryption Standard) και τα δύο με έγκριση από το NIST. Ένα άλλο ζήτημα εμπιστευτικότητας για την κρυπτογράφηση είναι η διαχείριση των κλειδιών. Δεν συνίσταται να δώσουμε σε κάποιο πάροχο να διαχειριστεί τα δικά μας κλειδιά, τουλάχιστον όχι τον ίδιο πάροχο που χειρίζεται τα δεδομένα μας. Αυτό δηλώνει περισσότερους πόρους και δυνατότητες και δεξιότητες που είναι ιδιαίτερα σημαντικές. Η σωστή διαχείριση κλειδιών είναι ένα δύσκολο και σύνθετο έργο. Ο χρήστης οφείλει να λαμβάνει υπόψιν και τα τρία μέρη του NIST 800-57, “Recommendation for Key Management”.

Καθώς η διαχείριση των κλειδιών δεν είναι εύκολη αλλά σύνθετη υπόθεση για έναν χρήστη, είναι ακόμη πιο σύνθετη και δύσκολη για τους CSP για να διαχειριστούν σωστά τα κλειδιά των χρηστών. Είναι εύκολο για έναν πάροχο να κρυπτογραφεί όλα τα δεδομένα ενός χρήστη με ένα μόνο κλειδί. Ακόμα είναι κάποιοι πάροχοι cloud αποθήκευσης οι οποίοι κάνουν χρήση ενός μόνο κλειδιού κρυπτογράφησης για όλους τους πελάτες τους. Ο Οργανισμός για την Προώθηση των Δομημένων Συστημάτων Πληροφοριών (OASIS) και το Βασικό Πρωτόκολλο διαχείρισης διαλειτουργικότητας (KMIP) προσπαθούν να αντιμετωπίσουν αυτά τα θέματα.

Ακεραιότητα

Ακόμη πέρα από τη σχετική εμπιστευτικότητα των δεδομένων μας, θα πρέπει οι χρήστες να ανησυχούν και για την ακεραιότητα των δεδομένων τους. Τα δεδομένα μπορεί να κρυπτογραφούνται για λόγους εμπιστευτικότητας και όμως μπορεί να μην έχουν τρόπο που να επιβεβαιώνει την ακεραιότητά τους. Η κρυπτογράφηση από μόνη της είναι αρκετή για την εμπιστευτικότητα, όμως η ακεραιότητα χρειάζεται επιπλέον τη χρήση του μηνύματος κωδικού ταυτότητας (MAC). Ο πιο εύκολος τρόπος για να χρησιμοποιήσουμε τις MAC για κρυπτογραφημένα δεδομένα, είναι να χρησιμοποιήσουμε έναν block συμμετρικό αλγόριθμο (σε αντίθεση με έναν streaming συμμετρικό αλγόριθμο) σε block chaining (CBC) θέση λειτουργίας, και να έχει μια one-way hash συνάρτηση. Αυτά δεν είναι για χρήστες που δεν είναι εξοικιωμένοι με την κρυπτογράφηση, και αυτός είναι ένας λόγος που η σωστή διαχείριση των κλειδιών είναι δύσκολη.

Οι χρήστες πρέπει να ζητάνε βοήθεια από τους παρόχους τους για αυτά τα θέματα. Αυτό είναι σημαντικό όχι μόνο για την ακεραιότητα των δεδομένων του χρήστη αλλά και για την παροχή πληροφοριών αναφορικά με το πόσο περίπλοκο είναι το πρόγραμμα ασφαλείας του παρόχου.

Αυτό που πρέπει να ενημερώνεται ο χρήστης είναι ότι δεν κρυπτογραφούν όλοι οι πάροχοι τα δεδομένα των χρηστών, ειδικά για PaaS και SaaS υπηρεσίες.
Πολύ ιδιαίτερη είναι και μια άλλη πτυχή της ακεραιότητας των δεδομένων, ειδικά με την αποθήκευση μεγάλου όγκου χρησιμοποιώντας IaaS. Υπάρχουν κόστη μεταβίβασης στο IaaS που συνδέονται με τη μετακίνηση των δεδομένων προς και πίσω από το cloud. Αυτό που ο χρήστης οφείλει να κάνει είναι να επαληθεύσει την ακεραιότητα των δεδομένων του, καθώς τα δεδομένα παραμένουν στο cloud χωρίς να έχουν κατέβει είτε ανέβει.

Η διαδικασία αυτή είναι ακόμα πιο δύσκολη, καθώς πρέπει να γίνει στο cloud με τη απόλυτη γνώση ολόκληρου του συνόλου δεδομένων. Οι χρήστες δεν ξέρουν σε ποιές φυσικές μηχανές αποθηκεύονται τα δεδομένα τους, είτε που βρίσκονται τα συστήματα αυτά. Ακόμη, αυτό το σύνολο δεδομένων είναι πιθανό να τροποποιείται συχνά. Αυτές οι αλλαγές κάνουν μη χρήσιμη την αποτελεσματικότητα των τεχνικών ασφάλειας της ακεραιότητας. Εν αντιθέσει αυτο που χρειάζεται, είναι μια απόδειξη

της ανάκτησης, δηλαδή ένας μαθηματικός τρόπος για να βεβαιωθεί ο χρήστης για την ακεραιότητα των δεδομένων που είναι αποθηκευμένα στο cloud.

Διαθεσιμότητα

Έχοντας ασφαλίσει ότι τα δεδομένα ενός χρήστη έχουν λάβει την εμπιστευτικότητα και την ακεραιότητά τους, ο χρήστης θα πρέπει να ενδιαφερθεί ακόμη και για την διαθεσιμότητα των δεδομένων του. Υπάρχουν τρείς βασικές απειλές, καμία από τις οποίες δεν είναι καινούργια στην πληροφορική, αλλά όλες είναι σημαντικές στην αύξηση της ιδιαιτερότητας του cloud computing, λόγω του αυξημένου κινδύνου.
Η πρώτη απειλή για την διαθεσιμότητα είναι οι network-based επιθέσεις.
Η δεύτερη απειλή για τη διαθεσιμότητα είναι η διαθεσιμότητα του ίδιου του CSP.
Τέλος, οι χρήστες του cloud θα πρέπει να εξακριβώσουν τις υπηρεσίες τις οποίες τους προσφέρει ο πάροχος. Ο αποθηκευτικός χώρος του cloud δεν σημαίνει ότι τα αποθηκευμένα δεδομένα είναι και backed up.

Ορισμένοι πάροχοι cloud αποθήκευσης έχουν αντίγραφα ασφαλείας των δεδομένων των χρηστών, είτε τα παρέχουν σαν πρόσθετη επι πληρωμή υπηρεσία. Για παράδειγμα τα δεδομένα που αποθηκεύονται στο Amazon S3, στο Amazon SimpleDB, είτε στο Amazon ElasticBlock Store αποθηκεύονται σε πολλαπλές φυσικές τοποθεσίες ως ένα κανονικό μέρος των υπηρεσιών αυτών και χωρίς επιπλέον χρέωση.

Όλες αυτές οι σχετικές εκτιμήσεις (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) θα πρέπει να είναι κομμάτι σε μια συμφωνία επιπέδου υπηρεσιών ενός SLA των χρηστών της. Παρόλα αυτά, αυτή τη στιγμή, τα SLAs των CSP είναι ιδιαίτερα αδύναμα, για την ακρίβεια, για όλους τους σχετικούς σκοπούς, είναι άνευ αξίας. Ακόμη και όταν ένας CSP παρουσιάζεται να έχει τουλάχιστον ένα επαρκή SLA, τον τρόπο κατά τον οποίο στην ακρίβεια μετριέται αυτή η SLA είναι ένα προβληματικό ζήτημα. Για τους αναφερόμενους αυτούς λόγους, για λόγους ασφάλειας των δεδομένων και για τον τρόπο κατά τον οποίο τα δεδομένα αποθηκεύονται στο cloud θα πρέπει να υπάρχει ιδιαίτερη προσοχή από τους χρήστες.

2.4. Όρια εμπιστοσύνης και IAM (Identity And Access Management)

Σε μια σχετική οργάνωση όπου οι εφαρμογές έχουν κατασκευαστεί εντός της περιμέτρου του οργανισμού το όριο εμπιστοσύνης “trust boundary” είναι κατά βασικό λόγο στατικό και παρακολουθείται από το τμήμα IT. Στο κλασσικό τύπο, το όριο εμπιστοσύνης περιλαμβάνει το δίκτυο, τα συστήματα και τις εφαρμογές και διατηρείται σε κάποιο ιδιωτικό κέντρο δεδομένων το οποίο ελέγχεται από το τμήμα πληροφορικής και κάποιες φορές από third-party παρόχους υπό την επίβλεψη του IT. Η πρόσβαση στο δίκτυο καθώς και οι εφαρμογές είναι εξασφαλισμένες μέσω των δικτυακών ελέγχων ασφάλειας και των εικονικών ιδιωτικών δικτύων (VPN), ανίχνευσης εισβολής συστημάτων (IDSs), τα συστήματα αποτροπής εισβολών (IPSS).

Με την διατήρηση των υπηρεσιών cloud, το όριο εμπιστοσύνης του οργανισμού θα είναι δυναμικό και θα προχωρήσει πέρα από τον έλεγχο της πληροφορικής. Με το cloud computing, το δίκτυο, το σύστημα και τα όρια της εφαρμογής ενός οργανισμού έχουν τη δυνατότητα να επεκταθούν στο domain του παρόχου της υπηρεσίας. Αυτή η έλλειψη του ελέγχου συνεχίζει να αμφιβάλει για το αξιόπιστο μοντέλο διακυβέρνησης και ελέγχου, και, σε περίπτωση που δεν διαχειριστούν σωστά, θα εμποδίσουν την διατήρηση cloud υπηρεσιών από ένα οργανισμό.

Για να εξισορροπήσει την έλλειψη του ελέγχου του δικτύου και για την ενίσχυση της ασφάλειας σε περίπτωση κινδύνου, οι οργανισμοί θα υποχρεωθούν να εξαρτηθούν σε άλλα στοιχεία ελέγχου λογισμικού καλύτερου επιπέδου, όπως η ασφάλεια των εφαρμογών και του ελέγχου πρόσβασης του χρήστη. Οι έλεγχοι αυτοί δηλώνονται ως δυναμικός έλεγχος ταυτότητας, ως άδεια με βάση το ρόλο είτε τις απαιτήσεις, αξιόπιστες πηγές με ακριβή χαρακτηριστικά, χρήση ομοσπονδιακών ταυτοτήτων, single sign-on (SSO), παρακολούθηση της δραστηριότητας του χρήστη, καθώς και τον έλεγχο. Ιδιαίτερα, οι οργανισμοί πρέπει να δώσουν σημασία στην αρχιτεκτονική και στις διαδικασίες, λόγο ότι μπορούν να καλυτερεύσουν τους ελέγχους και την εμπιστοσύνη μεταξύ των οργανισμών και των παρόχων cloud υπηρεσιών (CSPs).

Η ομοσπονδία ταυτοτήτων είναι μια αναπτυσσόμενη βιομηχανία των καλύτερων πρακτικών για την καταπολέμηση της ετερογενούς δυναμικής, χαλαρά

συνδεδεμένης σχέσης εμπιστοσύνης που δηλώνει μια οργάνωση εξωτερικών και εσωτερικών αλυσίδων εφοδιασμού και του τύπου συνεργασίας. Η ομοσπονδία αυτή δίνει τη δυνατότητα για την επικοινωνία μεταξύ των συστημάτων και τις εφαρμογές να χωρίζονται από το όριο εμπιστοσύνης ενός οργανισμού, όπως ένας πωλητής να επικοινωνεί με το Salesforce.com μέσω εταιρικού δικτύου. Εφόσον η ομοσπονδία εφοδιάστηκε με καλή πρακτική εξάσκηση IAM μπόρεσε να ενισχύσει την ισχυρή ταυτοποίηση μέσω εξουσιοδότησης, web single sign-on, και διαχείριση του δικαιώματος μέσω κεντρικής πρόσβασης των υπηρεσιών ελέγχου, θα έχει βασικό ρόλο στην ενίσχυση της διατήρησης του cloud computing από τους οργανισμούς.

Σε κάποιες περιπτώσεις, η διατήρηση της IAM μέσα σε έναν οργανισμό μπορεί να έχει πρόβλημα λόγω έλλειψης βασικής διακυβέρνησης και της ταυτοποιημένης αρχιτεκτονικής των πληροφοριών της. Τις πιο πολλές φορές, η ταυτοποιημένη αποθήκευση διαχειρίζεται μέσω χειροκίνητης εισαγωγής από ποικίλους διαχειριστές και η χρήση διαδικασιών παροχών δεν είναι καλά συντονισμένη. Αυτή η διαδικασία δεν είναι μόνο μη αποτελεσματική, αλλά θα δωθεί επίσης με την υπάρχουσα κακή διατήρηση των cloud υπηρεσιών. Σε τέτοιες καταστάσεις, το μη ικανό μοντέλο πρόσβασης θα έχει παραπάνω προνόμια για μη αδιοδοτούμενους χρήστες στις διάφορες cloud υπηρεσίες

2.4.1. Γιατί IAM ?

Σταθερά, οι οργανισμοί επενδύουν σε IAM πρακτικές για τη καλυτέρευση της λειτουργικής αποδοτικότητας και για τη τήρηση με τις ρυθμιστικές, σε ιδιωτικές και για τη ασφάλεια των δεδομένων απαιτήσεις:

Βελτίωση της λειτουργικής αποτελεσματικότητας

Η σωστά δομημένη IAM τεχνολογία και διαδικασίες δίνουν τη δυνατότητα για να καλυτερεύσουν την αποτελεσματικότητα αυτοματοποιώντας τον χρήστη για on-boarding και άλλες επαναλαμβανόμενες εργασίες, όπως self-service για τους χρήστες που θέλουν την επαναφορά του κωδικού πρόσβασης, δεν θα ζητούν την παρέμβαση των διαχειριστών του συστήματος, χρησιμοποιώντας μια βοήθεια από ένα desk σύστημα.

Regulatory Compliance Management

Για την ασφάλεια των συστημάτων, των εφαρμογών, και για πληροφορίες από εξωτερικές και εσωτερικές απειλές όπως δυσαρεστημένοι εργαζόμενοι που μπορεί να διαγράψουν σημαντικά δεδομένα και η τήρηση ποικίλων ρυθμιστικών, για τη προστασία της ιδιωτικής ζωής και απαιτήσεις για την ασφάλεια των αρχείων όπως HIPPA είτε SOX, οι οργανισμοί εφαρμόζουν ένα "IT general and application-level έλεγχο" πλαίσιο που προέρχεται από τη βιομηχανία προτύπων πλαισίων όπως το ISO 27002 και το Information Technology Infrastracture Library (ITIL). Οι IAM διαδικασίες και εφαρμογές που παρέχουν τη δυνατότητα για να βοηθήσουν τους οργανισμούς να έχουν τους στόχους στο τομέα του access control operational security όπως η εκχώρηση συγκεκριμένων δικαιωμάτων για τα μέλη προσωπικού για να εκτελούν τα καθήκοντά τους.

Η IAM έχει τη δυνατότητα να φέρει νέα IT μοντέλα παράδοσης και ανάπτυξης όπως cloud υπηρεσίες, ξεχωριστά από τη καλυτέρευση της λειτουργικής αποδοτικότητας και την αποτελεσματική διαχείριση των συστημάτων. Για παράδειγμα, κοινή ταυτότητα, που είναι κύριο στοιχείο της IAM, δίνει τη δυνατότητα για σύνδεση και δυνατότητα μεταφοράς των ταυτοποιημένων πληροφοριών πέρα των ορίων εμπιστοσύνης. Έτσι, δίνει την άδεια σε επιχειρήσεις και σε παρόχους cloud υπηρεσιών να γεφυρώσουν τον τομέα της ασφάλειας με web single-sign-on και της ομοσπονδίας μέσω του user provisioning.

Κάποιες από τις περιπτώσεις χρήσης του συννέφου που έχουν ανάγκη την IAM υποστήριξη από το CSP περιλαμβάνουν:

- Οι εργαζόμενοι και οι εργοδότες κάποιου οργανισμού οι οποίοι έχουν πρόσβαση σε μια υπηρεσία SaaS κάνοντας χρήση τη σχετική ταυτότητα από την ομοσπονδία όπως τις πωλήσεις και την υποστήριξη των μελών του προσωπικού με την πρόσβαση στο salesforce.com με εταιρική ταυτότητα και διαπιστευτήρια.

- Οι διαχειριστές του IT που έχουν πρόσβαση στην κονσόλα διαχείρισης CSP για να διαθέτουν πόρους και πρόσβαση στους χρήστες χρησιμοποιώντας μια εταιρική ταυτότητα όπως οι διαχειριστές του Newco.com οι οποίοι τροφοδοτούν εικονικές μηχανές είτε VMs στην υπηρεσία EC2 της Amazon, έχει σχεδιαστεί με

τις ταυτότητες, τα δικαιώματα και τα διαπιστευτήρια για τη λειτουργία των VMs δηλαδή, start, stop,suspend, και delete VMs.

❖ Προγραμματιστές που κατασκευάζουν λογαριασμούς για εταιρικούς χρήστες σε PaaS πλατφόρμα όπως οι προγραμματιστές από τη Newco.com οι οποίοι τροφοδοτούν λογαριασμούς στη Force.com για τους εργαζόμενους της Partnerco.com που έχουν σύμβαση να εκτελούν τα καθήκοντα της επιχειρησιακής διαδικασίας για την Newco.com.

❖ Οι τελικοί χρήστες οι οποίοι έχουν πρόσβαση στις υπηρεσίες αποθήκευσης στο cloud όπως το Amazon S3 και στη από κοινού χρήση δεδομένων και αντικειμένων με τους χρήστες, εντός και εκτός του τομέα και εκμεταλλεύονται τις δυνατότητες διαχείρισης της πολιτικής πρόσβασης.

Μια εφαρμογή που διατηρείται σε ένα πάροχο cloud όπως το Amazon EC2 έχει τη δυνατότητα για πρόσβαση αποθήκευσης από άλλη υπηρεσία cloud όπως το Mosso. Εφόσον το IAM επιτρέπει εφαρμογές για να εξωτερικεύσει τα στοιχεία γνησιότητας, χρήστες έχουν τη δυνατότητα να υιοθετήσουν γρήγορα υπηρεσίες όπως το Salesforce.com ελαττώνοντας το χρόνο που ζητείται για να ενσωματωθούν με τους παρόχους υπηρεσιών. Οι δυνατότητες του IAM μπορούν ακόμη να βοηθήσουν κάποιο χρήστη να αναθέσει μια διαδικασία είτε μια υπηρεσία προς τους άλλους με μειωμένες επιπτώσεις στην ιδιωτική ζωή και ασφάλεια του. Με λίγα λόγια, η επέκταση της IAM στρατηγικής, της πρακτικής και της αρχιτεκτονικής δίνει τη δυνατότητα στους χρήστες να επεκτείνουν τις πρακτικές για την πρόσβαση στη διαχείριση και στις διαδικασίες του cloud. Έτσι, οι χρήστες με τις βασικές πρακτικές IAM μπορούν να κάνουν χρήση γρήγορα των υπηρεσιών cloud διατηρώντας παράλληλα την αποδοτικότητα και την αποτελεσματικότητα των ελέγχων ασφάλειάς τους.

2.4.2. Προκλήσεις IAM

Μια σημαντική πρόκληση του IAM αφορά τη διαχείριση της πρόσβασης για διαφορετικές ομάδες χρηστών όσον αφορά τη πρόσβαση σε εσωτερικές και

εξωτερικές φιλοξενούμενες υπηρεσίες. Το IT είναι συνέχεια με την πρόκληση για την γρήγορη παροχή της κατάλληλης πρόσβασης στους χρήστες των οποίων οι ρόλοι και οι ευθύνες ποικίλουν για επαγγελματικούς λόγους. Ένα άλλο θέμα είναι ο κύκλος εργασιών (turnover) των χρηστών. Ο κύκλος εργασιών (turnover) μεταβάλλεται σύμφωνα με τη βιομηχανία και τη λειτουργία και μπορεί ακόμη να προκαλέσει αλλαγές από ανανεωμένες κυκλοφορίες προϊόντων και υπηρεσιών. Έτσι, η διατήρηση των IAM διαδικασιών μπορεί να γίνει σε μία συνεχής πρόκληση.

Οι πολιτικές πρόσβασης στα δεδομένα είναι σπάνια κεντρικές και εφαρμόζονται με συνέπεια. Οι χρήστες μπορεί να έχουν ανόμοιους καταλόγους, να δημιουργούν σύνθετα δίκτυα των ταυτοτήτων γνησιότητας, τα δικαιώματα πρόσβασης και τις διαδικασίες. Αυτό έχει κάνει ανεπάρκειες στην πρόσβαση των χρηστών και στις διαδικασίες διαχείρισης, ενώ εκθέτει τους οργανισμούς αυτούς σε σημαντική ασφάλεια, συμμόρφωση με τους κανονισμούς και των παραγόντων κινδύνου του κύρους τους.

Για την καταπολέμηση αυτών των προκλήσεων και των κινδύνων, πολλοί χρήστες έχουν ζητήσει τεχνολογικές λύσεις για την ενεργοποίηση κεντρικής και αυτοματοποιημένης διαχείρισης της πρόσβασης τους. Πολλές από αυτές τις πρωτοβουλίες σχετίζονται και με υψηλές προσδοκίες, που δεν θεωρούνται έκπληξη λόγω ότι το πρόβλημα είναι συνήθως μεγάλο και σύνθετο. Τις περισσότερες φορές αυτές οι πρωτοβουλίες για τη καλυτέρευση του IAM μπορεί να κάνει πολλά χρόνια και να μας επιζημειώσει με τεράστιο κόστος. Έτσι, οι χρήστες θα πρέπει να θεωρήσουν την IAM στρατηγική και αρχιτεκτονική με την επιχειρησιακή και με τους IT drivers οι οποίοι διευθυνσιοδοτούν τα πιο κύρια θέματα μη αποτελεσματικότητας, ενώ αντίστοιχα διατηρούν και την αποτελεσματικότητα του ελέγχου βάση ελέγχου πρόσβασης. Μόνο τότε οι χρήστες θα έχουν μεγαλύτερη πιθανότητα επιτυχίας και απόδοσης.

2.5. Διαχείριση Ασφάλειας στο cloud

Με την διατήρηση των δημόσιων cloud υπηρεσιών, ένα μεγάλο κομμάτι του δικτύου μας, τα συστήματα, οι εφαρμογές και τα δεδομένα βρίσκονται από τον έλεγχο

του παρόχου. Η παράδοση των cloud μοντέλων υπηρεσιών θα δημιουργήσει σύννεφα (clouds) εικονικών περιμέτρων καθώς και ένα πρότυπο ασφαλείας με τις αρμοδιότητες να παρέχονται μεταξύ του χρήστη και του παρόχου των cloud υπηρεσιών (CSP). Αυτό το στοιχείο κοινής ευθύνης θα δημιουργήσει καινούργιες προκλήσεις στη διαχείριση της ασφάλειας στο προσωπικό του IT ενός χρήστη. Έτσι, η κύρια ερώτηση που κάποιος υπεύθυνος ασφάλειας πληροφοριών θα πρέπει να απαντήσει είναι η επαρκής διαφάνεια από τις υπηρεσίες cloud για τη διαχείριση της διακυβέρνησης, κοινές ευθύνες και της εφαρμογής των διαδικασιών διαχείρισης της ασφάλειας για πρόληψη και καταπολέμηση ελέγχου, με σκοπό να εξασφαλίζει ο χρήστης ότι τα δεδομένα του στο cloud είναι κατάλληλα προστατευμένα.

Οι χρήστες του cloud, θα πρέπει να κατανοήσουν τα όρια της εμπιστοσύνης των υπηρεσιών τους στο cloud. Θα πρέπει να αντιληφθούν όλα τα στρώματα που έχουν στη κατοχή τους, το δίκτυο, το host, τις εφαρμογές, τη βάση δεδομένων, την αποθήκευση και τις web υπηρεσίες οι οποίες αποτελούνται και από υπηρεσίες γνησιότητας. Θα πρέπει ακόμη να αντιληφθούν το περιεχόμενο της διαχείρισης του συστήματος πληροφορικής και τις ευθύνες που εμπίπτουν πάνω τους.

Παρόλο που μπορεί να μεταφέρει κάποιες από τις ευθύνες στο πάροχο, το επίπεδο ευθυνών διαφοροποιείται από διάφορους παράγοντες, συμπεριλαμβανομένης της υπηρεσίας Service delivery model (SPI), service-level συμφωνία παρόχου (SLA), και του provider-specific ικανότητες να ενισχύσουν την επέκταση των εσωτερικών διαδικασιών διαχείρισης της ασφάλειας και των εργαλείων μας.

Διάφοροι IT χρήστες χρησιμοποιούν πλαίσια διαχείρισης της ασφάλειας, όπως το ISO/IEC 27000 και την Information Technology Infrastructure Library (ITIL) framework. Αυτά τα βιομηχανικά frameworks δίνουν οδηγίες για το σχεδιασμό και την εφαρμογή ενός προγράμματος διακυβέρνησης με τη διατήρηση των διαδικασιών διαχείρισης που προστατεύουν τα προσωπικά δεδομένα. Για παράδειγμα, το ITIL δίνει μια ενδελεχή περιγραφή ενός αριθμού σημαντικών IT πρακτικών με ολοκληρωμένες λίστες ελέγχου, εργασίες και διαδικασίες οι οποίες μπορούν να προσαρμοστούν. Ένα κύριο δόγμα του ITIL, και που ισχύει για το cloud computing, είναι ότι οι χρήστες και τα συστήματα πληροφοριών μεταβάλλονται συνεχώς. Έτσι, τα frameworks διαχείρισης, όπως το ITIL δίνουν τη δυνατότητα με τη συνεχή

ανάπτυξη των υπηρεσιών που είναι απαραίτητες για να ευθυγραμμιστούν και να επαναπροσδιοριστούν οι IT υπηρεσίες στις διάφορες ανάγκες των χρηστών. Η αυξανόμενη βελτίωση υπηρεσιών σημαίνει εντοπισμός και εφαρμογή βελτιώσεων στις υπηρεσίες IT που υποστηρίζουν διάφορες για τους χρήστες διαδικασίες, όπως η αυτοματοποίηση της δύναμης των πωλήσεων χρησιμοποιώντας πάροχο υπηρεσιών cloud. Δεδομένου των χαρακτηριστικών των υπηρεσιών του cloud computing, οι δραστηριότητες που υποβάλονται εντός των διαδικασιών διαχείρισης της ασφάλειας πρέπει να αλλάζουν συνέχεια και να είναι επίκαιρες και αποτελεσματικές. Η διαχείριση της ασφάλειας δηλαδή είναι μια συνεχόμενη διαδικασία και είναι πολύ ιδιαίτερη για την ασφάλεια της διαχείρισης του cloud.

Ο στόχος του πλαισίου διαχείρισης ITIL χωρίζεται σε δύο μέρη:

Εφαρμογή των απαιτήσεων ασφαλείας

Οι απαιτήσεις ασφαλείας καθορίζονται στο SLA, όπως και άλλες εξωτερικές απαιτήσεις, οι οποίες είναι η βάση του πλαισίου των σχετικών συμβάσεων, της νομοθεσίας, σε εσωτερικές είτε σε εξωτερικές πολιτικές.

Η πραγματοποίηση ενός βασικού επιπέδου ασφαλείας

Αυτό είναι ιδιαίτερο για να εξασφαλίσουν την ασφάλεια και τη συνέχεια του χρήστη και να φτάσουν την απλοποιημένη διαχείριση του service-level για τη διαχείριση ασφάλειας των πληροφοριών. Ακόμη, οι σταθερές διαδικασίες διαχείρισης της ασφάλειας είναι βασισμένες σε συγκεκριμένες πολιτικές και πρότυπα, με στόχο την ασφάλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Πρότυπα Διαχείρισης Ασφάλειας

Τα πρότυπα που έχουν σχετίζονται με τις πρακτικές διαχείρισης της ασφάλειας στο cloud είναι το ITIL και το ISO/IEC 27001 και 27002.

2.5.1. Έλεγχος Πρόσβασης στο Cloud

Σε ένα cloud computing μοντέλο κατανάλωσης, όπου οι χρήστες έχουν πρόσβαση σε υπηρεσίες cloud από οποιοδήποτε σημείο πρόσβασης στο διαδίκτυο, ο έλεγχος πρόσβασης θα παίζει διαρκώς όλο και πιο μειωμένο ρόλο. Ο λόγος είναι ότι οι παραδοσιακοί έλεγχοι πρόσβασης βασίζονται σε δίκτυο που επικεντρώνεται στη προστασία των πόρων από μη εξουσιοδοτημένη πρόσβαση με βάση τα χαρακτηριστικά του κεντρικού υπολογιστή, ο οποίος τις περισσότερες περιπτώσεις είναι ανεπαρκής, και μπορεί να προκαλέσει λανθασμένους υπολογισμούς. Στο cloud, ο έλεγχος πρόσβασης στο δίκτυο εκδηλώνεται ως πολιτικές firewall επιβάλλοντας την ύπαρξη host-based ελέγχου πρόσβασης στην είσοδο και στην έξοδο στα σημεία εισόδου του cloud και λογική ομαδοποίηση των instances μέσα στο cloud. Αυτό συνήθως επιτυγχάνεται με τη χρήση πολιτικών (κανόνες) χρησιμοποιώντας τυποποιημένο πρωτόκολλο μετάδοσης ελέγχου Protocol/Internet (TCP/IP) παραμέτρους, συμπεριλαμβανομένης της πηγής IP, τη θύρα πηγής, τη διεύθυνση προορισμού IP και το destination port.

Σε αντίθεση με το network-based έλεγχο πρόσβασης, θα πρέπει να δίνεται μεγάλη έμφαση μέσα στο cloud στον έλεγχο πρόσβασης των χρηστών, δεδομένου ότι η ταυτότητα ενός χρήστη μπορεί να συνδέεται ισχυρά με τους πόρους σε ένα cloud και θα μπορεί να βοηθήσει σχετικός λεπτομερής έλεγχος πρόσβασης, λογιστικοί υπολογισμοί του χρήστη, υποστήριξη για συμμόρφωση και τα δεδομένα προστασίας. Οι έλεγχοι διαχείρισης της πρόσβασης των χρηστών, συμπεριλαμβανομένων των single-sign-on (SSO), τα προνόμια διαχείρισης και η καταγραφή των πόρων του cloud, παίζουν σημαντικό ρόλο στη προστασία του απορρήτου και στην ακεραιότητα των πληροφοριών μας στο cloud.

2.5.2. Έλεγχος Πρόσβασης στο SaaS

Στο μοντέλο SaaS παράδοσης, το CSP είναι υπεύθυνο για τη διαχείριση όλων των πτυχών του δικτύου, την υποδομή του διακομιστή και την εφαρμογή. Σε αυτό το μοντέλο, δεδομένου ότι η εφαρμογή δίνεται ως υπηρεσία προς τους τελικούς χρήστες, συνήθως μέσω ενός web browser, οι έλεγχοι που βασίζονται στο δίκτυο γίνονται όλο και λιγότερο σχετικοί και αυξάνονται είτε αντικαθιστώνται από τους ελέγχους πρόσβασης των χρηστών, όπως με τη χρήση ταυτότητας one-time password. Έτσι, οι

χρήστες πρέπει να αναρωτηθούν για τον έλεγχο πρόσβασης των χρηστών για την προστασία των πληροφοριών που φιλοξενούνται από τις SaaS. Ορισμένες υπηρεσίες SaaS όπως η Slaesforce.com, βελτιώνουν τον έλεγχο πρόσβασης στο δίκτυο στον έλεγχο πρόσβασης των χρηστών στην οποία περίπτωση οι χρήστες έχουν την δυνατότητα να επιβάλλουν στην πρόσβαση με βάση το δίκτυο και τις παραμέτρους της πολιτικής των χρηστών.

Η υποστήριξη στον έλεγχο πρόσβασης των χρηστών δεν είναι συνεπής σε παρόχους και οι δυνατότητες μπορεί να ποικίλουν. Ένα μικρό σύνολο από CSPs (κυρίως μεγάλοι πάροχοι SaaS όπως η Salesforce.com, η Google και η Microsoft) αρχίζουν να δίνουν σημασία στις απαιτήσεις της IAM βιομηχανίας, συμπεριλαμβανομένης της υποστήριξης για πρότυπα όπως είναι το SAML το οποίο διευκολύνει την SSO να χρησιμοποιεί τεχνικές γνησιότητας. Παρόλα αυτά, δεδομένου του πρώιμου κύκλου έγκρισης από μεγάλες επιχειρήσεις, από τη σκοπιά των επιχειρήσεων, οι IAM δυνατότητες είναι πρωτόγονες, στην καλύτερη περίπτωση. Οι χρήστες πρέπει να συνεχίσουν να ζητούν τα CSP να παρέχουν IAM χαρακτηριστικά, περιλαμβάνοντας SAML υποστήριξη, user provisioning χρησιμοποιώντας SPML, και ένα ανοικτό API για την υποστήριξη διαφόρων χρηστών και την πρόσβαση σε διαδικασίες αυτοματισμών. Οι οργανισμοί θα πρέπει να αξιοποιήσουν τις καθιερωμένες μεθόδους τους, τις πρακτικές διαχείρισης ταυτότητας, τις διαδικασίες και την αρχιτεκτονική όπως Idp για τη στήριξη της πρόσβασης των χρηστών στη διαχείριση.

2.5.3. Έλεγχος Πρόσβασης στο PaaS

Στο τύπο παράδοσης PaaS, το CSP είναι υπεύθυνη για τη διαχείριση του ελέγχου πρόσβασης στο δίκτυο, τους servers και της υποδομής της πλατφόρμας των εφαρμογών. Παρόλα αυτά, ο χρήστης είναι υπεύθυνος για να ελέγχει την πρόσβαση στις εφαρμογές που αναπτύχθηκαν σε μια πλατφόρμα PaaS. Ο έλεγχος πρόσβασης στις εφαρμογές δηλώνεται ως διαχείριση πρόσβασης στους τελικούς χρήστες, η οποία αποτελείται από προβλέψεις και εξακρίβωση της γνησιότητας των χρηστών.

Η υποστήριξη για τον έλεγχο πρόσβασης των χρηστών δεν είναι συνεπής από τους παρόχους, και οι δυνατότητες μπορεί να διαφέρουν. Μεγάλοι πάροχοι PaaS, με την εξαίρεση του Force.com και του Microsoft Azure, δίνουν στοιχειώδη υποστήριξη για τον έλεγχο πρόσβασης των χρηστών. Για παράδειγμα η Google υποστηρίζει μια υβριδική έκδοση του OpenID και OAuth πρωτοκόλλου που συνδυάζει την έγκριση και την γνησιότητα της ροής σε λιγότερα βήματα έτσι ώστε να ενισχύεται η χρηστικότητα. Θα μπορούσαμε επίσης να αναθέσουμε την γνησιότητα του IdP μας εάν η CSP υποστηρίζει τα ομοσπονδιακά πρότυπα, όπως η Security Assertion Markup Language (SAML).

2.5.4. Έλεγχος Πρόσβασης στο IaaS

Οι χρήστες των IaaS είναι καθόλα υπεύθυνοι για τη διαχείριση όλων των πτυχών του ελέγχου πρόσβασης στους πόρους που έχουν στο cloud. Η πρόσβαση στα virtual servers, στα virtual δίκτυα, στην virtual αποθήκευση και στις εφαρμογές που φιλοξενούνται σε μια πλατφόρμα IaaS θα πρέπει να σχεδιάζεται και να διαχειρίζεται από τον χρήστη. Σε ένα τύπο χορήγησης IaaS, η διαχείριση ελέγχου πρόσβασης εμπίπτει σε μία από τις ακόλουθες δύο κατηγορίες:

CSP infrastructure access control

Είναι η διαχείριση του ελέγχου πρόσβασης στις εφαρμογές του κεντρικού υπολογιστή, του δικτύου και της διαχείρισης των εφαρμογών που ανήκουν και διοικούνται από τον CSP.

Customer virtual infrastructure access control

Η διαχείριση ελέγχου πρόσβασης στον εικονικό (virtual) server, στην εικονική αποθήκευση, στα εικονικά δίκτυα και στις εφαρμογές που φιλοξενούνται από τους εικονικούς servers.

2.5.5. Access Control (έλεγχος πρόσβασης)

Κατά βάση, η διαχείριση του ελέγχου πρόσβασης είναι μια ευρεία λειτουργία που περιλαμβάνει τις απαιτήσεις πρόσβασης για τους χρήστες και τους διαχειριστές

του συστήματος (προνομιούχων χρηστών), οι οποίοι έχουν πρόσβαση στο δίκτυο, στους πόρους του συστήματος και στην εφαρμογή. Οι λειτουργίες διαχείρισης ελέγχου πρόσβασης θα πρέπει να αντιμετωπίσουν τα ακόλουθα:

- Ποιός έχει πρόσβαση και σε ποιούς πόρους, έλεγχος και υποβολή εκθέσεων που επαληθεύουν τα δικαιώματα και τις αναθέσεις.

- Ποιός θα πρέπει να έχει πρόσβαση και σε τί πόρους, εκχώρηση δικαιωμάτων σε χρήστες.

- Γιατί θα πρέπει ο χρήστης να έχει πρόσβαση στο πόρο, εκχώρηση δικαιωμάτων με βάση τα καθήκοντα και τις ευθύνες του χρήστη.

- Το τρόπο πρόσβασης στους πόρους, το τύπο μεθόδου ελέγχου ταυτότητας και ισχύς η οποία πρέπει να απαιτείται πριν από τη χορήγηση της πρόσβασης στο πόρο.

Οι παραπάνω κατηγορίες του τομέα ελέγχου πρόσβασης πρέπει να αντιμετωπιστούν από τις πολιτικές των οργανισμών και τα πρότυπα πρόσβασης και να ευθυγραμμιστούν με τους ρόλους του χρήστη και τις ευθύνες του, συμπεριλαμβανομένων των τελικών χρηστών και των προνομιακών διαχειριστών του συστήματος.

2.5.6. ITIL

Η Information Technology Infrastructure Library (ITIL) είναι σύνολο βέλτιστων πρακτικών και κατευθυντηρίων γραμμών που καθορίζουν μια ολοκληρωμένη διαδικασία προσέγγισης για τη διαχείριση πληροφοριών των υπηρεσιών τεχνολογίας. Η ITIL μπορεί να εφαρμοστεί σε σχεδόν κάθε είδους περιβάλλον του IT, συμπεριλαμβανομένων και το περιβάλλον λειτουργίας του cloud. Η ITIL επιδιώκει να σιγουρέψει ότι τα αποτελεσματικά μέτρα ασφάλειας των πληροφοριών λαμβάνονται σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο. Η

ασφάλεια των πληροφοριών θεωρείται επαναληπτική διαδικασία που πρέπει να ελέγχεται, να σχεδιάζεται, να εφαρμόζεται, να αξιολογείται και να διατηρείται.

Η ITIL χωρίζει την ασφάλεια των πληροφοριών προς τα κάτω σε:

Διαδικασίες - ποιός κάνει τί και πότε για την επίτευξη των στόχων.
Οδηγίες εργασίας - οδηγίες για τη λήψη συγκεκριμένων δράσεων.
Πολιτικές - οι γενικοί στόχοι που προσπαθεί να πετύχει ένας οργανισμός.
Διεργασίες - τι πρέπει να συμβεί για την επίτευξη των στόχων.

Η διαχείριση της ασφάλειας κατά την ITIL διαδικασία με βάση το κώδικα πρακτικής για την ασφάλεια πληροφοριών είναι γνωστή ως το πρότυπο ISO/IEC 17799:2005. Η διαδικασία διαχείρισης της ασφάλειας ITIL έχει σχέση με όλες τις άλλες σχεδόν διαδικασίες ITIL.

Παρόλα αυτά, οι πιο προφανείς σχέσεις θα είναι στη διαδικασία παροχής υπηρεσιών σε επίπεδο διαχείρισης, σε διαδικασία διαχείρισης συμβάντων και διαδικασία αλλαγής διαχείρισης, δεδομένου ότι επηρεάζουν σε μεγάλο βαθμό την κατάσταση της ασφάλειας στο σύστημα, όπως το server, το δίκτυο είτε την εφαρμογή. Η ITIL επίσης σχετίζεται με το πρότυπο ISO/IEC 20000, καθώς αυτό είναι το πρώτο διεθνές πρότυπο για IT Service Management (ITSM). Βασίζεται και προορίζεται να αντικαταστήσει το εκ των πρωτέρων βρετανικό πρότυπο BS 15000.

Οι χρήστες και τα συστήματα διαχείρισης δεν μπορούν να πιστοποιηθούν ως “ITIL compliant”. Ένας οργανισμός που έχει εφαρμόσει καθοδήγηση ITIL σε ITSM μπορεί, παρόλα αυτά, να πετύχει τη συμμόρφωση και να ζητήσει πιστοποίηση σύμφωνα με το πρότυπο ISO/IEC 20000.

2.5.7. ISO 27001/27002

Το ISO/IEC 27001 καθορίζει επισήμως τις υποχρεωτικές απαιτήσεις για την ασφάλεια των πληροφοριών στο σύστημα διαχείρισης (ISMS). Είναι επίσης πρότυπο πιστοποίησης και χρησιμοποιεί το πρότυπο ISO/IEC 27002 για να αναφέρει σχετικούς ελέγχους ασφαλείας των πληροφοριών εντός των ISMS. Παρόλα αυτά, λόγω ότι το πρότυπο ISO/IEC 27002 είναι απλώς κώδικας πρακτικής/καθοδήγησης

και όχι πρότυπο πιστοποίησης, οι οργανισμοί είναι ελεύθεροι να επιλέξουν και να εφαρμόσουν τους ελέγχους κατά το δοκούν. Με δεδομένη την σχετική τάση σε οργανισμούς που κινούνται προς το πρότυπο ISO/IEC 27001 για πληροφορίες διαχείρισης της ασφάλειας, υπάρχει μια ευρύτερη συναίνεση μεταξύ των επαγγελματιών της ασφάλειας πληροφοριών να αναθεωρήσουν τη διαχείριση της ασφάλειας των βέλτιστων πρακτικών ITIL με στόχο την ενίσχυση της εφαρμογής και της λογικής ασφάλειας στο τομέα υποδομών Information and Communication Technology (ICT).

2.6. Security - As - a -[Cloud] Service

Μέχρι στιγμής έχουμε αντιμετωπίσει την ασφάλεια που παρέχεται από τους παρόχους cloud υπηρεσιών (CSP), όπως και την ασφάλεια που παρέχεται από τους χρήστες που χρησιμοποιούν τις υπηρεσίες του cloud. Σε αυτό το κεφάλαιο, θα δώσουμε έμφαση στην ασφάλεια που παρέχεται σαν υπηρεσία του cloud. Δηλαδή η ασφάλεια που παρέχεται μέσω του cloud γνωστή ως security-as-a-service.

Με το SaaS υπάρχουν δύο πάροχοι. Ο πρώτος τύπος περιλαμβάνει εγκατεστημένες πληροφορίες ασφάλειας των παρόχων οι οποίοι τροποποιούν τις μεθόδους παράδοσής τους για να συμπεριλάβουν τις υπηρεσίες που παραδίδονται μέσω του cloud. Ο δεύτερος τύπος περιλαμβάνει τις start-up πληροφορίες των εταιρειών ασφάλειας που εμφανίζονται επίσης σε αυτό το τομέα ως καθαρές, παίζοντας με τα CSPs πιο απλά, αυτές οι εταιρείες παρέχουν την ασφάλεια μόνο ως υπηρεσία cloud, και δεν παρέχουν την κλασσική ασφάλεια των πληροφοριών client/server στο δίκτυο, στους hosts και από είτε πρός τις εφαρμογές.

Στις καθιερωμένες εταιρείες ασφάλειας των πληροφοριών που αλλάζουν τα επιχειρηματικά τους μοντέλα για να συμπεριλάβουν ακόμη και το SaaS, οι πιο σημαντικές είναι αυτές με τα κλασσικά προγράμματα antimalware πωλητών. Παρόλα αυτά, άλλες καθιερωμένες εταιρείες ασφάλειας των πληροφοριών ασχολούνται επίσης στη παροχή SaaS, ιδιαίτερα σε σχέση με το φιλτράρισμα ηλεκτρονικού ταχυδρομείου.

2.6.1. Φιλτράρισμα WEB περιεχομένου

Όσο τα τελικά σημεία (endpoints) ανήκουν σε μια οργάνωση, είτε βρίσκονται εντός των εγκαταστάσεων ενός οργανισμού, στο σπίτι είτε στο δρόμο, προσπαθούμε να ανακτήσουμε την ιστοσελίδα της κυκλοφορίας, η κυκλοφορία εκτρέπεται σε ένα SaaS πάροχο που σαρώνει για απειλές malware και εξασφαλίζει ότι μόνο καθαρή κυκλοφορία θα παραδίδεται στους χρήστες. Οι οργανισμοί μπορούν ακόμη να καλυτερεύσουν τις πολιτικές τους επιτρέποντας, μπλοκάροντας είτε κάνοντας throttle την κυκλοφορία (χρήση του εύρους ζώνης για την εν λόγω κίνηση μειώνεται). Λόγω του αριθμού των δικτυακών τόπων που είναι προσβάσιμοι, παλαιότερες λύσεις φιλτραρίσματος URL αναπτύχθηκαν στις εγκαταστάσεις των οργανισμών με την προϋπόθεση να είναι πιο αποτελεσματικές. Οι πάροχοι SaaS συμπληρώνουν ότι το φιλτράρισμα URL με την εξέταση των Hypertext Transfer Protocol (HTTP) πληροφοριών, το περιεχόμενο της σελίδας, καθώς και οι ενσωματωμένες συνδέσεις να κατανοήσουν καλύτερα το περιεχόμενο της ιστοσελίδας. Ακόμη, οι υπηρεσίες αυτές χρησιμοποιούν ένα συλλογικό βαθμολογικό σύστημα για να καλυτερεύσει την ακρίβεια του φιλτραρίσματος

2.6.2. Email Filtering

Το SaaS για το ηλεκτρονικό ταχυδρομείο περιλαμβάνει κυρίως το καθαρισμό του spam, των phising emails και του κακόβουλου λογισμικού που περιλαμβάνεται στο email από το εισερχόμενο ρεύμα οργανισμού, και εν συνεχεία δίνει αυτό το καθαρό email ασφαλή στον οργανισμό έτσι ώστε να είναι αποτελεσματικό και όχι μολυσμένο. Τα οφέλη αυτής της προσέγγισης δεν είναι μόνο η πιο ολοκληρωμένη ασφάλεια για τους χρήστες λόγω της χρήσης πολλαπλών κινητήρων, αλλά και η καλύτερη απόδοση των συσκευών των χρηστών καθώς το antimalware λειτουργεί μέσα στο cloud και όχι απευθείας στο endpoint, καθώς και πολύ καλύτερη antimalware διαχείριση. Η antimalware διαχείριση είναι καλύτερη από τις endpoint λύσεις γιατί η antimalware έχει OS επεξεργαστή, έτσι ώστε να μπορεί να διαχειρίζεται κεντρικά μέσω του cloud από το να εργάζεται με διάφορα συστήματα διαχείρισης, πιθανότητα από διάφορους antimalware πωλητές. Αυτή η cleansing-in-the-cloud υπηρεσία έχει τα εξής οφέλη: χαμηλό εύρος ζώνης που χρησιμοποιεί το

ηλεκτρονικό ταχυδρομείο, χαμηλό φόρτο των email servers των οργανισμών και καλύτερη αποτελεσματικότητα των antimalware προσπαθειών των οργανισμών.

Παρότι οι περισσότεροι πάροχοι SaaS που αφορούν email τείνουν να δώσουν έμφαση σε εισερχόμενα email, συχνά πλέον χρησιμοποιούνται και για τα εξερχόμενα email. Πολλοί οργανισμοί θέλουν να εξασφαλίσουν ότι δεν θα στέλνουν εσφαλμένα μολυσμένα maleware email, καθώς και τον καθαρισμό των εξερχόμενων μηνυμάτων μέσω του SaaS που είναι μια καλή μέθοδος για τη πρόληψη αυτών των προβλημάτων και αμηχανιών. Ακόμη, το εξωτερικό SaaS email μπορεί να χρησιμοποιηθεί για να τονίσει τις οργανωτικές πολιτικές γύρω από την κρυπτογράφηση του ηλεκτρονικού ταχυδρομείου. Αυτή η κρυπτογράφηση email γίνεται γενικά στο server-to-server επίπεδο έτσι ώστε οι μοναδικές ενέργειες του έκαστου χρήστη και το κλειδί διαχείρισης να μην είναι υποχρεωτικά. Αυτό επιτυγχάνεται με τη χρήση είτε Secure Sockets Layer (SSL) είτε Transport Layer Security (TLS) στο δίκτυο επικοινωνιών στο στρώμα μεταφορών.

Επιπλέον πλεονέκτημα του SaaS anti-malware είναι η συλλογική νοημοσύνη που έχει αποκτηθεί από την προβολή όλων των malware απειλών για όλες τις παραμέτρους σε μια επιχείρηση, ανεξάρτητα από το είδος, όπως server, desktop, laptop, είτε κινητή συσκευή, τη θέση, το λειτουργικό σύστημα είτε την αρχιτεκτονική του επεξεργαστή.

Το SaaS για το ηλεκτρονικό ταχυδρομείο περιλαμβάνει επίσης email backup και αρχειοθέτηση. Αυτή η υπηρεσία περιλαμβάνει συνήθως την αποθήκευση και την εύρεση των μηνυμάτων ηλεκτρονικού ταχυδρομείου ενός οργανισμού σε ένα κεντρικό χώρο αποθήκευσης. Αυτός ο κεντρικός χώρος αποθήκευσης επιτρέπει σε έναν οργανισμό να αναζητά με βάση μιας σειράς παραμέτρων, συμπεριλαμβανομένου του εύρους, την ημερομηνία, τον αποδέκτη, τον αποστολέα, το θέμα και το περιεχόμενο. Οι δυνατότητες αυτές είναι ιδιαίτερα χρήσιμες για σκοπούς e-discovery, οι οποίοι μπορούν να είναι εξαιρετικά δαπανηροί χωρίς αυτές τις δυνατότητες.

2.6.3. Διαχείριση ευπάθειας (vulnerability management)

Καθώς η internet-facing παρουσία των οργανισμών στο διαδίκτυο έχει αυξηθεί σε μέγεθος και πολυπλοκότητα, η ασφαλής διαμόρφωση και λειτουργία των συστημάτων που εμπλέκονται έχει γίνει πιο δύσκολη και πιο σημαντική. Υπάρχουν πάροχοι SaaS που ανακαλύπτουν, δίνουν προτεραιότητα και αξιολογούν τα συστήματα για αδύναμα σημεία, και εν συνεχεία τα αναφέρουν με σκοπό την αποκατάσταση των σημείων αυτών έτσι ώστε να ελέγχεται η ασφαλής λειτουργία των συστημάτων. Οι πληροφορίες χρησιμοποιούνται επίσης για να ελέγχονται και να αναφέρονται ορισμένες κανονιστικές απαιτήσεις όπως το Payment Card Industry's Data Security Standard.

2.6.4. Identity Management - As - a–Service

Η Identity management-as-a-service (IDaaS) μόλις πρόσφατα αναδείχθηκε ως ένα κομματι του SaaS, σε σχέση με το φιλτράρισμα ηλεκτρονικού ταχυδρομείου, το φιλτράρισμα περιεχομένου ιστοσελίδων και τη διαχείριση ευπάθειας οι οποίες είναι καθιερωμένες ως υπηρεσίες SaaS. Υπάρχουν κάποιες ελλείψεις παρόλα αυτά στην ταυτότητα και στη διαχείριση της πρόσβασης (IAM) δυνατότητες σχετικά με τις χρήσεις στο cloud computing, όπως η επεκτασιμότητα. Το IDaaS παρέχει κάποιες υπηρεσίες IAM στο cloud, κάτι που έχει τάση να επικεντρωθεί στον έλεγχο της ταυτότητας αυτό που είναι το πιο σημαντικό πρόβλημα για τους χρήστες. Το IDaaS θα πρέπει επίσης να παρέχει άλλες IAM υπηρεσίες για τους χρήστες του cloud, συμπεριλαμβανομένης της έγκρισης, των προβλέψεων και του ελέγχου.

2.6.5. Chinese Wall Security Access Control in Cloud computing

Εισαγωγή

Το cloud computing μετατοπίζει τη θέση της υπολογιστικής υποδομής στο δίκτυο ως υπηρεσία. Αυτό επιτρέπει την ενίσχυση στη συνεργασία, στη κλίμακα, την ευκινησία και τη διαθεσιμότητα. Αυτό επιτρέπει επίσης στις εταιρείες να αλλάξουν είτε να ελαττώσουν τους πόρους τους, όπως απαιτείται από τις επιχειρήσεις. Αυτό δίνει τη δυνατότητα στους χρήστες με επεκτάσιμους πόρους σε pay-as-you-use να

έχουν ιδιαίτερα χαμηλό κόστος. Δεδομένου ότι ένας πάροχος υπηρεσιών μπορεί να έχει πρόσβαση σε ποικίλες εικονικές μηχανές του cloud όπου αποθηκεύονται τα δεδομένα των διάφορων χρηστών μπορεί να προκύψει ανασφαλή ροή πληροφοριών η οποία είναι ένα από τα μειονεκτήματα του cloud.

Η Chinese wall πολιτική ασφαλείας (Chinese Wall Security Access Policy, CWSAP) εφαρμόζει περιορισμούς στη πρόσβαση των πληροφοριών των subjects και objects που θα δημιουργούσαν σύγκρουση συμφερόντων. Μια εταιρεία που διαμορφώνει CWSAP τύπους στο cloud έχει πρόσβαση σε πληροφορίες, σε subjects και objects και σε λειτουργίες πρόσβασης για την σύγκρουση συμφερόντων Conflict Of Interest (COI) τάξη. Ένα subject μέσα σε ένα cloud instance που υλοποιεί CWSAP είναι ένας χρήστης που έχει πρόσβαση στις υπηρεσίες είτε τα δεδομένα που φιλοξενούνται στο cloud instance. Ένα object είναι η υπηρεσία του cloud instance που εγγυάται την πρόσβαση στη ροή πληροφοριών. Όλα τα αντικείμενα που ανήκουν στις ίδιες ομάδες ασφαλείας ανήκουν και στην ίδια COI. Έκαστο αντικείμενο που ανήκει σε διαφορετικές κατηγορίες COI ανήκει και σε διαφορετικές ομάδες ασφαλείας. Μια λειτουργία πρόσβασης έχει την ικανότητα να διαβάζει και να γράφει δεδομένα χρησιμοποιώντας υπηρεσίες που φιλοξενούνται στο cloud instance από ένα υποκείμενο. Μπορεί να υπάρχουν one to one, είτε many to many subject to object σχέσεις.

Chinese Wall Security Access Policy (CWSAP)

Η ποικιλογένεια των υπηρεσιών που δίνονται από το cloud για το μηχανισμό ελέγχου πρόσβασης, αποτρέπει τη μη εξουσιοδοτημένη χρήση των πόρων και των υπηρεσιών του cloud. Το Chinese wall security access policy που σκέφτηκαν οι Brewer και Nash εξασφαλίζει ότι καμία πληροφορία δεν μπορεί να ρέει μεταξύ του υποκειμένου και του αντικειμένου που θα μπορεί να δημιουργήσει μια σύγκρουση συμφερόντων (COI). Μία μηχανή αποθήκευσης cloud αποθηκεύει και διεξάγει ευαίσθητες πληροφορίες. Πολιτικές για τον καθορισμό πρόσβασης σε εικονικές μηχανές σε ένα cloud πρέπει να προέρχονται από αυτό για να μην έχει διαρροή πληροφοριών. Η επιβολή του CWSAP στο Iaas στρώμα αποτρέπει αυτή τη διαρροή πληροφοριών, όπως ο χρήστης ο οποίος ελέγχει τις εικονικές μηχανές που κρατούν

σημαντικές πληροφορίες. Μια συμβουλευτική εταιρεία η οποία συνεργάζεται με τους χρήστες, θα πρέπει να έχει πρόσβαση σε αυτές τις εικονικές μηχανές που κατέχουν αυτά τα ευαίσθητα δεδομένα. Έκαστη εικονική μηχανή που έχει πρόσβαση ο κάθε σύμβουλος σχετίζεται με το όνομα του συνόλου δεδομένων της εταιρείας και της τάξης COI που ανήκουν τα αντικείμενα. Το θέμα είναι ο σύμβουλος στο σύστημα που προσπαθεί να έχει πρόσβαση στα δεδομένα. Σε περίπτωση που η απόφαση δεν παραβιάζει τους κανόνες του CWSAP τότε η πρόσβαση του VM γίνεται αποδεκτή. Σε περίπτωση που η απόφαση παραβιάζει τους κανόνες του CWSAP τότε δεν χορηγείται καμία πρόσβαση. Όταν το αντικείμενο είναι εικονική μηχανή που κατέχει οικονομικά έγγραφα που περιέχουν σημαντικές πληροφορίες για κάθε εταιρεία τότε το αντικείμενο έχει τις εξής ιδιότητες:

- Κάθε αντικείμενο έχει many to one σχέση μέσα σε ένα cloud instance μεταξύ των ομάδων ασφαλείας που έχουνε πρόσβαση στο αντικείμενο.

- Κάθε ομάδα ασφαλείας μέσα σε ένα cloud instance έχει many to one σχέση μεταξύ της ομάδας ασφαλείας και των Conflict Of Interest (COI) τάξεων.

Το θέμα είναι ο σύμβουλος που προσπαθεί να έχει πρόσβαση σε εικονικές μηχανές είτε αντικείμενα. Κάθε υποκείμενο έχει πρόσβαση σε όλα τα αντικείμενα της ίδιας ομάδας ασφαλείας. Ένα υποκείμενο έχει επίσης πρόσβαση σε αντικείμενα που ανήκουν σε διαφορετικές COI τάξεις σε σύγκριση με την ομάδα ασφαλείας που έχει αυτό πρόσβαση. Κάθε αντικείμενο στην κοινή ομάδα ασφαλείας είναι προσβάσιμο από όλες τις ομάδες ασφαλείας. Τα αντικείμενα που ανήκουν στην ομάδα που έχει καθαριστεί από απειλές και συνήθως παρέχει utility υπηρεσίες. Τα αντικείμενα στην εξετασμένη από απειλές ομάδα δεν θα αποθηκεύουνε τις πληροφορίες που αφορούν τους πελάτες.

ΚΕΦΑΛΑΙΟ 3

Εφαρμογές του Cloud Computing

3.1. Nimbus

3.1.1. Τι είναι το Nimbus Cloud;

Το Nimbus είναι εργαλειοθήκη που, εφόσον εγκατασταθεί σε ένα σύμπλεγμα, παρέχει μια υποδομή ως σύννεφο υπηρεσίας στον πελάτη του μέσω των API web service που βασίζονται στο WSRF είτε του Amazon EC2 WSDL web service. Το Nimbus είναι δωρεάν λογισμικό ανοικτού κώδικα, σύμφωνα με τις απαιτήσεις της Άδειας Apache, έκδοση 2.

Ο Nimbus υποστηρίζει τόσο τους συγχρονιστές Xen και KVM όσο και τους προγραμματιστές εικονικών μηχανών Portable Batch System και Oracle Grid Engine. Επιτρέπει την ανάπτυξη αυτο-διαμορφωμένων εικονικών συμπλεγμάτων μέσω της δημιουργίας συμφραζομένων. Είναι διαμορφωμένο σε σχέση με τον προγραμματισμό, τις μισθώσεις δικτύωσης και τη λογιστική χρήση.

3.1.2. Αρχιτεκτονική Nimbus

Η αρχιτεκτονική του Nimbus έχει διαφορετικά στοιχεία όπως υπηρεσία εργασίας (work service), πλαίσιο πόρων υπηρεσίας ιστού web services resource framework (WSRF), σωρειτή (cumulus), πρωτόκολλο απλής πρόσβασης αντικειμένου Simple Object Access Protocol (SOAP) και ερώτημα APIs, RM-API, σύννεφο πελάτη (cloud client), αναφορά πελάτη (reference client), χώρος εργασίας πιλότου (workplace pilot), έλεγχος χώρου εργασίας (workspace control), περιεχόμενο εργασίας (content worker) και γενικό πλαίσιο πράκτορα εργασίας (context worker agent) είναι κάποια από αυτά. Η υπηρεσία εργασίας είναι ανεξάρτητη VMM για να οργανώνει τις σελίδες (sites). Το πλαίσιο πόρων υπηρεσίας ιστού WSRF είναι υπηρεσία ιστού, σταθερό σύνολο λειτουργιών υπηρεσιών ιστού για την απόκτηση / ρύθμιση ιδιοτήτων πόρων. Αυτά μπορούν να χρησιμοποιηθούν για να διαβάζουν και ίσως να γράφουν τη κατάσταση πόρων, κατά τρόπο παρόμοιο με το να έχουν μεταβλητές μελών ενός αντικειμένου παράλληλα με τις μεθόδους του. Ο κύριος δικαιούχος ενός τέτοιου μοντέλου είναι εργαλεία διαχείρισης, τα οποία μπορούν να απαριθμήσουν και να δουν τους πόρους, ακόμη και αν δεν έχουν άλλη γνώση γι αυτά. Επιτρέπει στους επιστήμονες να εκθέτουν εφαρμογές, γραπτά και εργασίες άμεσα ως υπηρεσίες ιστού. Είναι επίσης χρήσιμο για εγκατάσταση απομακρυσμένου πρωτοκόλλου. Ο σωρειτής (cumulus) είναι ανοιχτού τύπου εφαρμογή της Amazon S3 REST APIs. Το πρωτόκολλο απλής πρόσβασης αντικειμένου (SOAP) και το ερώτημα APIs είναι ενσωματωμένα βασισμένα στο EC2.

Το RM-API είναι η γέφυρα μεταξύ της ασφάλειας απομακρυσμένου έλεγχου και διαχειριστή συγκεκριμένων σελίδων εγκατάστασης. Η αναφορά πελάτη (reference client) μπορεί να χρησιμοποιηθεί για να εκθέσει ολόκληρα τα χαρακτηριστικά εγκατάστασης στο πρωτόκολλο WSRF ως γραμμή εντολών χρήστη με βιβλιοθήκη java. Επίσης εφαρμόζεται σε ανεπτυγμένου τύπου χρήσης, απάντησης είτε πύλη ενσωμάτωσης. Ο χώρος εργασίας πιλότου (workplace pilot) χρησιμοποιείται για να εφαρμόσει VM με πηγές.

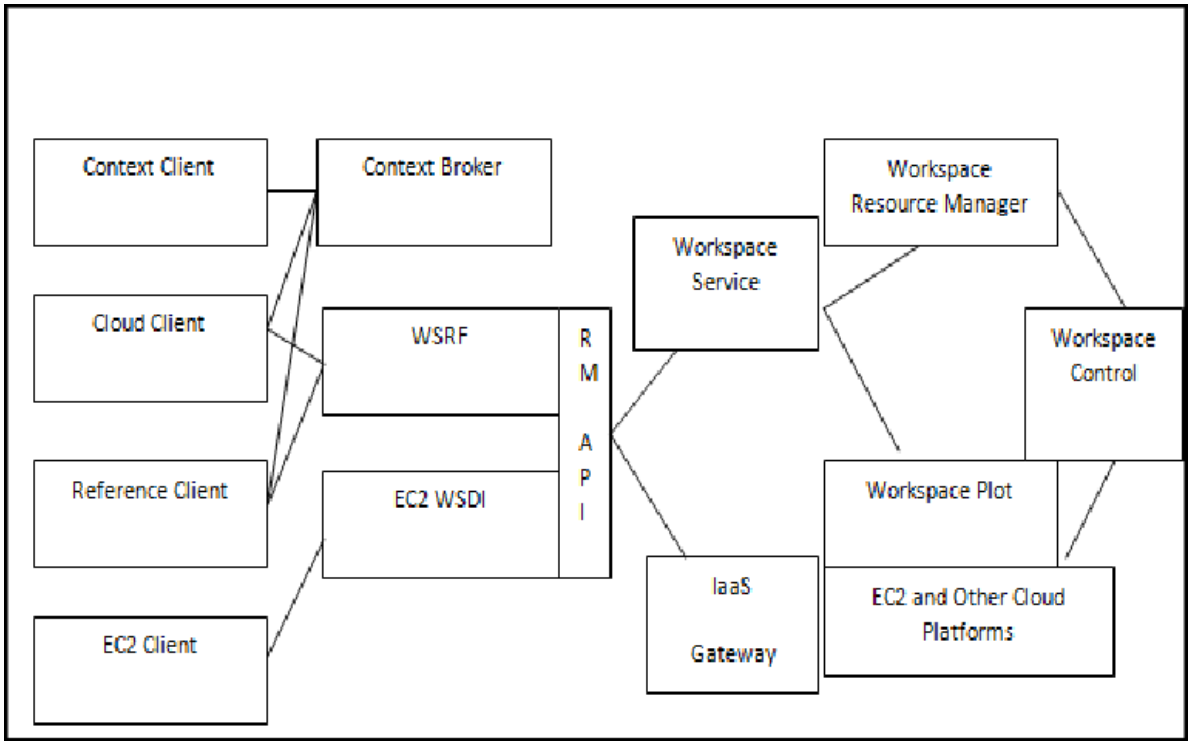
Το Nimbus περιλαμβάνει διάφορα οργανογράμματα γνωστά ως PBS.

Ο έλεγχος χώρου εργασίας (workspace control) χρησιμοποιείται για την ενσωμάτωση VM και για δίκτυο συγκεκριμένων σκοπών στο κάθε επιβλέποντα.

Το περιεχόμενο εργασίας (content broker) επιτρέπει στους χρήστες να συντονίζουν αυτόματα και επαναλαμβανόμενα μεγάλα εικονικά κομμάτια εκτοξευτές.

Το γενικό πλαίσιο πράκτορα εργασίας (context agents) ζει σε VMs και διαδρά με το content broker στην εκκίνηση του VM.

Τα κύρια χαρακτηριστικά του Nimbus είναι η υπηρεσία συννέφων αποθήκευσης, απομακρυσμένης ανάπτυξης διαχείρισης κύκλου ζωής VMs, συμβατότητα με το δίκτυο πρωτοκόλλων Amazon, υποστηρίζει X509 πιστοποιητικά διαπιστευτήρια, εύκολο στη χρήση σύννεφο πελάτη. Επίσης υποστηρίζει μεγάλη αναπαραγωγή, πολλαπλή υποστήριξη πρωτοκόλλου και εύκολη διαχείριση ομάδας, παρακολούθηση ανά χρήστη ξεχωριστά, αναλογία αποθήκευσης ανά πελάτη, εύκολο αίτημα αυθεντικότητας και εξουσιοδότησης. Ρυθμίσεις διαχείρισης, δημιουργία ομάδας με κλίκ (συγκεκριμενοποίηση), χώρος εργασίας πελάτη, ρυθμίσεις δικτύου VM είναι διαθέσιμα.



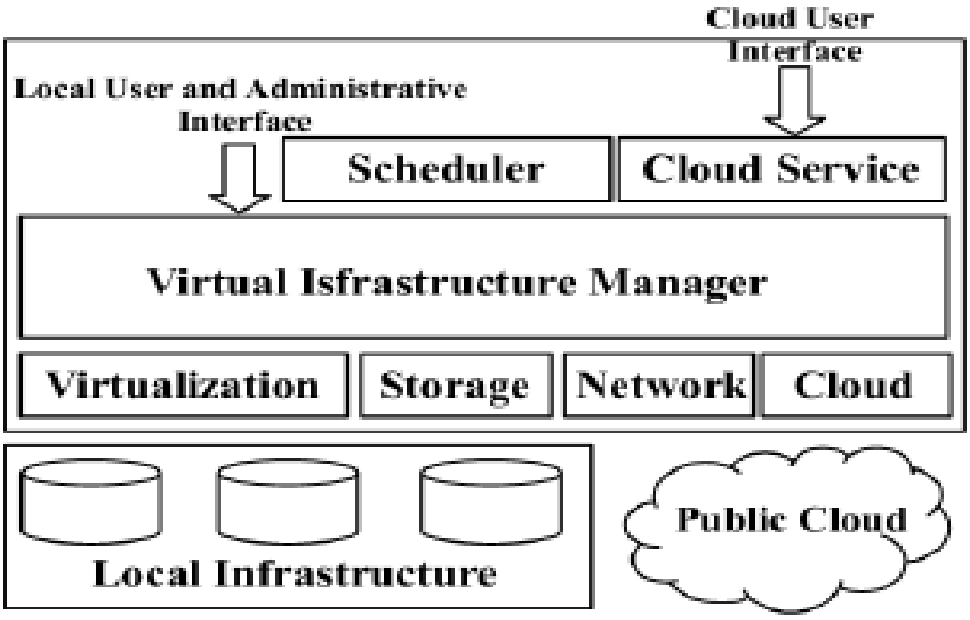
Εικόνα 2: Structure of Nimbus Cloud

3.2.OpenNebula

3.2.1. Τι είναι το OpenNebula

Το OpenNebula είναι από τις πιο πλούσιες εφαρμογές ανοιχτού κώδικα για τη πραγματοποίηση IaaS. Αρχικά είχε φτιαχτεί για τη διαχείριση εικονικών υποδομών και περιλάμβανε απομακρυσμένες διεπαφές που καθιστούσαν υλοποιήσιμη τη κατασκευή δημοσίων νεφών. Συνολικά τέσσερα APIs είναι διαθέσιμα:

- XML-RPC
- Libvirt
- EC2 (Query) APIs
- OpenNebulaCloud API (OCA)



Εικόνα 3: Structure of OpenNebula

3.2.2. Αρχιτεκτονική του OpenNebula

Η αρχιτεκτονική του περιλαμβάνει διάφορα ουσιαστικά συστατικά. Η κύρια ενότητα της αρχιτεκτονικής του περιλαμβάνει τους φυσικούς διακομιστές και τους επιβλέποντές τους ,τους κόμβους αποθήκευσης και τα δικτυακά υλικά network fabric. Η διαχείριση των εργασιών εκτελούνται από οδηγούς που αλληλεπιδρούν με τα API των αντίστοιχων επιβλεπόντων, με τις συσκευές αποθήκευσης και τις τεχνολογίες δικτύων των δημόσιων σύννεφων. Οι δυνατότητες που έχει το OpenNebula είναι:

- CLI, XML-RPC, EC2 συμβατό ερωτηματολόγιο και OCA διεπαφές
- Xen, KVM, και VMware backend
- Διεπαφή στο δημόσιο σύννεφο (Amazon EC2, Elastic Hosts)
- Εικονικά δίκτυα
- Δυναμική κατανομή πηγής
- Εκ των προτέρων κράτηση χωρητικότητας

Δικτύωση: Γενικά οι υπηρεσίες που αναπτύσσονται στο νέφος, από μία συστάδα υπολογιστών προς τη κλασσική three-tier επαγγελματική εφαρμογή, απαιτούν πολλές αλληλένδετες εικονικές μηχανές (VMs) με ένα εικονικό δίκτυο εφαρμογών (VAN) να είναι ο συνδετικός κρίκος μεταξύ τους. Το OpenNebula δημιουργεί δυναμικά αυτά τα εικονικά δίκτυα εφαρμογών και ακολουθεί τις MAC διευθύνσεις που χρησιμοποιήθηκαν στο δίκτυο για τις υπηρεσίες των VMs.

3.3.OpenStack

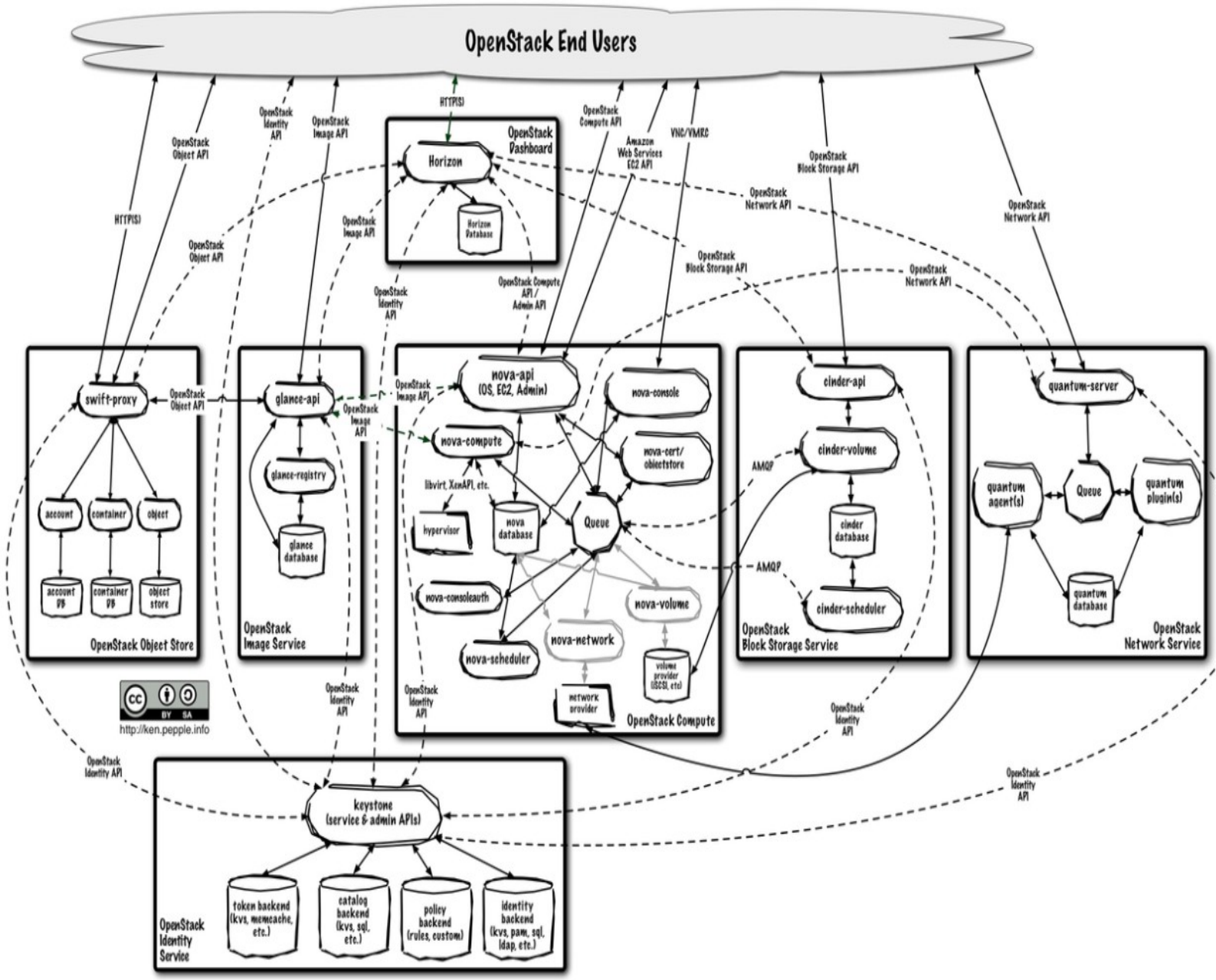
3.3.1.Τι είναι το OpenStack;

Το OpenStack είναι σύνολο από εργαλεία λογισμικού για την οικοδόμηση και τη διαχείριση πλατφόρμας cloud computing για τα δημόσια και ιδιωτικά σύννεφα αντιστοίχως. Κάποιες από τις μεγαλύτερες εταιρείες ανάπτυξης λογισμικού και φιλοξενίας, καθώς και χιλιάδες μεμονωμένα μέλη της κοινότητας την υποστηρίζουν πάρα πολύ, πολλοί πιστεύουν ότι το OpenStack είναι το μέλλον του cloud computing. Το OpenStack διοικείται από το Ίδρυμα OpenStack, το οποίο είναι μη κερδοσκοπικός οργανισμός, που επιβλέπει τόσο την ανάπτυξη όσο και την κοινότητα οικοδόμησης γύρω από το έργο.

Το OpenStack είναι ένα ανοιχτού κώδικα έργο παροχής υποδομής ως υπηρεσία που ιδρύθηκε από τη Rackspace και τη NASA το 2010 και τώρα έχει πάνω από σαράντα μέλη. Επιτρέπει στους χρήστες να αναπτύξουν εικονικές μηχανές και να χειρίζονται διάφορες εργασίες για τη διαχείριση ενός περιβάλλοντος “cloud on the fly”. Έχει αυξηθεί, κάτι που σημαίνει ότι τα καθήκοντα που επωφελούνται από το τρέξιμο παράλληλα μπορεί να εξυπηρετήσει εύκολα περισσότερους είτε λιγότερους χρήστες σχετικά με την εκάστοτε περίπτωση που θέλουν να το χρησιμοποιήσουν αντίστοιχα. Για παράδειγμα, ένα κινητό τηλέφωνο με την αντίστοιχη εφαρμογή που χρειάζεται να επικοινωνήσει με έναν απομακρυσμένο διακομιστή μπορεί να είναι σε θέση να διαιρέσει το έργο της επικοινωνίας με κάθε χρήστη σε πολλές διαφορετικές περιπτώσεις, όλα επικοινωνούν μεταξύ τους αλλά και γίνεται κλιμάκωση γρήγορα και εύκολα, επομένως κερδίζει περισσότερους χρήστες.

Το σύννεφο είναι σχετικό με την παροχή υπολογιστών για τους τελικούς χρήστες σε ένα απομακρυσμένο περιβάλλον, όπου το πραγματικό λογισμικό που τρέχει ως υπηρεσία στους αξιόπιστους και επεκτάσιμους διακομιστές και όχι στον

υπολογιστή του κάθε τελικού χρήστη. Το cloud computing μπορεί να αναφέρεται σε πολλά διαφορετικά πράγματα, αλλά συνήθως ως συνομιλίες της βιομηχανίας σχετικά με την εκτέλεση διαφόρων ειδών «ως υπηρεσία» με σχετικό λογισμικό, πλατφόρμες και υποδομές. Το OpenStack εμπίπτει στη δεύτερη κατηγορία και θεωρείται υπηρεσία υποδομής (IaaS). Σημαίνει ότι η παροχή της υποδομής που OpenStack καθιστά εύκολο για τους χρήστες να προσθέσουν γρήγορα νέα στοιχεία, πάνω στα οποία μπορούν να τρέξουν άλλα συστατικά του νέφους. Συνήθως, η υποδομή τρέχει συνέχεια μια «πλατφόρμα» πάνω στην οποία ένας προγραμματιστής μπορεί να δημιουργήσει εφαρμογές λογισμικού που παρέχονται στους τελικούς χρήστες.


OpenStack End Users
OpenStack Dashboard
Horizon
Horizon Database
swift-proxy
account
container
object
account DB
container DB
object store
OpenStack Object Store
glance-api
glance-registry
glance database
OpenStack Image Service
nova-api (OS, EC2, Admin)
nova-compute
nova-console
nova-cert/ objectstore
libvirt, XenAPI, etc.
hypervisor
nova database
Queue
nova-consoleauth
nova-volume
nova-network
nova-scheduler
volume provider (iSCSI, etc)
network provider
OpenStack Compute
cinder-api
cinder-volume
cinder database
cinder-scheduler
OpenStack Block Storage Service
quantum-server
quantum agent(s)
Queue
quantum plugin(s)
quantum database
OpenStack Network Service
keystone (service & admin APIs)
token backend (kvs, memcache, etc.)
catalog backend (kvs, sql, etc.)
policy backend (rules, custom)
identity backend (kvs, pam, sql, ldap, etc.)
OpenStack Identity Service
HTTP(S)
OpenStack Object API
OpenStack Identity API
OpenStack Image API
OpenStack Compute API
Amazon Web Services EC2 API
VNC/VMRC
OpenStack Block Storage API
OpenStack Network API
OpenStack Compute API / Admin API
AMQP
http://ken.pepple.info

Εικόνα 4: Structure of OpenStack

3.3.2. Αρχιτεκτονική της OpenStack

Το OpenStack αποτελείται από πολλά διαφορετικά κινούμενα μέρη. Εξαιτίας της ανοικτής φύσης της, ο καθένας μπορεί να προσθέσει επιπλέον συστατικά για να βοηθήσει είτε να καλύψει ανάγκες στο OpenStack. Η κοινότητα του OpenStack σε συνεργασία εντόπισε εννέα βασικά συστατικά που αποτελούν μέρος του «πυρήνα» της OpenStack, τα οποία διαχωρίζονται ως μέρος οποιουδήποτε συστήματος OpenStack και επίσημα συντηρούνται από την κοινότητα της OpenStack.

- **Nova**:

Είναι η βασική υπολογιστική μηχανή πίσω από το OpenStack. Χρησιμοποιείται για την ανάπτυξη και τη διαχείριση μεγάλου όγκου εικονικών μηχανών και για να χειριστεί τον υπολογισμό των καθηκόντων.

- **Swift**:

Είναι σύστημα αποθήκευσης για αντικείμενα και αρχεία. Αντί της παραδοσιακής ιδέας να αναφέρονται σε αρχεία από τη θέση τους σε μια μονάδα δίσκου, οι προγραμματιστές μπορούν αντί να αναφέρονται σε ένα μοναδικό αναγνωριστικό που αναφέρεται στο αρχείο είτε κομμάτι των πληροφοριών και αφήνουμε την OpenStack να αποφασίσει πού θα αποθηκεύσουμε αυτές τις πληροφορίες. Το γεγονός αυτό κάνει την κλιμάκωση εύκολη, εφόσον οι προγραμματιστές δεν έχουν την ανησυχία σχετικά με την χωρητικότητα σε ένα ενιαίο σύστημα πίσω από το λογισμικό. Ακόμη επιτρέπει το σύστημα, όχι τον κύριο του έργου, να αναλάβουν την κατανομή των δεδομένων για να υποστηρίζονται και διατηρούνται σε περίπτωση αποτυχίας της μηχανής είτε του δικτύου.

- **Νετρονίων:**

Παρέχει τη δυνατότητα δικτύωσης για OpenStack. Βοηθά στη διασφάλιση ότι όλα τα συστατικά μιας εγκατάστασης OpenStack μπορούν να επικοινωνούν μεταξύ τους γρήγορα και αποτελεσματικά.

- **Horizon**:

Είναι το ταμπλό πίσω από το OpenStack. Είναι το μόνο γραφικό περιβάλλον το οποίο διαθέτει το OpenStack, για τους χρήστες που θέλουν να δοκιμάσουν το OpenStack, είναι το πρώτο στοιχείο που πραγματικά έχει τη δυνατότητα κάποιος χρήστης να «δει». Οι προγραμματιστές μπορούν να έχουν πρόσβαση σε όλα τα στοιχεία της OpenStack μεμονωμένα μέσω μιας διεπαφής προγραμματισμού εφαρμογών (API), αλλά το ταμπλό παρέχει σύστημα για διαχειριστές που θέλουν απλώς να έχουν μια άποψη για το πώς χρησιμοποιείται το σύννεφο, και να το διαχειριστεί όπως απαιτείται.

- **Keystone**:

Παρέχει υπηρεσίες ταυτότητας για την OpenStack. Είναι βασικά κεντρικός κατάλογος όλων των χρηστών του OpenStack σύννεφου, που χαρτογραφήθηκαν εναντίον όλων των υπηρεσιών που παρέχονται από το σύννεφο και που έχουν την άδεια να το χρησιμοποιήσουν. Παρέχει διάφορα μέσα πρόσβασης, που σημαίνει ότι οι προγραμματιστές μπορούν εύκολα να χαρτογραφήσουν τις υπάρχουσες μεθόδους πρόσβασης των χρηστών τους ενάντια του Keystone.

- **Ceilometer**:

Παρέχει υπηρεσίες τηλεμετρίας, που επιτρέπουν στο σύννεφο την παροχή υπηρεσιών τιμολόγησης σε μεμονωμένους χρήστες του cloud. Διατηρεί επίσης μια επαληθεύσιμη μέτρηση της χρήσης του συστήματος του κάθε χρήστη καθενός από τα διάφορα στοιχεία ενός νέφους OpenStack.

Η θερμότητα είναι το στοιχείο ενορχήστρωση του OpenStack, η οποία επιτρέπει στους προγραμματιστές να αποθηκεύσουν τις απαιτήσεις της εφαρμογής σύννεφου σε ένα αρχείο που ορίζει τι είναι απαραίτητο για τη συγκεκριμένη εφαρμογή πόρων. Με αυτόν τον τρόπο, βοηθά να διαχειριστούμε την υποδομή που απαιτείται για μια υπηρεσία cloud για να λειτουργήσει.

3.4.Cloud Stack

Το Apache Cloud Stack είναι μια φόρμα διαχείρισης cloud με ανοιχτό κώδικα για τη παροχή υπηρεσιών Infrastructure-as-a-Service (IaaS) σε περιβάλλον υπολογιστικού νέφους. Χρησιμοποιεί υπάρχουσες hypervisors, όπως KVM, VMware ESXi και XenServer / XCP για εικονοποίηση. Εκτός από το δικό του API, το Cloud Stack υποστηρίζει επίσης την Amazon Web Services API (AWS) και τη Computing Interface Open Cloud από το Grid Forum Open. Το Cloud Stack αναπτύσσεται για να βοηθά τους διαχειριζόμενους πάροχους υπηρεσιών και τα τμήματα πληροφορικής των επιχειρήσεων να δημιουργούν και να λειτουργούν δημόσιο, ιδιωτικό σύννεφο είτε υβριδικά σύννεφα με δυνατότητες ισοδύναμες με το Amazon Elastic Compute Cloud (Amazon EC2).

Το Cloud Stack αναπτύχθηκε αρχικά από τη Cloud.com , παλαιότερα γνωστή ως VMOps. Το Μάιο του 2010, η Cloud.com κυκλοφόρησε περισσότερα κομμάτια Cloud Stack ως ελεύθερο λογισμικό υπό την άδεια GNU General Public License, έκδοση 3 (GPLv3) Η Cloud.com και η Citrix υποστήριξε το Open Stack ένα διαφορετικό Apache με άδεια χρήσης cloud computing, το οποίο ανακοίνωσε τον Ιουλιο του 2010 σχετικά.

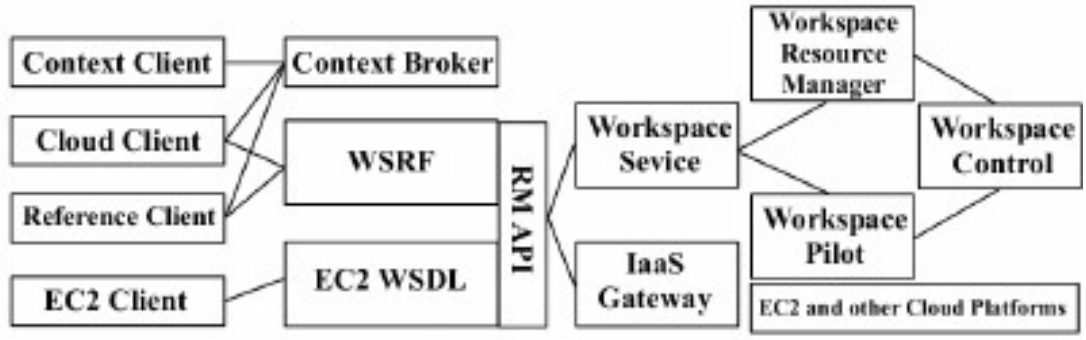
Η Citrix εξαγόρασε τη Cloud.com και το λογισμικό Cloud Stack έγινε διαθέσιμο υπό την άδεια της Apache Software . Το Cloud Stack, το οποίο αναπτύχτηκε από τη Citrix το 2011 και μετατράπηκε στο Apache Software Foundation το 2012. Η ανάπτυξη τώρα διέπεται από το ApacheFoundation με το κωδικό που διατίθεται με την άδεια Apache 2.0.

3.5. Eucalyptus Cloud

3.5.1. Τι είναι το Eucalyptus Cloud

Το Eucalyptus Cloud ήταν μια από τις πρώτες ανοιχτού τύπου εφαρμογές που επικεντρώθηκε στην δημιουργία των IaaS σύννεφων. Αποτελεί ακρωνύμιο του “Elastic Utility Computing Architecture for Linking your Programs To Useful Systems”. Είναι λογισμικό για την υλοποίηση ιδιωτικών συννέφων σε σύμπλεγμα υπολογιστών. Δημιουργήθηκε έτσι ώστε να παρέχει μια εφαρμογή ανοιχτού κώδικα (opensource) όμοια σε λειτουργία όπως το Amazon Web Services API. Έτσι οι

χρήστες μπορούν να αλληλεπιδρούν με το Eucalyptus cloud χρησιμοποιώντας τα ίδια εργαλεία που χρησιμοποιούν ώστε να έχουν πρόσβαση με αυτά στο Amazon EC2. Με το Eucalyptus Cloud μπορούν να δημιουργηθούν ιδιωτικά εσωτερικά και υβριδικά σύννεφα. Παρέχονται λειτουργίες για τη χρήση πόρων του εσωτερικού σύννεφου, όσο και των πόρων δημοσίου σύννεφου στην περίπτωση υβριδικού σύννεφου. Αν και για τη διαχείριση των πόρων του παρέχει δικό του σύνολο εργαλείων, υλοποιεί ένα API συμβατό με αυτό της Amazon επιτρέποντας τη διασυνεργασία αυτού με υπάρχοντα εργαλεία και υπηρεσίες της Amazons EC2.



Εικόνα 5: Structure of Eucalyptus Cloud

Βασικά Χαρακτηριστικά του Eucalyptus Cloud είναι:

Η ασφαλή ενδοεπικοινωνία με χρήση ασφαλών SOAP και Web υπηρεσιών, οι ομάδες ασφαλείας και ElasticsIPs, η διαχείριση ομάδων και χρηστών, η υποστήριξη για Linux και Windows Virtual Machines και η συμβατότητα με τα API της Amazon EC2.

3.5.2. Αρχιτεκτονική του Eucalyptus

Η αρχιτεκτονική του Eucalyptus περιλαμβάνει 5 βασικά συστατικά :

Cluster Controller (CC)
Cloud Controller (CLC)
Storage Controller (SC)
Node Controller (NC)
Walrus

Κάθε ένα από αυτά τα χαρακτηριστικά διαθέτει το δικό του web interface (διεπαφή ιστού) και είναι υλοποιημένο ως αυτόνομο web service (υπηρεσία ιστού). Παρέχοντας δύο βασικά πλεονεκτήματα. Αρχικά, κάθε συστατικό παρέχει τη λειτουργικότητά του μέσω από ένα API ανεξάρτητο από τη γλώσσα προγραμματισμού. Έπειτα ένα άλλο πλεονέκτημα είναι ότι αξιοποιούνται γνωστές και δεδομένες τεχνολογίες ασφαλείας των υπηρεσιών ιστού, για την ασφαλή επικοινωνία μεταξύ των επιμέρους συστατικών.

3.5.3. Συστατικά του Eucalyptus

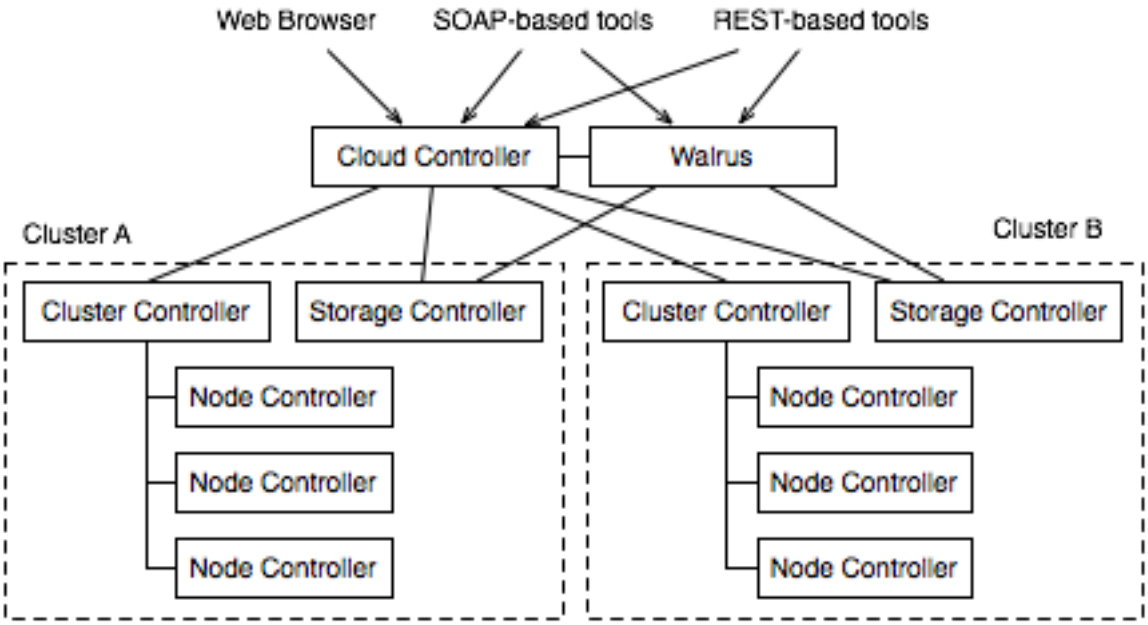
- **ClusterController(CC)**:Δίνει αναφορά για τους πόρους του συμπλέγματος στον CloudController και αναλαμβάνει τη διαχείριση της κίνησης στην περίπτωση της χρήσης εικονικού δικτύου στις εικονικές μηχανές. Είναι ένα κομμάτι το οποίο παίζει το ρόλο του διαμεσολαβητή μεταξύ του CloudController και των NodeControllers.

- **CloudController (CLC) :** Είναι το συστατικό που είναι υπεύθυνο για την έκθεση και διαχείριση των πόρων. Διαθέτει EC2, web interface (διεπαφή ιστού) καθώς και συμβατό API.
- **StorageController (SC):** Έχει τη δυνατότητα να δημιουργήσει στιγμιότυπα από συγκεκριμένες χρονικές στιγμές των δίσκων, το οποίο μπορεί να χρησιμοποιηθεί και από άλλη εικονική μηχανή. Τέλος, παρέχει υπηρεσίες αποθηκευτικού χώρου επιπέδου bock, δημιουργεί και διαχειρίζεται εικονικούς δίσκους , οι οποίοι χρησιμοποιούν εικονικές μηχανές.

- **Node Controller (NC):** Είναι τα μηχανήματα με virtualization extensions (επεκτάσεις εικονοποίησης) στους επεξεργαστές, βάση των οποίων τρέχουν οι επιβλέποντες παρακολουθούν την εκτέλεση των Virtual Machines (εικονικών μηχανών) και είναι υπεύθυνοι για την εκκίνηση, την εκτέλεση και τον τερματισμό τους.

- **Walrus:** Χρησιμοποιείται για την αποθήκευση των εικόνων των λειτουργικών συστημάτων που μπορούν να τρέξουν οποιαδήποτε στιγμή στο σύννεφο. Είναι συστατικό για την υλοποίηση του αποθηκευτικού χώρου συμβατό με το S3

(Simple Storage Service) της Amazon, παρέχοντας μηχανισμό μόνιμης αποθήκευσης.



Εικόνα 6: Architecture of Eucalyptus Cloud

Συμπεράσματα

Το cloud computing έχει ιδιαίτερη ανάπτυξη η οποία υποδηλώνει να έχει εκτεταμένες συνέπειες για τα συστήματα και τα δίκτυα υπηρεσιών και άλλων οργανισμών. Δίνει ιδιαίτερη σημασία στο κόστος και στην απόδοση των οφελών του δημοσίου cloud computing, παρόλα αυτά, έχει τη τάση να καλύπτει κάποια από τα βασικά προβλήματα ασφάλειας και ιδιωτικότητας, τα οποία αντιμετωπίζουν διάφορες υπηρεσίες και άλλοι οργανισμοί στα υπολογιστικά περιβάλλοντα. Κάποια από τα χαρακτηριστικά που κάνουν το cloud computing ελκυστικό μπορούν επίσης να αντικρούονται με την παραδοσιακή ασφάλεια, τα παραδοσιακά μοντέλα και τους παραδοσιακούς ελέγχους. Ποικίλα κρίσιμα κομμάτια της τεχνολογίας, όπως η λύση για την ομοσπονδιακή εμπιστοσύνη, δεν έχουν υλοποιηθεί πλήρως, με αποτέλεσμα να επηρεάζει την επιτυχή ανάπτυξη του cloud computing. Ο καθορισμός της ασφάλειας σύνθετων συστημάτων ηλεκτρονικών υπολογιστών είναι ακόμη ένα μακροχρόνιο θέμα που αφορά τους υπολογιστές και το cloud computing ειδικότερα. Η επίτευξη και υλοποίηση ιδιοτήτων μεγάλης αξιοπιστίας είναι ένας ψευδός στόχος της ασφάλειας των υπολογιστών για τους ερευνητές και τους επαγγελματίες και όπως φαίνεται είναι μια διαδικασία που προοδεύει στο cloud computing. Εν τούτοις, το δημόσιο cloud computing είναι ένα συναρπαστικό υπολογιστικό πλέγμα το οποίο οι οργανισμοί πρέπει να εφαρμόσουν ώς μέρος της τεχνολογίας των πληροφοριών τους.

Αυτός που δίνει αναφορά για την ασφάλεια και την προστασία της ιδιωτικής ζωής στα δημόσια cloud παραμένει να είναι ο οργανισμός. Οι διάφοροι οργανισμοί πρέπει να διασφαλίζουν ότι οποιαδήποτε λύση διαλέξει το δημόσιο cloud θα έχει διαμορφωθεί, αναπτυχθεί και τηρεί την ασφάλεια, την προστασία της ιδιωτικής ζωής και άλλες απαιτήσεις του οργανισμού. Τα εταιρικά δεδομένα πρέπει να προστατεύονται με τέτοιο τρόπο που να εφαρμόζεται με τις πολιτικές, είτε στο κέντρο πληροφορικής του οργανισμού είτε στο cloud. Ο οργανισμός πρέπει να εξασφαλίζει ότι η ασφάλεια και ο έλεγχος της ιδιωτικότητας θέτονται σωστά και λειτουργούν όπως προβλέπεται.

Η μετάβαση σε ένα εξωτερικό συνεργάτη δημοσίου cloud computing περιβάλλοντος είναι από διάφορες απόψεις μια άσκηση στη διαχείριση κινδύνου. Η διαχείριση κινδύνου σημαίνει τον προσδιορισμό και την αξιολόγηση του κινδύνου, και λαμβάνοντας τα μέτρα για τη μείωσή του σε ένα αποδεκτό επίπεδο.

Η εκτίμηση και η διαχείριση των κινδύνων σε ένα σύννεφο μπορεί να γίνει μια πρόκληση. Καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος, οι κίνδυνοι που εμφανίζονται πρέπει να εξισορροπούνται προσεκτικά σύμφωνα με τους ελέγχους ασφαλείας και ιδιωτικότητας που είναι διαθέσιμοι και με τα επιθυμητά οφέλη που προκύπτουν από την χρήση τους. Πάρα πολλοί έλεγχοι μπορεί να είναι περίπλοκοι και όχι ιδιαίτερα αποτελεσματικοί, σε περίπτωση που τα οφέλη υπερτερούν του κόστους και των συναφών κινδύνων. Οι διάφορες υπηρεσίες και οι οργανισμοί θα πρέπει να εργαστούν για να διασφαλίσουν την κατάλληλη ισορροπία μεταξύ του αριθμού και της ισχύος των ελέγχων και των κινδύνων που σχετίζονται με λύσεις του cloud computing.

Όπως αντιλαμβανόμαστε, οι κίνδυνοι και τα πλεονεκτήματα που προσφέρει το cloud computing είναι σημαντικά. Το cloud είναι η εξέλιξη των σημερινών δικτύων και υποδηλώνει πολύ ιδιαίτερες αλλαγές, που θα μας βοηθήσουν. Κάποιοι ίσως να μη το εμπιστεύονται σε περίπτωση που το αναλύσουμε καλύτερα όμως έχει πάρα πολλά οφέλη. Στη πραγματικότητα δεν είναι υποδεέστερο από τη σημερινή κλασική δικτυακή τεχνολογία. Η μόνη διαφορά με τη κλασική προσέγγιση δικτύων και ασφάλειας, είναι ότι θα προσφέρει νέες προκλήσεις που πρέπει να λυθούν. Με την εξάπλωση της τεχνολογίας θα επιβιώσουν οι πάροχοι που έχουν βοηθήσει τον χρήστη και τον έχουν διασφαλίσει όσο το δυνατόν καλύτερα. Το cloud μπορεί να μη θεωρείται ακόμα απόλυτα ασφαλές. Όσο όμως περνάει ο χρόνος, είναι πιθανό να αρθούν όλες οι επιφυλάξεις και τελικά το cloud computing να αποδειχθεί η πιο ασφαλής πλατφόρμα λειτουργίας των πληροφοριακών υποδομών μιας επιχείρησης είτε ενός οργανισμού.

Βιβλιογραφία:

NIST (National Institute of Standards and Technology) Guidelines on Security and Privacy in Public Cloud Computing, IT Professional.security

Cloud security and privacy, Above the clouds(A Berkeley View Of Cloud Computing Electrical engineering and Computer Sciences University of California at Berkeley

“Amazon: Hey Spammers, Get Off My Cloud!” reported in The Washington Post, July 1, 2008.

Likan Patra (2013), (http://www.optenet.com/enus/solutions-saas-providers.asp)

(http://rightyaleft.com/generaltalk/what-is-iaas-paas-saas-in-cloud-computing/)

Suhail (2012) (http://talkcloudcomputing.com/reasons-why-private-cloud-is-a-preferable-option/)

ArmediaBlog(2012)(http://www.armedia.com/blog/2012/03/federal-cloud-computing-challenges-part-1- cloud-deployment-models/)

TargetTech(2017)(http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud)

Eucalyptus 4.0.2 User Console Guide

https://www.eucalyptus.com/docs/eucalyptus.4.0.2/console-guide-4.0.2.pdf

Eucalyptus 3, Design Build and Manage – Eucalyptus University

GitHub2017https://github.com/eucalyptus/documentation/tree/master/content/en_us/training/XML%20Files/0-04CompleteDBMBook

Overview of AWS IAM Policies

AWS Identity and Access Management

http://docs .aws.amazon.com/IAM/latest/UserGuide/PoliciesOverview.html

Eucalyptus cloud Features

https://www.eucalyptus.com/eucalyptus-cloud/iaas/features

https://www.eucalyptus.com/sites/all/files/ds-eucalyptus-iaas.en.pdf

https://www.eucalyptus.com/docs/euca2ools/3.1.1/euca2ools-guide-3.1.1.pdf

https://eucalyptus.atlassian.net/wiki/display/EUCA/Eucalyptus+Reference+Architectures

http://www.enallaktikos.gr/ar28049el-ti-einai-to-cloud-computing-ypologistiko-nefos-kai-ti-i-eikonikopoiisi-virtualization.html

http://www.connect-line.gr/%CE%BD%CE%AD%CE%B1/%CF%84%CE%B1-%CE%BF%CF%86%CE%AD%CE%BB%CE%B7-%CF%84%CE%BF%CF%85-cloud-computing-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B9%CF%82-%CE%BC%CE%B9%CE%BA%CF%81%CE%AD%CF%82-%CE%B5%CF%80%CE%B9%CF%87%CE%B5%CE%B9%CF%81%CE%AE%CF%83%CE%B5%CE%B9%CF%82

https://prezi.com/nptzlsobjiux/cloud-/

https://www.openstack.org/

https://en.wikipedia.org/wiki/Nimbus_(cloud_computing)

HistoryofCloudComputing: https://scholar.google.gr/scholar?q=istoria+cloud+computing&hl=el&as_sdt=0&as_vis=1&oi=scholart&sa=X&ved=0ahUKEwjv4e2-oYbVAhXKK8AKHbJIDGQQgQMIJDAA

https://en.wikipedia.org/wiki/Eucalyptus_(software)