UNIVERISTY OF PIRAEUS
Department of Digital Systems

Postgraduate Program
«Security in Digital Systems»

SUBJECT THESIS

Security in Cloud Computing in e-Governance

Thomas Th. Katsaros

Supervisor: Dr. Konstantinos Lamprinoudakis
Assistant Professor

Piraeus, Feb 2012

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών
«Ασφάλεια Ψηφιακών Συστημάτων»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια σε συστήματα υπολογιστικού νέφους (cloud computing) στον τομέα της ηλεκτρονικής διακυβέρνησης

Θωμάς Θ. Κατσαρός

Υπεύθυνος Καθηγητής: Δρ. Κωνσταντίνος Λαμπρινουδάκης
Επίκουρος Καθηγητής Παν. Πειραιά

Πειραιάς, Φεβ 2012

ΕΥΧΑΡΙΣΤΙΕΣ

Χρέος έχω να ευχαριστήσω θερμά τον κ. Κωνσταντίνο Λαμπρινουδάκη, Επίκουρο Καθηγητή του Πανεπιστημίου Πειραιά πρώτον για την εμπιστοσύνη που μου έδειξε και την ανάθεση της παρούσας Διπλωματικής εργασίας και δεύτερον για την επίβλεψη του και την παροχή των ευρύτατων και πολύτιμων συμβουλών του τόσο πάνω στο θέμα της παρούσας εργασίας όσο και στο και γενικότερα στον τομέα της ασφάλειας των πληροφοριακών συστημάτων και δικτύων κατά την διάρκεια των σπουδών μου.

Επιπλέον θα πρέπει να ευχαριστήσω θερμά για τον πλούτο των γνώσεων σφαιρικά που μας καλλιέργησαν στο σύνολο τους οι καθηγητές του μεταπτυχιακού προγράμματος πάνω στα θέματα της ασφάλειας και της ιδιωτικότητας στην πληροφορική καθώς επίσης και για τις ευκαιρίες που μας έδωσαν τόσο μέσω του προγράμματος σπουδών όσο και από το θερινό σχολείο ασφάλειας που διοργανώθηκε στην Σάμο να γνωρίσουμε σπουδαίους διεθνείς καθηγητές του τομέα όσο και συμφοιτητές από ξένα πανεπιστήμια προκειμένου να διευρύνουμε τις γνώσεις μας και να ανταλλάξουμε τις ανησυχίες μας σε θέματα ασφάλειας.

Τέλος θα ήταν παράλειψη μου και αγνωμοσύνη αν δεν ευχαριστούσα την οικογένεια μου τόσο για την ηθική όσο και για την υλική υποστήριξη που μου παρείχαν όλο αυτό το διάστημα, μιας και χωρίς την στήριξη τους και την βοήθεια τους, η όλη μου προσπάθεια θα ήταν αδύνατη να καταστεί εφικτή.

ABSTRACT

In this project we study the assignment of eGovernment services in cloud computing. After a reference and examination of the cloud computing components we analyzed about security, reliability, attacks, countermeasures etc in these systems and how they returned, so that applications being safe, trustworthy, reliable and his data continue to be available.

Finally we study the transfer of an egoverment service “e-taxis” from traditional IT in cloud computing and what should be taken into account to ensure all the above about security, privacy, safety, confidenciality, reliability and integrity in e-government service and finally we think about what will happen both in Greece on the development of such services as for future scientific developments should be investigated immediately in order to optimize or solve imperfections in cloud computing systems.

Key words: Cloud computing, security, threats, attacks, privacy, e-goverment

ΠΕΡΙΛΗΨΗ

Στην παρούσα εργασία γίνεται λόγος και μελετάται η ανάθεση υπηρεσιών ηλεκτρονικής διακυβέρνησης στο υπολογιστικό νέφος. Αφού γίνει αναφορά και εξέταση των συστατικών του υπολογιστικού νέφους αναλύεται η ασφάλεια, η αξιοπιστία, οι επιθέσεις και το πώς αυτές μπορούν απωθηθούν από τέτοιου είδους συστήματα προκειμένου οι εφαρμογές να είναι ασφαλείς και έμπιστες ενώ παράλληλα να συνεχίσουν να είναι διαθέσιμες, τα δεδομένα να τους να μένουν ακέραια και τέλος να παραμένουν αξιόπιστες.

Τέλος γίνεται μελέτη μεταφοράς της υπηρεσίας του e-taxis από τις παραδοσιακές τεχνολογίες πληροφορικής στο υπολογιστικό νέφος και τι πρέπει να λαμβάνεται υπόψη προκειμένου να διασφαλιστούν όλα τα παραπάνω στον απαιτητικό τομέα της ηλεκτρονικής διακυβέρνησης ενώ τέλος λόγος γίνεται για το τι μέλλει γενέσθαι τόσο στον ελλαδικό χώρο σχετικά με την ανάπτυξη τέτοιου είδους υπηρεσιών όσο για τις μελλοντικές επιστημονικές εξελίξεις που πρέπει άμεσα να ερευνηθούν προκειμένου να βελτιστοποιηθούν ή να λυθούν ατέλειες.

Λέξεις κλειδιά: Υπολογιστικό νέφος, ασφάλεια, απειλές, επιθέσεις, ιδιωτικότητα, ηλεκτρονική διακυβέρνηση

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

1.1. Τι είναι τα συστήματα υπολογιστικού νέφους

Τα συστήματα υπολογιστικού νέφους (Cloud Computing Systems) αποτελούν την μεγαλύτερη εξέλιξη στο χώρο των Η/Υ . Τα κονδύλια που πρόκειται να αποδοθούν για τα CCS το 2012 ανέρχονται στα 42 δις εκατομμύρια.

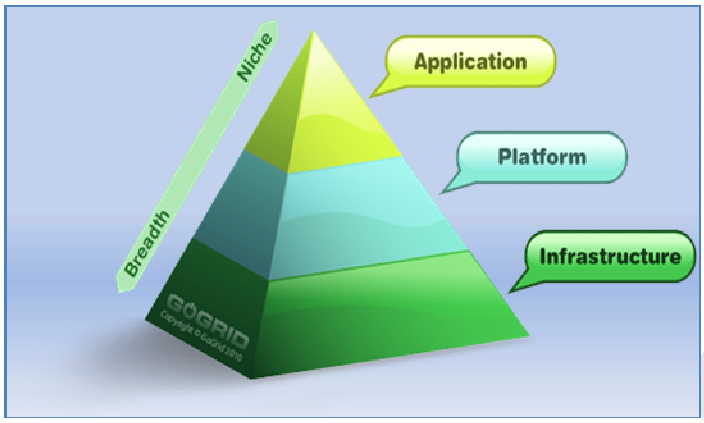
Πεπειραμένες εταιρείες στη παροχή νεφών διακρίνονται η Google, Amazon, Microsoft, Yahoo και Salesforce.com όπου χρησιμοποιούν συστήματα υπολογιστικού νέφους για την εξυπηρέτηση των πελατών τους αλλά και για την ίδια την υποδομή τους στο Διαδίκτυο.

Προϋποθέσεις των C.C.S. που τα κάνουν δημοφιλή:

- οι **κοινοί πόροι** (multitenancy),
- η τεράστια **επεκτασιμότητα** (scalability),
- η **ελαστικότητα** (elasticity),
- η **αυτο-τροφοδότηση** (self- provisioning) των πόρων.
- το **"instant hosting"** (cloud-hosting) που προσφέρεται.
- η εξοικονόμηση χρημάτων ("pay as you go on hardware or service").

Υπάρχουν τρία επίπεδα στην πυραμίδα του cloud computing.

Η βάση της πυραμίδας είναι η **υποδομή** (infastructure) το μεσαίο επίπεδο είναι η **πλατφόρμα** (platform) και η κορυφή της πυραμίδας που είναι η **εφαρμογή** (application). Οι εταιρείες παροχής νεφών προσεγγίζουν τα επίπεδα της πυραμίδας διαφορετικά ανάλογα με τις υπηρεσίες που προσφέρουν στους πελάτες τους κάθε μια ξεχωριστά.



Εικόνα 1 Οπτική αναπαράσταση C.C.S. στο μοντέλο πυραμίδας.

Η κύρια προϋπόθεση πίσω από την επιλογή μιας πυραμίδας είναι να σκεφτεί ο εκάστοτε πάροχος νεφών τη δημιουργία μιας διάρθρωσης, όπου κάθε στρώμα έχει χτιστεί πάνω από το επόμενο, ενδεχομένως, δημιουργώντας ένα ευρύτερο σύνολο. Ενώ κάθε επίπεδο μπορεί να είναι κάπως εξαρτημένο από το άλλο και συνδέονται άμεσα, στην πραγματικότητα δεν υπάρχει αλληλεξάρτηση μεταξύ τους. Στην πραγματικότητα, κάθε στρώμα μπορεί, και υπάρχει από μόνο του.

Μπορούν οι πάροχοι νεφών, για παράδειγμα, να κατασκευάζουν μια εφαρμογή πάνω από ένα σύννεφο πλατφόρμας ή Cloud υποδομής, αλλά η διαδικασία οικοδόμησης εργάζεται κυρίως με την προσέγγιση από κάτω προς τα πάνω (bottom - up view).

Το αντίστροφο δεν είναι δυνατό (π.χ., η δημιουργία μιας Cloud πλατφόρμας πάνω από μια εφαρμογή νέφους). Στο επίπεδο της υποδομής ξεκινάει να λαμβάνει δράση το hosting των C.C.S.

Το **hosting** είναι πολύ σημαντική αρχή στο CCS γιατί για παράδειγμα ας πούμε ότι έχουμε μια εταιρεία και έχουμε μια ιστοσελίδα στην οποία την διαφημίζουμε. Από την ιστοσελίδα υπάρχουν σχέσεις επικοινωνίας και συναλλαγών με τους πελάτες μας.

Με την διαφήμιση της εταιρείας ευρύτερα ας υποθέσουμε ότι ανά τακτά χρονικά διαστήματα πολλαπλασιάζονται με γοργούς ρυθμούς οι εγγεγραμμένοι χρήστες και συνάμα οι επισκέπτες του web site με αποτέλεσμα το υλικό να μην μπορεί να ανταποκριθεί στις προσδοκίες των απαιτήσεων δηλαδή στην ταυτόχρονη εξυπηρέτηση της πρόσβασης των μελών και των επισκεπτών στην ιστοσελίδα.

Ο εξυπηρετητής καθυστερεί υπερβολικά και πολλές φορές «πέφτει». Πριν μερικά χρόνια φιλοξενούσαμε τις ιστοσελίδες σε **εξυπηρετητές** όπου χρειαζόταν και χρόνος για να "ανεβούν" οι servers (όταν ήταν εκτός λειτουργίας) και να λειτουργούν ασταμάτητα ακόμα και όταν δεν υπήρχε φόρτος στο διαδίκτυο αλλά και χρήμα για την συνεχή αγορά υλικού στην περίπτωση που χρειαζόμασταν επιπρόσθετο χώρο για τις ανάγκες φιλοξενίας της ιστοσελίδας ή της διαδικτυακής εφαρμογής της επιχείρησης. Πληρώναμε ακόμα και όταν δεν χρησιμοποιούνταν αυτοί οι εξυπηρετητές.

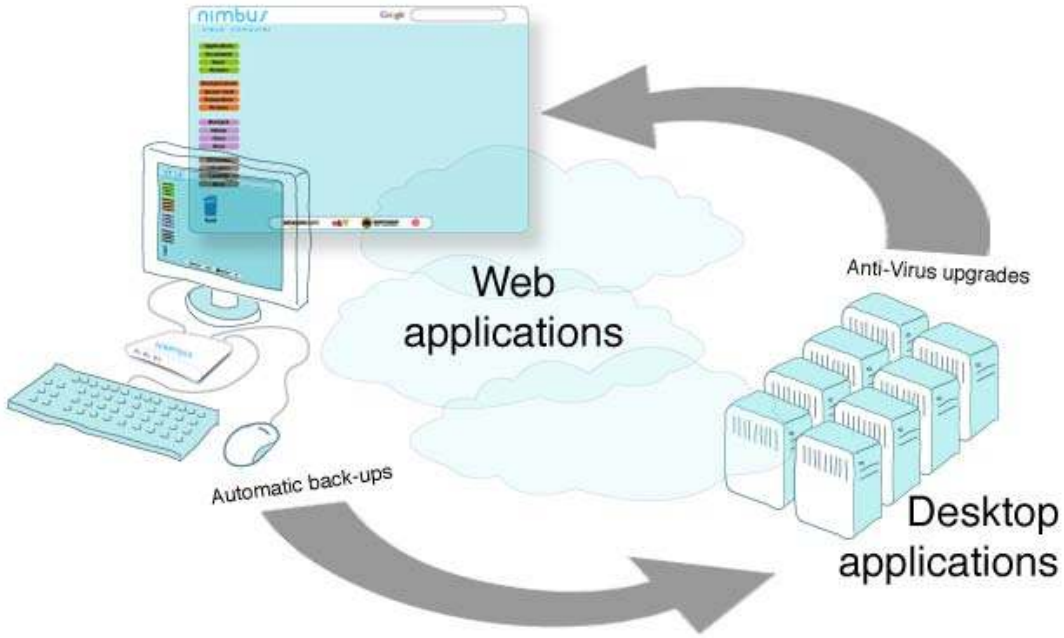
Μια καλύτερη επιλογή λοιπόν από το να έχουμε δυσαρεστημένους πελάτες από μηνύματα "server is down" ή "server is busy" και από το να αγοράζουμε συνεχώς υλικό εξοπλισμό για την κάλυψη των αυξημένων απαιτήσεων, ή ακόμα και για λόγους εξοικονόμησης ενέργειας η λύση είναι τα υπολογιστικά περιβάλλοντα νέφους.

Τοποθετούμε την ιστοσελίδα μας ή την διαδικτυακή εφαρμογή μας σε ένα cloud server όπως ακριβώς θα κάναμε με έναν αφιερωμένο εξυπηρετητή (dedicated server). Όταν αυξάνεται το πλήθος των επισκεπτών στο site δραματικά μπορούμε να ζητήσουμε κατ'απαίτηση πρόσθετη υπολογιστική ισχύ (όσο χρειαστούμε) ώστε να καλύψουμε τις ανάγκες από τον φόρτο των χρηστών άμεσα εύκολα και αποτελεσματικά ότι και αν είναι αυτό όπως υπολογιστική ισχύς, μνήμη, χώρος για όγκο δεδομένων κλπ.

Αυτό ονομάζεται "**cloud on demand**", και όταν για παράδειγμα μειωθεί η κίνηση από επισκέπτες ή μειωθεί η απαίτηση πόρων στην ιστοσελίδα-διαδικτυακή εφαρμογή μας κλπ, πλέον αποδεσμεύονται οι εξυπηρετητές του C.C.S. αυτόματα.

Η χρέωση στους πελάτες των παρόχων νεφών γίνεται είτε με κάποιου είδους συνδρομή είτε με βάση το μοντέλο "**pay as you go**" δηλ. σύμφωνα με τον χρόνο χρησιμοποίησης των υπηρεσιών ή του υλικού που προσφέρει το C.C.S.

Για παράδειγμα η χρέωση λειτουργεί ακριβώς όπως το ταξίμετρο. Ο μετρητής ξεκινάει την χρέωση όταν ο επιβάτης ξεκινήσει την διαδρομή. Χρεώνεται λιγότερο όταν το αμάξωμα σταματάει και όταν τελειώσει η προκαθορισμένη διαδρομή ο πελάτης πληρώνει το τελικό αντίτιμο στον οδηγό όπου και τελικά αποβιβάζεται.



Εικόνα 2 Γραφική αναπαράσταση εφαρμογών στο υπολογιστικό νέφος

Τα τελευταία δύο χρόνια οι πάροχοι λογισμικού αναπτύσσουν και στρέφουν όλο και περισσότερες εφαρμογές στο C.C.S.

1.2. Γιατί να χρησιμοποιήσω υπολογιστικά περιβάλλοντα νέφους

- **Λογισμικό ως συνδρομή (software as a subscription)**

Απομακρυσμένη διαχείριση της εφαρμογής του εκάστοτε χρήστη. Η εφαρμογή φιλοξενείται από τον ίδιο το πάροχο των υπηρεσιών νέφους και όχι πια στον υπολογιστή του χρήστη όπως συνηθίζονταν. Έτσι δεν χρειάζεται οι χρήστες να αγοράζουν ακριβά πακέτα λογισμικού όπως παλιά, καθώς μόνο με μια μικρή συνδρομή στον πάροχο χειρίζονται απομακρυσμένα full updated εφαρμογές.

Αυτό σημαίνει ότι όσοι χρήστες θέλουν να κάνουν διαχείριση μια εφαρμογής μόνο, αντί για να πληρώνουν παράδειγμα 150 € για την αγορά μιας full suite σειράς προγραμμάτων τώρα με το C.C.S. πληρώνουν 2.5 € το μήνα για την εφαρμογή μόνο που χειρίζονται (προσαρμόζοντας πάντα οι ίδιοι χρήστες την συνδρομή τους ή ακολουθώντας το μοντέλο “pay as you go”).

Ένα τέλειο τέτοιο παράδειγμα είναι η σειρά προγραμμάτων της Adobe Master Collection και του Microsoft Office suite.

Παράλληλα επιτυγχάνεται εξοικονόμηση των πόρων στα συστήματα των χρηστών με καλύτερη αξιοποίηση της υπολογιστικής τους ισχύς αφού λιγότερα προγράμματα είναι εγκατεστημένα στο υπολογιστικό σύστημα και «τρέχουν» σε αυτό.

- **Μειωμένη συντήρηση λογισμικού (Reduced Software Maintenance)**

Με την φιλοξενία τις εφαρμογής στο C.C.S. ελαχιστοποιούνται δραματικά οι διαδικασίες συντήρησης του συστήματος χρηστών. Αυτό οφείλεται στο γεγονός ότι κάθε πρόγραμμα έχει μια συνάρτηση ενημέρωσης που ψάχνει κάθε φορά για τις τελευταίες αλλαγές λογισμικού προκειμένου να επιδιορθωθούν κενά ασφαλείας που υπήρχαν, ή λανθασμένες λειτουργίες "bugs" του προγράμματος.
Όταν οι ενημερώσεις πραγματοποιούνται, δεν επηρεάζεται από τις αλλαγές το σύστημα του χρήστη αφού οι τροποποιήσεις γίνονται απομακρυσμένα στο C.C.S. χωρίς να επηρεάζεται η registrty του συστήματος του χρήστη.

Μια λοιπόν λογική ελάττωση των διαδικασιών συντήρησης του υπολογιστικού συστήματος είναι αναμενόμενη γι αυτό ακριβώς το λόγο.

- **Αυξημένη αξιοπιστία (Increased Reliability)**

Αυξημένη αξιοπιστία απορρέει από το γεγονός ότι το νέφος τρέχει σε συστήματα που είναι εξαιρετικά αξιόπιστα και παρέχουν περαιτέρω δυνατότητες. Αν ένας χρήστης αφιερώνει χρόνο στο να στήσει ένα εφεδρικό σύστημα ώστε να πραγματοποιεί διαδικασίες back-up σε σημαντικά αρχεία, διατρέχει τον κίνδυνο της απώλειας των δεδομένων του εγγυημένα. Τα νέφη παρέχουν την δυνατότητα απομακρυσμένης διαχείρισης και αποθήκευσης των αρχείων των χρηστών. Σε περίπτωση που αποτύχει ένα σύστημα του cloud να αποθηκεύσει-επανακτήσει δεδομένα (π.χ. λόγω σφάλματος υλικού) τότε ο πάροχος υπηρεσιών cloud μετατοπίζει το φορτίο σε άλλους servers και εμφανίζεται ένας εφεδρικός server στη θέση του αποτυχόντα αυτόματα και γρήγορα. Εάν συνέβαινε κάποια αντίστοιχη βλάβη σε σύστημα του χρήστη, αυτός θα κατέληγε σε μια χρονοβόρα και δαπανηρή διαδικασία τηλεφώνων τεχνικής υποστήριξης και επιδιορθώσεων λογισμικού με κίνδυνο πάντα την μόνιμη απώλεια δεδομένων από το σύστημα του.

- **Αυξημένη Επεκτασιμότητα (Increased Scalability)**

Η εξάντληση του φυσικού χώρου του σκληρού δίσκου είναι συχνό φαινόμενο και ειδικότερα όταν πραγματοποιούμε συχνά σε διαδικασίες back-up .

Το πρόβλημα αυτό λύνεται εφόσον μπορούμε να πληρώσουμε γι αυτό στους παρόχους υπηρεσιών νέφους. Με μια ειδοποίηση στον παροχέα για αίτημα πρόσθετων πόρων αμέσως ο πάροχος δεσμεύει πρόσθετο χώρο από το νέφος για την εξυπηρέτηση του αιτήματος του πελάτη του.

Το ίδιο αντίστοιχα συμβαίνει (εκτός από το υλικό) και για τις εφαρμογές των επιχειρήσεων που χειρίζονται πολύπλοκα δεδομένα και είναι επιτακτική η ανάγκη η τοποθέτηση πρόσθετης υπολογιστικής ισχύος.

Με το C.C.S. το μόνο που χρειάζεται είναι μια απλή ειδοποίηση από τον πελάτη στον πάροχο για πρόσθετους υπολογιστικούς πόρους καθώς η εφαρμογή της εταιρείας αδυνατεί να τρέξει στα ήδη υπάρχοντα συστήματα.

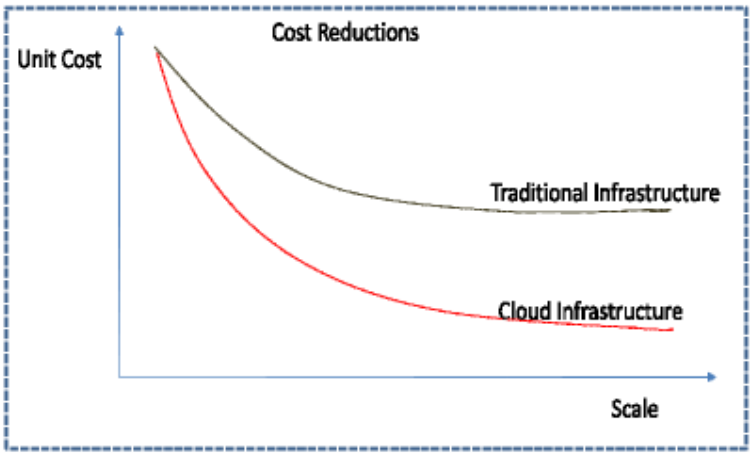
- **Ελάττωση Δαπανών (Cost Reduction)**

Οι συνολικές δαπάνες μειώνονται καθώς ο πάροχος προσφέρει υπηρεσίες στους πελάτες του με πολύ μικρό κόστος. Υπηρεσίες όπως αποθήκευσης διαχείρισης και συντήρησης.

Οι πελάτες πληρώνουν ελάχιστα χρήματα στο πάροχο με σκοπό την απομακρυσμένη αποθήκευση και διαχείριση των δεδομένων τους (φθηνότερο το κόστος δηλ. από το να αγόραζαν οι ίδιοι υπολογιστικά συστήματα).

Μειώνονται και οι δαπάνες λογισμικού καθώς ο διακανονισμός πληρωμής γι αυτού του είδους γίνεται με βάση το μοντέλο "pay ας you go" η συνδρομής.

Τέλος μειώνονται οι δαπάνες από την πρόσληψη προσωπικού συντήρησης στις επιχειρήσεις καθώς την συντήρηση σε επίπεδο λογισμικού και υλικού αναλαμβάνει ο ίδιος πάροχος του C.C.S.



Εικόνα 3 Κόστος υπολογιστικού νέφους σε σχέση με τις παραδοσιακές τεχνολογίες

- **Φιλικό προς το περιβάλλον (Environmentally Friendly)**

Ένα από τα μεγαλύτερα πλεονεκτήματα του C.C.S. είναι η αυξανόμενη μακροζωία και η χρήση του παλαιότερου υλικού που χρησιμοποιούνται από τα datacenters.

Αυτό ελαττώνει στη συνέχεια το ποσό ηλεκτρονικών αποβλήτων επειδή ο εξοπλισμός είναι παλιότερος και έχουμε αυξανόμενη χρήση αυτών των πόρων.

- **Σύγχρονες Τάσεις Πληροφορικής (Matches Current Computing Trends)**

Η εισαγωγή των netbooks στην αγορά έχει ξεπεράσει κατά πολύ τις πωλήσεις από τους υπολογιστές και τα lap-top με τους ισχυρότερους επεξεργαστές και τις εκτεταμένες ικανότητες προς τις λιγότερο ισχυρές και αποδοτικότερες πλατφόρμες. Έτσι αντιλαμβανόμαστε ότι οι χρήστες ψάχνουν τους υπολογιστές που ικανοποιούν τις ανάγκες τους και είναι προσιτοί σε τιμές. Η εμφάνιση του C.C.S. θα είναι σε θέση να ταιριάξει με αυτήν την τάση επειδή πολλά έξοδα επεξεργασίας εκτελούνται στους κεντρικούς υπολογιστές και όχι στον υπολογιστή του πελάτη.

Άρα η ανάγκη για έναν εξαιρετικά ισχυρό υπολογιστή χαμηλώνουν σε αντίθεση με παλιότερα. Δεδομένου ότι το C.C.S. ωριμάζει ενώ παράλληλα όλο και περισσότερος έλεγχος και επεξεργασία μετατοπίζεται στο νέφος, οι υπολογιστές θα απαιτήσουν τη λιγότερη δύναμη επεξεργασίας και θα έχουν τη βασική τους λειτουργία μόνο.

- **Φορητότητα / Προσβασιμότητα (Portability / Accessibility)**

Ένα από τα μεγαλύτερα πλεονεκτήματα C.C.S. είναι η διαθεσιμότητα των αρχείων και του λογισμικού οπουδήποτε υπάρχει σύνδεση στο internet.

Αυτό προσδίδει αυξανόμενη προσβασιμότητα και παραγωγικότητα για εκείνους που είναι στο δρόμο και απαιτούν πρόσβαση σε αρχεία και εφαρμογές καθώς επίσης και με ένα μεγάλο αριθμό εταιρειών που αναζητούν εναλλακτικές λύσεις για υπαλλήλους που εργάζονται στο γραφείο τους αλλά και για τον αυξανόμενο αριθμό των εργαζομένων που αποτελούν ένα κινητό εργατικό δυναμικό.

Η μείωση του κόστους εφαρμογής και τεχνικής υποστήριξης εύκολα θα συνεχίσει να υποστηρίζει αυτή την τάση προς μια κινητικότητα του παραπάνω εργατικού δυναμικού που θα αξιοποιήσει το συγκεκριμένο δίκτυο υπολογιστών.

- **Αποτελεσματική χρήση των υπολογιστικών πόρων (Efficient Use of Computer Resources)**

Η έλευση του virtualization παρέχει στις εταιρείες τρόπους για να χρησιμοποιούνται αποτελεσματικά οι υπολογιστικοί τους πόροι.

Με το virtualization πολλαπλές τεχνολογίες για εξυπηρετητές μπορούν να τρέξουν από έναν ενιαίο κεντρικό υπολογιστή και έτσι οι χρήστες δεν θα χρησιμοποιούν ξεχωριστούς εξυπηρετητές για διαφόρων ειδών εφαρμογές.

Για παράδειγμα σε ένα εξυπηρετητή του CCS εγκαθίστανται όλα τα προγράμματα και οι υπηρεσίες κανονικά. αλλά με τη μόνη διαφορά ότι όλα αυτά τα εγκατεστημένα προγράμματα και υπηρεσίες εκτελούνται με μεγαλύτερη επεξεργαστική ισχύ χωρίς να αναλώνονται οι πόροι των συστημάτων μας.

Όλοι οι clients είναι συνδεδεμένοι με το λογισμικό αυτό, εικονικά. Τα CCS είναι άμεσα ρητά συνδεδεμένα με την έννοια του **virtualization** γιατί οι υπηρεσίες τους παρέχονται εικονικά στους πελάτες.

Το paravirtualization ως έννοια εισάγει την ικανότητα στα CCS, οι πελάτες με διαφορετικά λειτουργικά συστήματα να είναι συνδεδεμένοι στον ίδιο διακομιστή με περισσότερη αποτελεσματικότητα.

Είναι καλύτερο από το virtualization γιατί όλοι οι χρήστες δεν είναι υποχρεωμένοι να εγκαταστήσουν virtual περιβάλλοντα με στόχο την διαχείριση υπηρεσιών και εφαρμογών.

Αυτή η στροφή προς το **Para/virtualization** υποστηρίζει την ανάπτυξη του cloud computing λόγω των αυξημένων δυνατοτήτων των διακομιστών.

Το cloud computing θα απλουστεύσει, επίσης το ρόλο στη διαχείριση των τεχνολογιών της πληροφορικής, εφόσον οι υπολογιστές θα είναι το μέσο ανάγνωσης υπηρεσιών και εφαρμογών και μόνο.

- **Λογισμικό Versionless (Versionless Software)**

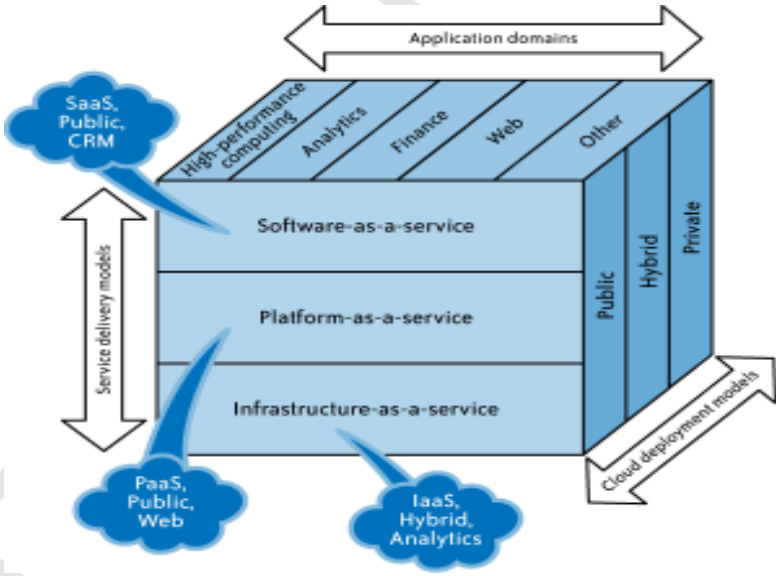
Γίνεται αναφορά στην εξάλειψη των έργων αναβάθμισης του λογισμικού.

Οι αλλαγές και οι ενημερώσεις του λογισμικού θα είναι συνεχής και έκδοση αριθμών θα είναι διαφανής για το χρήστη, ενώ ο χρήστης θα μπορεί να δει όλες τις πρόσθετες λειτουργίες. Θα δώσει επίσης στους χρήστες τη πρόσβαση στη νέα τεχνολογία νωρίς και συχνά, αντί αναγκάζοντάς τους να περιμένουν για την τελική έκδοση λογισμικού.

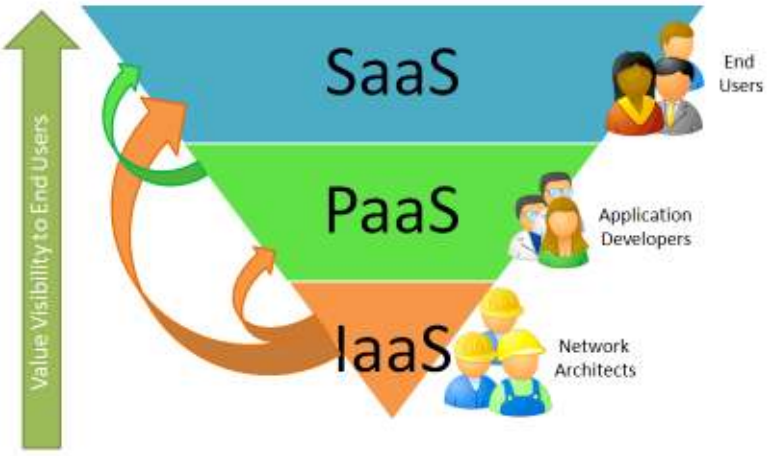
Η έννοια αυτή θα επιτρέψει στην επιχείρηση να παραμείνει στην αιχμή της τεχνολογίας και θα μειώσει το κόστος που συνδέεται με τις νέες εκδόσεις λογισμικού.

1.3. Το SPI μοντέλο στα CCS όπως αυτό καθορίζεται από τον NIST

Για την περιγραφή των υπηρεσιών που προσφέρονται στο C.C.S. το συμφωνηθέν ακρωνύμιο του ορίζεται ως "SPI" και αυτό λόγω των υπηρεσιών του κάθε επιπέδου της πυραμίδας που παρέχονται. Για παράδειγμα στο **υποδομής** επίπεδο **παρέχεται η υπηρεσία IaaS** (Infrastructure as a service), στο **πλατφόρμας επίπεδο η PaaS** (Platform as a service) και στο κυριότερο επίπεδο, **της εφαρμογής η SaaS** (Software as a service).



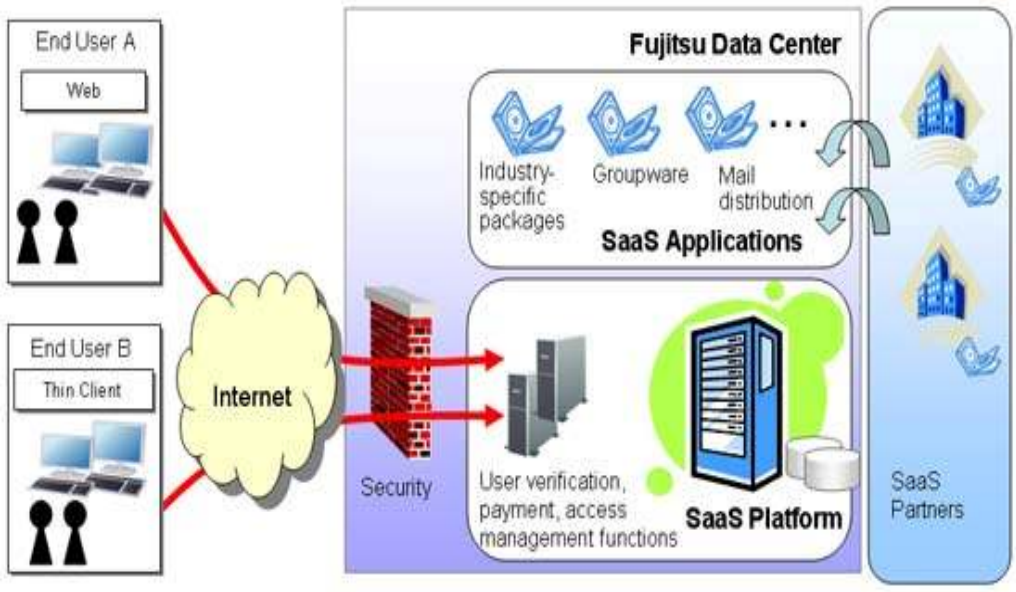
Εικόνα 4 Αναπαράσταση της σχέσης διαφόρων τύπων υπηρεσιών και χρήσης διαφόρων τύπων του C.C.S.



Εικόνα 5 Προβολή αξίας του νέφους με βάση τον τελικό χρήστη

1.3.1. Υπηρεσία Software as a Service (SaaS)

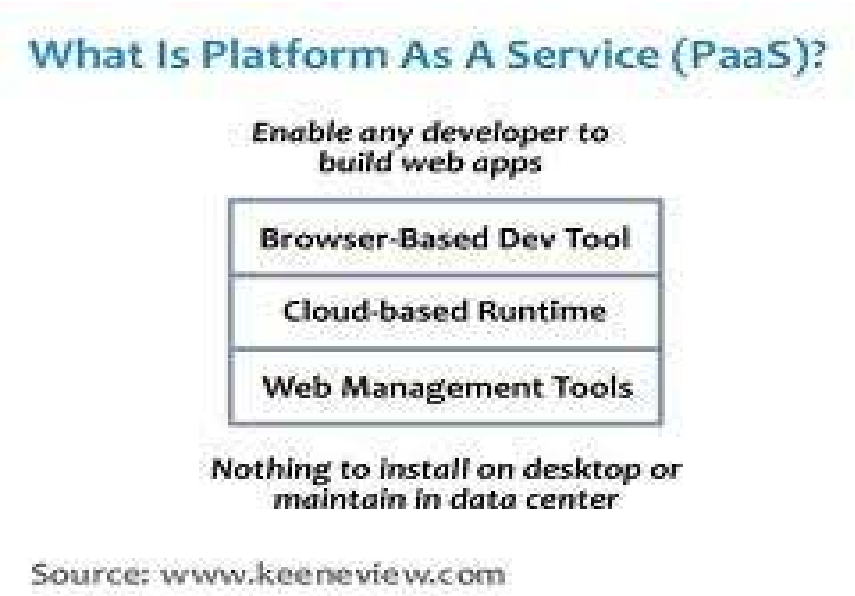
- Δίνει τη δυνατότητα στον οργανισμό να αναθέσει τη φιλοξενία και τη διαχείριση των εφαρμογών σε ένα τρίτο μέρος (προμηθευτής λογισμικού και πάροχος υπηρεσιών), ως μέσο για τη μείωση του κόστους των αδειών χρήσης λογισμικού εφαρμογών, servers, και άλλες υποδομές και το προσωπικό που απαιτείται για να φιλοξενήσει την εφαρμογή σε εσωτερικό επίπεδο.
- Επιτρέπει στους προμηθευτές λογισμικού τον έλεγχο και τον περιορισμό της χρήσης του λογισμικού, απαγορεύει την αντιγραφή και τη διανομή, και διευκολύνει τον έλεγχο όλων των παραγόμενων εκδόσεων του λογισμικού τους. Ένας τελικός χρήστης μπορεί να έχει πρόσβαση σε μια εφαρμογή SaaS μέσω ενός web browser. Μερικοί πωλητές SaaS παρέχουν δική τους διεπαφή που έχει σχεδιαστεί για να υποστηρίζει τα χαρακτηριστικά που είναι μοναδικά για τις εφαρμογές τους.
- Μια τυπική εγκατάσταση SaaS δεν απαιτεί κανένα υλικό και μπορεί να τρέξει πάνω από την υπάρχουσα υποδομή πρόσβασης στο Διαδίκτυο. Μερικές φορές οι αλλαγές στο firewall και στις ρυθμίσεις των πολιτικών ασφαλείας είναι υποχρεωτικές με στόχο να καταστεί δυνατή η εγκατάσταση και η λειτουργία της εφαρμογής SaaS.



Εικόνα 6 Τυπική υλοποίηση SaaS από παροχείς νεφών

1.3.2. Υπηρεσία Platform as a Service (PaaS)

- Σε μια πλατφόρμα, ο πωλητής προσφέρει ένα περιβάλλον ανάπτυξης για τους προγραμματιστές εφαρμογών, που αναπτύσσουν εφαρμογές και προσφέρουν τις υπηρεσίες αυτές μέσω της πλατφόρμας του παρόχου.
- Ο πάροχος αναπτύσσει συνήθως εργαλεία και πρότυπα για την ανάπτυξη και τους διακανονισμούς για τη διανομή και την πληρωμή της πλατφόρμας. Ο πάροχος λαμβάνει συνήθως μια πληρωμή για την παροχή της πλατφόρμας και των πωλήσεων και των υπηρεσιών διανομής.
  Αυτό επιτρέπει την ταχεία διάδοση των εφαρμογών λογισμικού, λόγω του χαμηλού κόστους της εισόδου στην πλατφόρμα.
- Η PaaS είναι μια παραλλαγή της SaaS την οποία το περιβάλλον ανάπτυξης προσφέρεται ως υπηρεσία. Οι προγραμματιστές χρησιμοποιούν δομικά στοιχεία (π.χ., προκαθορισμένα μπλοκ κώδικα) για τη δημιουργία δικών τους εφαρμογών.
- Με την PaaS, οι προγραμματιστές μπορούν να χτίσουν συχνά εφαρμογές web δεν απαιτείται εγκατάσταση οποιουδήποτε εργαλείου στον υπολογιστή τους και μπορούν να αναπτύξουν στη συνέχεια τις εφαρμογές αυτές χωρίς καμία εξειδικευμένη δεξιότητα διαχείρισης του συστήματός τους.



Εικόνα 7 Τυπική περιγραφή μοντέλου PaaS από παροχείς νεφών.

1.3.3. Υπηρεσία Infrastructure as a Service (IaaS)

- Ο πάροχος νεφών οφείλει να παραδίδει στο σύνολο της υποδομής του το υλικό για έναν πελάτη ώστε να τρέχει τις εφαρμογές του. Συχνά, αυτό συνεπάγεται τη στέγαση αφιερωμένου hardware από μεριάς του παρόχου, που έχει αγοράσει ή μισθώσει για τη συγκεκριμένη εφαρμογή.
- Το μοντέλο IAAS παρέχει επίσης την υποδομή για την εκτέλεση των εφαρμογών, αλλά η προσέγγιση στο cloud computing καθιστά δυνατή και την συνδρομητική παροχή.
- Ο πάροχος IAAS μπορεί να καλύψει την web-host εφαρμογή, ή μπορεί να επεκταθεί και σε άλλες υπηρεσίες (όπως την υποστήριξη εφαρμογής, ανάπτυξη εφαρμογών, καθώς και βελτιώσεις) και μπορεί να υποστηρίξει την πιο ολοκληρωμένη εξέλιξη στο χώρο των τεχνολογιών της πληροφορικής.
- Το μοντέλο IAAS έχει χρησιμότητα, κατά την οποία η βασική ιδέα είναι να προσφέρει υπηρεσίες πληροφορικής με τον ίδιο τρόπο όπως επιχειρήσεις κοινής ωφέλειας. Δηλαδή, πληρώνεται το ποσό της επεξεργαστικής ισχύς, του χώρου στο δίσκο, και των συνολικών πόρων που πραγματικά πάντα χρησιμοποιούνται.

Αναφερόμαστε στις υποδομές, συμπεριλαμβανομένων των φυσικών υπολογιστικών πόρων, την τοποθεσία, το διαμοιρασμό των πληροφοριών, κλιμάκωση, ασφάλεια, διαδικασίες backup.

Στο cloud computing, ο πάροχος έχει το πλήρη έλεγχο της υποδομής. Ωστόσο, ο πελάτης θέλει να έχει τον έλεγχο της γεωγραφικής θέσης των υποδομών και των τι τρέχει σε κάθε server.

Χαρακτηριστικά που περιλαμβάνονται σε ένα τυπικό μοντέλο IAAS:

- **Κλιμάκωση**

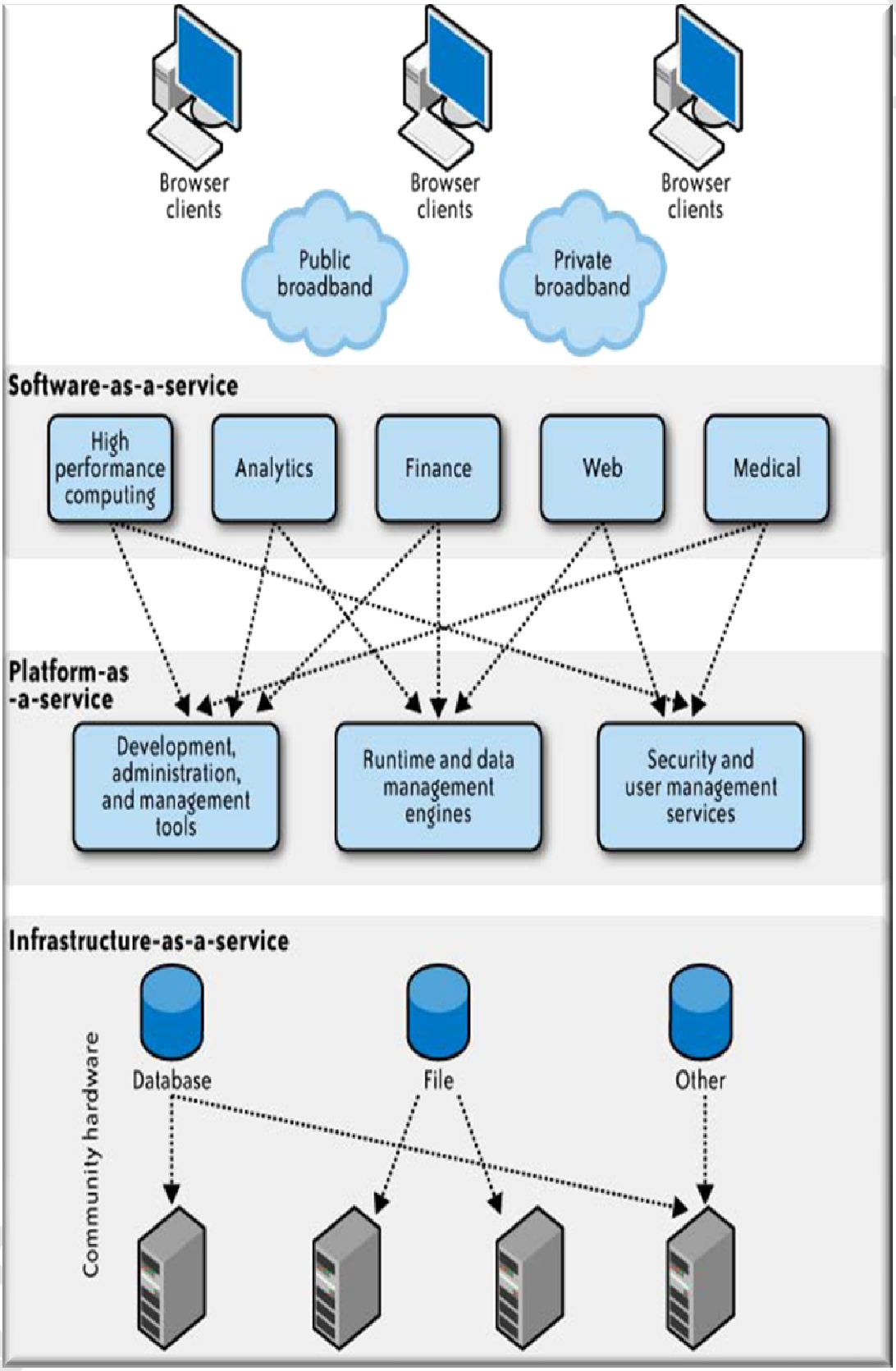
  Η ικανότητα της κλιμάκωσης στην υποδομή, όπως υπολογιστικούς πόρους, μνήμη και αποθηκευτικούς πόρους (σε σχεδόν πραγματικού χρόνου ταχύτητες) με βάση τις απαιτήσεις χρήσης πάντα.

- **"Pay as you go"**

  Η ικανότητα να αγοράσει το ακριβές ποσό των υποδομών που απαιτούνται σε κάθε συγκεκριμένη στιγμή τεχνολογίας και των πόρων.(ενοικίαση-παράδειγμα ταξίμετρο)

- **"Best-of-breed"**

  Πρόσβαση σε best-of-breed τεχνολογικών λύσεων και ανώτερη τεχνολογική εξελιξιμότητα.



➢

Εικόνα 8 Αρχιτεκτονικές στις αντίστοιχες υπηρεσίες των επιπέδων του S.P.I ¨

1.4. Μοντέλα ανάπτυξης νεφών στο CCS

Τα συστήματα υπολογιστικού νέφους μπορούν χωριστού σε τρείς μεγάλες κατηγορίες:

Δημόσια – Εξωτερικά CCS (Public Clouds).

Ιδιωτικά –Εσωτερικά CCS (Private Clouds).

Υβριδικά CCS (Hybrid Clouds).

Ο όρος σύννεφο είναι μια αλληγορία για το Διαδίκτυο και είναι μια απλοποιημένη αναπαράσταση του συγκροτήματος, από internetworked συσκευές και τις συνδέσεις που αποτελούν το Internet.

Τα ιδιωτικά και τα δημόσια σύννεφα είναι υποσύνολα του Διαδικτύου και ορίζονται με βάση της σχέσης τους με την επιχείρηση. Ακόμα τα ιδιωτικά και τα δημόσια σύννεφα μπορούν επίσης να αναφέρονται ως εσωτερικά ή εξωτερικά σύννεφα.

1.4.1. Δημόσια εξωτερικά CCS (Public clouds)

Δημόσια σύννεφα (ή εξωτερικά σύννεφα) καλούνται αυτά που περιγράφουν το cloud computing με την παραδοσιακή έννοια “mainstream”, όπου οι πόροι είναι δυναμικοί και τροφοδοτούνται με συγκεκριμένη διάταξη από το διαδίκτυο.

Τα δημόσια CCS λειτουργούν, και διοικούνται από έναν τρίτο προμηθευτή από ένα ή περισσότερα κέντρα δεδομένων. Η υπηρεσία παρέχεται σε πολλαπλούς πελάτες (το σύννεφο προσφέρεται για πολλαπλές μισθώσεις) σε μια κοινή υποδομή. Στα δημόσια cloud, η διαχείριση της λειτουργίας της ασφάλειας περνάει σε τρίτους πωλητές, οι οποίοι είναι αρμόδιοι για την δημόσια προσφορά των υπηρεσιών στο σύννεφο.

Ως εκ τούτου, ο πελάτης της δημόσιας προσφοράς υπηρεσιών νέφους έχει χαμηλό βαθμό του ελέγχου και της εποπτείας της φυσικής και λογικής των πτυχών ασφαλείας σε αντίθεση με ένα ιδιωτικό νέφος (private cloud).

Εικόνα 9 Δημόσια – Εξωτερικά C.C.S. και πάροχοι τέτοιων νεφών

1.4.2. Ιδιωτικά – εσωτερικά CCS (Private clouds)

Τα ιδιωτικά σύννεφα και τα εσωτερικά σύννεφα είναι όροι που χρησιμοποιούνται για να περιγράψουν τα νέφη υπολογίζοντας στις προσφορές των ιδιωτικών δικτύων. Αυτά τα προϊόντα-υπηρεσίες (virtualization και αυτοματοποίησης) αποτελούν οφέλη του νέφους χωρίς κινδύνους στις παγίδες, στην ασφάλεια δεδομένων, τη συνεργασία κυβερνήσεων, και τις ανησυχίες αξιοπιστίας. Οι οργανώσεις πρέπει να τα αγοράσουν, να τα χτίσουν, και να τα διαχειριστούν.

Ο οργανωτικός πελάτης για ένα ιδιωτικό σύννεφο είναι αρμόδιος για τη λειτουργία του ιδιωτικού νέφους του.

Τα ιδιωτικά σύννεφα διαφέρουν από τα δημόσια εξωτερικά σύννεφα στο ότι το δίκτυο, ο υπολογισμός, και η αποθήκευση της υποδομής που συνδέονται με τα ιδιωτικά νέφη είναι αφιερωμένα σε μια οργάνωση και δεν μοιράζονται με κανέναν

άλλο οργανισμό (δηλαδή, το σύννεφο είναι αφιερωμένο σε ένα μονό οργανωτικό ενοικιαστή).

Ως εκ τούτου, μια ποικιλία ιδιωτικών προτύπων νεφών έχουν εμφανιστεί:

- **Αφιερωμένα**

  Ιδιωτικά νέφη που φιλοξενούν πελάτες που τους ανήκει το κέντρο δεδομένων ή μια δυνατότητα συνεγκατάστασης, και λειτουργεί από το προσωπικό IT.

- **Κοινότητας**

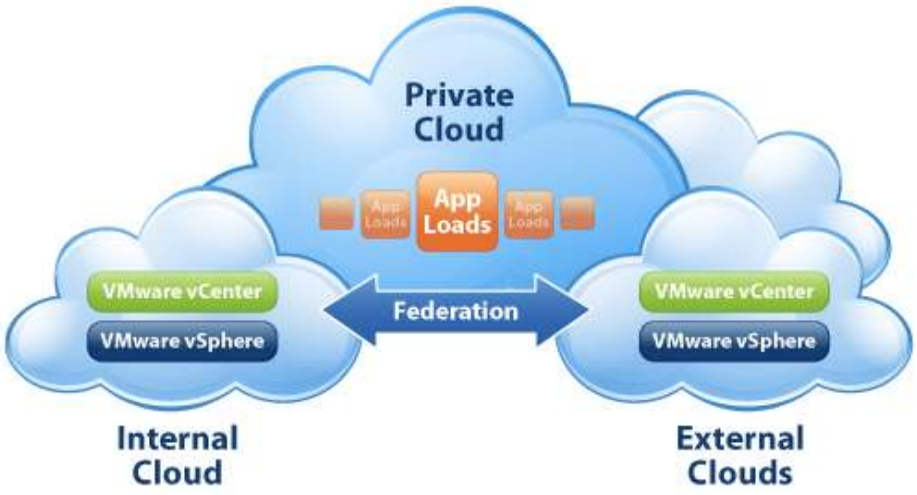
  Ιδιωτικά νέφη που βρίσκονται στις εγκαταστάσεις τρίτου. Η ιδιοκτησία, διαχείριση, και η λειτουργία γίνεται από έναν πωλητή-πάροχο ο οποίος δεσμεύεται από το πρότυπο SLA's (Service Level Agreement's) και συμβατικές ρήτρες για τη ασφάλεια και την τήρηση απαιτήσεων στα C.C.S.

- **Διαχείρισης**

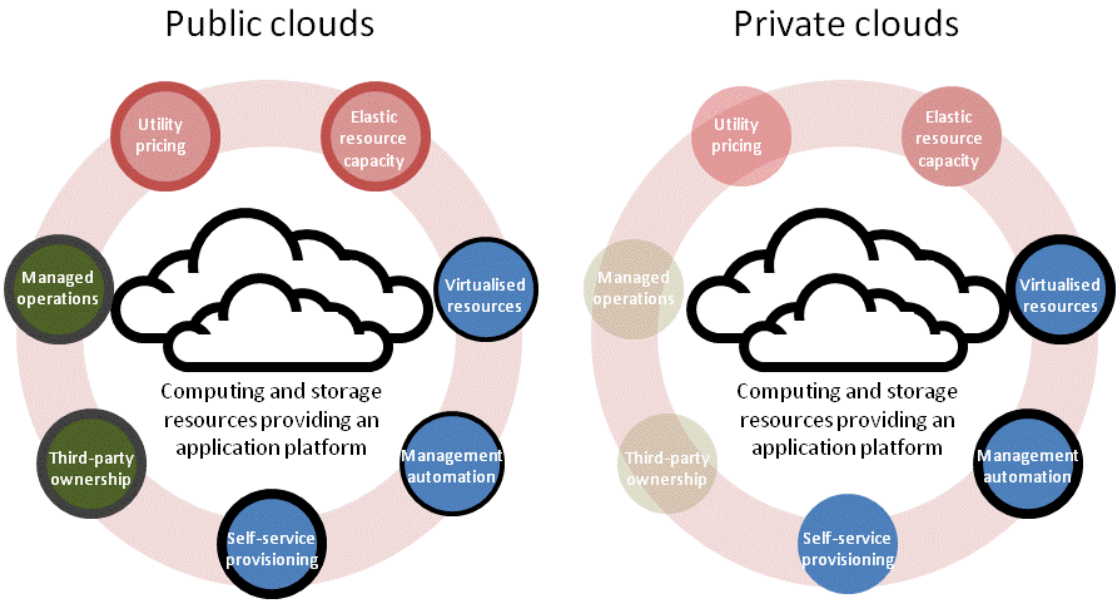
  Ιδιωτικές υποδομές cloud που ανήκουν σε πελάτη και διαχειρίζονται από έναν πωλητή.

Σημαντικό είναι πως τα ιδιωτικά νέφη πελάτη , θα πρέπει να έχουν υψηλό βαθμό ελέγχου και εποπτείας των φυσικών και λογικών πτυχών ασφάλειας της ιδιωτικής υποδομής cloud ,τόσο του hypervisor όσο και των hosted virtualized OS's (Operating System's).

Με αυτό τον υψηλό βαθμό ελέγχου και διαφάνειας, είναι ευκολότερο για έναν πελάτη να συμμορφώνεται με τις καθιερωμένες πολιτικές και κανονισμούς συμμόρφωσης σύμφωνα με τα εταιρικά πρότυπα ασφάλειας.



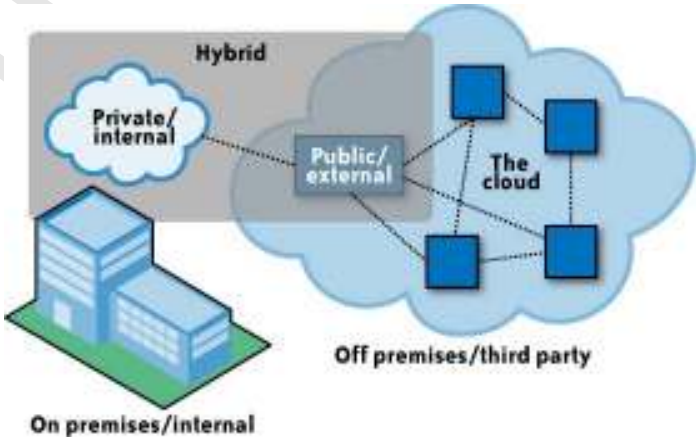
Εικόνα 10 Ιδιωτικό νέφος

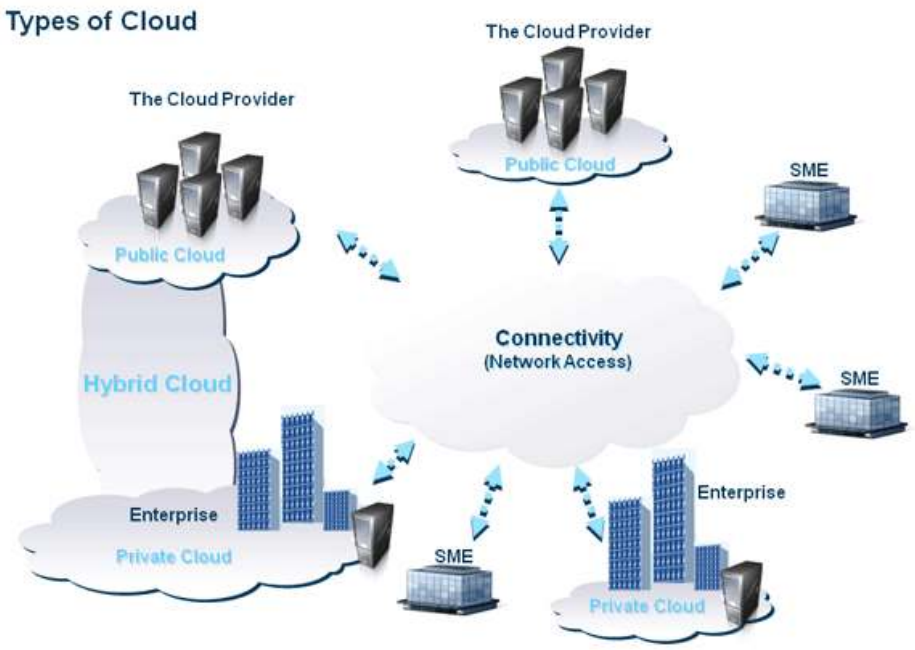


Εικόνα 11 Διαφορές δημόσιων και ιδιωτικών νεφών

1.4.3. Υβριδικά CCS (Hybrid clouds)

Ένα υβριδικό περιβάλλον νέφους που αποτελείται από πολλαπλούς εσωτερικούς ή εξωτερικούς παρόχους η συνδυασμό και των δύο όπου είναι δυνατή αξιοποίησή τους για τις οργανώσεις. Με ένα υβριδικό σύννεφο, οι εταιρείες μπορούν να τρέξουν μη βασικές εφαρμογές σε δημόσια cloud, διατηρώντας παράλληλα βασικές εφαρμογές και τα ευαίσθητα δεδομένα "in-house" στο ιδιωτικό νέφος.





Εικόνα 12 Υβριδικά CCS

1.4.4. Κριτήρια επιλογής παρόχου του νέφους

Οι προμηθευτές νεφών επενδύουν αρκετά στην εξασφάλιση της ασφάλειας στα νέφη τους με μεγάλη επιβάρυνση στο κόστος πάντα.

Η επιλογή παρόχου νεφών δεν πρέπει να γίνεται με βάση το χρηματικό όφελος μόνο σε μας. Υπάρχουν εταιρείες που ναι μεν παρέχουν υπηρεσίες με οικονομική επιβάρυνση στους πελάτες τους, προσφέρουν όμως με τη σειρά τους κρυπτογραφημένη αποθήκευση των δεδομένων των πελατών στο νέφος τους, έτσι ώστε να μην υπάρχει ανησυχία για το απόρρητο της πληροφορίας με τους πελάτες.

Άλλες εταιρείες προσφέρουν δωρεάν υπηρεσίες στους πελάτες τους από το διαφήμιση (advertisment) μόνο και συνήθως αυτές πιθανόν είναι που μαζεύουν τις πληροφορίες των χρηστών του CCS για εμπορικούς σκοπούς αποκομίζοντας χρηματικά κέρδη, κάνοντας τη χρήση του ίδιου του C.C.S. μη έμπιστη.

ΖΗΤΗΜΑΤΑ

Το αδιάβλητο της πληροφορίας είναι ένα από τα ζητήματα **κανονισμού και ασφάλειας** στα C.C.S. Πολλοί θεωρούν ότι τα C.C.S. είναι ασφαλή περιβάλλοντα εν αντιθέσει με άλλους που πιστεύουν το αντίθετο.

2. ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΗΣ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Σε αυτό το κεφάλαιο θα μιλήσουμε για τις απειλές, τις προκλήσεις αλλά και τις οδηγίες που αφορούνε για την ενίσχυση της ασφάλειας τεχνολογικά στις υποδομές πληροφορικής στο δίκτυο στον φορέα φιλοξενίας της υπηρεσίας και τα διάφορα επίπεδα εφαρμογής. Αυτή είναι μια πρακτική που ακολουθούνε συνήθως οι πρακτικοί της ασφάλειας και τους είναι ιδιαιτέρως γνωστή. Θα μιλήσουμε για την ασφάλεια αυτής της υποδομής στο περιβάλλον και τα μοντέλα μεταφοράς της υπηρεσίας SPI (SaaS, PaaS και IaaS). Σ' αυτό το σημείο εδώ καλό είναι να αναφέρουμε ότι άνθρωποι που δεν είναι εξειδικευμένοι στο χώρο της ασφάλειας καλό είναι να μην συγχέουν και εξομοιώνουν στο ίδιο επίπεδο την ασφάλεια υποδομής με την ασφάλεια υποδομής σαν υπηρεσία (IaaS). Παρόλο που η ασφάλεια υποδομής έχει ιδιαίτερη σημασία για τους πελάτες της IaaS, παρόμοια έμφαση θα πρέπει να δοθεί και στα περιβάλλοντα PaaS & SaaS. Μια άλλη διάσταση είναι το επιχειρηματικό μοντέλο χρήσης ενός συστήματος υπολογιστικού νέφους (όπως πχ δημόσιο ιδιωτικό και υβριδικό) το οποίο πάλι με τη σειρά του είναι ανάλογο με το μοντέλο της υπηρεσίας αναφοράς μεταφοράς SPI που θα χρησιμοποιηθεί. Συνοπτικά δηλαδή τονίζουμε την σημασία των σημείων συζήτησης που ισχύουν για τα δημόσια και ιδιωτικά συστήματα υπολογιστικού νέφους. Όταν μιλάμε για δημόσια συστήματα νέφους η ασφάλεια υποδομών περιορίζεται στα επίπεδα υποδομής που προχωρούν πέρα από τον έλεγχο του οργανισμού και φτάνει στα χέρια των φορέων παροχής υπηρεσιών (πχ όταν η ευθύνη για την ασφάλεια της υποδομής μεταφέρεται στον παροχέα της υπηρεσίας του υπολογιστικού νέφους - CSP-cloud service provider – βασισμένο στο μοντέλο μεταφοράς SPI). Οι πληροφορίες σ' αυτό το κεφάλαιο λοιπόν είναι κρίσιμες για τους πελάτες προκειμένου να κατανοήσουν τι είδους ασφάλεια παρέχει ένας παροχέας CSP και τι είδους ασφάλεια είναι υποχρεωμένος να παρέχει ένας πελάτης (αυτός δηλαδή που έχει αναπτύξει μια υπηρεσία νέφους και την φιλοξενεί ένας παροχέας CSP).

2.1. Ασφάλεια υποδομής στο επίπεδο δικτύου

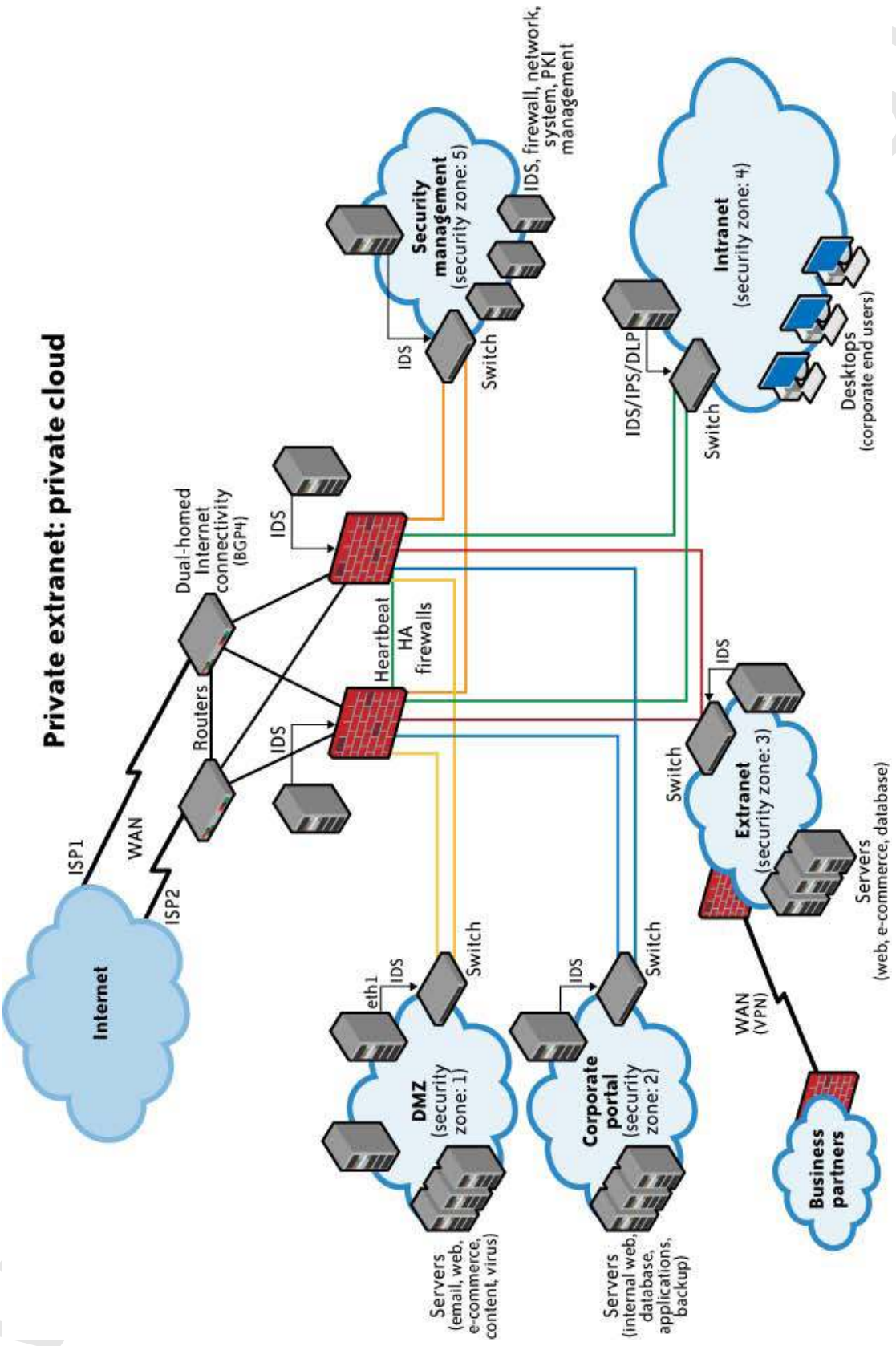
Όταν κοιτάμε στο επίπεδο δικτύου για την ασφάλεια υποδομής είναι σημαντικό να ξεχωρίζουμε και να διακρίνουμε τα μέρη μεταξύ του δημόσιου και ιδιωτικού

νέφους. Με τα ιδιωτικά νέφη δεν υπάρχουνε νέες επιθέσεις, ευπάθειες ή αλλαγές στην ανάλυση ρίσκου αυτής της τοπολογίας που πρέπει να εξετάσουμε. Ωστόσο αν αποφασίσουμε να χρησιμοποιήσουμε υπηρεσίες δημοσίου νέφους οι απαιτήσεις ασφάλειας θα απαιτήσουνε αλλαγές στην τοπολογία του δικτύου. Θα πρέπει να διευθυνσιοδοτήσουμε πως το ήδη υπάρχον δίκτυο αλληλεπιδρά με την δομή του παροχέα υπολογιστικού νέφους. Σ' αυτή την μελέτη περίπτωσης υπάρχουνε τέσσερεις σημαντικοί παράγοντες ρίσκου:

- Εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων του οργανισμού κατά την μεταφορά από και προς τον δημόσιο πάροχο.
- Εξασφάλιση ορθού ελέγχου πρόσβασης (αυθεντικόποιηση - πιστοποίηση, εξουσιοδότηση και παρακολούθηση για επαλήθευση - auditing) σε όλους τους πόρους χρησιμοποίησης νέφους στο δημόσιο πάροχο.
- Εξασφάλιση της διαθεσιμότητας διαδικτυακών πόρων του δημόσιου νέφους που χρησιμοποιεί ο οργανισμός ή έχουνε ανατεθεί στον οργανισμό από τον δημόσιο πάροχο.
- Αντικατάσταση του υπάρχοντος μοντέλου των ζωνών δικτύου με domain.

2.1.1. Ενίσχυση εμπιστευτικότητας & ακεραιότητας των δεδομένων

Κάποια δεδομένα που στο παρελθόν αποθηκεύονταν σε ένα ιδιωτικό δίκτυο πλέον εκτίθενται στο διαδίκτυο και σ' ένα διαμοιραζόμενο δίκτυο που ανήκει σ' ένα πάροχο υπολογιστικού νέφους, τρίτης διάστασης οντότητα. Ένα τέτοιο πρόβλημα ασφάλειας είναι και αυτό που παρουσιάστηκε στην εταιρεία Amazon Web Services (AWS) και αναφέρθηκε τον Δεκέμβριο του 2008. Σύμφωνα μ' αυτό σε μια δημοσίευση ενός ιστολογίου ο συγγραφέας έστειλε ένα ερώτημα (query) [aka REST] στην Amazon SimpleDB για το Amazon Elastic Compute Cloud (EC2) ή το Amazon Simple Queue Service (SQS) χρησιμοποιώντας το πρωτόκολλο HTTP. Με την χρησιμοποίηση όμως του HTTPS αντί του HTTP εξασφαλίζουμε το ρίσκο της ακεραιότητας και εδώ πλέον οι χρήστες χρησιμοποιώντας το HTTP κινδυνεύουν κατά την αποστολή δεδομένων τους να δεχτούνε αλλοίωση των διαφόρων στοιχείων τους χωρίς να το γνωρίζουν.



Εικόνα 13 Τεχνολογίες ενίσχυσης της ασφάλειας στο νέφος

2.1.2. Διασφάλιση του ορθού ελέγχου πρόσβασης

Από τότε που μερικά υποσύνολα αυτά των πόρων (ή όλα από αυτά) εκτίθενται στο διαδίκτυο, ένας οργανισμός που χρησιμοποιεί ένα δημόσιο υπολογιστικό νέφος αντιμετωπίζει σπουδαία αύξηση ρίσκου στα δεδομένα του. Η ικανότητα να ελέγχει τις πράξεις του παρόχου μιας υπηρεσίας υπολογιστικού νέφους (πόσο μάλλον όταν μιλάμε για την διεξαγωγή παρακολούθησης σε πραγματικό χρόνο όπως σε μια διάσταση όπως το προσωπικό μας δίκτυο) ακόμα και μετά το γεγονός δεν υπάρχει. Θα υπάρχει μειωμένη πρόσβαση στις σχετικές υπηρεσίες καταγραφής του δικτύου και μειωμένη ικανότητα να διεξαχθεί έρευνα και γίνει συλλογή εγκληματολογικών στοιχείων (forensics).

Ένα παράδειγμα με όλα τα προβλήματα που σχετίζονται με τον δεύτερο παράγοντα ρίσκου είναι το θέμα των επαναχρησιμοποιούμενων διευθύνσεων IP. Οι διευθύνσεις IP όταν αποδεσμεύονται από ένα πελάτη παραμένουνε διαθέσιμες με σκοπό την επαναχρησιμοποίηση τους από κάποιον επόμενο πελάτη. Οι IP διευθύνσεις από την άλλη επίσης είναι και χρεωστικό στοιχείο του πελάτη για την προσφορά της υπηρεσίας. Από την οπτική ενός παρόχου υπηρεσίας υπολογιστικού νέφους αυτό έχει νόημα αλλά από την σκοπιά του πελάτη η διατήρηση των διευθύνσεων IP που δεν είναι πλέον σε χρήση μπορεί να παρουσιάσουν πρόβλημα.

2.1.3. Διασφάλιση της διαθεσιμότητας του διαδικτύου-αντιμετώπιση πόρων

Η εμπιστοσύνη στην ασφάλεια των δικτύων έχει αναπτυχθεί αυξητικά και επιτυχημένα λόγω του αυξανόμενου αριθμού δεδομένων που εξαρτώνται από την φιλοξενία σε εξωτερικές συσκευές. Συνεπώς υπεισέρχονται τρείς παράγοντες κινδύνου που πρέπει να έχει κατά νου ένας οργανισμός. Για παράδειγμα η πειρατεία του προθέματος του BGP (η παραποίηση των στρωμάτων του δικτύου για την προσβασιμότητα της πληροφορίας) είναι ένα καλό παράδειγμα ενός τέτοιου κινδύνου. Η πειρατεία του προθέματος αυτού περιλαμβάνει την ανακοίνωση της διεύθυνσης ενός αυτόνομου συστήματος (σύμφωνα με το RFC 1930) σε κάποιο άλλο χωρίς την άδεια του. Αυτό πολλές φορές συμβαίνει σε σφάλμα κάποιας ρύθμισης (configuration) αλλά αυτή η λανθασμένη ρύθμιση μπορεί πολλές φορές να επηρεάσει την διαθεσιμότητα των πόρων μιας υπηρεσίας νέφους.

Επίσης λόγω τέτοιων προβληματικών ρυθμίσεων πολλές φορές υπάρχουν προμελετημένες επιθέσεις. Παρόλο όμως που ακόμα και αν τέτοιες επιθέσεις έχουν συχνότητα εμφάνισης μικρότερη από τις προβληματικές ρυθμίσεις εξακολουθούν να εμφανίζονται και να προκαλούν προβλήματα στην διαθεσιμότητα των δεδομένων. Τέλος αν και αυτού του τύπου η επίθεση της πειρατείας του προθέματος δεν είναι κάτι καινούργιο μπορεί να παρουσιάσει όμως πιθανή αύξηση συχνότητας σχετικά με την παράλληλη ανάπτυξη του υπολογιστικού νέφους. Επιπλέον μπορούμε να πούμε ότι όσο η χρηστικότητα ενός συστήματος υπολογιστικού νέφους αυξάνεται, η διαθεσιμότητα των πόρων που βασίζονται στο cloud αυξάνονται σε αξία στους πελάτες. Αυτή η αυξανόμενη αξία για τους πελάτες μεταφράζεται σε αυξανόμενο κίνδυνο κακόβουλης δραστηριότητας που καταλήγει σε απειλή για την διαθεσιμότητα.

Επιθέσεις στο DNS είναι ένα ακόμα πρόβλημα ρίσκου και υπάρχουν πολλών ειδών τύποι επιθέσεων αυτού του είδους που ελλοχεύουν κινδύνους για το cloud και τέλος κίνδυνο αποτελούνε και οι επιθέσεις άρνησης εξυπηρέτησης (DoS) καθώς επίσης και οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS). Και αυτού του τύπου οι επιθέσεις δεν είναι κάτι νέο αλλά αποτελούνε τεράστιο κίνδυνο για ένα cloud σύστημα στο επίπεδο του δικτύου μιας λόγω της χρήσης πόρων εκτός του οργανισμού. Ακόμα όταν χρησιμοποιούμε IaaS ο κίνδυνος μιας επίθεσης DoS δεν είναι μόνο εξωτερικός παράγοντας αλλά και εσωτερικός μέσω του τμήματος του δικτύου από το IaaS του παρόχου που χρησιμοποιείται από τους πελάτες (ξεχωριστό από το εταιρικό δίκτυο του παρόχου του IaaS). Αυτό το εσωτερικό (δεν αποτελεί δίκτυο δρομολόγησης) δίκτυο είναι ένας διαμοιραζόμενος πόρος που χρησιμοποιείται από τους πελάτες για πρόσβαση σε μη φυσικές παρουσιάσεις, όπως ο πάροχος για την διαχείριση του δικτύου και των πόρων (σαν φυσικούς εξυπηρετητές - servers). Εάν δηλαδή υπήρχε ένας κακόβουλος πελάτης δεν υπάρχει τίποτα που θα τον απέτρεπε να χρησιμοποιήσει την πρόσβαση του ως πελάτη στο εσωτερικό του δίκτυο όπου θα βρει και θα μπορέσει να επιτεθεί σε άλλους πελάτες ή στην IaaS υποδομή του παρόχου μιας και αυτός με την σειρά του δεν έχει τους κατάλληλους μηχανισμούς ανίχνευσης για να αποτρέψει μια τέτοιου είδους ενέργεια.

2.2. Ασφάλεια υποδομής στο επίπεδο του host

Όταν μιλάμε για ασφάλεια στον host ή για αποτίμηση ρίσκου σ' αυτόν τότε θα πρέπει πάντοτε να λαμβάνουμε υπόψη τόσο το περιεχόμενο των μεταφερόμενων μοντέλων υπηρεσιών από το cloud (SaaS, PaaS και IaaS) όσο και από το μοντέλο ανάπτυξης του cloud (ιδιωτικό, δημόσιο, υβριδικό). Αν και δεν υπάρχουν νέες απειλές στους hosters του υπολογιστικού νέφους, κάποιες απειλές ωστόσο όπως VM escape, λάθος παραμετροποίηση συστήματος και εσωτερικές απειλές μέσω του ασθενούς ελέγχου πρόσβασης στον hypervisor της υπηρεσίας cloud μπορεί να επιφέρουν επιπλέον προβλήματα ασφάλειας.

Επιπρόσθετα το γεγονός ότι το υπολογιστικό νέφος χρησιμοποιεί την δύναμη πολλών υπολογιστικών κόμβων και σε συνδυασμό με την ομογένεια του λειτουργικού συστήματος που χρησιμοποιούνται από τους hosts μπορεί κανείς να αντιληφθεί πόσο εύκολα μπορεί μια επίθεση να αναπτυχθεί και παράλληλα μπορεί πόσο εύκολα μπορεί να κλιμακωθεί σε διάστημα χρόνου μέσα στο νέφος. Από αυτό το πιο σημαντικό που πρέπει κάποιος να αντιληφθεί είναι τα όρια εμπιστοσύνης και οι ευθύνες που πέφτουν στους ώμους του host για την διαφύλαξη της ασφάλειας της υποδομής σε συνεργασία και σύγκριση πάντα που θα πρέπει να γίνεται με τις ευθύνες του παρόχου (CSP) στο αντίστοιχο κομμάτι.

2.2.1. SaaS και PaaS ασφάλεια

Σε γενικές γραμμές οι CSP δεν δημοσιοποιούν πληροφορίες που σχετίζονται με τις πλατφόρμες των hosts, τα λειτουργικά συστήματα των hosts καθώς και τις διαδικασίες που είναι θέση να διασφαλίσουν την ασφάλεια των hosts δεδομένου όμως ότι κάποιος κακόβουλος μπορεί να εκμεταλλευτεί αυτές τις πληροφορίες όταν διεισδύσει σε ένα σύστημα cloud. Ως εκ τούτου στα πλαίσια των SaaS (πχ saleforce.com , workday.com) και PaaS (πχ google app engine, saleforce.com, force.com) υπηρεσιών cloud η ασφάλεια του host είναι αδιαφανής διαδικασία για τον host και την ευθύνη εξασφάλισης της στους hosts μεταφέρεται στον CSP. Για να λάβει τώρα κάποιος διαβεβαίωση για αυτή την ασφάλεια πρέπει κάποιος να απευθυνθεί στον πωλητή της υπηρεσίας για ανταλλαγή πληροφοριών στα πλαίσια μιας συμφωνίας εμπιστευτικότητας (nondisclosure agreement - NDA) ή πολύ απλά θέσει το ερώτημα στον CSP μέσω ενός προτύπου αξιολόγησης ασφάλειας όπως SysTrust και το ISO 27002. Από την πλευρά τώρα της αξιοπιστίας των ελέγχων θα

πρέπει οι CSPs να εξασφαλίσουν τα κατάλληλα προληπτικά μέτρα και να διαθέτουν τους κατάλληλους ανιχνευτικούς μηχανισμούς προκειμένου να ενθαρρύνεται η εξασφάλιση ελέγχου από ένα τρίτο (third party assessment) και η αξιολόγηση από ένα πλαίσιο ISO 27002.

Δεδομένου ότι η χρήση εικονικών μηχανών (virtualization) είναι μια βασική τεχνολογία ευρείας διάδοσης που βελτιώνει την κεντρική χρήση του υλικού (hardware), πέρα των πολλών πλεονεκτημάτων είναι κοινό για τους CSPs να απασχολούν πλατφόρμες εικονικών μηχανών (virtualization platforms) συμπεριλαμβανομένων Xen και VMware hypervisors στην αρχιτεκτονική της πλατφόρμας τους. Θα πρέπει λοιπόν να γίνει κατανόηση πως οι πάροχοι χρησιμοποιούν τις τεχνολογίες εικονικοποίησης και πως γίνονται οι διαδικασίες για την εξασφάλιση ασφάλειας του επιπέδου εικονικοποίησης.

Συγκεντρωτικά μπορούμε να πούμε ότι οι ευθύνες ασφάλειας του host στις SaaS και PaaS μεταφέρονται στον CSP. Το γεγονός ότι δεν έχουμε να ανησυχούμε για την προστασία των hosts από απειλές για αυτούς είναι ένα τεράστιο όφελος από πλευράς κόστους και διαχείρισης ασφάλειας. Ωστόσο ο πελάτης δεν έχει απώλεια του ρίσκου διαχείρισης της πληροφορίας που φιλοξενείται στις υπηρεσίες του cloud και είναι δική του ευθύνη να πάρει το κατάλληλο επίπεδο βεβαιότητας για το πώς ο CSP διαχειρίζεται την «υγιή» και σωστή ασφάλεια του host.

2.2.2. IaaS ασφάλεια

Σε αντίθεση με τα SaaS και PaaS, οι πελάτες του IaaS είναι οι πρωταρχικά υπεύθυνοι για την ασφάλεια των hosts που τροφοδοτούνται σε ένα cloud. Δεδομένου ότι όλες οι υπηρεσίες σήμερα που έχουμε, αφορούνε την εικονικοποίηση στο επίπεδο του host, η ασφάλεια IaaS στο επίπεδο του host θα πρεπει να ταξινομηθεί ως εξής:

- Ασφάλεια λογισμικού εικονικοποίησης (virtualization software security)

Αφορά το λογισμικό εκείνο που καθιστά ικανότητα τους πελάτες για την δημιουργία και την καταστροφή εικονικών περιπτώσων. Εικονικοποίηση στο επίπεδο του host μπορεί να γίνει με οποιαδήποτε από τα μοντέλα εικονικοποίησης

- όπως το επίπεδο εικονικοποίησης λειτουργικού συστήματος (virtualization OS layer) (πχ Solaris containers, BSD jails, Linux Vserver)

- το μοντέλο paravirtualization που αποτελεί εκδοχή συνδυασμού του υλικού με Xen και VMware
- και τέλος το μοντέλο εικονικοποίησης βασισμένο στο επίπεδο του υλικού (hardware based virtualizaton) πχ με Xen, VMware, Microsoft Hyper-V.

Είναι σημαντική η διαφύλαξη της ασφάλειας στο επίπεδο του λογισμικού που τοποθετείται μεταξύ του υλικού και των εικονικών εξυπηρετητών. Σε μια δημόσια υπηρεσία IaaS οι πελάτες δεν έχουνε πρόσβαση σε ένα τέτοιο στρώμα λογισμικού. Αυτό παραμένει στην διαχείριση του CSP και μόνο.

- Λειτουργικό σύστημα πελάτη φιλοξενούμενου ή ασφάλεια εικονικού εξυπηρετητή (customer guest OS or virtual server security)

Αφορά την εικονική παρουσία ενός λειτουργικού συστήματος που βρίσκεται στην κορυφή του επιπέδου εικονικοποίησης και είναι ορατό σε πελάτες από το διαδίκτυο (πχ διάφορες εκδόσεις του Linux, Microsoft και Solaris) και οι πελάτες τους έχουνε πλήρη πρόσβαση σε εικονικούς εξυπηρετητές.

2.3. Ασφάλεια στον εικονικό εξυπηρετητή

Ένα δημόσιο IaaS όπως το Elastic Compute Cloud της Amazon (EC2), προσφέρει μια διεπαφή διαδικτυακής εφαρμογής (web services API) για την εκτέλεση λειτουργιών διαχείρισης όπως την πρόβλεψη, τον παροπλισμό και την κατανομή των εικονικών εξυπηρετητών στην πλατφόρμα IaaS. Αυτές οι λειτουργίες διαχείρισης όταν είναι ενορχηστρωμένες κατάλληλα μπορούν να παρέχουν ελαστικότητα για πόρους που μπορούν να αυξηθούν ή να συρρικνωθούν ανάλογα με την ζήτηση του φόρτου εργασίας. Ο δυναμικός κύκλος ζωής των εικονικών εξυπηρετητών μπορεί να οδηγήσει σε πολυπλοκότητα, εάν η διαδικασία της διαχείρισης των εικονικών εξυπηρετητών δεν είναι αυτοματοποιημένη με κατάλληλες διαδικασίες. Από την οπτική μιας επίθεσης, ο εικονικός εξυπηρετητής (windows, linux, solaris) μπορεί να είναι προσβάσιμος από όλους μέσω του διαδικτύου γι' αυτό πρέπει να παρθούν αμβλυμμένα μέτρα δικτυακής πρόσβασης προκειμένου να περιοριστεί η πρόσβαση σε εικονικές περιπτώσεις. Τυπικά ένας CSP μπλοκάρει όλες τις πόρτες πρόσβασης στους εικονικούς εξυπηρετητές και απαιτεί από τους πελάτες την χρήση της πόρτας 22 (Secure Shell ή SSH) για την διαχείριση τους. Η διεπαφή διαχείρησης του cloud προσθέτει ένα ακόμα επίπεδο που μπορεί να θιχτεί από κάποια επίθεση και πρέπει να

συμπεριληφθεί στην σκοπιά της ασφάλειας των εικονικών εξυπηρετητών στο δημόσιο cloud. Μερικές από τις καινούργιες απειλές στον host στο IaaS μπορεί να περιλαμβάνουν:

- Κλοπή κωδικών που χρησιμοποιούνται για την πρόσβαση και διαχείριση των hosts (πχ SSH private keys)
- Unpatched Attacking, οι τρωτές υπηρεσίες ακούνε σε συγκεκριμένες πόρτες (πχ FTP, NetBIOS, SSH)
- Πειρατεία λογαριασμών που δεν έχουνε ασφαλιστεί κατάλληλα. (πχ αδύναμοι κωδικοί ή ανύαρκτοι κωδικοί πρόσβασης για συγκεκριμένους τυπικούς λογαριασμούς)
- Συστήματα επιθέσεων που δεν ασφαλίζονται κατάλληλα με host firewalls
- Ανάπτυξη δούρειων ίππων (Trojan horses) που βρίσκονται ενσωματωμένα στο τμήμα λογισμικού μιας εικονικής μηχανής ή εντός της εικονικής μηχανής στο ίδιο δηλαδή το λειτουργικό σύστημα.

2.3.1. Ενίσχυση ασφάλειας στον εικονικό εξυπηρετητή

Η απλότητα αυτοτροφοδότησης με νέους εικονικούς εξυπηρετητές σε μια πλατφόρμα IaaS δημιουργεί κινδύνους από ανασφαλείς εξυπηρετητές. Η επίτευξη της ασφάλειας - by default – ενός τέτοιου συστήματος μπορεί να εξασφαλιστεί με την ακολουθία μεγαλύτερων διαθέσιμων κανόνων ασφάλειας που μοιάζουν με την γραμμή παραγωγής σε βιομηχανίες. Αυτό δηλαδή εν ολίγοις σημαίνει την χρήση διαδικασιών ασφάλειας που συνοδεύονται με αυτοματοποιημένες διαδικασίες. Μερικές υποδείξεις είναι οι ακόλουθες:

- Χρησιμοποίηση μιας ασφαλούς -by default- διαμόρφωσης (configuration). Ενίσχυση του image του λειτουργικού συστήματος του φιλοξενούμενου στην υπηρεσία ενός cloud χρησιμοποιώντας ένα τυποποιημένο ανθεκτικό από πλευράς ασφάλειας image στην εικονική μηχανή. Μια καλή πρακτική για εφαρμογές που βασίζονται σε cloud είναι η ανάπτυξη images εικονικών μηχανών που έχουνε μόνο τις δυνατότητες και τις προσφερόμενες υπηρεσίες που είναι απαραίτητες για την υποστήριξη της εφαρμογής. Περιορίζοντας τις υπηρεσίες της θεμελιώδους στοίβας της υπηρεσίας όχι μόνο περιορίζουμε της πιθανότητες κάποιας επίθεσης στον host αλλά ταυτόχρονα περιορίζουμε και

τις διεργασίες μπαλώματα (patches) που πρέπει να διαμορφώσουμε προκειμένου να κρατήσουμε την εφαρμογή ασφαλή.

- Απαραίτητη κρίνεται η καταγραφική απογραφή των images των εικονικών μηχανών και των λειτουργικών συστημάτων που ετοιμάζονται για την φιλοξενία της υπηρεσίας υπολογιστικού νέφους. Ο πάροχος IaaS προσφέρει μερικά από αυτά τα images των VMs. Όταν ένα εικονικό image από τον πάροχο IaaS χρησιμοποιείται, τότε αυτό θα πρέπει να υποβληθεί στο ίδιο επίπεδο ελέγχου ασφάλειας και στις ίδιες διαδικασίες ενίσχυσης ασφάλειας των hosts στο εσωτερικό της όλης υλοποίησης.

  Η καλύτερη εναλλακτική λύση είναι η παροχή ενός image από τον ίδιο τον οργανισμό τέτοιο που θα συμμορφώνεται με τα ίδια πρότυπα ασφάλειας καθιστώντας έτσι τους hosts σαν να είναι εσωτερικοί έμπιστοι hosts.
- Προστασία της ακεραιότητας του ενισχυμένου image από θέμα ασφάλειας, από τους μη έχοντες το δικαίωμα πρόσβασης
- Προστασία των κωδικών και μυστικών κλειδιών που απαιτούνται για την πρόσβαση των hosts στο δημόσιο cloud.
- Σε γενικές γραμμές προτείνεται η απομόνωση των κλειδιών αποκρυπτογράφησης από το cloud από εκεί που φιλοξενούνται τα δεδομένα εκτός αν είναι απαραίτητα για την αποκρυπτογράφηση και στη συνέχεια μόνο για την διάρκεια της πραγματικής διαδικασίας της αποκρυπτογράφησης από μια δραστηριότητα.
- Απαγορεύεται να συμπεριληφθούν πιστοποιητικά αυθεντικοποίησης σε εικονοποιημένα images (virtualized images) εκτός από ένα κλειδί που θα αποκρυπτογραφεί το κλειδί στο συστήματος αρχείων.
- Δεν επιτρέπεται η κωδικο-κεντρική πολιτική αυθεντικοποίησης για την πρόσβαση του πυρήνα (shell access).
- Απαίτηση κωδικών για τα δικαιώματα στην εντολή sudo ή στην πολιτική πρόβασης με ρόλους (πχ Solaris SE linux)
- Χρήση firewall όπου ανοιχτές θα είναι μόνο οι ελάχιστες απαραίτητες πόρτες την υποστήριξη των κατά περίπτωση υπηρεσιών.
- Χρήση μόνο των απαραίτητων υπηρεσιών συστήματος και κλείσιμο όλων εκείνων που δεν χρησιμοποιούνται από το σύστημα (για παράδειγμα κλείσιμο

υπηρεσίας FTP, υπηρεσία εκτυπωτών, υπηρεσία διαδικτυακού διαμοιραμού αρχείων και υπηρεσίες βάσεων δεδομένων που δεν απαιτούνται)

- Εγκαθίδρυση ανίχνευση εισβολών(host based IDS) όπως το OSSEC και το Samhain
- Ενεργοποίηση μηχανισμών παρακολούθησης συστήματος και καταγραφής αρχείων και παράλληλα ενημέρωση όλων των συμβάντων ασφάλειας σε ένα κεντρικό εξυπηρετητή αφοσιωμένο στην καταγραφή αρχείων (dedicated log server). Παράλληλα απομονώστε τον συγκεκριμένο εξυπηρετητή και διαφυλάξτε του την ασφάλεια με διαδικασίες ελέγχου πρόσβασης.
- Σε περίπτωση υποψιασμού κακόβουλης ενέργειας καταγράψτε το τρέχον στιγμιότυπο του συστήματος και αντιγράψτε (backup) το σε εφεδρικό υλικό με σκοπό την διενέργεια ψηφιακών πειστηρίων αργότερα
- Θέσπιση κανόνων για την ομαλή και επιτυχή εγκατάστασης patches στα διάφορα images του cloud – τόσο σε εκείνα που είναι ενεργά όσο και εκείνα που είναι στιγμιαία ανενεργά.
- Τέλος συνιστάται περιοδικός έλεγχος των αρχείων καταγραφής με σκοπό τον εντοπισμό κακόβουλων ενεργειών

2.4. Ασφάλεια υποδομής στο επίπεδο εφαρμογής

Η ασφάλεια στο επίπεδο λογισμικού ή το επίπεδο εφαρμογής θα πρέπει να είναι ένα από τα κρίσιμα σημεία του προγράμματος ασφάλειας. Σχεδιάζοντας και υλοποιώντας εφαρμογές με στόχο την ανάπτυξη τους σε μια πλατφόρμα υπολογιστικού νέφους υπάρχει η απαίτηση ότι τα υφιστάμενα προγράμματα ασφάλειας των εφαρμογών αυτών θα έχουνε αξιολογήσει εκ νέου τις τρέχουσες πρακτικές και πρότυπα. Το πρόγραμμα ασφάλειας αυτό δηλαδή οι κατευθυντήριες γραμμές που θα πρέπει να ακολουθήσει μια ομάδα για την ενίσχυση της ασφάλειας μιας τέτοιας εφαρμογής κάτω από κάποιες πολιτικές ποικίλουν και διαφέρουν ανάλογα ανάλογα με το είδος τους από αυτόνομες εφαρμογές ενός χρήστη σε πολλούς και από εξελιγμένες εφαρμογές της κατηγορίας e-commerce που χρησιμοποιούνται από εκατομμύρια χρήστες. Διαδικτυακές εφαρμογές όπως CMSs (content management systems), wikis, portals, bulletin boards και φόρουμ συζητήσεων χρησιμοποιούνται ραγδαία από μικρής ή μεγάλης κλίμακας

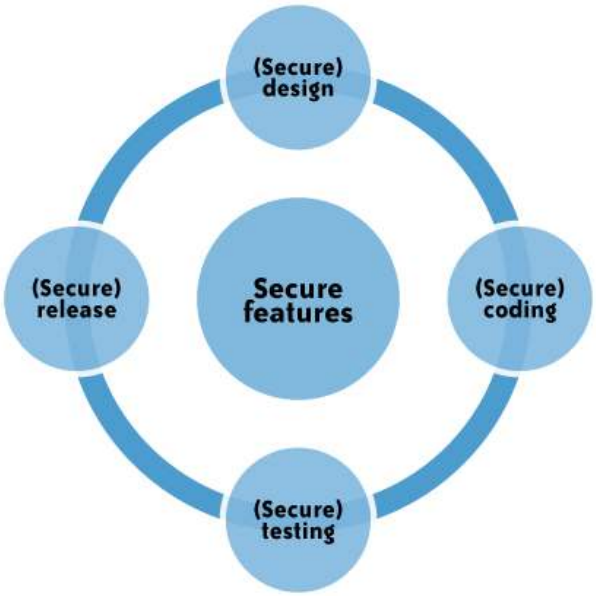
οργανισμούς. Άλλοι οργανισμοί η επιχειρήσεις επίσης χρησιμοποιούν και αναπτύσσουν τις δικές τους πλατφόρμες οι οποίες συνήθως βασίζονται σε διάφορα web frameworks (πχ PHP, .NET, J2EE, Python κλπ). Έτσι λοιπόν έχουνε παρατηρηθεί πολλές επιθέσεις που γίνονται σε τέτοιους οργανισμούς συνήθως με οικονομικό δόλο εξαιτίας προγραμματιστικών λαθών που υπάρχουν και τις αδυναμίες που εμφανίζονται κατά την πρόσβαση των τελικών χρηστών (end user clients) μέσω των φυλλομετρητών διαδικτύου όπου γίνεται αυτή η πρόσβαση στο cloud. Γι αυτό το λόγο είναι χρήσιμο και προφανές επειδή οι φυλλομετρητές διαδικτύου χρησιμοποιούνται από τους τελικούς χρήστες ως ο κρίκος πρόσβασης στο cloud, να γίνεται χρήση και να συμπεριλαμβάνονται οι δικλίδες ασφάλειας των φυλλομετρητών στην σκοπιά της οποιαδήποτε εφαρμογής του cloud. Με αυτό τον τρόπο θα πετύχουμε την ασφάλεια από άκρο σε άκρο –end to end- πετυχαίνοντας έτσι επαύξηση της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των επεξεργαζόμενων πληροφοριών από τις διάφορες υπηρεσίες του υπολογιστικού νέφους.

2.4.1. Απειλές ασφάλειας στο επίπεδο εφαρμογής

Οι απειλές ασφάλειας στο επίπεδο εφαρμογής είναι λίγο πολύ ίδιες μα αυτές που υπάρχουνε γενικά και περιλαμβάνουν cross-site scripting (XSS), SQL injection, εκτέλεση κακόβουλων κομματιών κώδικα στην εφαρμογή και άλλες τεχνικές εκμετάλλευσης ευπαθειών και αδυναμιών εξαιτίας προγραμματιστικών λαθών και λανθασμένων σχεδιασμών διεργασιών ροής. Οι hackers εφοδιασμένοι με εμπειρία και κατάλληλα εργαλεία σκανάροντας τις διαδικτυακές αυτές εφαρμογές του cloud ανιχνεύουν τις αδυναμίες αυτές και τις εκμεταλλεύονται με σκοπό πολλές φορές οικονομικές απάτες, κλοπή πνευματικής ιδιοκτησίας, μετατροπή των έμπιστων εξυπηρετητών σε κακόβουλους που εκμεταλλεύονται την πλευρά ενός πελάτη και απάτες ηλεκτρονικού ψαρέματος (phising). Όλα τα web frameworks και όλων των ειδών οι διαδικτυακές εφαρμογές υπόκεινται στις διάφορες ατέλειες ασφάλειας που υπόκεινται και οι κλασσικές διαδικτυακές εφαρμογές.

Είναι συνήθης η πολιτική χρήσης περιμετρικών ελέγχων ασφάλειας και από την πλευρά του δικτύου και από την πλευρά των hosts με σκοπό την προστασία των διαδικτυακών εφαρμογών που αναπτύσσονται σε ένα στενά ελεγχόμενα περιβάλλον,

συμπεριλαμβάνοντας συνεργαζόμενα intranets και δημόσια cloud, από εξωτερικούς κακόβουλους. Έτσι οι διαδικτυακές εφαρμογές που έχουνε αναπτυχθεί σε μια δημόσια πλατφόρμα στο cloud θα πρέπει να υποβάλλονται σε ελέγχους υψηλού επιπέδου απειλών προκειμένου να μην γίνονται αντικείμενο κακόβουλης εκμετάλλευσης. Έτσι λοιπόν σ' αυτό το μοντέλο απειλών οι διαδικτυακές εφαρμογές του cloud θα πρέπει να σχεδιάζονται για ένα μοντέλο απειλών διαδικτύου στο οποίο η ασφάλεια θα πρέπει να βρίσκεται ενσωματωμένη στον κύκλο ανάπτυξης του λογισμικού.



Εικόνα 14 κύκλος ασφαλούς ανάπτυξης λογισμικού

2.4.2. Επιθέσεις DoS και EDoS

Οι επιθέσεις DoS και EDoS στο επίπεδο εφαρμογής είναι επιθέσεις κλίμακας ψηλού κινδύνου μιας και μπορούνε να επηρεάσουνε την λειτουργία του cloud για αρκετά μεγάλο χρονικό διάστημα. Οι επιθέσεις στο επίπεδο διαδικτύου μπορούν να χαρακτηριστούν σαν υψηλού ρυθμού ανανέωση φόρτωσης σελίδας πάνω από τα πρωτόκολλα HTTP και HTTPS. Για παράδειγμα μια τέτοια επίθεση στο twitter επέφερε διακοπή της υπηρεσίας για πάρα πολλές ώρες το 2009. Τέλος μια τέτοιου μήκους επίθεση που θα μπορούσε να ξεκινήσει από ένα IaaS ή PaaS θα μπορέσει να περάσει και σε άλλες υπηρεσίες στο cloud με αποτέλεσμα κάποια στιγμή ενδεχομένως ο κακόβουλος να καταφέρει να αποκτήσει τεράστια υπολογιστική δύναμη.

2.4.3. Ασφάλεια στον τελικό χρήστη (end user security)

Ο πελάτης μιας υπηρεσίας υπολογιστικού νέφους είναι υπεύθυνος για την ασφάλεια ενεργειών τελικού χρήστη. Προληπτικά μέτρα προστασίας θα μπορούσαν να είναι η χρήση ασφαλούς λογισμικού όπως λογισμικό anti-malware, antivirus, προσωπικά firewall, διάφορα patches και ενημερώσεις ασφάλειας καθώς επίσης και συστήματα ανίχνευσης εισβολών μιας και επόμενος στόχος μέσω του φυλλομετρητή είναι το λειτουργικό σύστημα του με απώτερο σκοπό φυσικά την πλήξη της υπηρεσίας ή των υπηρεσιών του cloud. Αυτό λοιπόν εν ολίγοις προϋποθέτει την ύπαρξη εξασφάλισης των φυλλομετρητών να είναι ασφαλείς.

2.4.4. Ποιος είναι λοιπόν υπεύθυνος για την ασφάλεια εφαρμογής στο σύννεφο;

Βασιζόμενοι στο μοντέλο μεταφοράς υπηρεσιών του cloud (SPI) και την συμφωνία υπηρεσιών (SLA), η σκοπιά των ευθυνών ασφάλειας μεταφέρεται τόσο στον πελάτη όσο και στον CSP. Το κλειδί για έναν πελάτη είναι η κατανόηση των ευθυνών ασφάλειας που του αναλογούν έναντι του παρόχου του. Κατ' αρχάς οι πελάτες δεν έχουνε την απαιτούμενη διαφάνεια στον τομέα των τρωτών σημείων του λογισμικού στους τομείς των διαφόρων υπηρεσιών του cloud. Αυτό αποτρέπει τους πελάτες από την διαχείριση του λειτουργικού κινδύνου που μπορούν να έρθουν σε επαφή με τα τρωτά σημεία. Επιπλέον αντιμετωπίζοντας το λογισμικό τους ως βιομηχανική ιδιοκτησία οι CSPs παρεμποδίζουν ερευνητές ασφάλειας από την ανάλυση του λογισμικού για κενά ασφάλειας και bugs (αυτό εξαιρεί βέβαια τους CSPs που χρησιμοποιούν λογισμικό ελεύθερου κώδικα). Λόγω αυτού το γεγονότος οι πελάτες δεν έχουνε άλλη επιλογή από το να εμπιστευτούνε τον πάροχο τους μέχρι να αποκαλύψει εκείνος από την πλευρά του οποιαδήποτε ευπάθεια στο σύστημα που μπορεί να επηρεάζει την ακεραιότητα την εμπιστευτικότητα ή την διαθεσιμότητα της εφαρμογής του.

Εικόνα 15 Πλεονεκτήματα και μειονεκτήματα του νέφους ως προς την ασφάλεια

3. ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ

Ηλεκτρονική διακυβέρνηση είναι μια διαδικασία μεταρρύθμισης με τρόπο τέτοιο που μια κυβέρνηση εργάζεται, ώστε να μοιράζεται πληροφορίες, να εμπλέκει τους πολίτες σ αυτές τις υπηρεσίες και να παρέχει υπηρεσίες σε εξωτερικούς και εσωτερικούς πελάτες προς όφελος τόσο των κυβερνήσεων όσο και των πελατών που εξυπηρετούν.

Οι κυβερνήσεις έχουνε αμέτρητες εφαρμογές που μπορούν και πρέπει να αυτοματοποιηθούν και οι δημόσιες δαπάνες είναι πολλές που γίνονται προκειμένου να έχουνε αύξηση της παραγωγικότητας. Όλες οι υπηρεσίες ηλεκτρονικής διακυβέρνησης είτε λαμβάνουν χώρα υλοποίησης στο υπολογιστικό νέφος είτε όχι εμπίπτουν στις παρακάτω κατηγορίες:

Εικόνα 16 Κατηγορίες υπηρεσιών ηλεκτρονικής διακυβέρνησης

- Government to Government (G2G): Διάφορες κυβερνητικές λειτουργίες αλληλεπιδρούν για να εκπληρώσουν το έργο. Η πλειοψηφία αυτών των εφαρμογών είναι κατακόρυφες και οριζόντιες μαζί. Κατακόρυφες εφαρμογές εστιάζουν σε μια ειδική εφαρμογή διακυβέρνησης και η οριζόντια την κάνει πράξη. Οι εφαρμογές αυτές έχουνε υψηλό βαθμό μετάδοσης μηνυμάτων μεταξύ των τμημάτων.
- Government to Enterprise (G2E): Επιχειρήσεις όπως αυτή της Δημόσιας Ύδρευσης του ηλεκτρισμού ή των τηλεπικοινωνιών και οι οποίες

ελέγχονται από τις εκάστοτε κυβερνήσεις πρέπει να αλληλεπιδρούν γρήγορα και αποτελεσματικά με τις κυβερνητικές πολιτικές. Πολιτικές επιβολής, ασφάλεια και ελεγχος-auditing (για λογοδοσία) είναι από τις μεγαλύτερες προκλήσεις.

- Government to Business (G2B): Η κυβέρνηση αλληλεπιδρά με διάφορες επιχειρήσεις στους τομείς επιβολής πολιτικών, συλλογής φόρων και διαχείρισης συμβάσεων. Η μεγαλύτερη περιοχή που πέφτει στην κυβέρνηση είναι αυτή της διαχείρισης των συμβάσεων.
- Government to Consumer (G2C): Η κυβέρνηση παρέχει αριθμητικά πολλές υπηρεσίες στους πολίτες της. Διαφορετικά τμήματα ή υπουργεία προσφέρουν διάφορες υπηρεσίες που θα μπορούσε να κυμανθεί από ένα απλό αίτημα μέχρι διαδικασίες σύνθετες που θα απαιτούσαν σενάρια που θα απαιτούσαν την εκκίνηση σύνθετων ροών εργασίας.

Έτσι λοιπόν σύμφωνα με τα παραπάνω η εφαρμογή e-taxis στην μετάβαση της στο υπολογιστικό νέφος συγκαταλέγεται στην κατηγορία G2B.

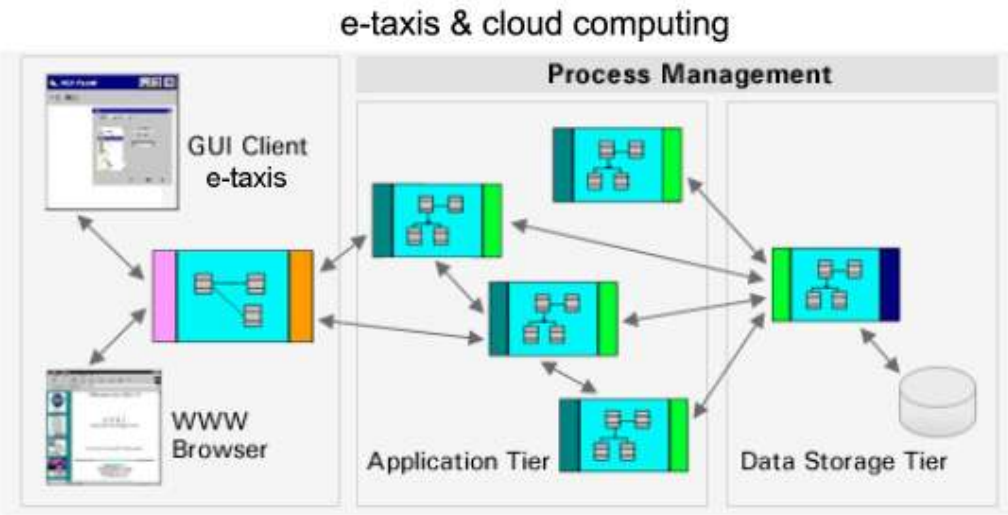
3.1. Συστατικά της εφαρμογής ηλεκτρονικής διακυβέρνησης e-taxis αλλά και γενικότερα των εφαρμογών του είδους

Στην ηλεκτρονική διακυβέρνηση για τις διάφορες υπηρεσίες αλλά και για το e-taxis της εφαρμογής μας χρησιμοποιείται το μοντέλο αρχιτεκτονικής 3-tier καλύπτοντας μας πλήρως καθότι παρέχει τα ακόλουθα πλεονεκτήματα:

- Ετερογενή συστήματα: Οι εφαρμογές μπορούν να χρησιμοποιήσουν την δύναμη διαφορετικών πλατφορμών και διαφορετικά συστατικά στοιχεία του λογισμικού σε διάφορα επίπεδα.
- Μετατρεψιμότητα (modifiability): όπως κατανέμονται οι ευθύνες κάνει εύκολο την αλλαγή κώδικα σε κάθε επίπεδο χωρίς την επιρροή ή την δυσλειτουργία των υπολοίπων επιπέδων.
- Κλιμάκωση για τον χειρισμό πολλών πελατών: όλη η πρόσβαση των πελατών γίνεται από το επίπεδο μέσης βαθμίδας. Η μεσαία βαθμίδα μπορεί να μοιράζεται τη σύνδεση βάσης δεδομένων σε όλους τους πελάτες, και αν προκύψει συμφόρηση, είναι ικανή να αναπτύξει αρκετούς διακομιστές

εκτέλεσης κώδικα της μέσης βαθμίδας με αποτέλεσμα οι πελάτες να μπορούν να συνδεθούν σε οποιοδήποτε από αυτούς τους διακομιστές.

- Ολοκληρωμένη πρόσβαση δεδομένων: Σε πολλές εφαρμογές, τα δεδομένα απαιτείται να προσεγγιστούν από διάφορες πηγές. Αυτό μπορεί να γίνεται με διαφάνεια στη μέση βαθμίδα, όπου μπορούν να διαχειρίζονται κεντρικά οι συνδέσεις με όλα τα εμπλεκόμενα συστήματα βάσης δεδομένων.



Εικόνα 17 Αρχιτεκοντική εφαρμογής e-taxis στο νέφος

3.2. Στρατηγική μετανάστευσης του e-taxis από τα παραδοσιακά μοντέλα πληροφορικής στο υπολογιστικό νέφος

Η μεταφορά τόσο του e-taxis όσο και οποιασδήποτε άλλης εφαρμογής ηλεκτρονικής διακυβέρνησης στο νέφος μπορεί και πρέπει να γίνεται κάτω από κάποιες κινήσεις που μπορούνε να συγκροτηθούνε σε έξι βήματα.

- **Βήμα 1^{ο} – Μάθηση (Learning):**

Η μετανάστευση της εφαρμογής στο νέφος αρχίζει με την εκμάθηση των βασικών γύρω από το νέφος. Το νέφος είναι μια τεχνολογία αιχμής στην πληροφορική. Θα είναι ιδιαίτερα σημαντικό να αφιερωθεί επαρκής χρηματοδότηση για έρευνα προκειμένου να διαπιστωθεί πώς το νέφος εργάζεται – ή όχι – σε διάφορους τομείς αλλά και σε όλα τα επίπεδα προς κυβέρνησης, έτσι ώστε να γίνει καθορισμός των πολιτικών και των πρακτικών που αφορούν την κυβερνητική χρήση του νέφους. Αυτό θα μπορούσε να γίνει με το ανατεθεί σε άτομα να μελετήσουν όλα τα παραπάνω τόσο

σε επιστήμονες της πληροφορικής και της τεχνολογίας όσο και μη όπως στελέχη της υπηρεσίας, επιτελικά στελέχη και νομοθέτες.

- **Βήμα 2^{ο} – Οργανωτική αξιολόγηση (Organizational Assessment):**

Στο δεύτερο βήμα οι επιστήμονες-υπάλληλοι πληροφορικής (IT officers) ή τα κυβερνητικά στελέχη θα πρέπει να προβούν σε αξιολόγηση προς σημερινής προς δομής των υπαρχόντων εγκαταστάσεων IT και να αξιολογήσουν τι περαιτέρω χρειάζεται και να αξιολογήσουν τη δομή, και τη χρησιμοποίηση προς παραγωγικής ικανότητας. Σε ένα περιβάλλον σύννεφου υπολογιστών, είναι απαραίτητη η μελέτη προς απαίτησης προς προσθήκης ή προς μείωσης των πόρων που μπορούν να προστεθούν ή να αφαιρεθούν με βάση προς ανάγκες και τη ζήτηση που μπορούν να προκύψουν.

- **Βήμα 3^{ο} : Προτυποποίηση του σύννεφου (Cloud Prototype):**

Στο τρίτο βήμα οι ειδικοί του IT πρέπει να αναπτύξουν την προτυποποίηση του υπολογιστικού νέφους βασισμένο στις απαιτήσεις του συγκεκριμένου έργου.

- **Βήμα 4ο : Αξιολόγηση του σύννεφου (Cloud Assessment):**

Μετά την εσωτερική και εξωτερική αξιολόγηση που απορρέουν από την πιλοτική προσπάθεια προτυποποίησης, το τμήμα IT πρέπει στη συνέχεια να καθορίσει μια συνολική αξιολόγηση στο σύννεφο προκειμένου να καθορίσει αν ο οργανισμός προς έχει στοιχεία και εφαρμογές που θα μπορούσαν εύκολα να κινηθούν σε ένα περιβάλλον νέφους, και ποιος τύπος του νέφους (δημόσιου / ιδιωτικού / υβριδικό) θα ήταν κατάλληλο-α ή θα μπορούσαν να χρησιμοποιηθούν για τα έργα αυτά. Δεδομένου ότι αυτή η αξιολόγηση εξελίσσεται, οι φορείς λήψης αποφάσεων του IT θα πρέπει να επικεντρωθούν στη θέσπιση κανόνων ως προς την απόφαση την οποία τα δεδομένα και οι εφαρμογές μπορούν – ή δεν μπορούν – να στεγάζονται σε οποιαδήποτε μορφή του σύννεφου. Κάνοντας αυτό το βήμα, θα ανακαλύψουν ένα καθορισμένο πεδίο των σύννεφο-επιλέξιμων (cloud-eligible) και σύννεφο-μη επιλέξιμων (cloud-ineligible) δεδομένων και εφαρμογών.

- **Βήμα 5^{ο} : Στρατηγική υλοποίησης (Cloud Rollout Strategy):**

Σε αυτό το στάδιο, είναι καιρός να λαμβάνουν τροχιά οι πολιτικές και η στρατηγική του νέφους τόσο από οργανωτική ηγεσία και επιτελικά στελέχη όσο και από το IT, και ταυτόχρονα να ξεκινήσει η επικοινωνία τόσο με τους εσωτερικούς όσο και με τους εξωτερικούς ενδιαφερόμενους φορείς ως προς τους στόχους, την πρόοδο, και τα κόστη / οφέλη του έργου. Αυτό το σημείο είναι και το σύνορο που το νέφος από δοκιμαστική προσπάθεια γίνεται υλοποίηση και ενσωματώνεται στο τρόπο που ο κυβερνητικός οργανισμός διαχειρίζεται τα δεδομένα του, τις επιχειρήσεις και το προσωπικό του. Γίνεται δηλαδή πλέον μέρος της κανονικής οργανωτικής λειτουργίας όπως οι λοιπές τεχνολογικές καινοτομίες (πχ από το τηλέφωνο στην τηλεομοιοτυπία-fax κλπ) που χρησιμοποιούνται για την υποστήριξη του οργανισμού.

- **Βήμα 6ο : Διαρκής βελτίωση (Continuous Improvement):**

Το τελευταίο βήμα είναι αυτό που αποκαλούμε «διαρκής βελτίωση» μέχρις ότου έχουμε το πλήρως λειτουργικό σύστημα βασισμένο στην τεχνολογία του υπολογιστικού νέφους με πραγματικά δεδομένα.

3.3. Κατανεμημένα κέντρα δεδομένων

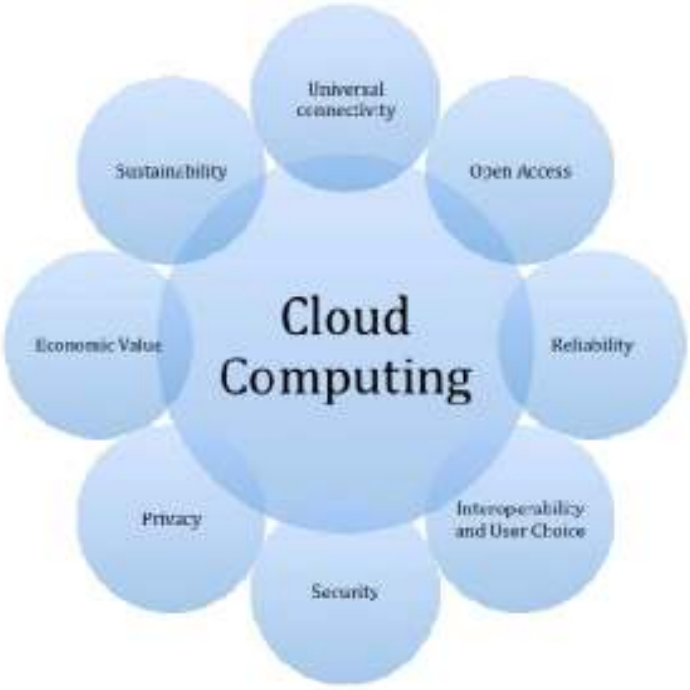
Τα συστήματα πληροφορικής έρχονται αντιμέτωπα με πολλά ρίσκα όπως ιοί, κακόβουλοι (hackers), φωτιά και τρομοκρατικές επιθέσεις. Μερικές τέτοιες καταστροφές μπορεί να έχουν σαν συχνό αποτέλεσμα μια μαζική ολοκληρωτική καταστροφή ή την επακολούθηση παρόμοιων προθέσεων και δραστηριοτήτων, συνεπώς τα κέντρα δεδομένων θα πρέπει να έχουν ανοχή μετά από τέτοιες καταστροφές. Τα κέντρα δεδομένων διευκολύνουν την ισχυρή υποστήριξη επικοινωνίας, τον αυτοέλεγχο και την πραγματική ικανότητα της συνεχούς παρακολούθησης της πλατφόρμας, η οποία θα βοηθήσει την εφαρμογή να τα χρησιμοποιήσει και να ανακάμψει.

Ασφάλεια κοινής χρήσης μπορεί να παρέχεται μέσω αυτών των κέντρων, έτσι ώστε τα κρίσιμα δεδομένα των πολιτών να είναι κάτω από μια ενιαία αρχή που θα παρέχει ασφάλεια ενάντια σε παράνομες δραστηριότητες.

Εικόνα 18 Κατανεμημένα κέντρα δεδομένων

3.4. Απαιτήσεις SLAs και Κατευθυντήριες γραμμές του NIST στο υπολογιστικό νέφος

Στην μετάβαση του e-taxis ως εφαρμογή στο υπολογιστικό νέφος ο NIST για τις υπηρεσίες ηλεκτρονικής διακυβέρνησης θέτει τις κατευθυντήριες γραμμές που πρέπει να εφαρμοστούνε και να τηρούνται σε κάθε υπηρεσία ηλεκτρονικής διακυβέρνησης στο νέφος.



Εικόνα 19 Οχτώ θεμελιώδη συστατικά του νέφους

3.4.1. Κλιμάκωση δεδομένων (data scaling)

Οι βάσεις δεδομένων πρέπει να είναι κλιμακούμενες ούτως ώστε να μπορούν να αντιμετωπίζουν διάφορα προβλήματα όπως φόρτο, διαθεσιμότητα, ανάκαμψη από κάποιο πρόβλημα κλπ αλλά και να αλληλεπιδρούν με το μεγάλο όγκο δεδομένων των εφαρμογών διακυβέρνησης στο χρόνο. Όπου οι σχεσιακές βάσεις δεδομένων ενισχύουν την ακεραιότητα των δεδομένων στα χαμηλότερα επίπεδα τότε *οι βάσεις στο νέφος μπορούν να έχουνε κλιμάκωση με αποτέλεσμα να μπορούν να χρησιμοποιηθούν από τέτοιες εφαρμογές που αποσκοπούν στην ηλεκτρονική διακυβέρνηση.*

3.4.2. Έλεγχος και παρακολούθηση αρχείων (auditing & logging)

Απαιτείται η ύπαρξη μηχανισμών ιχνηλασιμότητας σε οποιαδήποτε αλλαγή περιεχομένου πληροφορίας σε τέτοιες υπηρεσίες. Η διαφθορά σε κυβερνητικούς οργανισμούς μπορεί να ελεγχθεί χρησιμοποιώντας υπηρεσίες τεχνολογιών πληροφορικής και κρατώντας τους παρόχους των υπηρεσιών αυτών υπεύθυνους. Έλεγχοι διαδικασιών (process audits) και έλεγχοι ασφάλειας (security audits) πρέπει να γίνονται περιοδικά προκειμένου να ελέγχεται και να ενισχύεται η αξιοπιστία και η ασφάλεια του συστήματος.

Το υπολογιστικό νέφος από δομής του δίνει την δυνατότητα ανάλυσης μεγάλου όγκου δεδομένων με σκοπό την ανακάλυψη απάτης και δόλου. Μπορεί επίσης να βοηθήσει στην ορθή ανάπτυξη και τοποθέτηση μηχανισμών ασφαλείας τόσο για να ενισχύσει την ασφάλεια όσο και για να κάνει τις υπηρεσίες διαθέσιμες και αξιόπιστες.

3.4.3. Περιπτώσεις αντιγράφων και μετανάστευσης των δεδομένων (replication migration)

Παραδοσιακά οι εφαρμογές στην ηλεκτρονική διακυβέρνηση εργάζονται για διάφορα τμήματα δήμων ή πολιτειών και ως εκ τούτου δικαιούνται να λαμβάνουν περισσότερο χρήμα, πόρους, και μεγαλύτερο περιθώριο χρόνου για την υλοποίηση τους. Αυτό συμβαίνει με όλες τις περιπτώσεις τέτοιων εφαρμογών. Πρέπει να

υπάρχουνε οι δυνατότητες δημιουργία σωστών αντιγράφων η μετανάστευσης δεδομένων από τον ένα δήμο στον άλλο ή από το ένα υπουργεί στο άλλο λόγου χάρη.

Η αρχιτεκτονική του νέφους προσφέρει εξαιρετικές δυνατότητες για την δημιουργία μιας εφαρμογής λόγου χάρη στην εφορία ενός δήμου και ταυτόχρονα να μπορεί να εμφανιστεί χωρίς κόστος και στις λοιπές εφορίες του υπόλοιπου ελλαδικού χώρου.

3.4.4. Σχέδιο ανάκαμψης από καταστροφή (disaster recovery plan)

Φυσικές καταστροφές όπως πλημμύρες, σεισμοί, πόλεμοι, εσωτερικές διαταραχές κλπ μπορούν όχι απλά να βλάψουν μια εφαρμογή ηλεκτρονικής διακυβέρνησης αλλά πολλές φορές να την κάνουν και μη διαθέσιμη. Έτσι λοιπόν πρέπει να υπάρχουνε σε αρκετές και διαφορετικές περιοχές του Ελλαδικού χώρου πλήρη backup και επίσης λύσεις και διαδικασίες επαναφοράς. Επειδή ένα τέτοιο γεγονός θα προκαλούσε τεράστια προβλήματα οι διαδικασίες επαναφοράς και ανάκαμψης θα πρέπει τόσο στον τόπο και όσο και στον χρόνο να δοκιμάζονται στην πράξη τακτικά στο χρόνο ώστε να βελτιώνονται και να είναι αποτελεσματικές. Ο διαθέσιμος αριθμός αντιγράφων των δεδομένων στο νέφος θα πρέπει να είναι περιττός ώστε να είναι δυνατή η άμεση εμφάνιση τους μετά από απαίτηση από κέντρο δεομένων σε κέντρο.

Οι τεχνολογίες εικονικοποίησης του νέφους επιτρέπουν τόσο το backup όσο και την επαναφορά (restoring). Παράλληλα προσφέρει την ομαλή μετανάστευση των δεδομένων σε αντίθεση με τα παραδοσιακά κέντρα δεδομένων.

3.4.5. Απόδοση και επεκτασιμότητα (performance and scalability)

Η αρχιτεκτονική και η τεχνολογία που υιοθετείται για τις πρωτοβουλίες της ηλεκτρονικής διακυβέρνησης πρέπει να είναι επεκτάσιμη και κοινή απέναντι σε τεχνολογίες και διάφορα κανάλια μεταφοράς δεδομένων. Επίσης απαιτείται να γίνει μελέτη και να ανταποκρίνεται στις απαιτήσεις αλλά και τον αυξανόμενο αριθμό χρηστών-πολιτών. Εάν εφαρμόζονταν ποτέ οι πύλες ηλεκτρονικής διακυβέρνησης θα μπορούσαν να γίνουν οι μεγαλύτεροι χρήστες και δικαιούχοι των τεχνολογιών πληροφορικής.

Με τις αρχιτεκτονικές του νέφους η επεκτασιμότητα είναι προφανής. Οι εφαρμογές μπορούν να κλιμακωθούν μέσω της εσωτερικής μετακίνησης τους στο νέφος σε μια

μηχανή με πιο ισχυρούς πόρους και αντίστοιχα να δεσμεύσουν περισσότερη μνήμη χώρο, επεξεργαστική ισχύ κλπ ανάλογα με τις ανάγκες τους.

3.4.6. Αναφορές και ευφυΐα (reporting and intelligence – better governance)

Η χρησιμοποίηση των κέντρων δεδομένων (υπολογιστική ισχύς, δικτυακοί πόροι, αποθηκευτικός χώρος κλπ), φόρτος αιχμής, επίπεδα κατανάλωσης και η χρησιμοποίηση ισχύος σε σχέση πάντα με το χρόνο είναι μερικοί από τους παράγοντες οι οποίοι πρέπει να παρακολουθούνται ενδελεχώς και να γίνεται αναφορά και προσαρμογή ρυθμίσεων για την καλύτερη χρησιμοποίηση όλων αυτών των πόρων. Με αυτή την πολιτική μειώνεται το κόστος και ο σχεδιασμός ενώ και υπάρχει καλύτερη ορατότητα ξεχωριστά σε δεδομένα και τις διάφορες κυβερνητικές υπηρεσίες που προσφέρονται.

3.4.7. Διαχείριση πολιτικών (policy management)

Διαχείριση πολιτικών (Policy management): οι κυβερνητικές εφαρμογές πρέπει να τηρούν και να ενσωματώνουν πολιτικές σύμφωνες με όρους που οι κυβερνήσεις επικοινωνούν με τους πολίτες. Επίσης οι πολιτικές στο επίπεδο υποδομής όσο και στα κέντρα δεδομένων θα πρέπει να προσαρμόζονται μέρα με τη μέρα και πάντα σύμφωνα με τις ανάγκες ανάλογα.

Οι αρχιτεκτονικές του νέφους προσφέρουν πληθώρα επιλογών εφαρμογής πολιτικών στα κέντρα δεδομένων και οι πολιτικές αυτές προσβλέπουν στην ασφάλεια στην ανάπτυξη εφαρμογών κλπ και μπορούν όλες να μαζί να φορμαριστούν και ενδυναμώσουν τα κέντρα δεδομένων.

3.4.8. Ολοκλήρωση συστημάτων και νομιμότητα λογισμικών (Systems Integration and Legacy Software)

Ολοκλήρωση συστημάτων και νομιμότητα λογισμικών (Systems Integration and Legacy Software): Δεν είναι μόνο οι εφαρμογές που έχουν ήδη αναπτυχθεί και

παρέχουν υπηρεσίες που πρόκειται να μεταφερθούν στο σύννεφο, αλλά η ενσωμάτωση τους με εφαρμογές που αναπτύχθηκαν στο σύννεφο. Η δύναμη της τεχνολογίας των πληροφοριών έρχεται σε συνεργασία με τα δεδομένα που αφορούν όλες τις εφαρμογές και τα μηνύματα που περνούν σε διαφορετικά συστήματα να παρέχουν ταχύτερες υπηρεσίες στους τελικούς χρήστες.

Το νέφος είναι δομημένο πάνω στις αρχές του SOA με αποτέλεσμα να μπορεί να παρέχει εξαιρετικές λύσεις στην ενσωμάτωση διάφορων εφαρμογών. Επίσης, οι εφαρμογές μπορούν να μετακινηθούν εύκολα και απρόσκοπτα σε σύννεφο.

3.4.9. Παρωχημένες τεχνολογίες και μετάβαση στις νέες (Obsolete Technologies and Migration to New Technologies)

Παρωχημένες τεχνολογίες και μετάβαση στις νέες (Obsolete Technologies and Migration to New Technologies): η μετάβαση στις νέες τεχνολογίες αποτελεί την μέγιστη πρόκληση. Η μετακίνηση σε νέες εκδόσεις ενός λογισμικού, τα διάφορα πρόσθετα patches ασφάλειας κλπ στις διάφορες εφαρμογές και λογισμικά είναι μερικοί από τους σημαντικότερους παράγοντες για την μετακίνηση και την διασφάλιση των δεδομένων της ηλεκτρονικής διακυβέρνησης σε κέντρα δεδομένων ασφαλή στο νέφος.

Το νέφος προσφέρει ικανές αρχιτεκτονικές για τα παραπάνω και μπορεί να ενεργοποιεί διάφορες απαιτήσεις για ενεργοποίηση ή ταυτόχρονη ύπαρξη διαφορετικών εκδόσεων και ενημερώσεων ενός λογισμικού την ίδια χρονική στιγμή. Έτσι ενώ αυτά τεστάρονται η μετάβαση μπορεί να γίνει ομαλά σε όποια τελικά κριθεί πιο αξιόπιστη και ασφαλής.

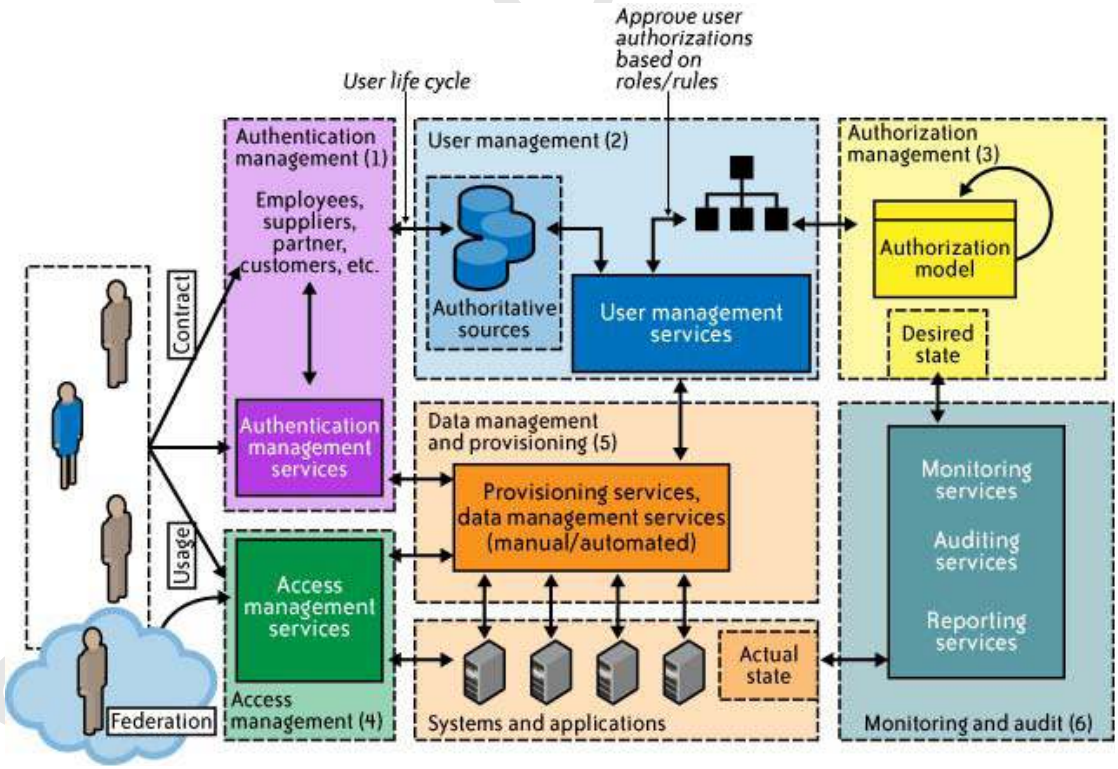
3.4.10. Οικολογική ανάπτυξη πληροφορικής (going green)

Μεγάλη έμφαση δίνεται σήμερα στην οικολογική ανάπτυξη τέτοιων ογκώδων εφαρμογών πληροφορικής που εστιάζεται στα κέντρα διαχείρισης τέτοιων υποδομών. Η χρησιμοποίηση ενέργειας, κλιματισμού και τα ηλεκτρονικά απόβλητα μπορούν να προκαλέσουν βιο-απόβλητα που μπορούν να μειωθούν κατά πολύ με την υποδομή του υπολογιστικού νέφους.

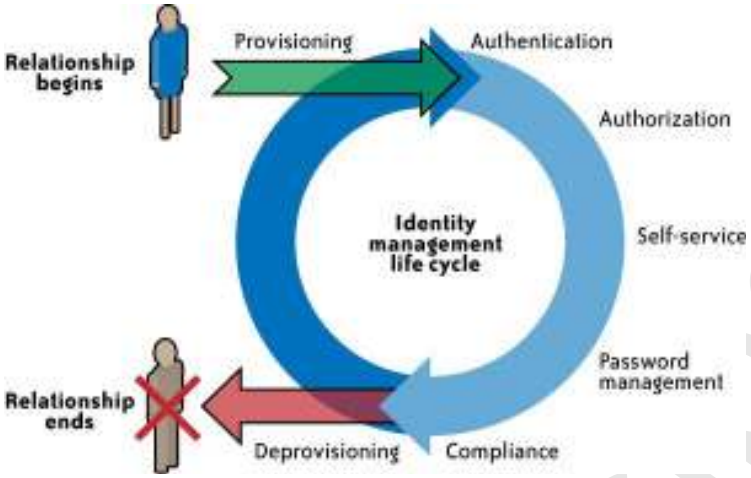
- Τέλος ο ENISA κάνει λόγο για ανησυχίες και κινδύνους που εμπλέκονται στη διαχείριση των δεδομένων σε περιβάλλοντα νέφους όπως είναι η απώλεια διακυβέρνησης, κλείδωμα των δεδομένων, συμμόρφωση με βάση τους κινδύνους, προστασία των δεδομένων από ανασφαλείς ή ημιτελείς-μη διεκπεραιωμένες διεργασίες συστήματος διαγραφής δεδομένων από τα αποθηκευτικά συστήματα και κάνει ειδική αναφορά ότι όλα αυτά πρέπει καλύπτονται και με προσοχή να παρακολουθούνται ενδελεχώς και αενάως πριν ανατεθεί η διαχείριση των δεδομένων (data management) σε τρίτους (outsourcing) παρόχους υπηρεσιών νεφών.

3.4.11. Auditing and monitoring

Η παρακολούθηση και το auditing των χρηστών μπορούν να προκύψουν από τις υπάρχουσες πολιτικές που έχουνε δημιουργηθεί και θα πρέπει πάντα να τηρείται η ορθή πολιτική και ο κύκλος πιστοποίησης των χρηστών.



Εικόνα 20 Αυθεντικοποίηση, πιστοποίηση και παρακολούθηση χρηστών του e-taxis στο νέφος



Εικόνα 21 Κύκλος ζωής διαχείρισης των ταυτοτήτων

Επίσης επειδή οι έλεγχοι κοστίζουν μπορεί ο πάροχος να θεσπίσει όρια και να ασκεί χρεώσεις για αυτά και ανάλογα οι χρήστες να πληρώνουν κατά περίπτωση.

3.4.12. Διαφάνεια (transparency)

Σύμφωνα με τα SLAs ορισμένων παρόχων σύννεφου, οι καταναλωτές φέρουν το βάρος να αποδείξουν ότι ο πάροχος απέτυχε να ανταποκριθεί στους όρους του SLA. Η υπηρεσία ενός παρόχου μπορεί να μην λειτουργεί για ώρες, συνεπώς οι καταναλωτές οι οποίοι αδυνατούν να αποδείξουν το παραπάνω δεν μπορούν να κάνουν λόγο για κανενός είδους αποζημίωση. Για τα κρίσιμα δεδομένα και τις κρίσιμες εφαρμογές οι πάροχοι πρέπει να είναι ενεργοί και να ενημερώνουν τους καταναλωτές όταν όροι του SLA παραβιάζονται.

3.4.13. Πιστοποίηση (certification)

Υπάρχουν πολλές πιστοποιήσεις που πρέπει να εφαρμόζονται σε τέτοιου είδους και εφαρμογές και δεδομένα. Οι καταναλωτές για παράδειγμα πρέπει να είναι ενήμεροι και θα πρέπει να έχουνε και την απαίτηση ο πάροχος του υπολογιστικού νέφους τους να είναι πιστοποιημένος με το ISO 27001. Τέλος ο πάροχος είναι υποχρεωμένος να διατηρεί το πιστοποιητικό κα να ενσωματώνει τις νέες εξελίξεις του.

3.4.14. Μετρικές (metrics)

Η παρακολούθηση και ο έλεγχος απαιτούν κάτι απτό, που μπορεί κάτι να παρακολουθείται καθώς αυτό συμβαίνει και θα μπορεί να ελέγχεται μετά από κάποιο γεγονός. Οι μετρήσεις του SLA πρέπει να είναι αντικειμενικά και επακριβώς καθορισμένες. Στο σύννεφο οι καταναλωτές έχουν μια ατελείωτη ποικιλία των μετρήσεων ανάλογα με την φύση των εφαρμογών και των δεδομένων τους. Όλες οι μετρικές είναι αδύνατο να μπουν σε μια λίστα και έτσι ενδεικτικά παρουσιάζονται οι σημαντικότερες:

- Ρυθμός διεκπεραίωσης (throughput): πόσο γρήγορα ανταποκρίνεται το νέφος
- Αξιοπιστία (reliable): πόσο συχνά είναι διαθέσιμη η υπηρεσία στην υποδομή του νέφους
- Καταμερισμός φόρτου (load balancing): όταν η ελαστικότητα δεν αποδίδει πχ νέα VMs εκκινούνται και άλλα παράλληλα τερματίζουν την λειτουργία τους.
- Ανθεκτικότητα (durability): πόσο πιθανό είναι τα δεδομένα να χαθούν
- Ελαστικότητα (elasticity): η δυνατότητα για ένα συγκεκριμένο πόρο να αυξάνεται στο διηνεκές με όρια πχ το μέγιστο ποσό αποθήκευσης ή εύρους ζώνης που μπορεί να χρησιμοποιηθεί από ένα πόρο
- Γραμμικότητα (linearity): πως ένα σύστημα εκτελείται καθώς ο φόρτος του αυξάνεται
- Ευελιξία (agility): πόσο γρήγορα ανταποκρίνεται ο πάροχος όταν ο καταναλωτής μιας υπηρεσίας κλιμακώνει ή ελαχιστοποιεί την χρησιμοποίηση της
- Αυτοματοποίηση (automation): ποιο είναι το ποσοστό των αιτήσεων στον πάροχο που γίνεται χωρίς την απαίτηση ανθρώπινης αλληλεπίδρασης
- Χρόνος εξυπηρέτησης πελατών: πόσο γρήγορα ανταποκρίνεται ο πάροχος σε μια αίτηση υπηρεσίας. Πρόκειται για τις ανθρώπινες αλληλεπιδράσεις που απαιτούνται όταν πάει κάτι στραβά με τις κατ' απαίτηση αυτοματοποιημένες πτυχές του σύννεφου

3.4.15. Ανάγνωση των SLAs από αυτοματοποιημένες μηχανές

Μια τέτοια αυτοματοποιημένη μηχανή θα ενεργοποιούσε ένα μεσίτη του νέφους (cloud broker) που θα μπορούσε να διαλέξει έναν πάροχο δυναμικά. Ένα από τα χαρακτηριστικά του νέφους είναι οι υπηρεσίες self-service και on-demand που μπορεί και διαχειρίζεται έτσι οι μεσίτες αυτοί του νέφους θα μπορούνε να εξωτερικεύσουν αυτό το χαρακτηριστικό ώστε να διαλέξουν τον κατάλληλο παροχο για την εκτέλεση μιας υπηρεσίας το ίδιο καλά. Για παράδειγμα για κάποιους θα γινόταν επιλογή φθηνότερου παρόχου για την εκτέλεση της υπηρεσίας και για άλλους ένας πιο ασφαλής πάροχος.

3.4.16. Απαιτήσεις SLA στα τρία μοντέλα μεταφοράς του νέφους

Στον ακόλουθο πίνακα γίνεται συγκεντρωτική παραπομπή των απαιτήσεων SLA του υπολογιστικού νέφους στα τρία μοντέλα μεταφοράς με βάση το NIST.

Requirement	Platform as a Service	Infrastructure as a Service	Software as a Service
Data Encryption	✓	✓	
Privacy	✓	✓	✓
Data Retention and Deletion		✓	✓
Hardware Erasure and Destruction		✓	✓
Regulatory Compliance	✓	✓	✓
Transparency	✓	✓	✓
Certification	✓	✓	✓
Terminology for Key Performance Indicators		✓	✓
Metrics	✓	✓	✓
Auditability	✓	✓	✓
Monitoring	✓	✓	✓
Machine-Readable SLAs		✓	

3.4.17. Απαιτήσεις SLA σύμφωνα με τα σενάρια χρήσης κατά περίπτωση

Requirement	End User to Cloud	Enterprise to Cloud to End User	Enterprise to Cloud	Enterprise to Cloud to Enterprise	Private Cloud	Changing Cloud Vendors	Hybrid Cloud
Data Encryption			✓				
Privacy	✓	✓	✓	✓	✓	✓	✓
Data Retention and Deletion			✓	✓			✓
Hardware Erasure and Destruction			✓	✓			✓
Regulatory Compliance	✓	✓	✓	✓	✓	✓	✓
Transparency	✓	✓	✓	✓	✓	✓	✓
Certification	✓	✓	✓	✓	✓		✓
Terminology for Key Performance Indicators			✓	✓	✓	✓	✓
Metrics	✓	✓	✓	✓	✓		✓
Auditability	✓						
Monitoring	✓	✓	✓	✓	✓		✓
Machine-Readable SLAs				✓			

4. ΕΠΙΛΟΓΟΣ – ΜΕΛΛΟΝΤΙΚΗ ΜΕΛΕΤΗ

4.1. Συμπεράσματα - Προβλήματα και προκλήσεις

Το βασικό πρόβλημα και το πρωταρχικό εμπόδιο που πρέπει να ξεπεραστεί για την υιοθέτηση τεχνολογιών νέφους σε εφαρμογές ηλεκτρονικής διακυβέρνησης είναι η ασφάλεια των δεδομένων και των υπηρεσιών. Στην περίπτωση που υιοθετούνται λύσεις public cloud θα πρέπει να δίνονται οι εγγυήσεις μέσω SLAs ότι τα δεδομένα είναι ασφαλή από μη εξουσιοδοτημένη πρόσβαση καθώς και ότι το απόρρητο και η ακεραιότητα τους εξασφαλισμένα. Για παράδειγμα η ασφάλεια και ιδιωτικότητα των δεδομένων μπορεί να εξασφαλιστεί με χρήση κρυπτογράφησης και υποδομές δημοσίου κλειδιού (PKI). Επίσης σε περίπτωση φυσικών καταστροφών ο πάροχος των υπηρεσιών cloud θα πρέπει να έχει λάβει όλα τα απαραίτητα μέτρα π.χ. μέσω διπλοτύπων σε απομακρυσμένα υπολογιστικά κέντρα ώστε η διαθεσιμότητά των δεδομένων να μην επηρεαστεί.

Άλλη παράμετρος που επηρεάζει αρνητικά τέτοιου είδους κυβερνητικές εφαρμογές είναι η τοποθεσία των δεδομένων. Τυπικά σε ένα public cloud, είναι άγνωστο στον τελικό χρήστη που βρίσκονται τα δεδομένα, τα οποία πιθανώς να έχουν αποθηκευθεί σε υπολογιστικά κέντρα εκτός συνόρων. Στην περίπτωση αυτή πιθανώς να ισχύουν διαφορετικοί νόμοι για τη διατήρηση του απορρήτου.

Ένα επιπλέον σημαντικό πρόβλημα αφορά τη μεταφερσιμότητα εφαρμογών δεδομένων και ένα πιθανό εγκλωβισμό σε συγκεκριμένους παρόχους και τεχνολογικές λύσεις (vendor lock-in) λόγω του ότι τα θέματα ασφαλείας ιδιωτικότητας και εμπιστοσύνης παραμένουν ανοιχτά. Θα πρέπει δηλαδή να είναι εξασφαλισμένη η δυνατότητα μεταφοράς των δεδομένων σε διαφορετικούς παρόχους cloud υπηρεσιών. Παρόμοια για εφαρμογές που αναπτύσσονται σε μια PaaS υπηρεσία θα πρέπει να μπορούν να μετεγκατασταθούν σε αντίστοιχη υπηρεσία διαφορετικού φορέα. Για τα παραπάνω η καλύτερη λύση φαίνεται να είναι η υιοθέτηση ανοιχτών προτύπων ανάπτυξης λογισμικού και παροχής cloud υπηρεσιών (όπως π.χ. καθορίζονται από δραστηριότητες όπως το OpenCloud manifesto).

Τέλος ο εν δυνάμει μεγάλος όγκος δεδομένων που παράγουν και εκμεταλλεύονται οι εφαρμογές Ηλεκτρονικής Διακυβέρνησης θα πρέπει να αποθηκεύονται με τις κατάλληλες δομές και να προσφέρονται από υπηρεσίες που διευκολύνουν της γρήγορη αναζήτηση και εντοπισμό δεδομένων (e-discovery).

4.2. Σχέδια δράσης στον Ελλαδικό χώρο άμεσα και μελλοντικά

Μια ασφαλή αλλά ταυτόχρονα αρκετά συντηρητική προσέγγιση για την μεταφορά της ηλεκτρονικής διακυβέρνησης όλων των οργανισμών τοπικής αυτοδιοίκησης, διαφόρων φορέων και υπουργείων στο νέφος είναι σε πρώτη φάση να ξεκινήσει η χρήση του νέφους με σκοπό την φιλοξενία δημόσιων και μη κρίσιμων δεδομένων, έπειτα αξιολόγηση του κατά πόσο κρατικά και ιδιωτικά δεδομένα μπορούν να αποθηκευτούν στο νέφος και τέλος να καταλήξουμε στην ανάπτυξη ιδιωτικής πλατφόρμας (private cloud) και αργότερα ίσως ανάπτυξη και σε δημόσιο νέφος με σκοπό να υπάρχει ασφάλεια και πλήρης έλεγχος αξιοποιώντας πάντα τα προσφερόμενα SLAs.

Όπως και να χει όμως άμεσα θα πρέπει να γίνουν τα παρακάτω:

- Εγκατάσταση λογισμικού διαχείρισης και παροχής εικονικών μηχανών και αποθηκευτικού χώρου ως υπηρεσία στα υπάρχοντα συστήματα για την αυτόματη διαχείρισή και δέσμευση πόρων από τους φορείς του δημοσίου.
- Ανάπτυξη τουλάχιστον δύο μεγάλων υπολογιστικών κέντρων με δυνατότητες ανάκαμψης (disaster recovery) για όλο το Δημόσιο. Οι κεντρικές αυτές υπολογιστικές υποδομές υλικού θα παρέχονται στους φορείς της Δημόσιας Διοίκησης ως οριζόντια υπηρεσία με τεχνολογίες τύπου Infrastructure as a Service (IaaS), Platform as a Service (PaaS) και Software as a Service (SaaS).
- Ο σχεδιασμός των μελλοντικών Πληροφοριακών Συστημάτων και εφαρμογών θα πραγματοποιείται λαμβάνοντας υπόψη τεχνολογίες Cloud Computing όπου υπάρχει ο διαχωρισμός υποδομών υλικού από τις εφαρμογές λογισμικού, αξιοποιώντας, κατά περίπτωση, όπου είναι εφικτό, σχεδιαστικές φιλοσοφίες τύπου Infrastructure as a Service (IaaS), Platform as a Service (PaaS) και Software as a Service (SaaS).

Αφού σχεδιαστούν κριθούν και λειτουργήσουν όλα τα παραπάνω βραχυπρόθεσμα και μελλοντικά θα πρέπει γίνουν:

- Καταγραφή αναγκών των υφιστάμενων εφαρμογών και των υπολογιστικών υποδομών που τις εξυπηρετούν σήμερα. Στο πλαίσιο αυτό

θα πρέπει να δημιουργηθεί ένα δελτίο ανά εφαρμογή το οποίο καλούνται να συμπληρώσουν οι φορείς, ώστε να γίνει πέραν της καταγραφής των χαρακτηριστικών λειτουργίας και των αναγκών των εφαρμογών σήμερα, και μια εκτίμηση των πόρων που θα απαιτηθούν για την λειτουργία των εφαρμογών στο άμεσο μέλλον. Επίσης, θα πρέπει να γίνει έρευνα ανά φορέα στο οποίο θα γίνει η καταγραφή των υφιστάμενων υποδομών φιλοξενίας υπολογιστικών συστημάτων.

- Μνημόνιο συνεργασίας μεταξύ των σημαντικότερων φορέων υποδομών Ηλεκτρονικής Διακυβέρνησης του ευρύτερου δημόσιου τομέα με σκοπό την ανάπτυξη υποδομών νέφους
- Διασύνδεση των μεγαλυτέρων αυτή τη στιγμή υπολογιστικών χώρων που λειτουργούν ως κέντρα δεδομένων (data centers) του δημοσίου (ΚτΠ ΑΕ, ΓΓΠΣ, Υπ. Παιδείας/ΕΔΕΤ) πάνω σε διπλό οπτικό δακτύλιο, και διασύνδεση με το δίκτυο ΣΥΖΕΥΞΙΣ και το δίκτυο σκοτεινής ίνας του ΕΔΕΤ.
- Δημιουργία κοινής διαχειριστικής ομάδας IT από τεχνικά στελέχη των φορέων (ΓΓΠΣ, ΥΠΕΣ, ΚτΠ ΑΕ, ΕΔΕΤ κλπ) η οποία θα είναι υπεύθυνη για την διαχείριση της υποδομής.
- Σταδιακός εξοπλισμός των μεγαλυτέρων υφιστάμενων κέντρων (ΚτΠ ΑΕ, ΓΓΠΣ, Υπ. Παιδείας/ΕΔΕΤ) με εξοπλισμό που προμηθεύονται οι φορείς με τις διαδικασίες τους, με βάση τις προδιαγραφές που απαιτούνται για υπηρεσίες τύπου υπολογιστικού νέφους
- Λειτουργία του παραπάνω εξοπλισμού με λογισμικό εικονηκοποίησης (virtualization) και κατά περίπτωση απόδοση (provisioning) μέσω της ομάδας διαχείρισης, εξυπηρετητών και αποθηκευτικού χώρου ως εικονικών πόρων (VMs) για την εξ' αποστάσεως λειτουργία απλών πληροφοριακών συστημάτων των φορέων πάνω σε εικονικές μηχανές.
- Μεταφορά επιλεγμένων εφαρμογών Ηλεκτρονικής Διακυβέρνησης στην υποδομή του νέφους
- Ανάπτυξη προεγκατεστημένων (precooked) στιγμιότυπων (instances) πρότυπων εφαρμογών και πληροφοριακών συστημάτων ως διαθέσιμες εικονικές μηχανές. Για παράδειγμα ένα απλό σύστημα διαχείρισης περιεχομένου (π.χ. ένα mediawiki) ή μια εφαρμογή ηλεκτρονικού

πρωτοκόλλου θα μπορεί να επιλέγεται για λειτουργία από πολλούς φορείς ταυτόχρονα, δυναμικά κατ΄ απαίτηση (on demand).

4.3. Μελλοντική μελέτη

Κλείνοντας την παρούσα εργασία καταλαβαίνει κανείς πως η υιοθέτηση του υπολογιστικού νέφους στην ηλεκτρονική διακυβέρνηση στην Ελλάδα κρίνεται απαραίτητη και θα πρέπει να υιοθετηθεί σύντομα. Δεν είναι άλλωστε λίγα τα παραδείγματα που άλλες χώρες έχουνε ξεκινήσει την υιοθέτηση τέτοιων τεχνολογιών αιχμής.

Για να εφαρμοστεί η τεχνολογία του υπολογιστικού νέφους στην ηλεκτρονική διακυβέρνηση θα πρέπει παράλληλα με τους μηχανισμούς ασφάλειας και διαφύλαξης της ιδιωτικότητας να θεσπιστεί κανονιστικό πλαίσιο νόμων που θα ενσωματώνει την έννοια του υπολογιστικού νέφους και θα μπορεί να διασφαλίζει την ιδιωτικότητα των δεδομένων των πολιτών σ' αυτό αλλά και των κυβερνητικών οργανισμών.

Σε ερευνητικό επίπεδο χρειάζεται συνεχής βελτίωση όλων των υπαρχόντων μοντέλων και τεχνολογιών του νέφους όπως γίνεται και σε όλες τις ΤΠΕ και επιπρόσθετα θα πρέπει να μελετηθεί και να ερευνηθεί η έννοια της εμπιστοσύνης (trust) στα VMs τα οποία μετά από κάποια επίθεση λόγω χάρη DoS κατέρρευσαν και οι εφαρμογές και οι χρήστες θα είναι σίγουροι για την εμπιστοσύνη που θα έχουνε από την καινούργια τους επιλογή ενός νέου VM στο νέφος. Τέλος το νέφος θα πρέπει να δομηθεί και να αναπτυχθεί έτσι ώστε να δίνεται η δυνατότητα εξιχνίασης ψηφιακών πειστηρίων και θα πρέπει να μελετηθεί που θα πρέπει να εφαρμοστεί κρυπτογραφία στις βάσεις και στα κέντρα δεδομένων ενώ παράλληλα ίσως χρειαζόταν μελέτη βάσεων δεδομένων περισσότερο ανοιχτού κώδικα μιας και στην ηλεκτρονική διακυβέρνηση υπάρχουνε πολλά έγγραφα που για να τοποθετηθούν και να διαχειριστούν εξ ολοκλήρου από μια υποδομή νέφους ηλεκτρονικής διακυβέρνησης ίσως απαιτούσε την επιλογή περισσότερων δυνατοτήτων για την οργάνωση τους που αυτό θα ερχόταν με την επιλογή μιας σχεσιακής βάσης δεδομένων περισσότερο ανοιχτού λογισμικού από την sql για παράδειγμα ενώ επίσης θα πρέπει να μελετηθεί η ανάπτυξη και η βελτιστοποίηση μεθόδων στο νέφος προκειμένου να υπάρχει η δυνατότητας καλύτερης εξέτασης ψηφιακών πειστηρίων (forensics).

5. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]: Cloud computing: a practical approach, Anthony T. Velte, Toby J. Velte, Ph.D., Robert Elsenpeter, ISBN: 978-0-07-162695-8

[2]: Digital forensics for network, internet and cloud computing, ISBN: 978-1-59749-537-0, chapter 12

[3]: Cloud Computing and Information Policy, Paul T. Jaeger, Jimmy Lin, Justin M. Grimes - University of Maryland

[4]: Cyber Crime Scene Investigations (C2SI) through Cloud Computing, Xinwen Fu, Zhen Ling, Wei Yu, Junzhou Luo

[5]: Announcing Elastic IP Addresses and Availability Zones for Amazon EC2". Though announced in March 2009, the Elastic IP service became available October 22, 2008

[6]: An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS, by Simson L. Garfinkel; TR-08-07, Computer Science Group, Harvard University, Cambridge, Massachusetts.

[7]: Instance Addressing and Network Security in the Amazon Elastic Compute Cloud Developer Guide (API Version 2008-12-01)

[8]: Multiple DNS implementations vulnerable to cache poisoning. As of December 31, 2008, the National Vulnerability Database lists 312 vulnerabilities for the DNS protocol and implementations of DNS. The National Vulnerability Database is sponsored by the U.S. Department of Homeland Security's US-CERT, and NIST

[9]: Rumor: Amazon Hit With Denial-of-Service Attack, Again, posted June 6, 2008 at http://www.appscout.com/2008/06/rumor_amazon_hit_with_denialof.php

[10]: http://www.cloud-standards.org

[11]: http://www.itl.nist.gov/fipspubs/.

[12]: Cloud Computing Use Cases, july 2010, http://cloudusecases.org.

[13]: Cloud computing in Australian government, Opportunities and applicability for use by the Australian Government, department of finance and deregulation, January 2011

[14]: Federal Cloud Computing Strategy, Vivek Kundra, U.S. Chief Information Officer, FEBRUARY 2 011, white house, Washington

[15]: E-Government as a Service, Javier Turıgano, Daniel Sanz, Jose Marva Olmo, Carlos Lozano, 2010

[16]: A Model based Approach to Implement Cloud Computing in E-Governance, Dr Ashish Rastogi, Nov 2010

[17]: THE CLOUDY FUTURE OF GOVERNMENT IT: CLOUD COMPUTING AND THE PUBLIC SECTOR AROUND THE WORLD, David C. Wyld, jan 2010

[18]: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Robert Gellman, World Privacy Forum, 2009

[19]: The Playground of Cloud Computing in Turkey, Asli Deniz Helvacioglu Kuyucu

[20]: Secure virtualization for cloud computing, Flavio Lombardi, RobertoDiPietro

[21]: Privacy and consumer risks in cloud computing, Dan Svantesson, Roger Clarke

[22]: Hybrid Computing—Where HPC meets grid and Cloud Computing, Gabriel Mateescu, Wolfgang Gentzsch, Calvin J. Ribbens

[23]: From infrastructure delivery to service management in clouds, Luis Rodero-Merino, Luis M. Vaquero, Victor Gil, Fermín Galán, Javier Fontán, Rubén S. Monteroc, Ignacio M. Llorente

[24]: Identifying the security risks associated with governmental use of cloud computing, Scott Paquette, Paul T. Jaeger, Susan C. Wilson

[25]: Digital evidence in cloud computing systems, M. Taylor, J.Haggerty, D.Gresty, R.Hegarty

[26]: Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks, Ashley Chonka,YangXiang n, WanleiZhou,AlessioBonti

[27]: A survey on security issues in service delivery models of cloud computing, S. Subashini, V.Kavitha

[28]: Eucalyptus cloud computing platform, administrator's guide, Enterprise Edition 2.0, Eucalyptus Systems, 2010