Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Ζητήματα Ασφάλειας και Προστασίας της Ιδιωτικότητας σε Περιβάλλον Νεφοϋπολογιστικής (Security and Privacy in Cloud Computing)

Κωνσταντίνος Ζιούρας

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Μάιος 2013

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ζητήματα Ασφάλειας και Προστασίας της Ιδιωτικότητας σε Περιβάλλον Νεφοϋπολογιστικής (Security and Privacy in Cloud Computing)

Κωνσταντίνος Ζιούρας

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2013

Περίληψη

Στις μέρες μας, η τεχνολογία περιβάλλοντος νεφοϋπολογιστικής αποτελεί ένα νέο υπολογιστικό πρότυπο, που είναι υπό πλήρη άνθηση. Βρισκόμαστε πλέον στην υλοποίηση και ραγδαία ανάπτυξη ενός μοντέλου, όπου η πληροφορική παρέχεται ως υπηρεσία και όχι ως προϊόν, ενώ όλο και περισσότεροι οργανισμοί, εταιρείες και φυσικά πρόσωπα εκμεταλλεύονται τα πλεονεκτήματα της χρήσης του. Έτσι μέσω του διαδικτύου οι τελικοί χρήστες μπορούν να μοιράζονται υπολογιστικούς πόρους, πληροφορίες και λογισμικό. Αποθηκεύουν λοιπόν τα δεδομένα τους σε απομακρυσμένους εξυπηρετητές, που ελέγχονται από άλλους (τους παρόχους) και χρησιμοποιούν εφαρμογές-υπολογιστικούς πόρους που εκτελούνται και βρίσκονται κάπου αλλού και όχι στην ιδιόκτητη υπολογιστική υποδομή τους.

Η παρούσα μεταπτυχιακή διατριβή περιλαμβάνει μια ολοκληρωμένη βιβλιογραφική μελέτη μέσα από την οποία παρουσιάζεται ο ορισμός, η αρχιτεκτονική του «νέφους», τα οφέλη που προκύπτουν από τη χρήση του καθώς και ποικίλα σενάρια χρήσης του. Κατόπιν αφού αναλύονται οι έννοιες της ιδιωτικότητας, των προσωπικών δεδομένων και της ασφάλειας δικτύων, παρουσιάζονται οι κίνδυνοι και τα ζητήματα ασφάλειας που σχετίζονται με τη χρήση του. Κίνδυνοι που πηγάζουν από τη φύση του νέφους και κυρίως από το γεγονός ότι οι χρήστες χάνουν τον έλεγχο των δεδομένων τους και χρησιμοποιούν κοινόχρηστους υπολογιστικούς πόρους.

Ακολουθεί μια «state-of-the-art» αναφορά διαδικασιών, πρακτικών, τεχνικών και ρυθμίσεων ασφάλειας και προστασίας των δεδομένων και της ιδιωτικότητας, ενώ αναφέρονται και εφαρμοσμένες επιλογές που προσφέρουν αυξημένη ασφάλεια.

Η πληθώρα διαθέσιμων τεχνικών και επιλογών μπορεί να αξιολογηθεί μέσα από πλαίσια, που έχουν εκδοθεί από διάφορους οργανισμούς, μέσα από τα οποία ο υποψήφιος πελάτης-χρήστης του νέφους θα μπορεί να προσδιορίσει το επίπεδο ασφαλείας που του παρέχεται κατά περίπτωση, ενώ παρουσιάζονται και συγκεκριμένα βήματα που πρέπει να περιλαμβάνει μία στρατηγική ομαλής μετακίνησης στο νέφος.

Σε κάθε περίπτωση η μετάβαση στο νέφος ενώ φαίνεται όλο και πιο δελεαστική, πρέπει να γίνεται προσεκτικά, μέσα από μία λεπτομερή αξιολόγηση για το πώς το νέφος μπορεί να ταιριάξει και συμβάλλει στη συνολική στρατηγική μιας εταιρείας.

Summary

Nowadays, cloud computing environment is a new computational model, which is in full bloom. We are now in the implementation and rapid development of a model where IT is provided as a service and not as a product, while more and more organizations, companies and individuals exploit the advantages of its use. Through internet, users are able to share computing resources, information, and software. So they store their data on remote servers, which are controlled by others (providers) and they use computing resources-applications that are run and located somewhere else and not on proprietary computational infrastructure.

This thesis includes a comprehensive literature study through which the definition, the architecture of the "cloud", the benefits arising from its use and a variety of use case scenarios are presented. After analyzing the concepts of privacy, personal data and network security, the hazards and safety issues associated with the cloud are described. Risks arising from the nature of the cloud and mainly from the fact that users lose control of their data and use shared computing resources.

A reference of «state-of-the-art» processes, practices, techniques and security settings for data protection and privacy follows. Applied options that offer increased security are also mentioned.

The variety of available techniques and options can be evaluated with the use of frameworks, which have been issued by various organizations, through which the prospective client-cloud user is able to determine the level of security provided. Additionally, the steps of a cloud migration strategy are presented.

In any case, the transition to the cloud even if it seems more and more tempting, it should be done carefully, through a detailed assessment of how cloud computing can fit and contribute to the overall strategy of a company.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Στέφανο Γκρίτζαλη για τη συνεργασία, την καθοδήγηση, τις συμβουλές και τη βοήθεια που μου παρείχε κατά τη διάρκεια εκπόνησης της μεταπτυχιακής διατριβής μου.

Επίσης θα ήθελα να ευχαριστήσω τη σύζυγό μου Αμαλία και τα αγόρια μου Αποστόλη και Δημήτρη (όταν ξεκίνησα ήταν μωράκια και έγιναν παλικαράκια), που με συνόδεψαν με αγάπη, κατανόηση, υποστήριξη και υπομονή σε όλη τη διάρκεια αυτής της πορείας μου.

Περιεχόμενα

1 Εισαγωγή 1

1.1 Τι Είναι Το Νέφος 2

1.2 Βασικά Χαρακτηριστικά 4

1.3 Οφέλη 5

2 Αρχιτεκτονική του νέφους 10

2.1 Τα Μοντέλα Υπηρεσίας 10

2.1.1 Λογισμικό ως Υπηρεσία (Software as a Service (SaaS)) 10

2.1.2 Πλατφόρμα ως Υπηρεσία (Platform as a Service (PaaS)) 11

2.1.2 Υποδομή ως Υπηρεσία (Infrastructure as a Service (IaaS)) 12

2.2 Τα Μοντέλα Ανάπτυξης 13

2.3 Παραδείγματα παρόχων 14

2.4 Σενάρια Χρήσης 16

2.4.1 Θυρίδα Υγείας 16

2.4.2 Εταιρεία Ανάπτυξης Εφαρμογών Ιστού(Web Applications) 17

2.4.3 Λογιστικό Γραφείο 19

3 Ιδιωτικότητα, Δεδομένα, Ασφάλεια Δικτύων, Πρότυπα 21

3.1 Ιδιωτικότητα 21

3.2 Δεδομένα (Data) 23

3.2.1 Προσωπικά Δεδομένα 23

3.2.2 Κύκλος Ζωής των Δεδομένων 24

3.3 Ασφάλεια Δικτύων 25

3.3.1 Εμπιστευτικότητα (Confidentiality) 25

3.3.2 Ακεραιότητα (Integrity) 26

3.3.3 Διαθεσιμότητα (Availability) 26

3.4 Πρότυπα 27

4 Κίνδυνοι και Ζητήματα Ασφάλειας 31

4.1 Τα Δεδομένα Εκτός του Οργανισμού 31

4.1.1 Απώλεια Διακυβέρνησης (Loss Of Governance) 32

4.1.2 Συμμόρφωση στους Κανονισμούς (Regulatory Compliance) 32

4.1.3 Τοποθεσία των δεδομένων (Data Location) 33
4.1.4 Πρόσβαση εκ των έσω ή κατ' εξαίρεση (Insider Access-Privileged User Access) 33
4.1.5 Διαχωρισμός των Δεδομένων (Data Segregation) 34
4.1.6 Προβλήματα Εφαρμογών, Διεπαφών Προγραμματισμού Εφαρμογών (Application Programming Interfaces (APIs)) 35
4.1.7 Επαναφορά (Recovery), Ανάκτηση δεδομένων 36
4.1.8 Μη ολοκληρωμένη διαγραφή δεδομένων(Incomplete data deletion) 36
4.1.9 Υποστήριξη Έρευνας (Investigative support) 37
4.1.10 Βιωσιμότητα σε Βάθος Χρόνου (Long-term Viability) 37
4.1.11 Αξιοπιστία, Διαθεσιμότητα Παρόχου 38
4.2 Θέματα Διαδικτύου 39
4.2.1 Διαθεσιμότητα Διαδικτύου 39
4.2.2 Ασφάλεια Φυλλομετρητή (Browser Security) 39
4.2.3 Επιθέσεις Άρνησης Παροχής Υπηρεσιών (Denial Of Service (D.O.S.) Attacks) 40
4.2.4 Επιθέσεις Ενδιάμεσου (Man in the Middle Attacks) 40
4.2.5 Επιθέσεις Παρακολούθησης Δικτύου (Network Sniffing Attacks) 41
4.2.6 Σάρωση Θυρών (Port scanning) 41
4.2.7 Επίθεση SQL (SQL Injection Attack) 41
4.2.8 Ιοί(Viruses) και Κακόβουλο λογισμικό (Malware) 41
4.3 Θέματα Εικονικοποίησης (Virtualization) 41
4.4 Νομικά Θέματα 42
4.5 Επικινδυνότητα (Risk) 43

5. Ασφάλεια στο Περιβάλλον Νεφοϋπολογιστικής 45
5.1 Διαδικασίες, Πρακτικές 45
5.1.1 Διαβάθμιση της Πληροφορίας 46
5.1.2 Πολιτική Ασφάλειας 47
5.1.3 Αποτελεσματική Διαχείριση Επικινδυνότητας (Risk) 48
5.1.4 Περιβάλλον διαμοιραζόμενης ευθύνης 50
5.1.5 Κύκλος Ζωής Υπαλλήλων 51
5.1.6 Παρακολούθηση (Monitoring) 51
5.1.7 Φυσική Ασφάλεια 52
5.1.8 Διαχείριση Διαμόρφωσης, Αλλαγών 53

5.1.9 Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan) 54
5.1.10 Διατήρηση Αντιγράφων Ασφάλειας 54
5.1.11 Έλεγχοι Ασφάλειας 55
5.1.12 Έλεγχος Πρόσβασης και Επαλήθευση Ταυτότητας 56
5.1.13 Συμφωνητικό Παροχής Υπηρεσιών (Service Level Agreement(SLA)) 57
5.1.14 Κατηγοριοποίηση μισθωτών (tenants) 59
5.2 Τεχνικές Εξασφάλισης Των Δεδομένων 59
5.2.1 Ασφαλή Μεταφορά Δεδομένων 60
5.2.2 Κρυπτογράφηση 61
5.2.3 Ασφάλεια Ταυτότητας (Identity Security) 64
5.2.4 Απόκρυψη, Ασφαλής Διαγραφή Δεδομένων 66
5.3 Ασφάλεια σε Βάθος (Defense in depth) 67
5.3.1 Λειτουργικό Σύστημα, Φυλλομετρητής 67
5.3.2 Ασφάλεια Εφαρμογών, Διεπαφών Προγραμματισμού Εφαρμογών 68
5.3.3 Προστασία από Ιούς , Κακόβουλο λογισμικό 68
5.3.4 Υποδομή δικτύου 69
5.3.5 Εικονικό Ιδιωτικό Νέφος 70
5.4 Ασφάλεια Εικονικοποίησης (Virtualization Security) 70
5.5 Αρχιτεκτονική Έμπιστης Νεφοϋπολογιστικής (Trusted Cloud Computing) 73
5.6 Η Λύση του Υβριδικού Νέφους (Hybrid Cloud) 74

6 Πλαίσιο Αξιολόγησης Ασφάλειας 76
6.1 Διαθέσιμες Εργασίες 76
6.2 Προτεινόμενα Βήματα 80
6.2.1 Προκαταρκτικές ενέργειες 80
6.2.2 Δοκιμαστική Χρήση-Σταδιακή Μετάπτωση 81

7 Συμπεράσματα 82

Βιβλιογραφία 85

Παράρτημα Α A-1

Παράρτημα Β B-1

Κεφάλαιο 1
Εισαγωγή

Η τεχνολογία περιβάλλοντος νεφοϋπολογιστικής ή υπολογιστικής νέφους(Cloud Computing) αποτελεί ένα νέο υπολογιστικό πρότυπο, που είναι υπό πλήρη άνθηση. Βασίζεται στην χρήση του διαδικτύου. Οι τελικοί χρήστες, μέσω ενός φυλλομετρητή ιστοσελίδων(Web Browser), έχουν πρόσβαση στις υπηρεσίες που προσφέρονται από το νέφος και ουσιαστικά μπορούν να μοιράζονται υπολογιστικούς πόρους, πληροφορίες και λογισμικό. Αντίστοιχα και οι εταιρείες, οργανισμοί μπορούν να εκμεταλλεύονται τις παροχές του μοντέλου, μέσω της εξωτερικής ανάθεσης υπηρεσιών (Public Cloud Outsourcing), με σημαντικά χαμηλότερο κόστος από το κόστος που θα απαιτούνταν για την ανάπτυξη ιδιόκτητων υπολογιστικών υποδομών, που να υποστηρίζουν αντίστοιχες παροχές.

Στο πρώτο κεφάλαιο περιγράφεται τι είναι το νέφος, ποια είναι τα βασικά χαρακτηριστικά του και ποια είναι τα οφέλη από τη χρήση του.

1.1 Τι Είναι Το Νέφος

Η ιδέα της νεφοϋπολογιστικής δεν είναι νέα στη ραγδαίως αναπτυσσόμενη τεχνολογία της πληροφορικής. Το 1961 ο John McCarthy, πρωτοπόρος της επιστήμης των υπολογιστών, πρόβλεψε ότι κάποια μέρα η υπολογιστική ισχύς θα παρέχεται ως δημόσια υπηρεσία, όπως παρέχεται το νερό και ο ηλεκτρισμός[081]. Την εποχή εκείνη, η υλοποίηση του οράματος του McCarthy δεν ήταν εφικτή, λόγω της έλλειψης των φυσικών υποδομών που απαιτούνται για την υλοποίηση του νέφους.

Με την πρόοδο όμως της επιστήμης της πληροφορικής και την ανάπτυξη του διαδικτύου βρισκόμαστε πλέον στην υλοποίηση και ραγδαία ανάπτυξη του μοντέλου, όπου η πληροφορική παρέχεται ως υπηρεσία και όχι ως προϊόν, στο μοντέλο δηλαδή του νέφους.

Γενικά η υπολογιστική νέφους είναι η μετάβαση από ιδιόκτητους σε κοινόχρηστους πόρους, όπου οι πελάτες-χρήστες λαμβάνουν υπηρεσίες πληροφορικής κατ' απαίτηση, από τρίτους που παρέχουν τις υπηρεσίες αυτές μέσω του διαδικτύου[033].

Σύμφωνα με τον M. Armbrust [007] ο όρος της υπολογιστικής νέφους αναφέρεται τόσο στις εφαρμογές που παρέχονται ως υπηρεσίες από το διαδίκτυο, όσο και στο υλικό (Hardware) αλλά και λογισμικό (Software) που απαιτείται στα κέντρα δεδομένων(Datacenters) για την παροχή των ανωτέρω υπηρεσιών .

Τα βασικά συστατικά του νέφους είναι τα ακόλουθα [081,041]:

1. Ο Πάροχος Υπηρεσιών Νέφους (Cloud Service Provider): Είναι η οντότητα που έχει στην ιδιοκτησία της και διαχειρίζεται την υποδομή που απαιτείται για τη λειτουργία του νέφους.

2. Ο Πελάτης/κάτοχος (Clients/Owner): Είναι η οντότητα που έχει αρχεία δεδομένων, τα αποθηκεύει στο νέφος και βασίζεται σε αυτό για τη διατήρησή τους, αλλά και χρησιμοποιεί τους υπολογιστικούς πόρους του νέφους για την επεξεργασία τους. Μπορεί να είναι είτε ιδιώτης είτε οργανισμός.

3. Ο Χρήστης (User): Είναι μία μονάδα η οποία είναι καταχωρημένη από τον κάτοχο και μπορεί να χρησιμοποιήσει τα δεδομένα του κατόχου που είναι αποθηκευμένα στο νέφος. Ο χρήστης μπορεί να είναι και ο ίδιος κάτοχος.

Οι απαιτήσεις των Πελατών/Χρηστών για τη λειτουργία σε περιβάλλον νέφους είναι οι ίδιες με αυτές που απαιτούνται για τη λειτουργία σε ένα Τοπικό Δίκτυο Περιοχής (Local Area Network (LAN)). Μπορούν να χρησιμοποιούν Η/Υ φορητούς ή γραφείου ή τύπου ταμπλέτας ή και άλλες φορητές συσκευές (όπως κινητά τηλέφωνα) για να έχουν πρόσβαση στα δεδομένα ή τις υπηρεσίες του διαδικτύου.

4. Το κέντρο δεδομένων(Datacenter): Το κέντρο δεδομένων είναι ένα σύνολο από εξυπηρετητές (servers), όπου φιλοξενούνται οι απαιτούμενες εφαρμογές. Η νέα αυξανόμενη τάση είναι η χρήση τεχνικών εικονικοποίησης (virtualization), με τις οποίες επιτυγχάνεται η δημιουργία πολλών εικονικών εξυπηρετητών σε ένα μόνο πραγματικό-φυσικό εξυπηρετητή. Ο αριθμός των εικονικών εξυπηρετητών που μπορούν να στηθούν σε ένα πραγματικό εξαρτάται από το μέγεθος και την ταχύτητά του, όπως και από τη φύση των εφαρμογών που θα τρέχουν στους εικονικούς εξυπηρετητές.

5. Οι Κατανεμημένοι Εξυπηρετητές (Distributed servers): Η δομή του νέφους επιτρέπει στους παρόχους να αναπτύσσουν τους φυσικούς τους εξυπηρετητές σε διαφορετικές γεωγραφικές περιοχές, χωρίς να επηρεάζεται η αλληλεπίδραση του νέφους με τους χρήστες –πελάτες. Αυξάνεται έτσι η ευελιξία και οι επιλογές ασφάλειας από την πλευρά του παρόχου. Έτσι για παράδειγμα, στην περίπτωση αστοχίας ενός κέντρου δεδομένων οι υπηρεσίες μπορούν να είναι διαθέσιμες από έναν άλλο κατανεμημένο εξυπηρετητή. Επίσης, σε περίπτωση που οι πόροι ενός κέντρου δεδομένων εξαντληθούν από αυξανόμενη ζήτηση, δεν απαιτείται η προμήθεια επιπλέον πόρων στο συγκεκριμένο κέντρο, αλλά αρκεί η ρύθμιση κάποιου άλλου συνόλου από κατανεμημένους ελεύθερους εξυπηρετητές, το οποίο μέσω του νέφους μπορεί να «ενσωματωθεί» με το κορεσμένο κέντρο δεδομένων.

Το National Institute of Standards and Technology (NIST)[055] έχει δώσει τον ακόλουθο ορισμό για το νέφος: «η υπολογιστική νέφους είναι το σύγχρονο μοντέλο που επιτρέπει εύκολη πρόσβαση, από παντού και κατ' απαίτηση σε ένα διαμοιραζόμενο, άμεσα διαθέσιμο και διαμορφούμενο σύνολο υπολογιστικών πόρων (πχ δίκτυα, εξυπηρετητές, αποθηκευτικός χώρος, εφαρμογές, υπηρεσίες) το οποίο σύνολο μπορεί ταχύτατα να διαμορφωθεί και να προσφερθεί μέσα από αυτοματοποιημένες διαδικασίες με ελάχιστες διαχειριστικές ενέργειες ή διαμεσολάβηση από τον πάροχο» .

1.2 Βασικά Χαρακτηριστικά

Στον ορισμό του NIST [055] περιλαμβάνονται τα ακόλουθα 5 βασικά χαρακτηριστικά του νέφους:

1. Κατ' απαίτηση αυτοεξυπηρέτηση (On-demand self-service): Ένας καταναλωτής μπορεί να δεσμεύσει από μόνος του τους υπολογιστικούς πόρους που χρειάζεται, όπως χρόνο στον εξυπηρετητή και αποθηκευτικό χώρο στο δίκτυο, ανάλογα με τις ανάγκες του αυτόματα, χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με το φορέα παροχής κάθε υπηρεσίας.

2. Ευρεία πρόσβαση στο δίκτυο (Broad network access): Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών, που προωθούν την χρήση από ετερογενείς συσκευές μειωμένων(thin client) ή αυξημένων επεξεργαστικών δυνατοτήτων (thick client) (για παράδειγμα κινητά τηλέφωνα, φορητούς Η/Υ και σταθμούς εργασίας).

3. Κοινή διάθεση πόρων (Resource pooling): Οι υπολογιστικοί πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλαπλούς καταναλωτές με τη χρήση του μοντέλου πολλαπλών μισθωτών (multi-tenant), με τους διάφορους φυσικούς και εικονικούς πόρους να ανατίθενται συνεχώς δυναμικά, ανάλογα με τη ζήτηση των καταναλωτών. Υπάρχει μια αίσθηση ανεξαρτησίας από τον τόπο, καθώς ο πελάτης γενικά δεν έχει έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να είναι σε θέση να προσδιορίζει την τοποθεσία σε ένα υψηλότερο αφαιρετικά επίπεδο (π.χ. χώρα, κράτος, ή κέντρο δεδομένων). Παραδείγματα πόρων αποτελούν οι αποθηκευτικοί χώροι, η επεξεργαστική ισχύς, η μνήμη, και το εύρος (bandwidth) του δικτύου.

4. Ταχεία ελαστικότητα (Rapid elasticity): Οι δυνατότητες μπορούν να δεσμευτούν-αποδεσμευτούν ελαστικά, σε ορισμένες περιπτώσεις αυτόματα, έτσι ώστε να κλιμακωθούν ταχέως προς τα πάνω ή προς τα κάτω αναλόγως της ζήτησης. Για τον καταναλωτή, οι διαθέσιμες δυνατότητες για δέσμευση – χρήση φαίνεται συχνά να είναι απεριόριστες και μπορούν να αγοραστούν σε οποιαδήποτε ποσότητα ανά πάσα στιγμή.

5. Μετρήσιμες υπηρεσίες (Measured services): Τα συστήματα του νέφους ελέγχουν και βελτιστοποιούν αυτόματα τη χρήση των πόρων, αξιοποιώντας δυνατότητες μέτρησης (στη βάση της πληρωμής- χρέωσης αναλόγως χρήσης) σε κάποιο επίπεδο αφαίρεσης κατάλληλο

για το είδος της υπηρεσίας (π.χ. αποθήκευση, επεξεργασία, εύρος, ενεργοί λογαριασμοί χρηστών). Η χρήση των πόρων μπορεί να παρακολουθείται, να ελέγχεται, και να παρουσιάζεται με τη μορφή αναφορών (reports), παρέχοντας διαφάνεια τόσο για τον πάροχο όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας.

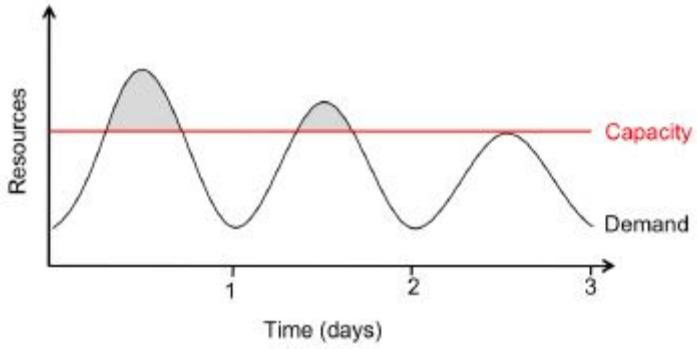
1.3 Οφέλη

Τα τελευταία χρόνια η ραγδαία ανάπτυξη της τεχνολογίας της επιστήμης της πληροφορικής, η ευκολία πρόσβασης στο διαδίκτυο καθώς και η αξιοποίηση των υπηρεσιών που προσφέρονται μέσω αυτού, τόσο από απλούς χρήστες, όσο και από εταιρίες-οργανισμούς έχουν αυξήσει σημαντικά τις ανάγκες σε τεχνολογικές υποδομές και υπολογιστικούς πόρους. Η προμήθεια της αντίστοιχης υποδομής συνεπάγεται κόστος για την αγορά, την εγκατάσταση, την λειτουργία και την συντήρησή της.

Επίσης λόγω του ρυθμού της ανάπτυξης της τεχνολογίας, παρατηρείται το γεγονός μέρος της υποδομής (πχ εξυπηρετητές) να θεωρείται παρωχημένο σε σχετικά μικρό χρονικό διάστημα, είτε λόγω ξεπερασμένων επιδόσεων είτε λόγω ασυμβατότητας με τις πιο πρόσφατες τεχνολογίες και εφαρμογές.

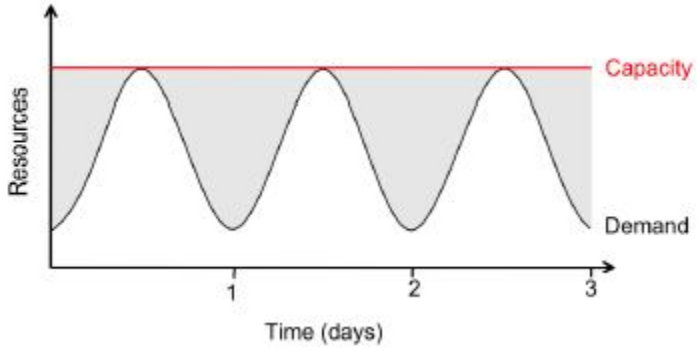
Επιπλέον ζητήματα που πρέπει να εξεταστούν είναι κατά πόσο η υφιστάμενη υπολογιστική υποδομή μίας εταιρείας μπορεί να ανταπεξέλθει σε περιόδους εποχικής αύξησης της ζήτησης μιας νέας, για παράδειγμα, ψηφιακής υπηρεσίας και κατά πόσο η ικανοποίηση της αυξημένης αυτής εποχικής ζήτησης απαιτεί υποδομές, οι οποίες όμως υποαπασχολούνται την υπόλοιπη διάρκεια μειωμένης ζήτησης.

Στην εικόνα 1.1 παρουσιάζεται ένα παράδειγμα όπου φαίνεται ότι η χωρητικότητα της υποδομής δεν καλύπτει τις απαιτήσεις κορύφωσης της ζήτησης (η γκρι περιοχή παρουσιάζει τη μη καλυπτόμενη ζήτηση), η οποία σταδιακά μειώνεται (με αποτέλεσμα να χάνονται πελάτες) στα επίπεδα της χωρητικότητας[007].



Εικόνα 1.1: Χωρητικότητα υποδομής που δεν αρκεί να καλύψει την κορύφωση της ζήτησης που βαίνει μειούμενη [007].

Στην εικόνα 1.2 παρουσιάζεται ένα παράδειγμα όπου φαίνεται ότι η χωρητικότητα έχει υπολογιστεί σωστά και καλύπτει τις απαιτήσεις κορύφωσης της ζήτησης, συνεπάγεται όμως σπατάλη (γκρι χρώμα) των υποδομών στις περιόδους χαμηλότερης ζήτησης[007].



Εικόνα 1.2: Υποδομή με χωρητικότητα που αρκεί να καλύψει την κορύφωση της ζήτησης, αλλά μεγάλο τμήμα της μένει για διαστήματα ανεκμετάλλευτο[007].

Τα παραπάνω ζητήματα έρχεται να καλύψει η υπολογιστική νέφους. Ουσιαστικά μέσω του νέφους αλλάζουν οι προοπτικές της πληροφορικής, καθώς δίνεται πλέον σε ιδιώτες, φυσικά πρόσωπα όπως και σε μικρές ή και μεσαίες επιχειρήσεις, πρόσβαση σε μια σειρά από υποδομές και ισχυρές εφαρμογές μέσω του διαδικτύου, οι οποίες μέχρι τώρα ήταν διαθέσιμες μόνο σε μεγάλες επιχειρήσεις και οργανισμούς. Μπορούν δηλαδή οι μικρές επιχειρήσεις να γίνουν ανταγωνιστικές απλά «νοικιάζοντας» ακριβές υποδομές, αντί να επενδύουν στην αγορά τους (με πολλές φορές απαγορευτικό κόστος γι' αυτές)[015].

Έτσι για παράδειγμα, κάποιος που αναπτύσσει εφαρμογές βασιζόμενος σε καινοτόμες ιδέες για παροχή νέων διαδικτυακών υπηρεσιών δεν απαιτείται να καλύψει δαπάνες για την προμήθεια

και λειτουργία υπολογιστικής υποδομής (τέτοιο παράδειγμα αναλύεται περισσότερο στο κεφάλαιο 2). Εξαλείφεται επίσης και το ρίσκο της λανθασμένης πρόβλεψης, που μπορεί να οδηγήσει είτε σε σπατάλη χρημάτων λόγω δέσμευσης περισσότερων πόρων (over provisioning) για μία υπηρεσία της οποίας η δημοτικότητα δεν ήταν η αναμενόμενη, είτε σε απώλεια πελατών και δυσφήμιση της εταιρείας, λόγω δέσμευσης λιγότερων πόρων (under provisioning) για μία εφαρμογή που έτυχε ευρείας αποδοχής αλλά οι πόροι δεν μπόρεσαν να την υποστηρίξουν[016]. Και αυτό διότι μέσω του νέφους επιτυγχάνεται ευελιξία ως προς την επεκτασιμότητα και την προσαρμογή των δεσμευμένων πόρων στις ανάγκες του πληροφοριακού συστήματος που καλείται να εξυπηρετήσει, με δυναμικό τρόπο.

Ακόμα και εταιρείες με μεγάλες υπολογιστικές απαιτήσεις δέσμης μπορούν να πάρουν γρήγορα αποτελέσματα, αφού τα προγράμματά τους μπορούν να κλιμακωθούν χρησιμοποιώντας για παράδειγμα 1000 εξυπηρετητές για μία ώρα, με το ίδιο κόστος χρήσης ενός εξυπηρετητή για 1000 ώρες. Η ελαστικότητα αυτή της διάθεσης των πόρων χωρίς να απαιτείται προκαταβολή πληρωμής για απαιτήσεις μεγάλης κλίμακας είναι πρωτοφανής στην ιστορία της πληροφορικής[006].

Αλλά και για τις μεγάλες επιχειρήσεις ή το δημόσιο τομέα, το νέφος προσφέρει επίσης σημαντικά πλεονεκτήματα, όπως η ομοιογένεια των εφαρμογών για την εύκολη ανταλλαγή δεδομένων μεταξύ των υπηρεσιών, η αδιάλειπτη διαθεσιμότητα αποθηκευτικού χώρου. Σε κάθε περίπτωση το νέφος αφορά όλες τις επιχειρήσεις, ανεξάρτητα από το μέγεθος ή τη δραστηριότητά τους, τις κυβερνήσεις αλλά και οποιονδήποτε χρησιμοποιεί τις νέες τεχνολογίες[106].

Η εταιρεία «Context Information Security Ltd»[020] επισημαίνει τα ακόλουθα τέσσερα οφέλη:

- Ταχύτερη υλοποίηση: Είναι χαρακτηριστική η ευκολία και η ταχύτητα με την οποία οι χρήστες και οργανισμοί μπορούν να βρουν λύσεις έτοιμες στο νέφος. Σε σύγκριση με τις διαδικασίες και το χρόνο που απαιτείται στηθούν αντίστοιχες λύσεις εσωτερικά με ιδιόκτητη υποδομή, οι υλοποιήσεις που βασίζονται στο νέφος μπορούν να υλοποιηθούν σχετικά πιο γρήγορα. Επιταχύνεται έτσι ο χρόνος που απαιτείται για να εμφανιστούν νέες υπηρεσίες είτε στην αγορά, είτε για εσωτερική χρήση. Επιπλέον, η ταχύτερη υλοποίηση αφορά και στην ταχύτητα με την οποία μπορούν να ολοκληρωθούν έλεγχοι, δοκιμές που απαιτούν μεγάλη υπολογιστική ισχύ. Καθώς παρέχεται η δυνατότητα ταυτόχρονης δέσμευσης πολλαπλών εξυπηρετητών, όπως προαναφέρθηκε, μπορούν να επιταχυνθούν τα αποτελέσματα ή τα στάδια ανάπτυξης λογισμικού[073]

- Χαμηλότερο κόστος: Όπως αναφέρθηκε, για τις καινούργιες και μικρές επιχειρήσεις οι λύσεις που προσφέρει η υπολογιστική νέφους μπορεί να είναι αρκετά φτηνότερες από την ανάπτυξη συστημάτων και υπηρεσιών εσωτερικά. Η κατ' απαίτηση φύση του νέφους είναι τέτοια ώστε οι χρήστες να πληρώνουν μόνο για τις υπηρεσίες που χρειάζονται, όταν τις χρειάζονται. Επίσης κέρδη μπορούν να προκύψουν από την έλλειψη εξόδων συντήρησης εξοπλισμού και λογισμικού. Από την πλευρά του λογισμικού, κέρδη μπορούν να προκύψουν καθώς πλέον δεν υφίσταται η ανάγκη για αγορά μόνιμων αδειών χρήσης, αλλά αρκεί η αγορά συνδρομής από τον πάροχο[010].

- Ασφάλεια: Πολλά έχουν αναφερθεί για τα ζητήματα ασφάλειας που μπορούν να προκύψουν από τη χρήση του νέφους, τα οποία θα αναλυθούν και στην παρούσα μεταπτυχιακή διατριβή. Παρ' όλα αυτά όμως, για πολλές μικρές ή μεσαίες επιχειρήσεις, οι οποίες δε διαθέτουν την απαραίτητη τεχνογνωσία ή την υποδομή ασφάλειας, η μετακίνηση στο νέφος μπορεί να συνεπάγεται ενισχυμένη ασφάλεια. Οι υποδομές μεγάλης κλίμακας που χρησιμοποιούνται στο νέφος συνεπάγονται οφέλη στην ασφάλεια, που προκύπτουν από το εξειδικευμένο προσωπικό, τις μεγάλες δυνατότητες τις υποδομής (που εγγυάται και μεγάλη διαθεσιμότητα), τις διαδικασίες δημιουργίας αντιγράφων ασφάλειας και τη συγκέντρωση των δεδομένων σε μεγάλα κέντρα δεδομένων που παρέχουν μεγάλη φυσική ασφάλεια[056].

- Συγκριτική αξιολόγηση(benchmarking): Ένα ακόμη όφελος από τη μετάβαση στο νέφος είναι η δυνατότητα συγκριτικής αξιολόγησης των εσωτερικών παρόχων με τους παρόχους υπηρεσιών νέφους. Συγκρίνοντας τα εσωτερικά επίπεδα υπηρεσιών με αυτά των παρόχων οι χρήστες, οργανισμοί μπορούν να αναγνωρίσουν περιοχές που οι εσωτερικές υπηρεσίες επιδέχονται βελτίωσης. Από την άλλη, μπορεί και να εντοπιστούν υπηρεσίες που παρέχονται καλύτερα εσωτερικά απ' ότι μπορούν να αποκτηθούν από το νέφος.

Εκτός από τα παραπάνω, η χρήση του νέφους βοηθάει σημαντικά στην προσήλωση μιας εταιρείας στο κυρίως έργο της. Καθώς η ευθύνη για ανάπτυξη, έλεγχο και λειτουργία τόσο των υποδομών αλλά και του λογισμικού ανατίθεται πλέον στον πάροχο του νέφους, το προσωπικό της εταιρείας μπορεί να απαλλαχτεί από το βάρος αυτής της εργασίας και να εστιάσει, αφιερώσει το χρόνο του σε στρατηγικές και δραστηριότητες που σχετίζονται με το κυρίως έργο της εταιρείας και μπορούν να αυξήσουν την αξία της[010].

Όσο αφορά τις ελληνικές επιχειρήσεις, από μελέτη του ΙΟΒΕ σχετικά με την επίδραση του νέφους στην ελληνική οικονομία, το συνολικό όφελος για την Ελλάδα εκτιμάται ότι μπορεί να

φτάσει μέχρι και τα 21 δισ. ευρώ, συμβάλλοντας στη δημιουργία 38.000 θέσεων εργασίας. Μόνο από τη συγκέντρωση των δαπανών τεχνολογίας πληροφορικής για εξοπλισμό, τεχνογνωσία και ενέργεια, το νέφος μπορεί να αποφέρει στην εγχώρια οικονομία εξοικονόμηση κόστους ύψους 4,8 δισ. ευρώ κατά την επόμενη δεκαετία. Επιπρόσθετα, μέσω της αυξημένης επεκτασιμότητας των οικονομικών δραστηριοτήτων και την εξάλειψη των φραγμών για την είσοδο σε νέες αγορές το νέφος μπορεί να αποφέρει πρόσθετο όφελος στην οικονομία, ύψους 5 δισ. Ευρώ[013, 106].

Πέρα από τα οφέλη των επιχειρήσεων, το υπολογιστικό νέφος μπορεί να συμβάλει και στην προστασία του περιβάλλοντος. Η ραγδαία ανάπτυξη των υπολογιστών τους μετέτρεψε σε μια από τις ταχύτερα αναπτυσσόμενες πηγές εκπομπής διοξειδίου του άνθρακα. Ταυτόχρονα, το υπολογιστικό νέφος είναι ο καλύτερος τρόπος για τη βελτίωση της ενεργειακής απόδοσης και τη μείωση των περιβαλλοντικών οχλήσεων λόγω των εκπομπών άνθρακα στον εν λόγω κλάδο. Αυτό οφείλεται στο γεγονός ότι μεγάλες επενδύσεις που σχετίζονται με το υπολογιστικό νέφος μπορούν να προγραμματιστούν με εξυπηρετητές χαμηλής ενεργειακής κατανάλωσης και με βάση πράσινες πηγές ενέργειας, πολύ πιο εύκολα απ' ότι να εξασφαλιστεί ότι εκατοντάδες εκατομμύρια χρήστες ηλεκτρονικών υπολογιστών θα κάνουν επιλογές φιλικές για το περιβάλλον. Επιπλέον, η χρήση του υλικού μπορεί να βελτιστοποιηθεί μειώνοντας τον αριθμό των φυσικών μηχανών που απαιτούνται για να εκτελεσθεί συγκεκριμένη αλληλουχία εργασιών[097].

Μάλιστα, η Ευρωπαϊκή Επιτροπή χρηματοδοτεί ένα ερευνητικό έργο (το Eurocloud Server Project) του οποίου τα πρώτα αποτελέσματα καταδεικνύουν ότι θα ήταν δυνατόν να μειωθεί κατά 90% η χρησιμοποιούμενη ενέργεια στα κέντρα δεδομένων του υπολογιστικού νέφους και ότι αυτό θα αποτελέσει επιπλέον βελτίωση πέραν της ήδη επιτευχθείσας εξοικονόμησης, με την στροφή από τις λύσεις τύπου απομονωμένων σταθμών εργασίας και εξυπηρετητών σε λύσεις που να βασίζονται στο υπολογιστικό νέφος[097].

Κεφάλαιο 2
Αρχιτεκτονική του νέφους

Στο κεφάλαιο αυτό περιγράφονται τα είδη των υπηρεσιών, τα μοντέλα ανάπτυξης, παραδείγματα παρόχων και σενάρια χρήσης του νέφους.

2.1 Τα Μοντέλα Υπηρεσίας

Το NIST [055] έχει χωρίσει τα είδη των υπηρεσιών που παρέχονται στα ακόλουθα τρία μοντέλα.

2.1.1 Λογισμικό ως Υπηρεσία (Software as a Service (SaaS))

Η δυνατότητα που παρέχεται στον χρήστη είναι να χρησιμοποιήσει εφαρμογές που έχουν δημιουργηθεί από τον πάροχο και εκτελούνται στην υποδομή του νέφους (ο όρος υποδομή αναφέρεται τόσο στο λογισμικό όσο και υλικό που επιτρέπει τη λειτουργία του νέφους, εξασφαλίζοντας τα πέντε βασικά χαρακτηριστικά του που αναφέρθηκαν στην παράγραφο 1.2). Οι εφαρμογές είναι προσβάσιμες από διάφορες συσκευές των πελατών είτε με τη χρήση συσκευών μειωμένων επεξεργαστικών δυνατοτήτων μέσω ενός φυλλομετρητή ιστοσελίδων(π.χ. το WEB ηλεκτρονικό ταχυδρομείο), είτε μέσω ειδικής διεπαφής(interface) ενός προγράμματος. Ο χρήστης δεν διαχειρίζεται ή ελέγχει την υποδομή του νέφους που

περιλαμβάνει τα δίκτυα, τους εξυπηρετητές, τα λειτουργικά συστήματα, την υποδομή αποθήκευσης δεδομένων (storage), ούτε ακόμη και τις δυνατότητες τις κάθε εφαρμογής που χρησιμοποιεί. Συνήθως μπορεί απλά να εξατομικεύσει κάποιες ρυθμίσεις της εφαρμογής.

Ο M. Sharma κ.α. [071] αναφέρουν τα βασικά χαρακτηριστικά του SaaS:

1. Πρόσβαση σε εμπορικό λογισμικό μέσω διαδικτύου.

2. Το λογισμικό διαχειρίζεται από μία κεντρική τοποθεσία.

3. Το λογισμικό παρέχεται συνήθως με μοντέλο «από έναν σε πολλούς».

4. Οι χρήστες δεν απαιτείται να χειρίζονται αναβαθμίσεις και ενημερώσεις του λογισμικού.

5. Για την ολοκλήρωση, ενσωμάτωση των διαφορετικών τμημάτων του λογισμικού χρησιμοποιούνται Διεπαφές Προγραμματισμού Εφαρμογών (Application Programming Interfaces (APIs)).

2.1.2 Πλατφόρμα ως Υπηρεσία (Platform as a Service (PaaS))

Η δυνατότητα που παρέχεται στο χρήστη είναι να εγκαταστήσει στην υποδομή του νέφους εφαρμογές (που ο ίδιος είτε δημιούργησε, είτε προμηθεύτηκε) που δημιουργήθηκαν χρησιμοποιώντας γλώσσες προγραμματισμού, βιβλιοθήκες, υπηρεσίες και εργαλεία που είτε υποστηρίζονται από τον πάροχο είτε είναι συμβατές με την υποδομή του παρόχου. Ο χρήστης δεν διαχειρίζεται ή ελέγχει την υποδομή του νέφους, που περιλαμβάνει τα δίκτυα, τους εξυπηρετητές, τα λειτουργικά συστήματα, την υποδομή αποθήκευσης δεδομένων, αλλά έχει τον έλεγχο πάνω στις χρησιμοποιούμενες εφαρμογές και ενδεχομένως σε ρυθμίσεις στο περιβάλλον ανάπτυξης των εφαρμογών.

Τα βασικά χαρακτηριστικά του PaaS είναι[071]:

1. Οι υπηρεσίες για την ανάπτυξη, τον έλεγχο, τη φιλοξενία, τη λειτουργία και τη συντήρηση των εφαρμογών συμπεριλαμβάνονται σε ένα ολοκληρωμένο περιβάλλον ανάπτυξης. Οι διάφορες υπηρεσίες πρέπει να πληρούν τη διαδικασία ανάπτυξης εφαρμογής.

2. Υπάρχουν εργαλεία διεπαφής χρήστη (user interface), που βασίζονται στο δίκτυο (web based), που βοηθούν τη δημιουργία, την τροποποίηση, τον έλεγχο και την ανάπτυξη διαφόρων σεναρίων διεπαφών χρήστη.

3. Αρχιτεκτονική πολλαπλών μισθωτών, όπου ταυτόχρονα πολλαπλοί χρήστες χρησιμοποιούν την ίδια εφαρμογή ανάπτυξης,

4. Ενσωματωμένη επεκτασιμότητα του αναπτυγμένου λογισμικού με δυνατότητες διαμοίρασης φόρτου εργασίας (load balancing) και ανάκαμψης (failover).

5. Χρήση κοινών προτύπων (standards) για ενοποίηση με εφαρμογές δικτύου και βάσεις δεδομένων.

6. Υποστήριξη συνεργασίας ομάδων ανάπτυξης, ενώ συχνά είναι διαθέσιμα εργαλεία επικοινωνίας και εργαλεία σχεδίασης πλάνων.

7. Εργαλεία για χειρισμό χρεώσεων και συνδρομών.

2.1.2 Υποδομή ως Υπηρεσία (Infrastructure as a Service (IaaS))

Η δυνατότητα που παρέχεται στο χρήστη είναι να δεσμεύσει επεξεργαστική ισχύ, υποδομή αποθήκευσης, δίκτυα και άλλους βασικούς υπολογιστικούς πόρους, τους οποίους να χρησιμοποιήσει για την ανάπτυξη και εκτέλεση τυχαίου λογισμικού, που μπορεί να περιλαμβάνει λειτουργικά συστήματα ή εφαρμογές. Ο χρήστης δε διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή του νέφους, αλλά έχει έλεγχο στα λειτουργικά συστήματα, στην αποθήκευση και στις αναπτυγμένες εφαρμογές ενώ μπορεί να έχει και περιορισμένο έλεγχο και σε κάποια από τα συστατικά του δικτύου (όπως για παράδειγμα οι ρυθμίσεις του αναχώματος ασφάλειας (firewall)).

Τα βασικά χαρακτηριστικά του IaaS είναι[071]:

1. Οι πόροι διανέμονται ως υπηρεσία..

2. Επιτρέπει δυναμική κλιμάκωση.

3. Διαθέτει ευέλικτο μοντέλο τιμολόγησης.

4. Γενικά πολλαπλοί χρήστες διαμοιράζονται κοινά τμήματα του υλικού.

2.2 Τα Μοντέλα Ανάπτυξης

Τα μοντέλα υπηρεσίας που προαναφέρθηκαν μπορούν να προσφερθούν μέσα από διάφορα μοντέλα ανάπτυξης του νέφους. Το NIST [055] περιγράφει τέσσερα μοντέλα, δηλαδή τέσσερα είδη νέφους:

1. Ιδιωτικό Νέφος (Private cloud): Η υποδομή του νέφους προορίζεται για αποκλειστική χρήση από έναν οργανισμό που μπορεί να περιλαμβάνει πολλαπλούς χρήστες (για παράδειγμα, διάφορα τμήματα της επιχείρησης). Μπορεί να κατέχεται, διαχειρίζεται και λειτουργεί από τον οργανισμό, ή από κάποιον τρίτο ή και από τους δύο και μπορεί να είναι αναπτυγμένο εντός, είτε εκτός εγκαταστάσεων του οργανισμού.

2. Νέφος Κοινότητας (Community cloud): Η υποδομή του νέφους προορίζεται για αποκλειστική χρήση από μία συγκεκριμένη κοινότητα χρηστών από οργανισμούς που έχουν κοινά ενδιαφέροντα (για παράδειγμα κοινή αποστολή, απαιτήσεις ασφάλειας, πολιτική, εκτιμήσεις συμμόρφωσης). Μπορεί να κατέχεται, διαχειρίζεται και λειτουργεί από έναν ή περισσότερους από τους οργανισμούς της κοινότητας ή από κάποιον τρίτο ή από συνδυασμό αυτών και μπορεί να είναι αναπτυγμένο εντός, είτε εκτός εγκαταστάσεων του οργανισμού.

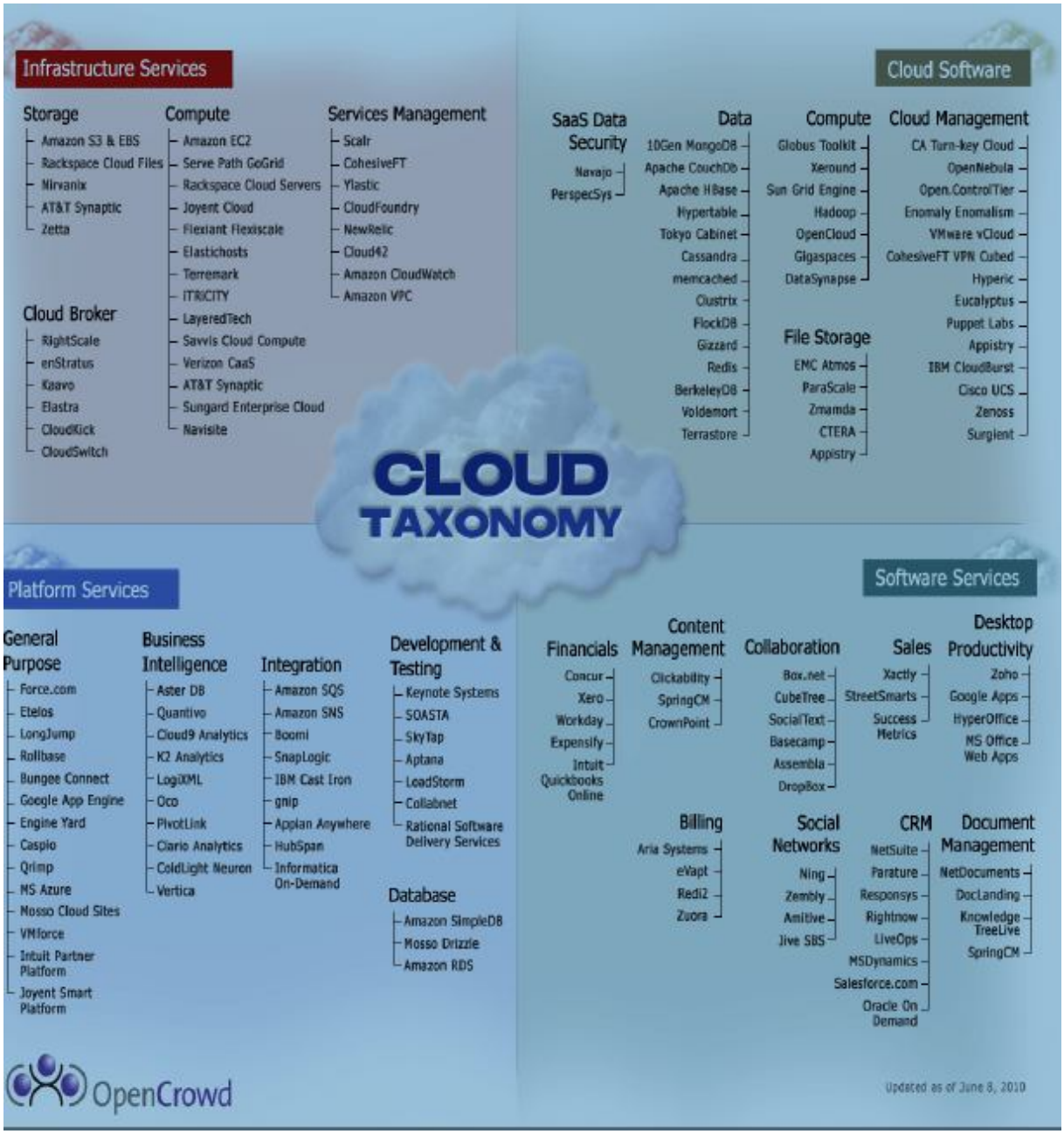
3. Δημόσιο Νέφος (Public cloud): Η υποδομή του νέφους προορίζεται να είναι διαθέσιμη στο ευρύ κοινό για κάθε χρήση. Μπορεί να κατέχεται, διαχειρίζεται και λειτουργεί από επιχείρηση, από ακαδημαϊκό ίδρυμα, από κυβερνητικό οργανισμό ή από συνδυασμό αυτών. Είναι αναπτυγμένο εντός εγκαταστάσεων του παρόχου.

4. Υβριδικό Νέφος (Hybrid cloud): Η υποδομή του νέφους είναι μία σύνθεση από δύο ή περισσότερες ξεχωριστές υποδομές νέφους (ιδιωτικό, κοινότητας ή δημόσιο) που παραμένουν διακριτές οντότητες, αλλά είναι συνδεδεμένες μεταξύ τους, μέσω τυποποιημένων ή ιδιόκτητων τεχνολογιών που επιτρέπουν την φορητότητα των εφαρμογών και δεδομένων (για παράδειγμα, δίνοντας τη δυνατότητα δυναμικής ανάπτυξης των εφαρμογών μεταξύ των νεφών αναλόγως της ζήτησης, της κυκλοφορίας του δικτύου και της διαθεσιμότητας των πόρων κάθε νέφους).

Είναι σημαντικό να διευκρινιστεί ότι ενώ η επιλογή του μοντέλου ανάπτυξης έχει επιπτώσεις για την ασφάλεια και την προστασία της ιδιωτικότητας ενός συστήματος, το μοντέλο ανάπτυξης από μόνο του δεν καθορίζει το επίπεδο της ασφάλειας και της ιδιωτικότητας των συγκεκριμένων ειδών νέφους. Αυτό το επίπεδο εξαρτάται κυρίως από διασφαλίσεις που προκύπτουν από την αξιοπιστία των πολιτικών ασφάλειας και πολιτικών εξασφάλισης της ιδιωτικότητας, την ευρωστία των ελέγχων της ασφάλειας και εξασφάλισης ιδιωτικότητας, καθώς και την έκταση της διαφάνειας στην λειτουργία και διαχείριση των λεπτομερειών του περιβάλλοντος νέφους, οι οποίες είτε παρέχονται από τον πάροχο είτε ανεξάρτητα επιτυγχάνονται από τον οργανισμό (για παράδειγμα, μέσω ανεξάρτητων δοκιμών τρωτότητας ή καταγραφής των λειτουργιών)[056]. Στο κεφάλαιο 5 περιγράφονται αναλυτικά διαδικασίες, πρακτικές και τεχνικές που συμβάλουν στην επίτευξη της ασφάλειας στο περιβάλλον της νεφοϋπολογιστικής.

2.3 Παραδείγματα παρόχων

Στις μέρες μας οι πάροχοι υπηρεσιών νέφους αυξάνονται συνεχώς, γεγονός που δηλώνει και τη μεγάλη δυναμική που έχει ο τομέας της νεφοϋπολογιστικής. Η Cloud Security Alliance (CSA) στον οδηγό ασφάλειας που έχει εκδώσει για το νέφος [021] συμπεριλαμβάνει τον ακόλουθο συγκεντρωτικό πίνακα, με ταξινόμηση των παρόχων.



Πίνακας 2.1: Ταξινόμηση των παρόχων υπηρεσιών νέφους [021].

Όσο αφορά τον ελληνικό χώρο, ισχυροί τηλεπικοινωνιακοί πάροχοι της ελληνικής αγοράς, και ειδικότερα ο ΟΤΕ(με το ΟΤΕ Business Cloud), η Wind Ελλάς(με το Wind Business Cloud), η Hellas Online(με το HOL Cloud), η Vodafone(προσφέροντας πρόσβαση σε εφαρμογές moRE της Singular Logic) αλλά και η Cyta Ελλάδας(προσφέροντας στην επιχειρηματική αγορά την υπηρεσία τηλεφωνικού κέντρου νέφους) έχουν ήδη επιβιβαστεί στο υπολογιστικό νέφος, παρέχοντας στις εγχώριες επιχειρήσεις σχετικές υπηρεσίες. Ειδικά για τους τηλεπικοινωνιακούς παρόχους η αύξηση των πωλήσεων σε εταιρικούς πελάτες μέσα από τη διάθεση υπηρεσιών νέφους έχει καταλάβει κορυφαία θέση στην επενδυτική τους ατζέντα.

Μάλιστα, όπως επισημαίνουν στελέχη τους, παρά το γεγονός ότι - στην ουσία - η αγορά των υπηρεσιών του νέφους στην Ελλάδα τώρα δημιουργείται, η ανταπόκριση από πλευράς των ελληνικών εταιρειών και δη των μικρομεσαίων είναι αρκετά ενθαρρυντική[106].

2.4 Σενάρια Χρήσης

Στην παράγραφο αυτή θα παρουσιαστούν ενδεικτικά σενάρια που αφορούν στην επιλογή χρήσης υπηρεσιών του νέφους για τα τρία μοντέλα υπηρεσίας που προαναφέρθηκαν.

2.4.1 Θυρίδα Υγείας

Ξεκινώντας από το μοντέλο του SaaS, αξίζει να σημειωθεί ότι πάρα πολλοί άνθρωποι χρησιμοποιούν σήμερα το υπολογιστικό νέφος μέσα από αυτό το μοντέλο, χωρίς να το έχουν συνειδητοποιήσει. Υπηρεσίες όπως το διαδικτυακό ηλεκτρονικό ταχυδρομείο(Hotmail, Gmail, Yahoo Mail κ.α.), τα κοινωνικά δίκτυα (Facebook, Tweeter κ.α.), η χρήση διαδικτυακού αποθηκευτικού χώρου(Dropbox κ.α.) που χρησιμοποιούνται καθημερινά από εκατομμύρια χρήστες, βασίζονται στην τεχνολογία του υπολογιστικού νέφους.

Για το λόγο αυτό θα αναφερθεί ένα σενάριο το οποίο ξεφεύγει από τις παραπάνω υπηρεσίες, που είναι τόσο ευρέως διαδεδομένες και αφορά στη χρήση μίας θυρίδας υγείας. Ας υποτεθεί ότι τα ακόλουθα αφορούν μία οικογένεια με δύο παιδιά που φροντίζει και έναν ηλικιωμένο, που ακολουθεί μία τακτική αγωγή υγείας.

Στη σημερινή πραγματικότητα το ιστορικό των εξετάσεων, των εμβολίων, των φαρμάκων διατηρούνται σε έντυπη μορφή (στα βιβλιάρια υγείας, σε έντυπα αποτελεσμάτων εξετάσεων, ακτινογραφίες, σε συνταγολόγια κ.α.). Αυτό γίνεται, παρότι που πλέον σχεδόν στο σύνολο των ιατρικών πράξεων εμπλέκεται η χρήση τεχνολογιών πληροφορικής και πλέον η ιατρική πληροφορία παράγεται πρώτα σε ηλεκτρονική μορφή (ψηφιακές ακτινογραφίες, αρχεία με αποτελέσματα μετρήσεων, ηλεκτρονική συνταγογράφηση κ.α.) και κατόπιν εκτυπώνεται για τη διατήρηση του αρχείου, από τη μεριά του χρήστη, της οικογένειας.

Η ιδέα και η χρήση της θυρίδας υγείας ουσιαστικά σημαίνει τη δημιουργία ενός εικονικού χώρου στο νέφος, μίας θυρίδας, στην οποία θα συγκεντρώνονται, αποθηκεύονται και μέσω αυτής θα διαμοιράζονται εκεί που πρέπει, όλες οι πληροφορίες υγείας της οικογένειας. Έτσι όλα τα ιατρικά

αρχεία φυλάσσονται σε ένα μέρος, οργανωμένα και είναι στη διάθεση τόσο της οικογένειας όσο και του ενδιαφερόμενου γιατρού κατά περίπτωση μέσω μίας σύνδεσης διαδικτύου.

Με τον τρόπο αυτό πιστοποιητικά υγείας (όπως το ιστορικό ανοσοποίησης, εμβολιασμών) ή συνταγογραφήσεις σταθερών αγωγών μπορούν να εξασφαλιστούν σε συνεργασία με τον γιατρό ηλεκτρονικά, χωρίς να χρειάζεται επίσκεψη στο ιατρείο, καθώς αυτός θα έχει πρόσβαση σε όλο το ιστορικό.

Επίσης μπορούν να παρακολουθηθούν όλες οι λεπτομέρειες που αφορούν τη διατήρηση αναλυτικού ιστορικού υγείας του καθενός μέλους της οικογένειας όπως φάρμακα, αλλεργίες, μετρήσεις πίεσης, βάρος, ακτινογραφίες, υπέρηχοι, αποτελέσματα εργαστηρίων που μπορούν να είναι πολύ σημαντικά στη διαχείριση σύνθετων προβλημάτων υγείας. Αντίστοιχα συνεργαζόμενα εργαστήρια, νοσοκομεία, φαρμακεία μπορούν να ενημερώνουν τα αρχεία της θυρίδας με σχετικές πληροφορίες. Κάποιες από τις πληροφορίες αυτές (για παράδειγμα η εξέλιξη της κατάστασης του ηλικιωμένου) μπορούν μέσω του διαδικτύου να είναι προσβάσιμες και από άλλους (για παράδειγμα κάποιος συγγενείς που βρίσκεται μακριά).

Τέλος υπάρχει και μία σειρά από διαθέσιμες εφαρμογές για χρήση από έξυπνα κινητά (Smart phones) για την εκμετάλλευση των πληροφοριών της θυρίδας καθώς και μία σειρά από οικιακές συσκευές, που χρησιμοποιούνται για μετρήσεις(για παράδειγμα πίεσης αίματος) που ανεβάζουν αυτόματα τις πληροφορίες στη θυρίδα.

Ένας πάροχος θυρίδας υγείας είναι η Microsoft και η υπηρεσία της ονομάζεται HealthVault. Το Μάρτιο του 2013, η υπηρεσία είχε διαθέσιμες για την Ελλάδα 10 εφαρμογές και 171 συνεργαζόμενες συσκευές, ενώ η χρήση της υπηρεσίας είναι χωρίς χρέωση[050].

2.4.2 Εταιρεία Ανάπτυξης Εφαρμογών Ιστού(Web Applications)

Μελετώντας το μοντέλο του PaaS αξίζει να σημειωθεί η δυνατότητα και η ευκολία που παρέχει για την ανάπτυξη εφαρμογών ιστού.

Έστω μία μικρή εταιρεία που εξειδικεύεται στην ανάπτυξη τέτοιου είδους εφαρμογών, το μόνο που χρειάζεται είναι αρχικά να επιλέξει τον πάροχο με τον οποίο θα συνεργαστεί. Ένας από αυτούς είναι η Google, που προσφέρει το Google App Engine(GAE).

Στη συνέχεια επιλέγεται ένα από τα διαθέσιμα περιβάλλοντα, γλώσσες ανάπτυξης της εφαρμογής. Το GAE προσφέρει τα γνωστά και ευρέως διαδεδομένα περιβάλλοντα της JAVA και της PYTHON καθώς και το νέο πειραματικό της GO. Κατόπιν γράφεται ο κώδικας της εφαρμογής σε ένα από αυτά τα περιβάλλοντα, δοκιμάζεται εντός της εταιρείας στην ιδιόκτητη υποδομή και φορτώνεται στην Google, η οποία αναλαμβάνει τη φιλοξενία και την κλιμάκωση της εφαρμογής αναλόγως των αναγκών της και της ζήτησής της από τους χρήστες της.

Με τον τρόπο αυτό η μικρή εταιρεία εκμεταλλεύεται και βασίζεται στην αξιοπιστία, στην απόδοση και στην ασφάλεια των υποδομών της Google. Με τη χρήση του GAE η εταιρεία μπορεί να επωφεληθεί από τα 10 και πλέον χρόνια εμπειρίας της Google, που έχει στη λειτουργία μαζικά επεκτάσιμων συστημάτων, με βάση την απόδοσή τους. Επιπλέον, οι ίδιες πολιτικές ασφάλειας, προστασίας της ιδιωτικότητας και προστασίας των δεδομένων που ισχύουν για τις ιδιόκτητες εφαρμογές της Google, ισχύουν και για όλες τις εφαρμογές που μέσω του GAE θα αναπτύξει η μικρή εταιρεία. Η ίδια η Google ισχυρίζεται ότι παίρνει την ασφάλεια πολύ σοβαρά και έχει θεσπίσει μέτρα για την προστασία του κώδικα και των δεδομένα των εφαρμογών των πελατών της.

Όσο αφορά τη χρέωση, αυτή γίνεται βάσει χρήσης. Δεν υπάρχουν έξοδα εγκατάστασης και πάγια έξοδα. Οι πόροι που χρησιμοποιούνται από την εφαρμογή, όπως η αποθήκευση, το εύρος ζώνης, μετρούνται σε Gigabytes, και τιμολογούνται αντίστοιχα. Επιπλέον η μικρή εταιρεία μπορεί να ελέγξει τα ανώτατα όρια των πόρων που οι εφαρμογές τις μπορούν να καταναλώσουν, έτσι ώστε οι χρεώσεις να παραμένουν πάντα στα πλαίσια του προϋπολογισμού της.

Η Google προσφέρει το GAE δωρεάν (το Μάρτιο του 2013) σε κάποιον που ξεκινάει με αυτό, για εφαρμογές που συνολικά χρησιμοποιούν έως 1 GB αποθήκευσης, υπολογιστική ισχύ και εύρος ζώνης αρκετά για να υποστηρίξουν περίπου 5 εκατομμύρια προσβάσεις σε ιστοσελίδα μηνιαίως. Η χρέωση γίνεται όταν ξεπεραστούν τα όρια δωρεάν χρήσης και μόνο για τους επιπλέον πόρους[036].

Γίνεται εύκολα αντιληπτό ότι η μετάβαση στο νέφος με τους παραπάνω όρους είναι αρκετά δελεαστική για την μικρή εταιρεία. Της δίνεται η ευκαιρία να αναπτύσσει τις εφαρμογές της, να τις δοκιμάσει χωρίς καθόλου επενδύσεις σε ιδιόκτητη υποδομή δικτύου και να μελετήσει την ανταπόκριση που αυτές έχουν στο κοινό, ώστε αντίστοιχα να εστιάσει σε κάποιες ή κάποιες να τις εγκαταλείψει.

2.4.3 Λογιστικό Γραφείο

Για το μοντέλο του IaaS θα εξεταστεί η δυνατότητα δέσμευσης υπολογιστικής ισχύς στο νέφος όταν συγκυριακά οι απαιτήσεις ξεπερνούν τις διαθέσιμες ιδιόκτητες δυνατότητες.

Έστω ένα λογιστικό γραφείο που προσφέρει διαδικτυακά τις υπηρεσίες του σε απομακρυσμένους πελάτες του. Οι πελάτες, ή εκπρόσωποι του γραφείου από την έδρα των πελατών, μέσω διαδικτύου συμπληρώνουν μέσα από μία εφαρμογή που διαθέτει το γραφείο τα απαραίτητα στοιχεία για παράδειγμα υποβολής ΦΠΑ , εισόδημα, έξοδα κ.α. Στη συνέχεια αφού αυτά ελεγχθούν, διορθωθούν και υπολογιστούν τα στοιχεία ενδιαφέροντος (ποσά φόρων, επιστροφές κλπ) προωθούνται στο σύστημα της εφορίας.

Έχει παρατηρηθεί ότι τις περιόδους όπου λήγουν οι προθεσμίες που θέτει η εφορία, παρουσιάζεται πολύ αυξημένος φόρτος εργασίας και η υποδομή του γραφείου δεν αρκεί να καλύψει όλους τους πελάτες[029]. Για τις περιόδους αυτές, το γραφείο επιλέγει να καταφεύγει στην αναζήτηση επιπλέον υπολογιστικής ισχύς στο νέφος.

Στην περίπτωση αυτή, η Amazon με το Elastic Compute Cloud (Amazon EC2) είναι ένας πάροχος στον οποίο μπορεί να απευθυνθεί το γραφείο. Το EC2 είναι ένα παράδειγμα μοντέλου IaaS που προσφέρει εικονικούς εξυπηρετητές, που είναι προδιαμορφωμένοι με προεγκατεστημένα λειτουργικά συστήματα, οι οποίοι μπορούν να συνεργαστούν και με τις άλλες υπηρεσίες νέφους που παρέχει η Amazon, όπως χώρος αποθήκευσης δεδομένων και διαμοίραση φόρτου εργασίας (load balancing).

Η διαμοίραση φόρτου εργασίας και η αυτόματη επέκταση αποτελούν πολύ σημαντικές λειτουργίες για το EC2, δίνοντας τη δυνατότητα στο γραφείο να φτιάξει κανόνες με βάση τους οποίους θα είναι δυνατό να αυξηθεί αυτόματα και ομαλά ή να μειωθεί ο αριθμός των χρησιμοποιούμενων εξυπηρετητών, αναλόγως της ζήτησης, για τη διατήρηση σταθερών επιδόσεων από τη μία, αλλά και την αποφυγή χρεώσεων που δε χρειάζονται.

Όσο αφορά την ασφάλεια, η Amazon αναφέρει ότι στις υψηλότερες προτεραιότητές της συμπεριλαμβάνεται η προσπάθειά της να βοηθήσει στην προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των συστημάτων και δεδομένων των πελατών της (έννοιες που αναλύονται στο επόμενο κεφάλαιο). Έτσι ακολουθεί μία σειρά από φυσικές και λειτουργικές διαδικασίες ασφάλειας για την υποδομή του δικτύου και των εξυπηρετητών της

ενώ προσφέρει ένα μεγάλο πακέτο από ρυθμίσεις ασφάλειας που αφορούν στην ρύθμιση των IPs των εξυπηρετητών, την ύπαρξη αναχώματος ασφάλειας (firewall), ακόμα και τη δυνατότητα δημιουργίας εικονικού ιδιωτικού νέφους(αναφέρεται στο κεφάλαιο 5)[002].

Οι χρεώσεις υπολογίζονται με την ώρα χρήσης αναλόγως του λειτουργικού συστήματος και του τύπου(μικρός, μεσαίος κ.α) του εικονικού εξυπηρετητή που θα χρησιμοποιηθεί[003].

Με την επιλογή της λύσης του νέφους το λογιστικό γραφείο μπορεί πλέον να ανταπεξέρθει στις περιόδους μεγάλης ζήτησης, χωρίς επιπλέον κόστος για την επέκταση-αναβάθμισης της υποδομής του και να ανταποκριθεί καλύτερα στις απαιτήσεις των πελατών του.

Κεφάλαιο 3
Ιδιωτικότητα, Δεδομένα, Ασφάλεια Δικτύων, Πρότυπα

Στο κεφάλαιο αυτό γίνεται μια ανάλυση εννοιών, όρων που έχουν σχέση με την ασφάλεια και επηρεάζονται από την αρχιτεκτονική και λειτουργία του νέφους. Γίνεται μία συνοπτική περιγραφή της ιδιωτικότητας, δίνεται ο ορισμός των προσωπικών δεδομένων (συμπεριλαμβανομένου και των ευαίσθητων) και αναλύεται ο κύκλος ζωής των δεδομένων. Επιπλέον αναλύεται η έννοια της Ασφάλειας Δικτύων και γίνεται μία συνοπτική παρουσίαση των πιο καθιερωμένων διεθνών προτύπων ασφάλειας.

3.1 Ιδιωτικότητα

Η ιδιωτικότητα είναι η επιθυμία ενός ατόμου να ελέγχει την αποκάλυψη προσωπικών πληροφοριών. Οι οργανισμοί που διαχειρίζονται προσωπικά δεδομένα απαιτείται να συμμορφώνονται με το νομικό πλαίσιο της χώρας που εξασφαλίζει την προστασία της ιδιωτικότητας και της εμπιστευτικότητας [078].

Τα ζητήματα της ιδιωτικότητας, έχουν επί μακρόν απασχολήσει του κοινωνικούς επιστήμονες, τους φιλοσόφους και τους νομικούς. Η ιδιωτικότητα έχει αναγνωριστεί ως βασικό πανανθρώπινο δικαίωμα στη Διακήρυξη Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών, στη Συνθήκη για τα Αστικά και Πολιτικά Δικαιώματα και σε πολλές άλλες εθνικές και διεθνείς συνθήκες [101]. Μία από τις πιο περιεκτικές νομοθεσίες για την προστασία της ιδιωτικότητας είναι η πρόσφατη νομοθεσία της Ε.Ε. , η Οδηγία (Council Directive) 95/46/EC)[001].

Ο Κ. Λαμπρινουδάκης κ.α. [101] αναφέρουν αναλυτικότερα ότι «Στις σύγχρονες δημοκρατικές κοινωνίες η απαίτηση διασφάλισης της ιδιωτικότητας αποτελεί συνθήκη εκ των ων ουκ άνευ (sine qua non), αλλά με την αξιοποίηση των τεχνολογιών πληροφοριακών και επικοινωνιακών συστημάτων, η ιδιωτικότητα βρίσκεται σε ολοένα αυξανόμενο κίνδυνο.

Οι Αμερικανοί νομικοί S. Warren και ο L. Brandeis όρισαν την ιδιωτικότητα ως *«το δικαίωμα να είναι κάποιος μόνος (the right to be alone)»*. Γενικά, η έννοια της ιδιωτικότητας μπορεί να αναλυθεί υπό την οπτική τριών συμπληρωματικών θεωρήσεων :

1. τη χωρική ιδιωτικότητα (territorial privacy), δηλαδή την προστασία της κοντινής φυσικής περιοχής που περιβάλει ένα άτομο,

2. την ιδιωτικότητα του ατόμου (privacy of the person), δηλαδή την προστασία του ατόμου από αδικαιολόγητες παρεμβάσεις

3. την πληροφοριακή ιδιωτικότητα (informational privacy), δηλαδή τον έλεγχο αν και με ποιο τρόπο προσωπικά δεδομένα συλλέγονται, αποθηκεύονται, επεξεργάζονται ή διαδίδονται επιλεκτικά.»

Σύμφωνα με τον Dr. Mohammed A. T. AlSudiari κ.α. [001], η ιδιωτικότητα αποτελεί μία από τις τρεις κορυφές ενός τριγώνου, όπου οι άλλες δύο είναι η ασφάλεια και το δικαίωμα στην πληροφορία. Αν κάποιος θέλει ιδιωτικότητα, τότε πρέπει να γίνουν συμβιβασμοί στην ασφάλεια και στο δικαίωμα στην πληροφορία και αντίστροφα.

Στο περιβάλλον της νεφοϋπολογιστικής, η διατήρηση της ιδιωτικότητας των χρηστών αποτελεί ένα από τα σημαντικότερα ζητήματα ασφάλειας, διότι ότι οι χρήστες δεν έχουν πλέον τον έλεγχο από τη μία των δεδομένων τους σε ότι αφορά το πώς αποθηκεύονται, πως μοιράζονται και χρησιμοποιούνται και από την άλλη των μέτρων ασφάλειας που χρησιμοποιούνται για την

προστασία των δεδομένων αυτών. Έτσι ένα μεγάλο μέρος από την αρμοδιότητα αλλά και την ευθύνη για την εξασφάλιση της ιδιωτικότητας των χρηστών περνάει στους παρόχους των υπηρεσιών του νέφους.

3.2 Δεδομένα (Data)

Ως δεδομένα ορίζεται ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί, τα οποία μαζί με την έννοια που τους αποδίδεται διαμορφώνουν την πληροφορία (information) [099].

3.2.1 Προσωπικά Δεδομένα

Στην Ελλάδα ισχύει ο Νόμος 2472/1997 «Προστασία Του Ατόμου Από Την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα», με αντικείμενο τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής, ο οποίος εποπτεύεται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[102].

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, διεύθυνση ηλεκτρονικού ταχυδρομείου, ειδικοί αριθμοί αναγνώρισης (πχ Α.Φ.Μ.), επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων [102,104].

Κάποια από τα προσωπικά δεδομένα χαρακτηρίζονται ως ευαίσθητα. Αυτά είναι «τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων."[102]

Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα, ενώ στο Άρθρο 10 του συγκεκριμένου Νόμου αναφέρεται ότι «Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του».

Ενδιαφέρον παρουσιάζει και το Άρθρο 14 του Νόμου. που προστατεύει την αξιολόγηση της προσωπικότητας, συμπεριφορά ενός ατόμου μέσα από αυτοματοποιημένες επεξεργασίες στοιχείων, όπως συνήθειες προσπέλασης ψηφιακού περιεχομένου, πρόσφατα επισκεπτόμενες ιστοσελίδες, αγορά-χρήση προϊόντων κλπ[061]. Επίσης, ισχύει ο Νόμος 3471/2006 για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες [104].

3.2.2 Κύκλος Ζωής των Δεδομένων

Η Cloud Security Alliance (CSA) [021] αναγνωρίζει έξι φάσεις από την δημιουργία μέχρι την καταστροφή στον κύκλο ζωής των δεδομένων. Παρότι αναφέρονται με αύξοντα αριθμό , σαν γραμμική ακολουθία, από τη στιγμή που θα δημιουργηθούν μπορούν να μεταπηδούν μεταξύ των φάσεων χωρίς περιορισμούς και μπορεί να μην περάσουν από όλες τις φάσεις (για παράδειγμα δεν καταστρέφονται όλα τα δεδομένα).

1. Δημιουργία: Είναι η παραγωγή νέου ψηφιακού περιεχομένου, ή η τροποποίηση, ενημέρωση υπάρχοντος περιεχομένου.

2. Αποθήκευση: Είναι η πράξη μεταφοράς των ψηφιακών δεδομένων σε κάποια μορφή αποθήκης μνήμης και τυπικά συμβαίνει σχεδόν ταυτόχρονα με τη δημιουργία των δεδομένων.

3. Χρήση: Τα δεδομένα προσπελαύνονται, επεξεργάζονται ή χρησιμοποιούνται με κάποιο είδος δραστηριότητας, χωρίς όμως να τροποποιούνται.

4. Διαμοιρασμός: Η πληροφορία γίνεται προσβάσιμη και σε άλλους όπως μεταξύ των χρηστών, σε πελάτες ή συνεργάτες.

5. Αρχειοθέτηση: Τα δεδομένα παύουν να χρησιμοποιούνται ενεργά και τίθενται σε κατάσταση μακράς αποθήκευσης.

6. Καταστροφή: Τα δεδομένα οριστικά καταστρέφονται με τη χρήση φυσικών ή ψηφιακών μέσων.

Ο παραπάνω κύκλος παριστάνει τις φάσεις από τις οποίες διέρχεται η πληροφορία, αλλά δεν αναφέρεται στην τοποθεσία της ή στο πως γίνεται προσπελάσιμη. Σχεδόν σε κάθε φάση τα δεδομένα μπορούν να μετακινηθούν μέσα, έξω και μεταξύ των λειτουργικών περιβαλλόντων που απαρτίζουν το νέφος (ιδιωτική υποδομή , υποδομή του παρόχου κλπ), ενώ πλέον τα δεδομένα μπορούν να προσπελαστούν από μία ποικιλία συσκευών.

3.3 Ασφάλεια Δικτύων

Στην Wikipedia [092] αναφέρονται τα ακόλουθα: «Η έννοια της **Ασφάλειας Δικτύου Υπολογιστών** σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών».

Η έννοια της ασφάλειας των δικτύων υπολογιστών συνδέεται στενά με τις βασικές έννοιες που ακολουθούν.

3.3.1 Εμπιστευτικότητα (Confidentiality)

Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, τα δεδομένα σε όλο τον κύκλο ζωής τους που υφίστανται στο νέφος, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Η εμπιστευτικότητα εξασφαλίζει την ιδιωτικότητα, την προστασία των προσωπικών δεδομένων αλλά και τη μυστικότητα την προστασία, δηλαδή, των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση[092].

Στο περιβάλλον της νεφοϋπολογιστικής η εμπιστευτικότητα παίζει σημαντικό ρόλο κυρίως στην διατήρηση του ελέγχου πάνω στα δεδομένα ενός οργανισμού που μπορεί να είναι αναπτυγμένα σε διάφορα κέντρα δεδομένων ή κατανεμημένους εξυπηρετητές ενός ή περισσοτέρων παρόχων[078].

3.3.2 Ακεραιότητα (Integrity)

Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων [092]. Η ακεραιότητα μπορεί να συνδεθεί με τα δεδομένα, το λογισμικό αλλά και το υλικό ενός πληροφοριακού συστήματος.

Ελέγχοντας τα δικαιώματα εισόδου- χρήσης μιας οντότητας σε συγκεκριμένους πόρους της επιχείρησης εξασφαλίζεται ότι τα δεδομένα και οι υπηρεσίες δεν χρησιμοποιούνται κακώς ή παράνομα. Παράλληλα οι μηχανισμοί διατήρησης της ακεραιότητας παρέχουν καλύτερη διαφάνεια στον καθορισμό ποιος ή τι μπορεί να έχει αλλάξει τα δεδομένα ή τις πληροφορίες συστήματος, πιθανώς επηρεάζοντας την ακεραιότητά τους [078].

Στο περιβάλλον της νεφοϋπολογιστικής η ακεραιότητα σχετίζεται επίσης με την ικανότητα του παρόχου να εξασφαλίσει αξιόπιστη και ορθή λειτουργία του νέφους, ώστε να καλύπτονται οι νομικές του υποχρεώσεις που προέρχονται, για παράδειγμα, από τα Συμφωνητικά Παροχής Υπηρεσιών (Service Level Agreements(SLA))(αναλύονται στο κεφάλαιο 4) και από τα τεχνικά πρότυπα(αναλύονται στην παράγραφο 3.4) με τα οποία πρέπει να συμμορφώνεται [078].

3.3.3 Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός συστήματος, όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με απλούς όρους η διαθεσιμότητα σημαίνει ότι ένας οργανισμός έχει το σύνολο των υπολογιστικών πόρων που διαθέτει προσβάσιμους και έτοιμους για χρήση κάθε στιγμή. Η διαθεσιμότητα μπορεί να επηρεαστεί προσωρινά ή μόνιμα και η απώλεια μπορεί να είναι μερική ή πλήρης[078].

Σκοπός της διαθεσιμότητας για τα συστήματα νεφοϋπολογιστικής (συμπεριλαμβανομένων εφαρμογών και υποδομών) είναι να εξασφαλίσει ότι οι χρήστες μπορούν να χρησιμοποιήσουν τα συστήματα αυτά ανά πάσα στιγμή και από οπουδήποτε. Αυτό αποτελεί μία από τις κύριες ανησυχίες οργανισμών με κρίσιμη αποστολή ή με δραστηριότητες που μπορεί να σχετίζονται με την ασφάλεια του κοινού (όπως για παράδειγμα υπηρεσίες παροχής υγείας)[078].

Για την επίτευξη της διαθεσιμότητας ένα σύστημα πρέπει να έχει την ικανότητα να λειτουργεί, έστω και αν δέχεται επιθέσεις από μη εξουσιοδοτημένους χρήστες, ή αν κάποιοι από τους εξουσιοδοτημένους χρήστες δεν λειτουργούν σύμφωνα με τα προβλεπόμενα ή έστω και αν υπάρχει διαρροή ασφάλειας [078].

Για σκοπούς ασφάλειας, ιδιαίτερη προσοχή δίνεται στην παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα και ουσιαστικά στρέφονται ενάντια της διαθεσιμότητας ενός συστήματος. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών (Denial Of Service (D.O.S.))[092].

3.4 Πρότυπα

Η τυποποίηση και η ύπαρξη διεθνών προτύπων είναι καθοριστικής σημασίας βήμα που επιτρέπει την αξιοποίηση των νέων τεχνολογικών τάσεων της νεφοϋπολογιστικής. Στην παράγραφο αυτή θα γίνει μία συνοπτική παρουσίαση των πιο καθιερωμένων προτύπων.

Ο Διεθνής Οργανισμός Τυποποίησης (ΔΟΤ) (International Organization for Standardization(ISO)) σε συνεργασία με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission (IEC)) έχουν εκδώσει μία σειρά από πρότυπα αφιερωμένα στον τομέα της ασφάλειας των πληροφοριακών συστημάτων, που έχουν εφαρμογή στην ασφάλεια της νεφοϋπολογιστικής. Είναι η σειρά ISO/IEC 27000 και περιλαμβάνει τα πρότυπα που φαίνονται στον ακόλουθο πίνακα [037].

ΠΡΟΤΥΠΟ ISO/IEC	ΟΝΟΜΑ	ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ
27001:2005	Information security management systems	Καλύπτει όλους τους τύπους των οργανισμών και προσδιορίζει τις απαιτήσεις για σχεδιασμό, υλοποίηση, έλεγχο και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System(ISMS)) που να συμβαδίζει με το ευρύτερο πλαίσιο των επιχειρηματικών ρίσκων του οργανισμού.
27002:2005	Code of practice for information security management	Αποτελεί ένα γενικό οδηγό για την επίτευξη των κοινά αποδεκτών στόχων της Διαχείρισης της Ασφάλειας των Πληροφοριών
27003:2010	Information security management system implementation guidance	Εστιάζει στις κρίσιμες πτυχές που χρειάζονται για το σχεδιασμό και την υλοποίηση ενός ISMS σύμφωνα με το πρότυπο 27001:2005.
27004:2009	Information security management -- Measurement	Παρέχει οδηγίες για την ανάπτυξη και χρήση μέτρων και μετρήσεων με σκοπό να αξιολογηθεί η αποτελεσματικότητα ενός ISMS σύμφωνα με το πρότυπο 27001:2005.
27005:2011	Information security risk management	Παρέχει οδηγίες για τη διαχείριση κινδύνων ασφάλειας. Υποστηρίζει τις γενικές έννοιες του 27001:2005, ενώ απαιτείται και η γνώση του 27002:2005 για την κατανόησή του.
27006:2011	Requirements for bodies providing audit and certification of information security management systems	Καθορίζει τις απαιτήσεις και παρέχει οδηγίες για οντότητες που παρέχουν έλεγχο και πιστοποίηση ενός ISMS σύμφωνα με το πρότυπο 27001:2005.

Πίνακας 3.1: Η σειρά του προτύπου ISO/IEC 27000 .

Επιπλέον ο ΔΟΤ έχει ορίσει και μία τεχνική επιτροπή , την «JTC 1/SC 38 - Distributed application platforms and services» που περιέχει δύο ομάδες εργασίας, το «Working Group 3 on Cloud

Computing» και το «Study Group on Cloud Computing» που ασχολούνται με την ορολογία και την τυποποίηση της νεφοϋπολογιστικής[037].

Στις ΗΠΑ ισχύει η Ομοσπονδιακή Πράξη Διαχείρισης Ασφάλειας Πληροφοριών(Federal Information Security Management Act (FISMA)) του 2002, που στην ουσία απαιτεί από τη διοίκηση κάθε υπηρεσίας να εφαρμόσει πολιτικές και διαδικασίες, ώστε με οικονομικά αποτελεσματικό τρόπο να μειώσει στα πληροφοριακά συστήματα του κινδύνους ασφάλειας σε ένα αποδεκτό επίπεδο. Επιπλέον αναθέτει στο National Institute of Standards and Technology (NIST) την έκδοση αντίστοιχων οδηγιών[085].

Έτσι το NIST έχει εκδώσει την οδηγία Special Publication 800-39: «Managing Information Security Risk»[058], που αφορά τη διαχείριση κινδύνων ασφάλειας και την οδηγία Special Publication 800-53 Revision 3: «Recommended Security Controls for Federal Information Systems and Organizations» [059], που αποτελεί έναν οδηγό ελέγχων ασφάλειας.

Το πρότυπο «Statement on Auditing Standards No. 70: Service Organizations» γνωστό ως SAS 70, παρέχει οδηγίες σε υπηρεσίες ελεγκτών για την αξιολόγηση του συστήματος εσωτερικού ελέγχου μίας οργάνωσης και την έκδοση σχετικού πιστοποιητικού. Το πιστοποιητικό μπορεί να είναι τύπου I (Type I) ή τύπου II (Type II). Στο πιστοποιητικό τύπου I ο ελεγκτής περιλαμβάνει την άποψή του για την ορθότητα της περιγραφής των ελέγχων ασφάλειας του οργανισμού που έχουν τεθεί σε λειτουργία και την καταλληλότητα του σχεδιασμού των ελέγχων αυτών για την επίτευξη των απαιτούμενων στόχων. Στο πιστοποιητικό τύπου II ο ελεγκτής επιπλέον από αυτά που περιγράφονται στο τύπου I καταγράφει και τη γνώμη του για το αν οι συγκεκριμένοι έλεγχοι λειτουργούσαν ικανοποιητικά κατά την περίοδο της αξιολόγησης. Το SAS 70 έχει πλέον αντικατασταθεί από το νέο αντίστοιχο πρότυπο Statement on Standards for Attestation Engagements (SSAE) No.16 «Reporting on Controls at a Service Organization» που έχει ημερομηνία εφαρμογής από 15 Ιουνίου 2011 [004,005].

Πέρα από τα πρότυπα γενικού σκοπού υπάρχουν και κάποια που αφορούν συγκεκριμένους τομείς. Για παράδειγμα το HIPAA ασχολείται με την ασφάλεια και την ιδιωτικότητα προσωπικών δεδομένων που αφορούν την υγεία, ενώ το PCI DSS V2.0 ασχολείται με την ασφάλεια οργανισμών που διατηρούν στοιχεία πιστωτικών καρτών[066].

Τέλος, υπάρχουν εξειδικευμένα πρότυπα και πλαίσια που εστιάζουν στα πληροφοριακά συστήματα και συμπεριλαμβάνουν τη διαχείριση κινδύνων, όπως το COBIT[086], το Information Technology Infrastructure Library (ITIL) [042] και τοVal IT[038] .

Κεφάλαιο 4
Κίνδυνοι και Ζητήματα Ασφάλειας

Στο κεφάλαιο αυτό παρουσιάζονται οι κίνδυνοι και τα ζητήματα ασφάλειας που σχετίζονται με τη χρήση του νέφους. Οι κίνδυνοι αυτοί κατ' αρχάς πηγάζουν από το γεγονός ότι οι χρήστες χάνουν τον έλεγχο των δεδομένων τους καθώς αποθηκεύονται εκτός οργανισμού. Επιπλέον καθώς όλη η αρχιτεκτονική της λειτουργίας του νέφους βασίζεται στο διαδίκτυο, συνεχίζουν να υφίστανται οι κίνδυνοι που σχετίζονται με τη λειτουργία του διαδικτύου. Κινδύνους συνεπάγεται και η χρήση της τεχνολογίας της εικονικοποίησης που είναι βασική για τη λειτουργία του νέφους. Τέλος παρουσιάζονται και μία σειρά από νομικά θέματα που προκύπτουν, που αφορούν και τα Συμφωνητικά Παροχής Υπηρεσιών (ΣΠΥ) (Service Level Agreement(SLA)),που καθορίζουν τη συμφωνία παρόχου -πελάτη, καθώς και ο τρόπος εκτίμησης των επιπτώσεων σε έναν οργανισμό.

4.1 Τα Δεδομένα Εκτός του Οργανισμού

Το κύριο χαρακτηριστικό της λειτουργίας του νέφους είναι ότι οι χρήστες «αποχωρίζονται» από τα δεδομένα τους, τα οποία αποθηκεύονται πλέον στις εγκαταστάσεις και στην υποδομή του

παρόχου, ενώ οι χρήστες έχουν πρόσβαση σε αυτά μέσω του διαδικτύου. Στη συνέχεια αναλύονται τα ζητήματα που προκύπτουν από αυτό το διαχωρισμό.

4.1.1 Απώλεια Διακυβέρνησης (Loss Of Governance)

Με τη χρήση των υποδομών του νέφους, ο πελάτης εκχωρεί τον έλεγχο κατ' ανάγκη στον πάροχο, για μια σειρά από θέματα που μπορεί να επηρεάσουν την ασφάλεια. Ταυτόχρονα, το ΣΠΥ μπορεί να μην προβλέπει δέσμευση για την παροχή τέτοιων υπηρεσιών εκ μέρους του παρόχου, αφήνοντας έτσι κενά στην ασφάλεια[031].

Έτσι από τη μία ο πελάτης δεν είναι σε θέση να ελέγχει την ασφάλεια των περιουσιακών του στοιχείων, που εμπιστεύεται στον πάροχο, αλλά ούτε και την ποιότητα ή την ασφάλεια υπηρεσιών άλλων πελατών με τους οποίους μοιράζεται την ίδια υποδομή του παρόχου. Από την άλλη η απώλεια του ελέγχου επηρεάζει και τον ίδιο τον πάροχο, καθώς και αυτός δεν είναι ενήμερος του περιεχομένου, των απαιτήσεων ασφάλειας αλλά και της ποιότητας των υπηρεσιών που φιλοξενεί[078].

4.1.2 Συμμόρφωση στους Κανονισμούς (Regulatory Compliance)

Στο περιβάλλον του νέφους ο πελάτης αλλά και ο πάροχος μοιράζονται ευθύνες για τη διαχείριση των δεδομένων. Ο πελάτης ανάλογα με τα δεδομένα που διαχειρίζεται είναι ήδη υπεύθυνος για την εξασφάλιση της εμπιστευτικότητας και τις ακεραιότητά τους. Επιπλέον μπορεί να έχει κάνει σημαντικές επενδύσεις στον εξοπλισμό του, για την επίτευξη συγκεκριμένης πιστοποίησης (π.χ. βιομηχανικά πρότυπα ή συμμόρφωση με συγκεκριμένους κανονισμούς), που μπορεί να τεθεί σε κίνδυνο από τη μετακίνηση στο νέφος είτε επειδή ο πάροχος δεν μπορεί να παράσχει αποδεικτικά στοιχεία της συμμόρφωσής του με τις σχετικές απαιτήσεις είτε επειδή δεν επιτρέπει τον έλεγχο από τον πελάτη[031].

Είναι γεγονός ότι σε ορισμένες περιπτώσεις η χρήση δημόσιων υποδομών νέφους συνεπάγεται ότι ορισμένα είδη συμμόρφωσης δεν μπορούν να επιτευχθούν. Για παράδειγμα συμμόρφωση με τους κανονισμούς της ΕΕ, που δεν επιτρέπουν προσωπικά δεδομένα πολιτών να αποθηκεύονται εκτός της ΕΕ ή συμμόρφωση με τα ειδικά πρότυπα HIPAA ή PCI DSS, που αναφέρθηκαν στο κεφάλαιο 3. Για το λόγο αυτό, όλες οι μεσαίες και μεγάλους μεγέθους επιχειρήσεις προτιμούν κατά κύριο λόγο ιδιωτικά νέφη[019,031,073,078].

4.1.3 Τοποθεσία των δεδομένων (Data Location)

Ένας από τους πιο κοινούς προβληματισμούς κατά την υιοθέτηση της λύσης του νέφους είναι η θέση, τοποθεσία που θα αποθηκεύονται τα δεδομένα. Η χρήση ιδιόκτητης υποδομής πληροφορικής επιτρέπει σε έναν οργανισμό να δομήσει το δικό του υπολογιστικό περιβάλλον και να γνωρίζει λεπτομερώς που αποθηκεύονται τα δεδομένα και τι εγγυήσεις χρησιμοποιούνται για την προστασία τους. Από την άλλη, το χαρακτηριστικό πολλών υπηρεσιών νέφους είναι ότι τα δεδομένα μπορεί να είναι αποθηκευμένα σε πολλές φυσικές τοποθεσίες.

Όπως αναφέρθηκε στο κεφάλαιο 1, η δομή του νέφους επιτρέπει στους παρόχους να αναπτύσσουν τους φυσικούς τους εξυπηρετητές σε διαφορετικές γεωγραφικές περιοχές. Ο πάροχος μπορεί να έχει εκατοντάδες κατανεμημένους εξυπηρετητές στην κατοχή του, διεσπαρμένους σε όλον τον κόσμο. Έτσι λεπτομερείς πληροφορίες σχετικά με την τοποθεσία των δεδομένων του οργανισμού δεν είναι διαθέσιμες ή δεν γνωστοποιούνται στους καταναλωτές υπηρεσιών.

Καθώς η νομοθεσία από χώρα σε χώρα μπορεί να διαφέρει σχετικά με την προστασία της ιδιωτικότητας και της ασφάλειας των πληροφοριών, όταν αυτές διασχίζουν τα σύνορα μπορεί να προκύψουν νομικά και άλλα ζητήματα. Έτσι δεδομένα που θεωρούνται ασφαλή και μη προσβάσιμα σε μία χώρα, σε μία άλλη μπορεί να μην θεωρούνται ασφαλή και να μην προβλέπεται προστασία πρόσβασης[011,056].

4.1.4 Πρόσβαση εκ των έσω ή κατ' εξαίρεση (Insider Access-Privileged User Access)

Στο περιβάλλον του νέφους, καθώς τα δεδομένα του οργανισμού φιλοξενούνται στις εγκαταστάσεις του παρόχου προκύπτει άμεσα το ζήτημα για το ποιος, από την πλευρά του παρόχου, έχει πρόσβαση σε αυτά. Σε κάθε περίπτωση ευαίσθητα δεδομένα που υφίστανται επεξεργασία έξω από τον οργανισμό φέρουν μαζί τους ένα εγγενές επίπεδο του κινδύνου καθώς διαδικασίες ελέγχου φυσικής και λογική πρόσβασης, που ισχύουν εντός του οργανισμού, δεν ισχύουν για προσωπικό του παρόχου, που μπορεί να έχει πλέον πρόσβαση εκ των έσω ή με αυξημένα προνόμια[011].

Οι κακόβουλες δραστηριότητες εκ των έσω θα μπορούσαν να έχουν αντίκτυπο στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα όλων των ειδών των δεδομένων ή ακόμα και

σε όλα τα είδη των υπηρεσιών και ως εκ τούτου έμμεσα στη φήμη του οργανισμού και στην εμπιστοσύνη των πελατών. Αξίζει να τονιστεί ότι στην περίπτωση του υπολογιστικού νέφους οι αρχιτεκτονικές υλοποίησης απαιτούν ορισμένους ρόλους που είναι εξαιρετικά υψηλού κινδύνου. Για παράδειγμα τέτοιους ρόλους μπορεί να έχουν οι διαχειριστές του συστήματος, ορισμένοι ελεγκτές ή αντιπρόσωποι φορέων διαχείρισης και παροχής ασφάλειας, που ασχολούνται με εκθέσεις ανίχνευσης εισβολών και αντιμετώπιση περιστατικών. Καθώς αυξάνεται η χρήση των υπηρεσιών νέφους, οι εργαζόμενοι σε αυτό όλο και πιο συχνά γίνονται στόχοι εγκληματικών ενεργειών[031].

Μια πρόσφατη έρευνα αναφέρει ότι το ένα τέταρτο των ηλεκτρονικών εγκλημάτων με αναγνωρισμένους τους δράστες διαπράχθηκαν από υπαλλήλους με πρόσβαση εκ των έσω[014].

4.1.5 Διαχωρισμός των Δεδομένων (Data Segregation)

Ένα από τα 5 βασικά χαρακτηριστικά του νέφους που αναφέρθηκαν στο κεφάλαιο 1 είναι η κοινή διάθεση πόρων: οι υπολογιστικοί πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλαπλούς καταναλωτές με τη χρήση του μοντέλου πολλαπλών μισθωτών. Η υπολογιστική ισχύς, η αποθήκευση και το δίκτυο χρησιμοποιούνται από πολλούς χρήστες ταυτόχρονα.

Ειδικά στο μοντέλου του IaaS χρησιμοποιείται κυρίως η τεχνολογία της εικονικοποίησης (virtualization), όπου οι φυσικοί πόροι διαιρούνται σε πολλές εικονικές συσκευές που μοιράζονται στους χρήστες. Ο Hypervisor είναι ένα λογισμικό, το οποίο εγκαθίσταται στο υλικό (hardware) και δημιουργεί και ελέγχει τις πολλαπλές εικονικές συσκευές. Κάθε εικονική συσκευή μπορεί να δεσμευτεί και από διαφορετικό χρήστη.

Η κατηγορία αυτή των κινδύνων περιλαμβάνει την αποτυχία των μηχανισμών που εξασφαλίζουν το διαχωρισμό της αποθήκευσης, τη μνήμης, της δρομολόγησης μεταξύ των διαφόρων χρηστών της κοινής υποδομής. Αυτό μπορεί να έχει ως αποτέλεσμα κάποιος χρήστης να έχει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του άλλου που μοιράζονται την ίδια φυσική υποδομή. Επιπλέον μπορεί να περιορίσει ή να επηρεάσει τις εφαρμογές και τις υπηρεσίες του άλλου (για παράδειγμα, κλείνοντας εικονικές συσκευές ή εξαντλώντας τους κοινούς φυσικούς πόρους).

Ο αντίκτυπος μπορεί να είναι απώλεια πολύτιμων ή ευαίσθητων δεδομένων για τους πελάτες και για τους παρόχους δυσφήμιση ή και πιθανή διακοπή παρεχομένων υπηρεσιών του νέφους[031].

Ακόμα και η λύση της κρυπτογράφησης των δεδομένων που προωθούνται στο νέφος(που αναλύεται στο επόμενο κεφάλαιο) μπορεί να παρουσιάσει δυσλειτουργίες και προβλήματα που μπορεί να οδηγήσουν σε αποκάλυψη των δεδομένων από χρήστες που μοιράζονται την ίδια υποδομή ή και σε καταστροφή των δεδομένων[011,087].

4.1.6 Προβλήματα Εφαρμογών, Διεπαφών Προγραμματισμού Εφαρμογών (Application Programming Interfaces (APIs))

Οι πάροχοι υπηρεσιών του νέφους μπορούν να προσφέρουν ολόκληρες εφαρμογές (για παράδειγμα στο μοντέλο του SaaS) ή και μία σειρά από διεπαφές προγραμματισμού εφαρμογών μέσω των οποίων οι χρήστες διαχειρίζονται και αλληλεπιδρούν με τις υπηρεσίες του νέφους. Γενικά μέσω των διεπαφών καθορίζεται ο τρόπος με τον οποίο ένα πρόγραμμα ή μία εφαρμογή μπορεί να ζητήσει υπηρεσίες από άλλα προγράμματα, βιβλιοθήκες ή λειτουργικά συστήματα[002]. Η ασφάλεια και η διαθεσιμότητα γενικά των υπηρεσιών του νέφους εξαρτάται από την ασφάλεια αυτών των βασικών διεπαφών.

Τόσο οι εφαρμογές όσο και οι διεπαφές μπορεί να παρουσιάζουν προβλήματα ή κενά ασφάλειας που να βάζουν σε κίνδυνο τα δεδομένα των χρηστών.

Ένα παράδειγμα σε αυτόν τον τομέα παρέχεται από το Facebook. Οι χρήστες του Facebook ανεβάζουν σε αυτό ευαίσθητα και μη ευαίσθητα δεδομένα. Και τα δύο είδη δεδομένων χρησιμοποιούνται από το Facebook για να παρουσιάσει δεδομένα σε άλλους χρήστες, καθώς επίσης χρησιμοποιούνται από εφαρμογές τρίτων που τρέχουν στην πλατφόρμα του Facebook. Αυτές οι εφαρμογές συνήθως δεν ελέγχεται από το Facebook. Έχει παρατηρηθεί ότι υπάρχει μια τάση να δημιουργούνται κακόβουλες εφαρμογές που τρέχουν στο νέφος του Facebook για να κλέψουν ευαίσθητα δεδομένα των χρηστών[017].

Αντίστοιχα μπορεί να χρησιμοποιούνται διεπαφές που να μην είναι κατάλληλα σχεδιασμένες για να προστατεύουν από τυχαίες ή κακόβουλες προσπάθειες παράκαμψης της πολιτική ασφάλειας, για παράδειγμα να μην προσφέρουν έλεγχο ταυτότητας πρόσβασης.

4.1.7 Επαναφορά (Recovery), Ανάκτηση δεδομένων

Όπως προαναφέρθηκε, συχνά πληροφορίες σχετικά με την τοποθεσία των δεδομένων ενός οργανισμού που αποθηκεύονται στο νέφος δεν είναι διαθέσιμες. Ακόμα όμως και όταν δεν είναι γνωστή η θέση των δεδομένων, ο πάροχος είναι υποχρεωμένος να προβλέπει τι θα γίνει σε αυτά και στις παρεχόμενες υπηρεσίες σε περίπτωση καταστροφής. Κάθε προσφορά υπηρεσίας νέφους που δεν τηρεί αντίγραφα ασφάλειας των δεδομένων και της δομής των εφαρμογών σε διάφορες τοποθεσίες είναι ευάλωτη σε μία ολική καταστροφή. Ο πάροχος πρέπει να παρέχει την ικανότητα της επαναφοράς των υπηρεσιών και ανάκτησης των δεδομένων και μάλιστα να έχει εκτιμήσει σε πόσο χρόνο μπορεί να το κάνει αυτό[011,042,078].

4.1.8 Μη ολοκληρωμένη διαγραφή δεδομένων(Incomplete data deletion)

Το πρόβλημα με τη μη ολοκληρωμένη διαγραφή των δεδομένων έχει δύο πτυχές. Από τη μία ο συνηθισμένος τρόπος διαγραφής των αρχείων στους υπολογιστές δεν αφαιρεί πραγματικά τα δεδομένα από τον σκληρό δίσκο, απλώς αφαιρεί την αναφορά σε αυτά. Αφήνει έτσι υπολείμματα που μπορούν να είναι χρήσιμα, μετά από ειδική επεξεργασία από κάποιον που θα έχει πρόσβαση σε αυτά. Στην περίπτωση του νέφους αυτός ο κάποιος μπορεί να είναι ο επόμενος πελάτης που θα δεσμεύσει τον αποθηκευτικό χώρο από τον οποίο διαγράφηκαν τα δεδομένα[087].

Από τη άλλη είναι δυνατό να υπάρχουν αντίγραφα ασφάλειας των δεδομένων σε διάφορες τοποθεσίες στους κατανεμημένους εξυπηρετητές που έχει στην κατοχή του ο πάροχος. Τα αντίγραφα αυτά μπορεί να μην διαγράφονται ταυτόχρονα με τα δεδομένα του πρωτοτύπου[033,064].

Για παράδειγμα η GOOGLE όσο αφορά την υπηρεσία Google Doc's αναφέρει ότι τα δεδομένα των πελατών μπορεί και να παραμείνουν στην κατοχή της GOOGLE ακόμα και αν ο πελάτης έχει διαγράψει τα δεδομένα. Συγκεκριμένα αναφέρει ότι «μετά τη διαγραφή των στοιχείων σας από τις υπηρεσίες μας, ενδέχεται να μην διαγράψουμε αυτόματα κάποια εναπομείναντα αντίγραφα από τους ενεργούς διακομιστές μας και να μην απομακρύνουμε τα στοιχεία από τα συστήματά μας αντιγράφων ασφάλειας»[035].

Ένα επιπλέον ζήτημα που προκύπτει είναι το τι συμβαίνει στα δεδομένα ενός πελάτη όταν τερματίσει την συνεργασία με τον πάροχο. Εκτός από τη διαγραφή των ίδιων των δεδομένων

είναι γεγονός ότι, μετά από ένα εύλογο διάστημα χρήσης του νέφους έχουν συγκεντρωθεί στον πάροχο πολλά δεδομένα για τα δεδομένα (metadata). Πρόκειται για υψηλού επιπέδου πληροφορίες για παράδειγμα σχετικά με το από πού προήρθαν τα δεδομένα,, ποιος είχε πρόσβαση σε τι και άλλα, που τελικά με τους κατάλληλους συνδυασμούς μπορούν να οδηγήσουν σε αποκάλυψη προσωπικών ή ευαίσθητων δεδομένων[075,087]

4.1.9 Υποστήριξη Έρευνας (Investigative support)

Στο περιβάλλον του νέφους με τη διασπορά των δεδομένων σε διάφορες τοποθεσίες και τη χρήση πολλών εικονικών συσκευών διαφόρων χρηστών, που μοιράζονται το ίδιο φυσικό μέσο, η διερεύνηση μη προβλεπόμενης ή παράνομης δραστηριότητας μπορεί να είναι αδύνατη. Η δυναμική και η ρευστή φύση των εικονικών μηχανών θα καταστήσει δύσκολη τη διατήρηση της συνοχής της ασφάλειας και την εξασφάλιση της δυνατότητας ελέγχου των εγγραφών[042]. Έτσι είναι πιθανό να συμβεί απώλεια ή διαρροή των καταγραφών ασφάλειας (Security Logs)[031].

Επιπλέον στην περίπτωση που ένας τρίτος εκτός του νέφους, παραβιάσει έναν μισθωτή μέσω των υποδομών του νέφους, που ο μισθωτής απαγορεύεται να παρακολουθήσει, μπορεί να είναι αδύνατο για το μισθωτή να προσδιορίσει την αιτία της παραβίασης και να λάβει τα μέτρα για την μελλοντική αποτροπή του. Επειδή η υποδομή είναι κοινή και σε άλλους μισθωτές, οι μισθωτές μπορεί να απαγορεύεται ρητά να διερευνήσουν τα στοιχεία υποδομής, καθώς με αυτόν τον τρόπο θα μπορούσαν να παραβιάζουν τις εγγυήσεις ασφάλειας του παρόχου προς τους άλλους ενοίκους της υποδομής του [052].

Μία άλλη πιθανή επιπλοκή εμφανίζεται στην περίπτωση που πελάτης του νέφους είναι ο ίδιος επιχείρηση που έχει αναλάβει υποχρέωση να παρέχει νόμιμα και συμφωνηθέντα στοιχεία καταγραφών στους δικούς του πελάτες, τα οποία όμως ο πάροχος του νέφους δε δύναται ή δε διατίθεται να τα παρέχει[084].

4.1.10 Βιωσιμότητα σε Βάθος Χρόνου (Long-term Viability)

Σε μία ιδανική περίπτωση ο πάροχος θα είναι πάντα διαθέσιμος να υποστηρίζει τους πελάτες του. Σε βάθος χρόνου πάντως υπάρχει μία αβεβαιότητα και κανείς δεν μπορεί να προβλέψει αν

θα χρεοκοπήσει ή θα αποκτηθεί από μία άλλη εταιρεία μεγαλύτερη, που μπορεί να έχει ανταγωνιστικά συμφέροντα με κάποιους από τους πελάτες[011,042].

Γενικά υφίσταται το ζήτημα κατά πόσο οι πελάτες έχουν τη δυνατότητα να μετακινήσουν τα δεδομένα τους από έναν πάροχο και αυτά να είναι σε τέτοια μορφή που να μπορούν να χρησιμοποιηθούν και σε άλλους παρόχους ή ακόμα από τους ίδιους πελάτες στην ιδιωτική τους υποδομή. Καθώς οι πάροχοι προσφέρουν διάφορα εργαλεία ή διεπαφές που είναι πνευματική τους ιδιοκτησία, είναι πιθανό οι εφαρμογές που δημιουργήθηκαν ή τα δεδομένα που αποθηκεύτηκαν με αυτά τα εργαλεία να είναι ακατάληπτα από την υποδομή άλλων παρόχων.

Μέχρι σήμερα υπάρχει περιορισμένη προσφορά εργαλείων, διαδικασιών ή διεπαφών που να πληρούν τυποποιημένα πρότυπα και να μπορούν να εγγυηθούν φορητότητα των δεδομένων, των εφαρμογών και των υπηρεσιών. Δημιουργείται με αυτόν τον τρόπο εξάρτηση του πελάτη σε συγκεκριμένο πάροχο(lock in)[017,064,091]. Για παράδειγμα το κλείσιμο του παρόχου Coghead που τελικά αγοράστηκε από άλλο πάροχο, άφησε εκτεθειμένους τους πελάτες που έπρεπε να ξαναγράψουν τις εφαρμογές τους να τρέχουν σε άλλες πλατφόρμες[017].

4.1.11 Αξιοπιστία, Διαθεσιμότητα Παρόχου

Συνήθως οι πάροχοι διαφημίζουν ποσοστό διαθεσιμότητας και αξιοπιστίας που φτάνει και το 99%. Καθώς όμως η υποδομή των παρόχων γίνεται όλο και πιο πολύπλοκη και σε αυτή εκτελείται μία μεγάλη ποικιλία από περιβάλλοντα των πελατών τίθεται το ζήτημα κατά πόσο αυτό είναι ρεαλιστικό και τηρείται από τους παρόχους[063]. Τυχόν διακοπές μπορεί να οδηγήσουν σε διαστήματα χωρίς δυνατότητα λειτουργίας, γεγονός που μπορεί να μειώσει τα έσοδα και να αμαυρώσει τη φήμη ενός οργανισμού[048].

Στο παρελθόν έχουν υπάρξει διαστήματα ωρών κατά τις οποίες ήταν μη διαθέσιμες οι υπηρεσίες ενός παρόχου. Ένα σχετικά πρόσφατο παράδειγμα είναι η διακοπή των υπηρεσιών video streaming του NETFLIX την παραμονή των Χριστουγέννων του 2012 στις ΗΠΑ, Καναδά και Λατινική Αμερική, που όπως αποδείχτηκε οφείλονταν σε πρόβλημα της υπολογιστικής υποδομής του παρόχου(AMAZON)[065].

4.2 Θέματα Διαδικτύου

Όλη η αρχιτεκτονική της λειτουργίας του νέφους βασίζεται στο διαδίκτυο, συνεπώς συνεχίζουν να υφίστανται οι κίνδυνοι που σχετίζονται με τη λειτουργία του διαδικτύου.

4.2.1 Διαθεσιμότητα Διαδικτύου

Η ίδια η λειτουργία του διαδικτύου είναι σημαντική και απαραίτητη για την παροχή των υπηρεσιών νέφους. Μία πιθανή διακοπή μπορεί να επηρεάσει χιλιάδες πελατών[031].

Επιπλέον σε διεθνές επίπεδο έχει αρχίσει να δημιουργείται μία διαμάχη για τον έλεγχο του διαδικτύου. Η Ρωσία και η Κίνα συμμαχούν εναντίον των ΗΠΑ και τίθενται επικεφαλής και άλλων χωρών, επιζητώντας να αποσπάσουν τον έλεγχο και την εκχώρηση διευθύνσεων του διαδικτύου από τον αρμόδιο- αμερικάνικο- οργανισμό. Πρόκειται για τον οργανισμό με έδρα την Καλιφόρνια, ονόματι Internet Corporation for Assigned Names and Numbers (ICANN), του οποίου η αποστολή συνίσταται στη «διατήρηση της λειτουργικής σταθερότητας του Διαδικτύου». Πλέον η Ρωσία αμφισβητεί την ανεξαρτησία του οργανισμού και απαιτεί είτε τη δημιουργία άλλου διεθνούς πλήρως ανεξάρτητου οργανισμού, είτε την αλλαγή του καθεστώτος λειτουργίας του ICANN[096, 100].

Είναι προφανές ότι εξελίσσεται μία διακρατική διαμάχη γύρω από την πολιτική οικονομία του κυβερνοχώρου και του διαδικτύου, χωρίς να είναι δυνατό να προβλεφθούν τα αποτελέσματά της.

4.2.2 Ασφάλεια Φυλλομετρητή (Browser Security)

Η στροφή στη χρήση του νέφους μετακίνησε μεγάλο μέρος της συνήθους δραστηριότητας του χρήστη να εκτελείται μέσω του προγράμματος περιήγησης στο δίκτυο, του φυλλομετρητή ιστοσελίδων. Τα προγράμματα αυτά γενικά αποθηκεύουν όλους τους κωδικούς πρόσβασης ενός χρήστη, το ιστορικό περιήγησης και άλλες ευαίσθητες πληροφορίες σε ένα μόνο σημείο. Ως εκ τούτου, είναι δυνατό κακόβουλες ιστοσελίδες να εκμεταλλεύονται τρωτότητες των προγραμμάτων περιήγησης, προκειμένου να υποκλέψουν πληροφορίες που σχετίζονται με άλλες υφιστάμενες ή προηγούμενες συνόδους περιήγησης, όπως τη σύνδεση σε λογαριασμό ηλεκτρονικού ταχυδρομείου ή τη σύνδεση για διενέργεια τραπεζικών συναλλαγών[077].

4.2.3 Επιθέσεις Άρνησης Παροχής Υπηρεσιών (Denial Of Service (D.O.S.) Attacks)

Μία συνηθισμένη επίθεση στο χώρο του διαδικτύου αλλά και στο περιβάλλον του νέφους είναι αυτή της Άρνησης Παροχής Υπηρεσιών. Έχει ως σκοπό να υπερφορτώσει τόσο πολύ το σύστημα στόχο καταναλώνοντας μνήμη, εύρος ζώνης επικοινωνίας, εικονικές μηχανές και γενικά πόρους του, έτσι ώστε να μην είναι σε θέση πλέον να εξυπηρετήσει τους κανονικούς χρήστες του.

Αυτό επιτυγχάνεται είτε μέσω αποστολής πακέτων δεδομένων (data packets) σε υπερβολικά μεγάλο ρυθμό έτσι ώστε το σύστημα στόχος να αδυνατεί να τα επεξεργαστεί, είτε μέσω εκμετάλλευσης των αδυναμιών του πρωτοκόλλου TCP/IP, είτε στέλνοντας μαζικές απαιτήσεις στους εξυπηρετητές του νέφους, που δεν μπορούν να τις διαχειριστούν. Στο περιβάλλον του νέφους οι επιθέσεις αυτές μπορεί να ξεκινούν και μέσα από αυτό με στόχο άλλους πελάτες που μοιράζονται την ίδια φυσική υποδομή. Με τον τρόπο αυτό έμμεσα εμποδίζεται ή περιορίζεται η πρόσβαση των κανονικών πελατών στους πόρους και στις υπηρεσίες του νέφους[045,064].

Οι επιθέσεις αυτές μπορούν να χωριστούν σε τρεις κατηγορίες: επιθέσεις πλημμυρίδας (Flooding Attacks), Επιθέσεις Στέρησης Πόρων(Resource Starvation Attacks) και Διακοπής Υπηρεσιών (Disruption of Service).

4.2.4 Επιθέσεις Ενδιάμεσου (Man in the Middle Attacks)

Αυτό το είδος της επίθεσης συμβαίνει όταν ένας επιτιθέμενος διεισδύσει στο κανάλι επικοινωνίας προκειμένου να παρακολουθεί την επικοινωνία και να τροποποιήσει τα μηνύματα για κακόβουλους σκοπούς[008]. Το περιβάλλον του νέφους, όπου πολλοί χρήστες μοιράζονται την ίδια υποδομή μπορεί να χρησιμοποιηθεί για τέτοιες επιθέσεις.

Μπορεί να συμβεί ακόμα και αν γίνεται χρήση της τεχνολογίας Secure Socket Layer (SSL) (αναφέρεται στο κεφάλαιο 5) που δεν είναι σωστά ρυθμισμένη. Για παράδειγμα, αν δύο μέρη επικοινωνούν μεταξύ τους με SSL και δεν έχει γίνει σωστή πιστοποίηση της ταυτότητας μεταξύ τους ή η επικοινωνία δεν είναι επαρκώς κρυπτασφαλισμένη, τότε κάποιος ενδιάμεσος θα μπορούσε να εισχωρήσει στην επικοινωνία [039,064].

4.2.5 Επιθέσεις Παρακολούθησης Δικτύου (Network Sniffing Attacks)

Ένα παρόμοιο είδος επίθεσης είναι η παρακολούθηση του δικτύου. Είναι ένα κρίσιμο ζήτημα της ασφάλειας του δικτύου, στο οποίο τα μη κρυπτογραφημένα δεδομένα υποκλέπτονται μέσω της παρακολούθησης της κίνησης του δικτύου. Για παράδειγμα, ένας εισβολέας παρακολουθεί όλη την κίνηση του δικτύου και μπορεί να υποκλέψει ότι δεν είναι κρυπτασφαλισμένο, όπως όνομα και κωδικό πρόσβασης κάποιου νόμιμου χρήστη κ.α [039,064].

4.2.6 Σάρωση Θυρών (Port scanning)

Στην επίθεση αυτή ο επιτιθέμενος προσπαθεί να ανακαλύψει θύρες που είναι ανοιχτές σε έναν εξυπηρετητή ή σε μία εικονική συσκευή, ώστε να αποκτήσει πρόσβαση σε αυτές. Συνήθως η σάρωση ξεκινάει από θύρες, που λόγω κοινών προτύπων είναι συνήθως ανοιχτές όπως η θύρα 80 για το HTTP ή η θύρα 21 για το FTP [039,064].

4.2.7 Επίθεση SQL (SQL Injection Attack)

Μέσα απ' αυτή την επίθεση δίνεται η δυνατότητα σε κάποιον κακόβουλο, μέσα από εισαγωγή ειδικών χαρακτήρων, ακόμα και στο πεδίο εισαγωγής διεύθυνσης ενός φυλλομετρητή, να δώσει εντολές SQL σε ένα εξυπηρετητή στόχο που φιλοξενεί στοιχεία βάσης δεδομένων, ώστε να αποσπάσει αρκετά ευαίσθητες πληροφορίες (όπως για παράδειγμα κωδικοί πρόσβασης, ονόματα χρηστών, διευθύνσεις ηλεκτρονικών ταχυδρομείων, αριθμοί πιστωτικών καρτών κ.α.) μέσα από την βάση[039,064].

4.2.8 Ιοί(Viruses) και Κακόβουλο λογισμικό (Malware)

Οι ιοί και το κακόβουλο λογισμικό είναι πολύ συχνές και γνωστές επιθέσεις. Συνήθως πρόκειται για κομμάτι κώδικα, με σκοπό να μειώσει την απόδοση του εξοπλισμού και των εφαρμογών ή και να καταστρέψει αποθηκευμένα αρχεία ή δεδομένα[008].

4.3 Θέματα Εικονικοποίησης (Virtualization)

Η χρήση της τεχνολογίας της εικονικοποίησης είναι βασική για τη λειτουργία του νέφους. Ένα ειδικό λογισμικό, συνήθως ο Hypervisor, εγκαθίσταται στο υλικό (hardware) και δημιουργεί

πολλαπλές εικονικές συσκευές, που τρέχουν πάνω στο υλικό, παρέχοντας απομόνωση μεταξύ των διαφόρων εικονικών συσκευών των πελατών[056].

Οι επιθέσεις στο επίπεδο του Hypervisor είναι πολύ ελκυστικές, γιατί καθώς είναι το λογισμικό που ελέγχει τους φυσικούς πόρους και τις εικονικές συσκευές που «τρέχουν» πάνω σε αυτόν, κάθε ευπάθεια σε αυτό το επίπεδο είναι εξαιρετικά κρίσιμη. Η εξασφάλιση δυνατότητας πρόσβασης και εκμετάλλευσης του Hypervisor δυνητικά σημαίνει εκμετάλλευση κάθε εικονικής συσκευής που αυτός διαχειρίζεται[031].

Ο Hypervisor θεωρητικά μπορεί να είναι μικρότερος και πιο απλός από ένα λειτουργικό σύστημα. Με αυτά τα χαρακτηριστικά γίνεται ευκολότερο να αναλυθεί σε βάθος και να βελτιωθεί η ποιότητα της ασφάλειας, δίνοντάς του τη δυνατότητα να είναι καλύτερα προσαρμοσμένος στη διατήρηση της ισχυρής απομόνωση μεταξύ των φιλοξενούμενων εικονικών συσκευών, από ό τι είναι αντίστοιχα ένα λειτουργικό σύστημα στην απομόνωση των διαδικασιών. Στην πράξη όμως οι σύγχρονοι Hypervisors είναι πλέον τόσο μεγάλοι και πολύπλοκοι που συγκρίνονται πλέον με ένα λειτουργικό σύστημα. Το μέγεθος αυτό και η πολυπλοκότητα κάνει πλέον δύσκολο τον πλήρη έλεγχο και τη θωράκιση απέναντι σε επιθέσεις[031,043].

Ήδη κατά καιρούς έχουν εμφανιστεί τρωτότητες σε διάφορα είδη Hypervisor όπως στον VMWare , στον Xen κ.α [017].

4.4 Νομικά Θέματα

Το περιβάλλον της νεφοϋπολογιστικής ουσιαστικά συνεπάγεται την ύπαρξη κάποιου διακανονισμού, μέσα από τον οποίο οι χρήστες αποθηκεύουν τα δεδομένα τους σε απομακρυσμένους κατανεμημένους εξυπηρετητές, που ελέγχονται από άλλους(τους παρόχους) και χρησιμοποιούν εφαρμογές, υπολογιστικούς πόρους που εκτελούνται και βρίσκονται κάπου αλλού και όχι στην ιδιόκτητη υπολογιστική υποδομή τους. Διάφορα νομικά θέματα μπορεί να προκύψουν από αυτόν το διακανονισμό.

Είναι γεγονός ότι υπάρχει αντίφαση μεταξύ της εστίασης κάποιων νόμων σε περιορισμούς σχετικά με τις γεωγραφικές περιοχές των δεδομένων και της πανταχού παρούσας φύσης του νέφους. Για παράδειγμα όσον αφορά τα προσωπικά δεδομένα τρίτων, η οδηγία για την

προστασία των δεδομένων επιβάλλει τα δεδομένα να αποθηκεύονται είτε στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ) ή σε επικράτεια διεπόμενη από ισοδύναμους νόμους περί ιδιωτικότητας [097].

Έτσι επί του παρόντος, δεν είναι σαφές κατά πόσον ένα άτομο στην Ευρώπη, ο οποίος ανεβάζει προσωπικές πληροφορίες σχετικά με κάποιο άλλο άτομο στη σελίδα του στο Facebook, παραβιάζει την Ευρωπαϊκή Οδηγία 95/46 αν το πρόσωπο που ανεβάζει τις πληροφορίες, έχει «φίλους» έξω από την ΕΕ. Ο νόμος απλά δεν είναι αρκετά σαφής για κάποιον για να γνωρίζει το νομικό καθεστώς μιας αντίστοιχης πράξης, και είναι στην ευθύνη των καταναλωτών να καταλάβουν ότι υπάρχει κάποιος «κρυφός κίνδυνος» [075].

Γενικά η συμφωνία μεταξύ του παρόχου και του πελάτη για τις παρεχόμενες υπηρεσίες, το επίπεδο ασφάλειας, τη συμβατότητα, τις ευθύνες, τις χρεώσεις περιγράφεται αναλυτικά στο Συμφωνητικό Παροχής Υπηρεσιών (ΣΠΥ) που ουσιαστικά αποτελεί ένα είδος σύμβασης μεταξύ των εμπλεκομένων. Μέχρι τώρα έχουν εντοπιστεί αρκετές αδυναμίες σε αυτά τα συμφωνητικά. Για παράδειγμα τα περισσότερα είναι προσανατολισμένα με τα συμφέροντα του παρόχου, είναι αδιαφανή, αλλάζουν εύκολα(συχνά χωρίς την ειδοποίηση του πελάτη) και δεν περιγράφουν ξεκάθαρα τις υποχρεώσεις παροχής υπηρεσιών του παρόχου κ.α.[020].

4.5 Επικινδυνότητα (Risk)

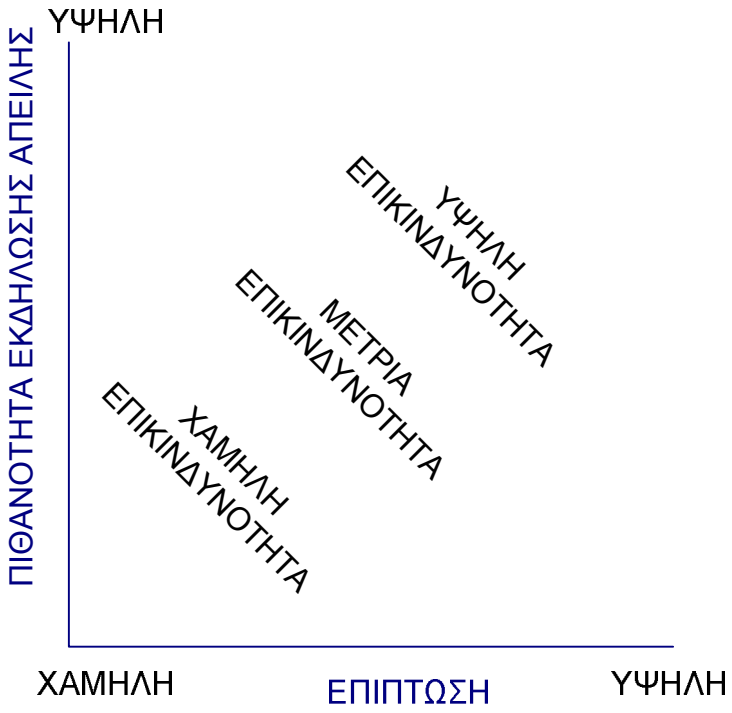
Μέχρι τώρα στο κεφάλαιο αυτό αναφέρθηκαν οι κίνδυνοι και τα ζητήματα ασφάλειας που σχετίζονται με τη χρήση του νέφους. Οι επιπτώσεις(impacts) που μπορεί να αυτά να επιφέρουν είναι οι απώλειες στα «αγαθά», τόσο του παρόχου όσο και του οργανισμού – χρήστη.

Με τον όρο αγαθό(asset) περιγράφονται οι πληροφορίες, τα δεδομένα, οι υπολογιστικοί πόροι που έχουν αξία για τους ιδιοκτήτες(owners) τους[099].

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Network and Information Security Agency (ENISA)) σε μελέτη που εκδόθηκε το Νοέμβριο του 2009 [031] αναγνώρισε 23 αγαθά που σχετίζονται με το νέφος. Με βάση την επίπτωση που θα έχει πιθανή απώλεια των αγαθών κατηγοριοποιήθηκε η αξία τους σε τέσσερις διαβαθμίσεις: χαμηλή , μέση , υψηλή , πολύ υψηλή.

Στην βαθμίδα με πολύ υψηλή αξία περιλαμβάνονται τα ακόλουθα αγαθά: η φήμη του οργανισμού, η εμπιστοσύνη των πελατών, τα ευαίσθητα προσωπικά δεδομένα, η παροχή υπηρεσιών πραγματικού χρόνου (real time services delivery) , τα διαπιστευτήρια (credentials) πελατών ή προσωπικού και η διαχείριση των διεπαφών παροχής των υπηρεσιών του νέφους.

Η επικινδυνότητα είναι ανάλογη της επίπτωσης και της πιθανότητας εκδήλωσης μίας απειλής που μπορεί να προκαλέσει ζημία σε ένα αγαθό. Ο βαθμός επικινδυνότητας αναλόγως της επίπτωσης και της πιθανότητας της απειλής παρουσιάζεται στο ακόλουθο σχήμα[031,099].



Σχήμα 4.1: Υπολογισμός επικινδυνότητας αναλόγως επίπτωσης και πιθανότητας μιας απειλής.

Κεφάλαιο 5
Ασφάλεια στο Περιβάλλον Νεφοϋπολογιστικής

Στο κεφάλαιο αυτό αναλύεται ότι, για να επιτευχθεί η ασφάλεια στο «νεφελώδες» περιβάλλον της νεφοϋπολογιστικής, απαιτούνται διάφορα βήματα που ξεκινούν από θέσπιση κατάλληλων διαδικασιών, πρακτικών, χρήση ειδικών τεχνικών εξασφάλισης των δεδομένων και εφαρμογή ρυθμίσεων, που συνεισφέρουν στην ασφάλεια σε βάθος. Αναφέρονται, επίσης, λύσεις για την ασφαλή χρήση της εικονικοποίησης και άλλες εφαρμοσμένες επιλογές, όπως είναι η περίπτωση του Trusted Cloud Computing και του υβριδικού νέφους.

5.1 Διαδικασίες, Πρακτικές

Η προσπάθεια επίτευξης του αναμενόμενου επιπέδου ασφάλειας σε ένα πληροφοριακό σύστημα ξεκινάει με τη θέσπιση κατάλληλων διαδικασιών-πρακτικών, όπως αυτές περιγράφονται ακολούθως.

5.1.1 Διαβάθμιση της Πληροφορίας

Υπάρχουν πολλοί λόγοι για τη διαβάθμιση της πληροφορίας, καθώς όλα τα δεδομένα δεν έχουν την ίδια αξία για έναν οργανισμό. Για παράδειγμα, κάποια μπορεί να είναι περισσότερο πολύτιμα για τα ανώτερα επίπεδα διοίκησης και σκοπό έχουν τη βοήθεια της διοίκησης στη λήψη αποφάσεων, κάποια άλλα μπορεί να περιέχουν εταιρικά μυστικά ή πληροφορίες για νέα προϊόντα. Η διαρροή ή απώλεια δεδομένων τέτοιου τύπου μπορεί να προκαλέσει σημαντικά προβλήματα σε έναν οργανισμό [046].

Η πληροφορία πρέπει να διαβαθμίζεται αναλόγως της ευαισθησίας του οργανισμού στην απώλεια ή διαρροή της. Ο ιδιοκτήτης της πληροφορίας είναι υπεύθυνος για τον προσδιορισμό της διαβάθμισή της.

Μερικές τυποποιημένες βαθμίδες διαβάθμισης ακολουθούν[046].

- Δημόσια δεδομένα: αφορούν πληροφορίες που είναι μη διαβαθμισμένες καθώς και όλες τις πληροφορίες ενός οργανισμού που δεν ανήκουν σε κάποια από τις επόμενες κατηγορίες.

- Ευαίσθητα δεδομένα: αφορούν πληροφορίες που απαιτούν ένα υψηλότερο επίπεδο διαβάθμισης από τα δημόσια δεδομένα. Οι πληροφορίες αυτές πρέπει να προστατεύονται από την απώλεια της εμπιστευτικότητας καθώς και από την απώλεια της ακεραιότητας που μπορεί να οφείλεται σε μη εξουσιοδοτημένη αλλοίωση.

- Προσωπικά δεδομένα: τα δεδομένα αυτά αναλύθηκαν στο κεφάλαιο 3.2.1 της μεταπτυχιακής διατριβής, σε αυτά περιλαμβάνονται και τα ευαίσθητα προσωπικά δεδομένα. Η μη εξουσιοδοτημένη αποκάλυψη αυτών μπορεί να επιφέρει σοβαρές και δυσμενείς επιπτώσεις για έναν οργανισμό και / ή τους υπαλλήλους του.

- Εμπιστευτικά δεδομένα: η διαβάθμιση αυτή ισχύει για το πιο ευαίσθητες πληροφορίες ενός οργανισμού, που προορίζονται αποκλειστικά για χρήση εντός του οργανισμού. Μη εξουσιοδοτημένη αποκάλυψή τους, θα μπορούσε να επηρεάσει αρνητικά τον οργανισμό, τους μετόχους του, τους συνεργάτες του, και / ή τους πελάτες του.

Κριτήρια που μπορούν να χρησιμοποιηθούν για τη διαβάθμιση μιας πληροφορίας είναι η αξία της, η ηλικία της, η χρήσιμη διάρκεια ζωής της, η συσχέτισή της με προσωπικά δεδομένα. Μετά τον καθορισμό της διαβάθμισης μίας πληροφορίας απαιτείται να καθοριστεί και η λίστα

διανομής της διαβαθμισμένης πληροφορίας, δηλαδή ποιοι και πότε θα έχουν πρόσβαση στην πληροφορία αυτή.

Η σωστή διαβάθμιση της πληροφορίας συμβάλλει στην εξασφάλιση ιδιωτικότητας και στην κανονιστική συμμόρφωση ενός οργανισμού.

5.1.2 Πολιτική Ασφάλειας

Για την επίτευξη της ασφάλειας των δικτύων υπολογιστών, είτε αυτό αναπτύσσεται σε περιβάλλον νέφους είτε όχι, και τελικά της ασφάλειας των πληροφοριών, το πρώτο πράγμα που πρέπει να γίνει, είναι να καθοριστούν οι πολιτικές και οι διαδικασίες που θα προστατεύουν την πληροφορία.

Η Πολιτική Ασφάλειας ενός πληροφοριακού συστήματος περιγράφει το σκοπό και τους στόχους της ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία του πληροφοριακού συστήματος [098]. Δημιουργείται δηλαδή ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν το ρόλο, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντα κάθε εμπλεκόμενου μέσα σε μια εταιρεία ή οργανισμό, που χρησιμοποιεί το πληροφορικό σύστημα .

Το ινστιτούτο SANS αναφέρει ότι η Πολιτική Ασφάλειας αποτελεί τη βάση της ασφάλειας πληροφορικής σε έναν οργανισμό[069] και προτείνει τα ακόλουθα βασικά βήματα για τη δημιουργία της:

1. Προσδιορισμός αγαθών(assets) που πρέπει να προστατευτούν.

2. Προσδιορισμός τρωτοτήτων, απειλών και πιθανότητα των απειλών να συμβούν.

3. Επιλογή μέτρων που θα προστατεύσουν τα αγαθά με αποδοτικό και οικονομικό τρόπο.

4. Γνωστοποίηση των ευρημάτων και των αποτελεσμάτων στους αρμόδιους.

5. Παρακολούθηση και αναθεώρηση της όλης διαδικασίας συνεχώς για βελτιώσεις.

Ενδεικτικά ζητήματα που πρέπει να αντιμετωπίζονται, αναλύονται σε μία πολιτική ασφάλειας είναι η φυσική ασφάλεια των υποδομών, η ασφάλεια λογισμικού, το σχέδιο αντιμετώπισης εκτάκτων αναγκών καθώς και οι διαδικασίες αντιμετώπισης ζητημάτων ασφάλειας.

Στο περιβάλλον της νεφοϋπολογιστικής ο σκοπός της πολιτικής θα ποικίλει αναλόγως του μοντέλου υπηρεσίας του νέφους, θα υπάρχει μια επικάλυψη μεταξύ πολιτικών SaaS, PaaS, και IaaS αλλά σε μεγάλο βαθμό η πολιτική θα γίνεται ευρύτερη όταν κινούμαστε από το SaaS προς το IaaS. Συνήθως, ο σκοπός της εταιρικής πολιτικής που καθορίζει τη χρήση του δημόσιου νέφους διαφέρει από την πολιτική του ίδιου του οργανισμού για τη χρήση ιδιόκτητου νέφους [087].

Η σωστή πρακτική για έναν πάροχο και έναν καταναλωτή υπηρεσιών νέφους είναι να δημιουργήσουν και να καθορίσουν μία ξεκάθαρη πολιτική, που θα καλύπτει όλα τα θέματα σχετικά με την ασφάλεια , θα αναθέτει ευθύνες και θα είναι προσπελάσιμη από όλους αυτούς που αφορά[087].

5.1.3 Αποτελεσματική Διαχείριση Επικινδυνότητας (Risk)

Η διαχείριση της επικινδυνότητας είναι η διαδικασία της αναγνώρισης, μέτρησης, παρακολούθησης του βαθμού της, όπως παρουσιάστηκε στο κεφάλαιο 4, και τελικά διαχείρισης του εναπομείναντος κινδύνου. Επικινδυνότητα υπάρχει είτε αν ένας οργανισμός διατηρεί πληροφορίες και υπηρεσίες τεχνολογίας εσωτερικά είτε αν επιλέγει να τα αναθέσει σε τρίτους (για παράδειγμα σε παρόχους)[031].

Ένας οργανισμός πρέπει περιοδικά να αξιολογεί τους κινδύνους, που σχετίζονται με τις επιχειρήσεις του (συμπεριλαμβανομένου της αποστολής, της λειτουργίας, της εικόνας ή της φήμης), τα αγαθά του οργανισμού και τους ιδιώτες, που πηγάζουν από τη λειτουργία των πληροφοριακών συστημάτων και την αντίστοιχη επεξεργασία, αποθήκευση, ή μεταφορά των πληροφοριών του οργανισμού[054].

Το Federal Financial Institutions Examination Council [034] αναφέρει ότι μια αποτελεσματική διαδικασία διαχείρισης επικινδυνότητας περιλαμβάνει τα ακόλουθα βήματα:

1. Καθιέρωση, για τα ανώτερα επίπεδα διοίκησης του οργανισμού, της επίγνωσης των κινδύνων, που συνδέονται με τις συμφωνίες εξωτερικής ανάθεσης υπηρεσιών, προκειμένου να διασφαλιστούν αποτελεσματικές πρακτικές διαχείρισής των.

2. Εξασφάλιση ότι η συμφωνία εξωτερικής ανάθεσης συνάδει, από την σκοπιά των κινδύνων που συνεπάγεται, με τους επιχειρηματικούς στόχους του οργανισμού.

3. Συστηματική αξιολόγηση των αναγκών, καθώς καθιερώνονται απαιτήσεις βάσει κινδύνου.

4. Εφαρμογή αποτελεσματικών ελέγχων για την αντιμετώπιση των κινδύνων που εντοπίζονται.

5. Εκτέλεση συνεχής παρακολούθησης για τον εντοπισμό και την αξιολόγηση των μεταβολών του κινδύνου από την αρχική εκτίμηση.

6. Καταγραφή των διαδικασιών, των ρόλων / αρμοδιοτήτων, καθώς των μηχανισμών υποβολής αναφορών.

Με απλά λόγια η διαχείριση επικινδυνότητας πρέπει να γίνει η κύρια δραστηριότητα γύρω από την οποία θα περιστρέφονται οι πρακτικές ασφάλειας[087].

Σε ένα περιβάλλον νέφους η διοίκηση μετά την ανάλυση της επικινδυνότητας μπορεί να επιλέξει μία από τις ακόλουθες τακτικές για συγκεκριμένους κινδύνους[021]:

1. Αποφυγή: Μη επιλέγοντας τις δραστηριότητες που αυξάνουν την επικινδυνότητα.

2. Μείωση: Παίρνοντας μέτρα που ελαττώνουν την πιθανότητα ή την επίπτωση ενός κινδύνου.

3. Διαμοιρασμός ή ασφάλιση: Μεταφέροντας ή αναθέτοντας μέρος της επικινδυνότητας για χρηματοδότηση.

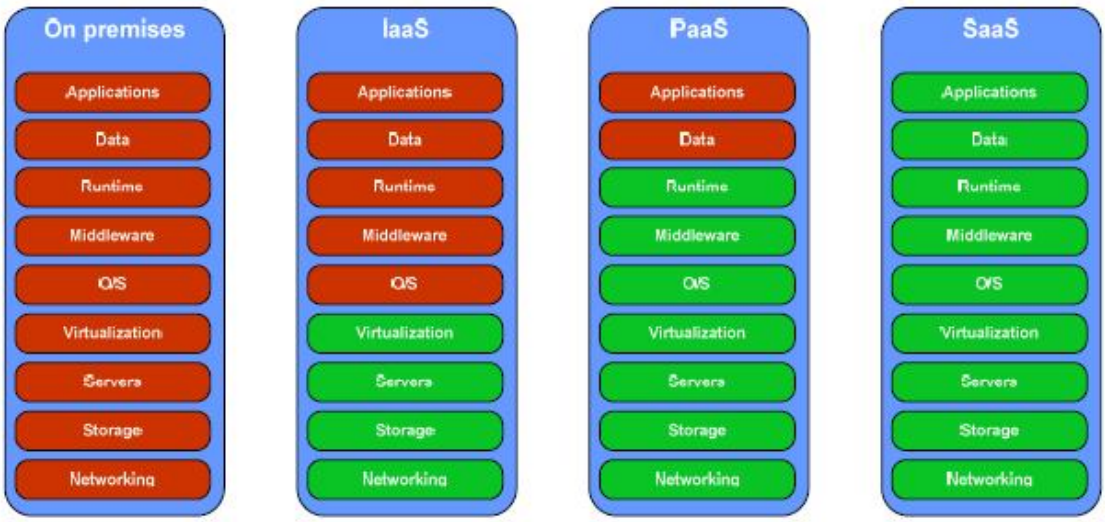
4. Αποδοχή: Καμία ενέργεια δεν εκτελείται λόγω του συσχετισμού κόστους/κέρδους.

Η διαχείριση επικινδυνότητας είναι στην ουσία μια διαδικασία εξισορρόπησης με στόχο, όχι απαραίτητα την ελαχιστοποίηση της αβεβαιότητας, αλλά μάλλον την μεγιστοποίηση της αξίας και του κέρδους ανάλογα με την διάθεση ανάληψης κινδύνου και τη συνολική στρατηγική. Υπάρχουν πολλές μεταβλητές, αξίες και κίνδυνοι σε κάθε ευκαιρία που προσφέρει το νέφος που επηρεάζουν την απόφαση αν ένας συγκεκριμένος πάροχος πρέπει να επιλεγεί από την άποψη της επικινδυνότητας ή της αξίας του οργανισμού. Κάθε οργανισμός πρέπει να σταθμίσει τους παράγοντες αυτούς για να αποφασίσει αν η επιλογή της λύσης του νέφους είναι η καταλληλότερη[021].

5.1.4 Περιβάλλον διαμοιραζόμενης ευθύνης

Κάνοντας χρήση των υπηρεσιών του νέφους, δημιουργείται ένα μοντέλο κοινής (διαμοιραζόμενης) ευθύνης μεταξύ του πελάτη-χρήστη και του παρόχου. Σύμφωνα με το μοντέλο αυτό μπορεί ο πελάτης να απαλλαγεί από το βάρος της ευθύνης να λειτουργεί, να ελέγχει και να διαχειρίζεται συστατικά της υποδομής, όπως από το λειτουργικό σύστημα μέχρι και τη φυσική ασφάλεια των εγκαταστάσεων στις οποίες λειτουργούν οι υπηρεσίες, καθώς την αποκλειστική ευθύνη γι' αυτά την αναλαμβάνει ο πάροχος.

Στο σχήμα που ακολουθεί φαίνεται ξεκάθαρα ότι η ευθύνη για όλα τα μέρη ενός πληροφοριακού συστήματος που βρίσκονται εντός εγκαταστάσεων αφορά τον ιδιοκτήτη(κόκκινο χρώμα) των εγκαταστάσεων. Στην περίπτωση που ο ιδιοκτήτης γίνει και πελάτης του νέφους, αναλόγως του μοντέλου παροχής υπηρεσιών που θα επιλέξει και πηγαίνοντας από το IaaS προς το SaaS όλο και περισσότερες ευθύνες μεταφέρονται στον πάροχο (πράσινο χρώμα)[066].



Σχήμα 5.1: Παρουσίαση ευθυνών (καταναλωτή, παρόχου) σε ένα ιδιόκτητο πληροφοριακό σύστημα, και στο μοντέλα IaaS,PaaS και SaaS [066].

Για να είναι καλυμμένος ο πελάτης, χρήστης του νέφους πρέπει αφού ξεκαθαριστούν τα όρια της ευθύνης του παρόχου, αυτά να περιγράφονται αναλυτικά στο μεταξύ τους Συμφωνητικό Παροχής Υπηρεσιών. Παράλληλα μπορεί ο πάροχος να κάνει και συστάσεις προς τον πελάτη για την χρήση επιπλέον τεχνολογιών που θα αυξάνουν την ασφάλεια στα μέρη που αυτός έχει την ευθύνη[002].

5.1.5 Κύκλος Ζωής Υπαλλήλων

Ο πάροχος πρέπει να καθιερώσει επίσημες πολιτικές και διαδικασίες για να οριοθετηθούν τα ελάχιστα πρότυπα για την πρόσβαση των υπαλλήλων στην υποδομή και στο λογισμικό του νέφους. Η αρχή του ελάχιστου προνομίου (Least Privilege) είναι η πιο δεδομένη πολιτική παροχής προνομίων-δικαιωμάτων στους υπαλλήλους, σύμφωνα με την οποία, σε ένα υπάλληλο δίνονται τα ελάχιστα προνόμια και μόνο για το διάστημα που απαιτείται για την εκτέλεση της εργασίας του. Η προσέγγιση αυτή ελαττώνει την πιθανότητα της μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες[046], ενώ έτσι περιορίζονται και οι δυνατότητες των υπαλλήλων για κακόβουλες δραστηριότητες εκ των έσω, που αναφέρθηκαν στο κεφάλαιο 4.

Σε κάποιους παρόχους το προσωπικό με δυνατότητα πρόσβασης στα δεδομένα των πελατών υποβάλλονται σε εκτενή έλεγχο του ιστορικού τους (όσο επιτρέπεται από το νόμο), ανάλογα με τη θέση τους και το επίπεδο πρόσβασης στα δεδομένα[002].

Τα βασικά στάδια στον κύκλο ζωής ενός υπαλλήλου σχετικά με τις δυνατότητες πρόσβασης είναι η παροχή λογαριασμού (αναλόγως της θέσης), αξιολόγηση λογαριασμού (περιοδικά ώστε να εξακριβώνεται ότι η θέση του υπαλλήλου δικαιολογεί τα δικαιώματα που του έχουν ανατεθεί) και η ακύρωση λογαριασμού- δυνατότητας πρόσβασης (όταν ένας υπάλληλος σταματάει να εργάζεται)[002].

5.1.6 Παρακολούθηση (Monitoring)

Η χρησιμοποίηση αυτοματοποιημένων συστημάτων παρακολούθησης προσφέρει ένα υψηλό επίπεδο απόδοσης και διαθεσιμότητας. Η προληπτική παρακολούθηση πρέπει να είναι διαθέσιμη μέσα από μια ποικιλία Online εργαλείων, τόσο για εσωτερική, από τον πάροχο, όσο και εξωτερική, από τον πελάτη, χρήση. Επιπλέον τα συστήματα πρέπει να διαθέτουν τα κατάλληλα όργανα για την παρακολούθηση βασικών μετρήσεων. Αντίστοιχα συστήματα συνέγερσης του προσωπικού πρέπει να είναι εγκατεστημένα και ρυθμισμένα έτσι, ώστε αν κάποιες μετρήσεις πλησιάζουν ή ξεπερνούν το κατώφλι ασφάλειας, να ειδοποιείται εγκαίρως το κατάλληλο προσωπικό για τη λήψη κατάλληλων μέτρων[002].

Η παρακολούθηση της ασφάλειας μπορεί να στηρίζεται σε αρχεία καταγραφής ελέγχου (audit logs), στην επιτήρηση της κίνησης του δικτύου (εσωτερικού και εξωτερικού), στην παρακολούθηση περιβαλλοντικών δεδομένων κ.α.[087].

5.1.7 Φυσική Ασφάλεια

Ο οποιοσδήποτε εξυπηρετητής ενός παρόχου νέφους είναι ευάλωτος σε έναν εισβολέα με απεριόριστο χρόνο και φυσική πρόσβαση στον εξυπηρετητή. Επίσης, διακοπές τάσεως ή διάφορα έντονα φυσικά φαινόμενα μπορούν να προκαλέσουν την απώλεια της διαθεσιμότητας ή καταστροφές στον εξοπλισμό.

Στο Προσχέδιο Κοινής Υπουργικής Απόφασης με θέμα «Ελάχιστες Υποχρεώσεις για τη διασφάλιση της ακεραιότητας δημόσιων τηλεφωνικών δικτύων και διαθεσιμότητα δημόσιων τηλεφωνικών υπηρεσιών σε σταθερές θέσεις»[103] περιγράφονται στο Άρθρο 9 οι υποχρεώσεις φυσικής ασφάλειας που πρέπει να καλύπτει ένας πάροχος δημόσιων τηλεφωνικών δικτύων. Οι ακόλουθες ισχύουν αυτούσιες και για παρόχους υπηρεσιών νέφους:

1. Ο πάροχος οφείλει να μεριμνά για τη φυσική ασφάλεια των εγκαταστάσεων στις οποίες βρίσκονται εγκατεστημένα τα στοιχεία του δικτύου του, η οποία είναι ανάλογη της κρισιμότητας των στοιχείων αυτών. Τα μέτρα που λαμβάνει ο πάροχος για τη φυσική ασφάλεια περιλαμβάνουν, ενδεικτικά, έλεγχο πρόσβασης, προστασία από σεισμό, υγρασία, πλημμύρες, υπερθέρμανση, φωτιά, κεραυνούς.

2. Κατά την επιλογή ή κατασκευή των εγκαταστάσεων στους οποίους εγκαθιστά στοιχεία του δικτύου του, καθώς και κατά την τοποθέτηση εξοπλισμού και υλοποίηση μέτρων φυσικής προστασίας, ο πάροχος λαμβάνει υπόψη του τις ιδιαίτερες φυσικές και άλλες συνθήκες οι οποίες επικρατούν στην περιοχή.

3. Ο πάροχος οφείλει να μεριμνά ώστε τα κρίσιμα στοιχεία του δικτύου να είναι εγκατεστημένα σε διαφορετικές εγκαταστάσεις ή σε χώρους φυσικά ανεξάρτητους. Όπου αυτό δεν είναι δυνατόν, αυτά θα πρέπει να προστατεύονται από ανεξάρτητα μέσα φυσικής προστασίας.

4. Ο πάροχος μεριμνά ώστε, σε χώρους στους οποίους είναι εγκατεστημένα στοιχεία του δικτύου, χρησιμοποιώντας συστήματα ή διαδικασίες ασφάλειας, ηλεκτρονικά ή μη, να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση, να ελέγχεται η πρόσβαση του προσωπικού και των συνεργατών του παρόχου μέσω καρτών πρόσβασης ή άλλων σχετικών διαδικασιών οι οποίες επιτρέπουν την αναγνώριση του προσωπικού και των συνεργατών του παρόχου, και να ελέγχεται η πρόσβαση των επισκεπτών.

5. Ο πάροχος οφείλει να μεριμνά για τη φυσική ακεραιότητα, ανθεκτικότητα και τακτική συντήρηση των εγκαταστάσεων στους οποίους είναι εγκατεστημένα στοιχεία του δικτύου του.

6. Ο πάροχος οφείλει να διαθέτει μηχανισμούς και διαδικασίες για την άμεση ενημέρωσή του ως προς γεγονότα που απειλούν την φυσική ασφάλεια των στοιχείων του δικτύου του και των χώρων που αυτά είναι εγκατεστημένα.

7. Ο πάροχος μεριμνά για τον τακτικό έλεγχο των μέτρων φυσικής ασφάλειας για τη διαπίστωση της εύρυθμης λειτουργίας τους.

8. Ο πάροχος τηρεί, για εύλογο χρονικό διάστημα, καταγεγραμμένα: α) περιγραφή της εφαρμοσθείσας μεθοδολογίας ελέγχου φυσικής ασφάλειας, β) τα αποτελέσματα του ελέγχου φυσικής ασφάλειας.

Επιπλέον υποχρεώσεις του παρόχου υπηρεσιών νέφους θα πρέπει να είναι[046]:

9. Η εξασφάλιση μέσων εφεδρικής τροφοδοσίας (για παράδειγμα, εφεδρικές συστοιχίες μπαταρίες, γεννήτριες κλπ.) τα οποία να έχουν επαρκή ικανότητα να υποστηρίξουν τη λειτουργία του δικτύου σε περιπτώσεις διακοπών της κύριας τροφοδοσίας.

10. Η εξασφάλιση επαρκούς ψύξης και εξαερισμού για τον ενεργό εξοπλισμό.

11. Η εξασφάλιση επαρκούς φωτισμού αλλά και δυνατότητα πρόσβασης - χώρου εργασίας για τη συντήρηση και αναβάθμιση του συστήματος.

5.1.8 Διαχείριση Διαμόρφωσης, Αλλαγών

Απαιτείται η καθιέρωση διαδικασίας διαχείρισης της διαμόρφωσης και των αλλαγών με την οποία θα είναι δυνατός ο έλεγχος των προτεινόμενων αλλαγών, ο προσδιορισμός πιθανών συνεπειών ασφάλειας καθώς και η διαβεβαίωση ότι το τρέχον λειτουργικό σύστημα είναι σωστό όσο αφορά την έκδοση και τη διαμόρφωση[087].

Όλες οι αλλαγές (τόσο στο λογισμικό όσο και στην υποδομή) πρέπει να γίνονται από εξουσιοδοτημένα άτομα ,να έχουν ελεγχθεί, εγκριθεί , καταγραφεί και κοινοποιηθεί σε όλους τους εμπλεκόμενους.

Οι οποιεσδήποτε αλλαγές θα πρέπει να γίνονται με τέτοιον τρόπο ώστε να δημιουργούν τις ελάχιστες δυνατές επιπτώσεις στη λειτουργία του νέφους και στις παρεχόμενες υπηρεσίες . Αν οι αλλαγές αυτές πρόκειται αναπόφευκτα να επηρεάσουν τη λειτουργία του νέφους ή τις υπηρεσίες, ο πάροχος έχει την υποχρέωση να ενημερώσει τους πελάτες, ώστε να ελαχιστοποιηθούν οι οποιεσδήποτε επιπτώσεις [002,087].

Συχνά ειδικά τμήματα λογισμικού αναπτύσσονται για αυτοματοποιημένη παρακολούθηση αλλαγών και ενημερώσεων[002,087].

5.1.9 Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan)

Ο σκοπός ενός Σχεδίου Επιχειρησιακής Συνέχειας είναι ελαχιστοποιήσει τις επιπτώσεις ενός δυσμενούς γεγονότος και έχει ως στόχο τη διασφάλιση της αδιάλειπτης λειτουργίας του νέφους και των υπηρεσιών αυτού. Το Σχέδιο αυτό περιέχει περιγραφή των μέτρων που λαμβάνει ο πάροχος και των απαιτούμενων ενεργειών για την αποκατάσταση λειτουργίας των τμημάτων του νέφους και την αποκατάσταση της πληροφορίας η οποία έχει αλλοιωθεί ή χαθεί και η οποία απαιτείται για την παροχή των υπηρεσιών.

Ενδεικτικά ένα τέτοιο Σχέδιο περιγράφει το προσωπικό που εμπλέκεται στην περίπτωση όπου απειλείται η επιχειρησιακή συνέχεια του παρόχου, τις συνθήκες κατά τις οποίες ενεργοποιείται το Σχέδιο, λειτουργικές διαδικασίες για την ανάλυση και εκτίμηση του προβλήματος, εκτιμώμενους χρόνους αποκατάστασης σε διαφορετικές συνθήκες βλάβης κ.α. Κάθε φορά που ενεργοποιείται πρέπει να γίνεται και αξιολόγηση των μέτρων που λήφθηκαν για την επίλυση συγκεκριμένου προβλήματος και αν απαιτείται αναθεώρησή του[103].

5.1.10 Διατήρηση Αντιγράφων Ασφάλειας

Η Διατήρηση Αντιγράφων Ασφάλειας είναι απαραίτητη τόσο για την εξασφάλιση των πελατών ότι δεν θα χαθούν τα δεδομένα τους, που έχουν προωθήσει στο νέφος, σε περίπτωση για παράδειγμα βλάβης της υποδομής αποθήκευσης όσο και για τον ίδιο τον πάροχο που εξασφαλίζει ότι υπάρχουν ανά πάσα στιγμή διαθέσιμα αντίγραφα ασφάλειας της πλέον

πρόσφατης παραμετροποίησης (configuration) του εξοπλισμού του, τα οποία είναι απαραίτητα για την γρήγορη αποκατάσταση του δικτύου του και των παρεχόμενων υπηρεσιών[087,103].

Οι πάροχοι είναι υποχρεωμένοι να δηλώνουν ξεκάθαρα για ποια δεδομένα των πελατών διατηρούν αντίγραφα ασφάλειας και για πόσο καιρό.

5.1.11 Έλεγχοι Ασφάλειας

Στην ουσία, οι έλεγχοι ασφάλειας είναι αντίμετρα ή μέτρα για την πρόληψη, την αποφυγή, την αντιμετώπιση, την ανίχνευση, ή ότι μπορεί να ανταποκριθεί στους κινδύνους ασφάλειας. Μπορούν να είναι τεχνικοί μηχανισμοί, πρακτικές ή διαδικασίες.

Όπως αναφέρθηκε στο κεφάλαιο 3, το National Institute of Standards and Technology έχει εκδώσει την οδηγία NIST Special Publication 800-53 Revision 3: «Recommended Security Controls for Federal Information Systems and Organizations»[059] που αποτελεί έναν οδηγό ελέγχων ασφάλειας. Παρότι απευθύνεται σε Ομοσπονδιακές Υπηρεσίες των ΗΠΑ , οι οδηγίες μπορούν αντίστοιχα να χρησιμοποιηθούν από παρόχους αλλά και από πιθανούς πελάτες των υπηρεσιών του νέφους. Στην οδηγία αυτή οι έλεγχοι είναι χωρισμένοι σε 18 ομάδες που υπάγονται σε τρεις κατηγορίες : τεχνικοί, λειτουργικοί και διαχειριστικοί.

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Πίνακας 5.1: Έλεγχοι Ασφάλειας , ομάδες(families), κατηγορίες(classes) σύμφωνα με το NIST[059]

Πέρα όμως από τους ελέγχους που εσωτερικά πρέπει να εκτελεί ένας πάροχος πολύ σημαντική είναι και η πιστοποίησή του από ανεξάρτητους τρίτους φορείς σχετικά με τον αν γίνονται οι προβλεπόμενοι έλεγχοι, την πληρότητα και την αποτελεσματικότητά τους και γενικά τον βαθμό εφαρμογής της πολιτικής ασφάλειας .

Για παράδειγμα η AMAZON ως πάροχος του Amazon Web Services(AWS) έχει τα ακόλουθα πιστοποιητικά συμμόρφωσης (που αναφέρθηκαν στο κεφάλαιο 3) : SAS70 Type II, PCI DSS Level 1, ISO 27001 και συμβατότητα με το FISMA Low Level [002].

5.1.12 Έλεγχος Πρόσβασης και Επαλήθευση Ταυτότητας

Ο έλεγχος πρόσβασης παραπέμπει σε ένα σύνολο λογικών ή φυσικών μηχανισμών ασφάλειας που σχεδιάζονται-εφαρμόζονται για να προστατέψουν από τη μη εξουσιοδοτημένη πρόσβαση (π.χ. είσοδος στο σύστημα, ανάγνωση, εγγραφή, είσοδος στο δίκτυο, κ.α.), στους πόρους-αγαθά του συστήματος. Συχνά χρησιμοποιείται για να περιγράψει ένα σύνολο διαδικασιών στο οποίο συμμετέχουν άνθρωποι, ηλεκτρονικές διατάξεις, προγράμματα, και άλλος ηλεκτρονικός ή μη εξοπλισμός, με σκοπό μόνο ο εξουσιοδοτημένος χρήστης να έχει πρόσβαση στο σύστημα.

Η επαλήθευση της ταυτότητας κάποιου χρήστη μπορεί να γίνει χρησιμοποιώντας κάτι που ξέρει (πχ κωδικός), είτε κάτι που κατέχει (πχ μαγνητική κάρτα, security token) είτε βιομετρικά στοιχεία (πχ δακτυλικά αποτυπώματα)[087]. Ο συνδυασμός και των τριών επιλογών προσφέρει μέγιστη ασφάλεια.

Στην περίπτωση του νέφους, όπου τα δεδομένα και οι εφαρμογές ενός οργανισμού ξεφεύγουν από τα όρια της «ασφαλής περίφραξης» του ιδιόκτητου εξοπλισμού, η εξασφάλιση της μη εξουσιοδοτημένη πρόσβαση σε υποδομές και πληροφορίες αποτελεί μείζον ζήτημα. Ένα επαναλαμβανόμενο θέμα είναι ότι το πλαίσιο ελέγχου ταυτότητας και αναγνώρισης που εφαρμόζεται εντός ενός οργανισμού δεν μπορεί να επεκταθεί φυσικά ώστε να ισχύει και στο δημόσιο νέφος και η επέκταση ή η αλλαγή του υφιστάμενου πλαισίου για την υποστήριξη των υπηρεσιών του νέφους μπορεί να είναι ιδιαίτερα δύσκολη. Η εναλλακτική της εμπλοκής δύο διαφορετικών συστημάτων αυθεντικοποίησης, ένα εντός του οργανισμού και ένα για τις υπηρεσίες του νέφους είναι περίπλοκη και μπορεί να μην τελικά αποτελεσματική[056].

Η ασφάλεια των εφαρμογών και ο έλεγχος πρόσβασης των χρηστών θα αντισταθμίσει την απώλεια της «ασφαλής περίφραξης» και του ελέγχου του δικτύου. Ο αυστηρός έλεγχος

ταυτότητας, η εξουσιοδότηση αναλόγως των απαιτήσεων ή του ρόλο του χρήστη, η τεχνολογία της Ομοσπονδιακής Ταυτότητας (Federated Identity) και του Ενιαίου Σημείου Πρόσβασης (Single Sign-On (SSO)), είναι προτεινόμενες λύσεις[045] που αναλύονται παρακάτω στην ενότητα 5.2.3 «Ασφάλεια Ταυτότητας».

Επιπλέον γενικά αποδεκτές πρακτικές είναι οι ακόλουθες[087]:

- Το προσωπικό του παρόχου πρέπει γενικά να έχει περιορισμένη πρόσβαση στα δεδομένα των πελατών. Μπορεί να απαιτηθεί πρόσβαση στο λειτουργικό της εικονικής συσκευής που είναι δεσμευμένη από κάποιο πελάτη, αλλά σε μία τέτοια περίπτωση η πρόσβαση πρέπει να είναι αυστηρώς περιορισμένη και συσχετισμένη με συγκεκριμένες λειτουργίες, που θα περιγράφονται στην Πολιτική Ασφάλειας και στο Συμφωνητικό Παροχής Υπηρεσιών.

- Επιλογή της επαλήθευση της ταυτότητας με συνδυασμό και των τριών επιλογών(κάτι που ξέρει κ.α.) που αναφέρθηκαν προηγουμένως και ειδικά για χρήστες με υψηλά προνόμια.

- Δεν θα πρέπει να γίνεται χρήση κοινόχρηστων λογαριασμών (για παράδειγμα διαχειριστή).

- Εφαρμογή της αρχής των ελάχιστων προνομίων (Least Privilege Principal (LPP) των ομάδων των χρηστών, βασισμένη και στο ρόλο τους (Role-Based Access Controls RBAC) .

5.1.13 Συμφωνητικό Παροχής Υπηρεσιών (Service Level Agreement(SLA))

Όπως αναφέρθηκε στο κεφάλαιο 4, στο περιβάλλον της νεφοϋπολογιστικής, η συμφωνία μεταξύ του παρόχου και του πελάτη-χρήστη για τις παρεχόμενες υπηρεσίες, το επίπεδο ασφάλειας, τη συμβατότητα, τις ευθύνες, τις χρεώσεις περιγράφεται αναλυτικά στο Συμφωνητικό Παροχής Υπηρεσιών (ΣΠΥ) που ουσιαστικά αποτελεί ένα είδος σύμβασης μεταξύ των εμπλεκομένων. Υπάρχουν δύο τύποι ΣΠΥ αυτά που είναι διαπραγματεύσιμα και αυτά που είναι τυποποιημένα από τους παρόχους και μη διαπραγματεύσιμα[021]. Ο τύπος του ΣΠΥ εξαρτάται από το μοντέλο παροχής υπηρεσιών και το μέγεθος της συναλλαγής. Για παράδειγμα στην περίπτωση του PaaS ή του IaaS είναι συνήθως ευθύνη του πελάτη να καθορίσει τις λεπτομέρειες στο ΣΠΥ που θα τον καλύψουν. Το συμφωνητικό των υπηρεσιών νέφους αποτελεί ένα σύνθετο θέμα.

Ανάμεσα στα σημεία που θα πρέπει να περιλαμβάνονται σε ένα συμφωνητικό ενός οργανισμού-πελάτη είναι τα παρακάτω[034,053]:

- Η διαθεσιμότητα και ποιότητα των υπηρεσιών.

- Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων. Ιδιαίτερη μνεία πρέπει να γίνεται για τα δεδομένα των πελατών ενός οργανισμού, που είναι πελάτης του νέφους, και τα οποία ανήκουν στον οργανισμό και θα πρέπει να αντιμετωπίζονται σαν εμπιστευτική πληροφορία.

- Διευκρινίσεις σχετικά με το πού θα αποθηκεύονται τα δεδομένα, σε τι είδους επεξεργασία θα υπόκεινται και για πόσο χρόνο θα διατηρούνται.

- Διαβεβαίωση ότι τα δεδομένα θα είναι άμεσα διαθέσιμα κατόπιν σχετικού αιτήματος, ανεξάρτητα από το αν υπάρχει κάποια διαφωνία μεταξύ των δύο μερών ή αν εκκρεμεί κάποια πληρωμή.

- Οι διαδικασίες χρέωσης των υπηρεσιών.

- Διασφάλιση της προθυμίας του προμηθευτή υπηρεσιών νέφους να συνεργαστεί με τον οργανισμό και με τυχόν νέους προμηθευτές για τη μετακίνηση των δεδομένων όταν λήξει το συμβόλαιο.

- Καθορισμός της συχνότητας των αντιγράφων ασφάλειας και της τιμολόγησης για επιπρόσθετα αντίγραφα ασφάλειας και αποθηκευτικές ανάγκες.

- Καταγραφή των προτύπων ασφάλειας που πληροί ο προμηθευτής και των πρακτικών ασφάλειας που εφαρμόζει.

- Ο τρόπος αντίδρασης και αναφοράς στα περιστατικά ασφάλειας.

- Οι έλεγχοι που μπορεί υλοποιήσει ο οργανισμός (ακόμα και με τη συνεισφορά τρίτων ανεξάρτητων φορέων) στον πάροχο ,για το πόσο τηρεί τα συμφωνηθέντα.

- Κυρώσεις για μειωμένη απόδοση, αποζημιώσεις.

- Διαπραγμάτευση και καταγραφή του ρόλου του προμηθευτή, στην υπεράσπιση του οργανισμού, σε περίπτωση που προκύψει κάποια καταγγελία εκ μέρους τρίτου (για παράδειγμα, από πελάτη του οργανισμού) για παραβίαση δεδομένων.

Γενικά , οι προσπάθειες θα πρέπει να εστιάζουν σε ολόκληρο τον κύκλο ζωής των δεδομένων.

5.1.14 Κατηγοριοποίηση μισθωτών (tenants)

Όπως ήδη αναφέρθηκε, στο περιβάλλον της νεφοϋπολογιστικής και κυρίως στα μοντέλα IaaS και PaaS, χρησιμοποιώντας τεχνικές εικονικοποίησης και το μοντέλο των πολλαπλών μισθωτών γίνεται χρήση του ίδιου φυσικού μέσου-εξοπλισμού από διάφορους χρήστες. Μια ενδιαφέρουσα πρόταση- πρακτική παρουσιάστηκε από τον Sasko Ristov κ.α. [066], που προτείνει στους παρόχους να αναπτύξουν μεθοδολογία η οποία θα αξιολογεί τους μισθωτές και θα τους κατηγοριοποιεί. Για παράδειγμα σε 5 κατηγορίες, ανάλογα με το επίπεδο αξιοπιστίας τους από πολύ αξιόπιστους ως καθόλου αξιόπιστους.

Κατόπιν μόνο μισθωτές της ίδιας κατηγορίας θα μπορούν να μοιράζονται το ίδιο φυσικό μέσο. Με τον τρόπο αυτό ως ένα σημείο εξασφαλίζονται οι αξιόπιστοι πελάτες ότι δεν μοιράζονται υποδομή με κάποιον άλλο, μη αξιόπιστο πελάτη και έτσι μειώνονται και οι πιθανότητες να δεχτούν επιθέσεις από αυτούς.

Βέβαια υπάρχει και η λύση της αποκλειστικής χρήσης μέρους της υποδομής (single tenant hardware) για ακόμη μεγαλύτερη ασφάλεια. Για παράδειγμα, τέτοια επιλογή παρέχει η Amazon για το EC2[002].

5.2 Τεχνικές Εξασφάλισης Των Δεδομένων

Μετά τη θέσπιση και τήρηση κατάλληλων διαδικασιών-πρακτικών, η προσπάθεια επίτευξης του αναμενόμενου επιπέδου ασφάλειας σε ένα πληροφοριακό σύστημα συνεχίζεται με τεχνικές εξασφάλισης των δεδομένων. Καθώς το μοντέλο του νέφους συνεπάγεται συνεχή μεταφορά δεδομένων (από τον χρήστη στον πάροχο, σε άλλους χρήστες κλπ) σημαντική συνεισφορά έχουν οι τεχνικές ασφαλής μεταφοράς των δεδομένων. Επίσης, σημαντική συνεισφορά έχουν εφαρμογές της επιστήμης της Κρυπτογραφίας (cryptography), γνωστές ως ψηφιακές υπογραφές (digital signatures) και κρυπτογράφηση (encryption). Οι ψηφιακές υπογραφές

χρησιμοποιούνται για να επαληθεύσουν το φορέα αποστολής δεδομένων(πιστοποίηση ταυτότητας (authentication)), να επιβεβαιώσουν ότι τα δεδομένα που στάλθηκαν δεν έχουν τροποποιηθεί (ακεραιότητα) και να διασφαλίσουν τη μη αποποίηση (non-repudiation) της αποστολής ενός μηνύματος. Η κρυπτογράφηση αξιοποιείται για τη διατήρηση της εμπιστευτικότητας των δεδομένων και της επικοινωνίας [095]. Επιπλέον αναφέρεται η ανάγκη εφαρμογής τεχνικής απόκρυψης δεδομένων και διαγραφή τους.

5.2.1 Ασφαλή Μεταφορά Δεδομένων

Η ανάγκη για ασφαλή μεταφορά δεδομένων δεν είναι καινούργια στον χώρο του διαδικτύου και σίγουρα αποτελεί ένα δύσκολο και πολύπλοκο θέμα. Το περιβάλλον της νεφοϋπολογιστικής αυξάνει την πολυπλοκότητα αυτή, καθώς εκτός από την κυκλοφορία προς το νέφος υπάρχει και η κυκλοφορία μεταξύ των κόμβων του νέφους (cloud hosts), που συνήθως είναι εικονικοί και στερούνται της παραδοσιακής φυσικής σύνδεσης[091]. Η τεχνολογία Secure Socket Layer (SSL) και η πιο πρόσφατη Transport Layer Security(TLS), που είναι μία ελαφρώς τροποποίηση της SSL version 3, χρησιμοποιούνται για την εξασφάλιση της μεταφοράς των δεδομένων στο επίπεδο μεταφοράς του μοντέλου 5 επιπέδων του διαδικτύου. Στο επίπεδο δικτύου χρησιμοποιείται η τεχνολογία IPsec με την οποία είναι δυνατή και δημιουργία των Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks)[047].

Το IPsec επιτρέπει την αποστολή και λήψη κρυπτογραφημένων πακέτων κάθε τύπου(TCP, UDP, ICMP κ.α.) χωρίς καμία τροποποίηση. Αναλόγως της αναγκαιότητας μπορεί να παρέχει πιστοποίηση ταυτότητας του χρήστη, εμπιστευτικότητα και ακεραιότητα των δεδομένων ή μόνο πιστοποίηση ταυτότητας του χρήστη[091].

Το πρωτόκολλο SSL, που ουσιαστικά μεσολαβεί μεταξύ των εφαρμογών και του TCP/IP πρωτοκόλλου, παρέχει ασφαλή διασύνδεση μεταξύ ενός εξυπηρετητή και ενός πελάτη (client). Η ασφάλεια στην επικοινωνία επιτυγχάνεται μέσω της πιστοποίησης της ταυτότητας των πλευρών που επικοινωνούν καθώς και της κρυπτογράφησης της κίνησης που πραγματοποιείται μεταξύ τους[091].

Το IPsec είναι συμβατό με κάθε εφαρμογή, αλλά απαιτεί την εγκατάσταση ειδικού λογισμικού (IPsec client) σε κάθε συσκευή πρόσβασης (πχ Η/Υ, κινητό τηλέφωνο κλπ) για να λειτουργήσει η κρυπτογράφηση γεγονός που το καθιστά λίγο δύσχρηστο. Αντίθετα το SSL είναι ενσωματωμένο σε κάθε φυλλομετρητή (browser), που είναι και το κύριο μέσο πρόσβασης στις υπηρεσίες

νέφους. Από την άλλη το πλεονέκτημα του IPsec είναι ότι μπορεί να χρησιμοποιεί τεχνικές συμπίεσης. Φαίνεται δηλαδή ότι το IPsec είναι καταλληλότερο για τις επικοινωνίες μεταξύ των κόμβων ενώ το SSL είναι καταλληλότερο για επικοινωνίες πελάτη-κόμβου [091].

Και οι δύο τεχνολογίες βασίζονται στην υποδομή δημοσίου κλειδιού, και στην κρυπτογράφηση που αναλύονται παρακάτω.

5.2.2 Κρυπτογράφηση

Στο περιβάλλον του νέφους η κρυπτογραφία έχει αναγνωριστεί ότι είναι ο κρίσιμος τεχνολογικός παράγοντας που συνέβαλε στην ασφάλεια. Μια από τις εφαρμογές της κρυπτογραφίας είναι η κρυπτογράφηση. Υπάρχουν δύο βασικά είδη κρυπτογράφησης των πληροφοριών-δεδομένων: η συμμετρική κρυπτογράφηση (επίσης ονομάζεται κρυπτογράφηση μυστικού κλειδιού) και ασύμμετρη κρυπτογράφηση (επίσης ονομάζεται κρυπτογράφηση δημόσιου κλειδιού)[087].

Κατά τη λειτουργία της κρυπτογράφησης το απλό κείμενο (plaintext) κρυπτογραφείται σε κωδικοποιημένο κείμενο (cyphertext) με τη χρήση ενός κλειδιού κρυπτογράφησης και ενός αλγόριθμου κρυπτογράφησης. Αργότερα το κωδικοποιημένο κείμενο αποκρυπτογραφείται με τη χρήση κλειδιού αποκρυπτογράφησης. Στην συμμετρική κρυπτογράφηση τα δύο παραπάνω κλειδιά είναι τα ίδια, το κοινό μυστικό κλειδί. Για όσο χρονικό διάστημα ο αποστολέας και ο παραλήπτης γνωρίζουν το μυστικό κλειδί, μπορούν να κρυπτογραφούν και να αποκρυπτογραφούν όλα τα μηνύματα που χρησιμοποιούν αυτό το κλειδί. Το πλεονέκτημα της συμμετρικής κρυπτογράφησης είναι ότι αναλόγως του αλγορίθμου και του κλειδιού η διαδικασία δεν απαιτεί ιδιαίτερη υπολογιστική ισχύ και είναι σχετικά γρήγορη και γι' αυτό μπορεί να χρησιμοποιηθεί σε μεγάλο όγκο δεδομένων. Συνηθισμένοι αλγόριθμοι συμμετρικής κρυπτογράφησης είναι ο DES ,ο AES, ο 3DES, ο RC4 κ.α. [047].

Το πρόβλημα με τα μυστικά κλειδιά είναι η ανταλλαγή τους, όταν δεν υπάρχουν ασφαλή κανάλια επικοινωνίας, μέσω του διαδικτύου ή ενός άλλου δικτύου, που να εξασφαλίζουν ότι δεν πέσουν σε λάθος χέρια. Όποιος γνωρίζει το μυστικό κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα.

Μία λύση στο ανωτέρω πρόβλημα προσφέρει η ασύμμετρη κρυπτογράφηση. Σε αυτήν το κλειδί κρυπτογράφησης (γνωστό και ως δημόσιο κλειδί) είναι διαφορετικό αλλά μαθηματικά συσχετισμένο με το κλειδί αποκρυπτογράφησης (ιδιωτικό κλειδί). Το δημόσιο κλειδί της

οντότητας Α είναι ελεύθερα διαθέσιμο σε όποιον θέλει να στείλει ένα μήνυμα στον Α. Το δεύτερο, το ιδιωτικό κλειδί του Α είναι απόρρητο και το γνωρίζει μόνο αυτός. Έτσι το πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι ότι μόνο το ιδιωτικό κλειδί πρέπει να είναι μυστικό και δεν χρειάζεται να το γνωρίζει άλλος, παρά μόνο ο Α και άρα δεν χρειάζεται η μεταφορά του. Παρότι το ζεύγος δημόσιο-ιδιωτικό κλειδί έχουν συσχέτιση, είναι αδύνατον από το δημόσιο να παραχθεί το ιδιωτικό. Ένα πρόβλημα με την ασύμμετρη κρυπτογράφηση, ωστόσο, είναι ότι είναι σημαντικά πιο αργή από τη συμμετρική κρυπτογράφηση. Απαιτεί πολύ περισσότερη επεξεργαστική ισχύ για να κρυπτογραφήσει και να αποκρυπτογραφήσει το περιεχόμενο του μηνύματος. Για το λόγο αυτό προτιμάται για την κωδικοποίηση μικρού όγκου δεδομένων (που μπορεί για παράδειγμα να είναι το κοινό μυστικό κλειδί αλγορίθμου συμμετρικής κρυπτογράφησης). Συνηθισμένοι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι ο RSA, ο Diffie-Hellman, ο ElGamal, ο Digital Signature Standard κ.α. [047,087,094].

Για να χρησιμοποιηθεί η ασύμμετρη κρυπτογράφηση, πρέπει να υπάρχει ένας τρόπος για τους χρήστες να μπορούν να αντιστοιχίσουν αξιόπιστα τα δημόσια κλειδιά των άλλων. Η χαρακτηριστική τεχνική είναι η χρήση ψηφιακών πιστοποιητικών(certificates). Ένα πιστοποιητικό είναι ένα πακέτο πληροφοριών που προσδιορίζει τον χρήστης ή έναν εξυπηρετητή, και περιέχει πληροφορίες όπως το όνομα της εταιρείας, τον οργανισμό που εξέδωσε το πιστοποιητικό, διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη και χώρα, και το δημόσιο κλειδί του χρήστη. Οι Αρχές Πιστοποίησης (Certification Authorities(CA)) αναλαμβάνουν να εκδώσουν τα πιστοποιητικά, με τα οποία μπορεί να πιστοποιηθεί (εξακριβωθεί) η ταυτότητα ενός προσώπου αλλά και ενός δικτυακού τόπου[046].

Η χρήση του ζεύγους δημόσιο-ιδιωτικό κλειδιών συμβάλλει στην επίτευξη της εμπιστευτικότητας στο περιβάλλον της νεφοϋπολογιστικής και όχι μόνο λόγω της κρυπτογράφησης του περιεχομένου. Ένα ιδιωτικό κλειδί μπορεί να χρησιμοποιηθεί για την πιστοποίηση ταυτότητας ενός χρήστη ή ενός υπολογιστικό συστήματος και μπορεί επίσης να χρησιμοποιηθεί για να κινήσει η διαπραγμάτευση ενός ασφαλούς καναλιού ή σύνδεση μεταξύ των επικοινωνούντων μερών (για παράδειγμα με την τεχνολογία IPsec που προαναφέρθηκε)[087].

Η κρυπτογράφηση είναι επίσης σημαντικός παράγοντας σε ότι αφορά την προστασία των δεδομένων που είναι αποθηκευμένα στο νέφος. Μπορεί να εφαρμοστεί ώστε να κρυπτογραφηθούν τα δεδομένα είτε σε επίπεδο ολόκληρου σκληρού δίσκου, είτε σε επίπεδο

καταλόγων, είτε σε επίπεδο αρχείων ή ακόμα και σε επίπεδο εφαρμογών (όπου η εφαρμογή διαχειρίζεται την κρυπτογράφηση δεδομένων που έχουν σχέση με την εφαρμογή) [087].

Το πρόβλημα με την κρυπτογράφηση είναι ότι περιορίζει τη δυνατότητα χρήσης των δεδομένων. Ειδικά η αναζήτηση και οι λειτουργίες ευρετηρίου γίνονται προβληματικές. Για παράδειγμα, ενώ όταν τα δεδομένα είναι αποθηκευμένα σε μορφή απλού κειμένου, κάποιος μπορεί να ψάξει για ένα κείμενο δίνοντας συγκεκριμένα κλειδιά αναζήτησης, αυτό είναι αδύνατο να γίνει στα κρυπτογραφημένα δεδομένα. Νέες state of the art τεχνικές είναι υπό ανάπτυξη που επιτρέπουν λειτουργίες και υπολογισμούς ακόμα και στα κρυπτογραφημένα δεδομένα[017]. Τέτοιες είναι οι ακόλουθες.

- Η Κρυπτογράφηση Αναζήτησης (Searchable Encryption) που συχνά αναφέρεται και ως Κρυπτογράφηση Κατηγορήματος(Predicate Encryption): Επιτρέπει σε μία οντότητα την εξωτερική ανάθεση υπηρεσιών αποθήκευσης δεδομένων σε μία άλλη οντότητα με έναν ιδιωτικό τρόπο, ενώ παράλληλα διατηρεί την ικανότητα επιλεκτικής ανίχνευσης σε αυτά. [017,024,032].

- Η Ομομορφική Κρυπτογράφηση (Homomorphic Encryption): Επιτρέπει στο να γίνονται λειτουργίες (πράξεις όπως πρόσθεση και πολλαπλασιασμός) στα κρυπτογραφημένα δεδομένα χωρίς την ανάγκη αποκρυπτογράφησής τους, ενώ το αποτέλεσμα της πράξης των κρυπτογραφημένων δεδομένων αν αποκρυπτογραφηθεί με το κλειδί που κρυπτογραφήθηκαν τα αρχικά δεδομένα μας ισούται με το αποτέλεσμα της ίδιας πράξης στα αρχικά δεδομένα [068,076].

Επιπλέον μια άλλη μορφή ασύμμετρης κρυπτογραφίας είναι η ελλειπτική κρυπτογραφία που παρέχει το ίδιο επίπεδο ασφάλειας όπως ο αλγόριθμος RSA, αλλά με μικρότερο μέγεθος κλειδιού γεγονός που την κάνει πιο γρήγορη χωρίς ιδιαίτερες απαιτήσεις υπολογιστικής ισχύς[079].

Οι προαναφερθέντες μορφές κρυπτογράφησης είναι ακόμα σε ανάπτυξη, δεν έχουν καθιερωθεί και ακόμα παρουσιάζονται δυσκολίες που εμποδίζουν την καθημερινή χρήση τους. Γενικά συνιστάται [021] η χρήση δοκιμασμένων τεχνικών κρυπτογράφησης και η εξεύρεση λύσεων που θα ταιριάζουν καλύτερα στις ανάγκες και τις απαιτήσεις ενός οργανισμού, όπως για παράδειγμα συνδυασμός τεχνικών συμμετρικής και ασύμμετρης κρυπτογράφησης[072], που ονομάζεται και υβριδική κρυπτογραφία [091,094].

Τέλος πρέπει να αναφερθεί ότι για να έχει τη μέγιστη αποτελεσματικότητα κάθε μορφή κρυπτογράφησης η διαχείριση των κλειδιών πρέπει να σχεδιαστεί και να υλοποιηθεί πολύ προσεκτικά. Υπάρχει η επιλογή της τοπικής διαχείριση των κλειδιών, όπου αυτά παραμένουν έξω από τις υποδομές του νέφους στην υποδομή του οργανισμού, και η επιλογή της κρυπτογράφησης και διαχείρισης κλειδιών στην πλευρά του νέφους. Η δεύτερη επιλογή παρέχει μεγαλύτερη ευελιξία ειδικά στην κοινή χρήση δεδομένων και στη διαλειτουργικότητα μεταξύ των εικονικών συσκευών του νέφους , αλλά η πρώτη παρέχει μεγαλύτερη ασφάλεια [021,046]. Μία άλλη λύση που αρχίζει να έχει μεγάλη εφαρμογή είναι τα κλειδιά να είναι αποθηκευμένα σε ειδικές συσκευές με προστασία παραβίασης (tamperproof devices), όπως έξυπνες κάρτες εφοδιασμένες με «ασφαλές» εξάρτημα για την αποθήκευση των κλειδιών [091].

5.2.3 Ασφάλεια Ταυτότητας (Identity Security)

Με τον όρο ασφάλεια ταυτότητας εννοούνται οι τεχνικές που ο συνδυασμός τους συμβάλει αρχικά στην πιστοποίηση της ταυτότητας του χρήστη(authentication) και αναλόγως εξουσιοδότησής (authorization) του για πρόσβαση στις υποδομές- υπηρεσίες του νέφους.

Η Ψηφιακή Υπογραφή είναι δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό κείμενο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητάς-γνησιότητάς του. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης(digest) του μηνύματος σε συνδυασμό με ασύμμετρη κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση της σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασύμμετρη κρυπτογραφία αποδεικνύει την ακεραιότητα του εγγράφου, αλλά και την απόδειξη ταυτότητας του αποστολέα)[093,095].

Η χρήση τόσο των ψηφιακών πιστοποιητικών όσο και των ψηφιακών υπογραφών βασίζεται στην Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure(PKI)), η οποία είναι ένας συνδυασμός από προγράμματα, τεχνολογίες κρυπτογράφησης και υπηρεσίες, με τον οποίο μπορεί να πιστοποιηθεί (επαληθευθεί) η ταυτότητα ενός φυσικού προσώπου, ενός εξυπηρετητή ή και η γνησιότητα μιας ιστοσελίδας. Κύριο ρόλο σε αυτή τη διαδικασία διαδραματίζουν οι Αρχές Πιστοποίησης (ΑΠ) που αναλαμβάνουν την έκδοση αυτών των πιστοποιητικών (για παράδειγμα, τα X.509 certificates). Στην Ελλάδα υπάρχει για παράδειγμα η Αρχή Πιστοποίησης

του Ελληνικού Δημοσίου (ΑΠΕΔ) [www.yap.gov] ενώ και αρκετά Πανεπιστήμια έχουν καθιερώσει τις δικές τους Αρχές.

Στο περιβάλλον του νέφους μία ΑΠ απαιτείται για να πιστοποιήσει τις οντότητες που εμπλέκονται και συνεργάζονται. Απαιτείται δηλαδή η πιστοποίηση των φυσικών εξυπηρετητών της υποδομής, των εικονικών εξυπηρετητών, των χρηστών και των συσκευών δικτύου. Παρέχοντας η ΑΠ τα απαραίτητα ισχυρά διαπιστευτήρια για όλες τις φυσικές και εικονικές οντότητες, στην ουσία δημιουργεί έναν τομέα ασφάλειας με συγκεκριμένα όρια εντός του, κατά τα άλλα ασαφές, συνόλου των φορέων ενός νέφους [091].

Καθώς το νέφος γίνεται η κοινή λειτουργική πλατφόρμα, κάθε υπηρεσία απαιτεί ασφαλή πιστοποίηση και εξουσιοδότηση. Επιπλέον διάφορες οντότητες εμπλέκονται στην χρήση των υπηρεσιών, όπως οργανισμοί , πελάτες του οργανισμού, συνεργάτες κ.α. οπότε δημιουργείται η ανάγκη ο χρήστης να «φέρει τη δική του ταυτότητα» και οι εφαρμογές του νέφους να μπορούν δεχτούν ταυτότητες και χαρακτηριστικά χρηστών από πολλούς οργανισμούς. Η πρόσβαση στις εφαρμογές με βάση την ταυτότητα του χρήστη, που δεν θα βασίζεται απλά στο συνδυασμό «Όνομα Χρήστη- Κωδικός» αλλά σε ψηφιακές υπογραφές προτείνεται ως ένας ασφαλής τρόπος πιστοποίησης[051, 091].

Βέβαια υπάρχουν και άλλοι τρόποι για την πιστοποίηση της ταυτότητας ενός χρήστη πέρα από την Υποδομή Δημόσιου Κλειδιού και την εμπλοκή της ΑΠ, που μπορεί να είναι η χρήση κωδικού μιας φοράς (one-time password (OTP)) και αποστολή του τηλεφωνικώς ή με μήνυμα SMS , η χρήση έξυπνων καρτών ή ακόμα και η χρήση βιομετρικών χαρακτηριστικών (όπως αναφέρθηκε στην παράγραφο 5.1.12)[021].

Μία λύση για να μην επαναλαμβάνει ο χρήστης τη διαδικασία πιστοποίησης σε κάθε υπηρεσία που προσπαθεί να έχει πρόσβαση και να μην έχει να απομνημονεύσει πολλούς κωδικούς πρόσβασης είναι η χρήση της Ομοσπονδιακής Ταυτότητας (Federated Identity). Η Ομοσπονδιακή ταυτότητα παρέχει τα μέσα ώστε να αντιστοιχεί την ηλεκτρονική ταυτότητα και τα χαρακτηριστικά ενός χρήστη με τον χρήστη, παρότι αυτά είναι αποθηκευμένα σε διαφορετικά διασυνδεδεμένα συστήματα διαχείρισης ταυτότητας. Με την χρήση της Ομοσπονδιακής Ταυτότητας είναι δυνατή η χρήση της τεχνολογία του Ενιαίου Σημείου Πρόσβασης (Single Sign-On), όπου ο χρήστης κάνει μία φορά τη διαδικασία πιστοποίησης και στη συνέχεια εξουσιοδοτείται να χρησιμοποιεί τις αντίστοιχες υπηρεσίες από όλα τα μέρη που συνεργάζονται μεταξύ τους (σαν ομοσπονδία) και με την ΑΠ[015,040,091].

Το Shibboleth είναι ένα ανοιχτού κώδικα λογισμικό, που χρησιμοποιείται για να παρέχει τεχνολογία του Ενιαίου Σημείου Πρόσβασης εντός ή μεταξύ οργανισμών, βασίζεται στην Security Assertion Markup Language (SAML), που είναι ένα πρότυπο βασισμένο σε XML για την ανταλλαγή δεδομένων πιστοποίησης και εξουσιοδότησης των χρηστών (όπως ταυτότητες, κωδικούς κ.α.)[025,091].

Άλλα διαδεδομένα πρότυπα για τη διαχείριση πιστοποίησης ταυτοτήτων και εξουσιοδοτήσεων είναι το OpenID, το WS federation, το OAuth , και το νέο Simple Cloud Identity Management(SCIM) [021,063,067].

5.2.4 Απόκρυψη, Ασφαλής Διαγραφή Δεδομένων

Η απόκρυψη δεδομένων(data masking) είναι μία τεχνική που σκοπό έχει να απομακρυνθούν όλα τα αναγνωρίσιμα και διακριτικά χαρακτηριστικά από τα δεδομένα, ώστε να καταστούν ανώνυμα και όμως ακόμα να είναι λειτουργικά και μπορεί να εφαρμοστεί σε δεδομένα που δεν είναι κρυπτογραφημένα. Σκοπό έχει τη διατήρηση της προστασία της ιδιωτικότητας των εγγραφών με την αλλαγή των δεδομένων, έτσι ώστε οι πραγματικές τιμές να μην μπορούν να προσδιοριστούν ή να αναπαραχθούν από τρίτους. Μια συνηθισμένη τεχνική απόκρυψης δεδομένων περιλαμβάνει αντικατάσταση των πραγματικών τιμών δεδομένων με κλειδιά-τιμές από έναν εξωτερικό πίνακα αναζήτησης που κρατά τις πραγματικές τιμές δεδομένων και την αντιστοίχιση. Το όφελος είναι ότι εκτός οργανισμού, στη μεριά του νέφους, η λειτουργία-επεξεργασία των δεδομένων που έχουν υποστεί απόκρυψη μπορεί να γίνει με λιγότερους ελέγχους, δικλείδες ασφάλειας από ότι τα αρχικά δεδομένα ενώ παράλληλα μπορεί να καλύψει τη συμβατότητα με απαιτήσεις προστασίας της ιδιωτικότητας και μη αποκάλυψης ευαίσθητων, εμπιστευτικών δεδομένων[087].

Η ασφαλής διαγραφή δεδομένων αφορά τις τεχνικές με τις οποίες τα δεδομένα απομακρύνονται από τα αποθηκευτικά μέσα χωρίς να αφήσουν «υπόλοιπα» τα οποία να μπορούν να αξιοποιηθούν. Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, ο συνηθισμένος τρόπος διαγραφής των αρχείων στους υπολογιστές δεν αφαιρεί πραγματικά τα δεδομένα από τον σκληρό δίσκο, απλώς αφαιρεί την αναφορά σε αυτά. Είναι επομένως δυνατό και συχνά εύκολο, με το κατάλληλο λογισμικό να ανακτηθούν δεδομένα από τον δίσκο, τα οποία θεωρούνταν διαγραμμένα[087]. Υπάρχουν διάφορα λογισμικά αναλόγως του λειτουργικού συστήματος που εκτελούν ασφαλή διαγραφή των δεδομένων, ενώ το NIST έχει εκδώσει την οδηγία Special

Publication 800-88 «Guidelines for Media Sanitization» [060], που αφορά τον «καθαρισμό» των μέσων από τα ευαίσθητα δεδομένα.

Κατά την ασφαλή διαγραφή δεδομένων στο περιβάλλον του νέφους, πρέπει επίσης να ληφθεί υπόψη η διαδικασία διατήρησης αντιγράφων ασφάλειας που τηρεί ο πάροχος και να προσδιοριστεί ο τρόπος (συνήθως μέσω της πολιτικής ασφάλειας και του ΣΠΥ) με τον οποίο θα γίνει ασφαλής διαγραφή όλων των αντιγράφων.

5.3 Ασφάλεια σε Βάθος (Defense in depth)

Μια βασική φιλοσοφία της ασφάλειας είναι να έχει διαφορετικά επίπεδα άμυνας, δηλαδή να έχει επικαλυπτόμενα συστήματα σχεδιασμένα να παρέχουν ασφάλεια ακόμα και αν ένα από αυτά αποτύχει. Η θεώρηση αυτή ονομάζεται ασφάλεια σε βάθος και βρίσκεται υπό πλήρη εφαρμογή και ανάπτυξη στο περιβάλλον του νέφους[067].

5.3.1 Λειτουργικό Σύστημα, Φυλλομετρητής

Από την μεριά του παρόχου, το λειτουργικό σύστημα πρέπει να είναι δοκιμασμένο, κατάλληλα στημένο και με όλες τις ρυθμίσεις ασφάλειας ενεργοποιημένες. Συγκεκριμένοι διαχειριστές, όταν απαιτείται θα έχουν πρόσβαση σε αυτό, μέσα από ειδικές θέσεις όπου θα γίνεται καταγραφή και τήρηση αρχείου των ενεργειών τους. Όταν δεν υπάρχει πλέον απαίτηση για πρόσβαση τα δικαιώματα θα αφαιρούνται.

Από τη μεριά του πελάτη το λειτουργικό σύστημα πρέπει να είναι επίσης ενημερωμένο και με ενεργοποιημένες ρυθμίσεις ασφάλειας τόσο στις εικονικές συσκευές που τρέχουν στο νέφος όσο και στις συσκευές που παρέχουν πρόσβαση σε αυτές (τερματικά, φορητοί υπολογιστές κ.α.). Αντίστοιχα μηχανισμοί ελέγχου προνομίων και κλιμάκωσης δικαιωμάτων αναλόγως της ανάγκης χρήσης πρέπει να χρησιμοποιούνται[002, 062].

Αντίστοιχα ενημερωμένος από την πλευρά του πελάτη πρέπει να είναι και ο φυλλομετρητής ιστοσελίδων που χρησιμοποιείται, με ενεργοποιημένες τις ρυθμίσεις ασφάλειας. Γενικά συνιστάται στους πελάτες να χρησιμοποιούν ένα φυλλομετρητή για περιπτώσεις πρόσβασης στο διαδίκτυο γενικής φύσεως και άλλον για ειδικούς- ευαίσθητους σκοπούς[077]. Επιπλέον

υπάρχουν πάροχοι που δεν επιτρέπουν την πρόσβαση στις υπηρεσίες τους αν διαπιστώσουν μη ενημερωμένη έκδοση του φυλλομετρητή.

5.3.2 Ασφάλεια Εφαρμογών, Διεπαφών Προγραμματισμού Εφαρμογών

Οι εφαρμογές που προορίζονται για χρήση στο περιβάλλον του νέφους απαιτούν μια σχεδιαστική αυστηρότητα παρόμοια με μία εφαρμογή που πρόκειται να συνδεθεί στο διαδίκτυο. Η ασφάλεια πρέπει να παρέχεται από την ίδια την εφαρμογή, χωρίς καμία υπόθεση για το εξωτερικό περιβάλλον. Να προβλέπονται και να ενσωματώνονται δηλαδή στην εφαρμογή, όλα τα μέτρα προστασίας απέναντι στις κοινές τρωτότητες του διαδικτύου [027].

Όταν δεν χρησιμοποιούνται γνωστές και δοκιμασμένες εφαρμογές, η ανάπτυξη καινούργιων εφαρμογών πρέπει να γίνεται με τη διαδικασία Ασφαλής Ανάπτυξης Κύκλου Ζωή Λογισμικού Secure Software Development Life Cycle(SSDL). Να χρησιμοποιούνται και να ενσωματώνονται οι καλύτερες πρακτικές για την ασφάλεια , τη διαχείριση ταυτοτήτων και δεδομένων κατά την ανάπτυξη και σε όλο τον κύκλο ζωής της εφαρμογής, ενώ πρέπει να λαμβάνονται υπόψη και οι ιδιαιτερότητες του νέφους (για παράδειγμα περιορισμένος φυσικός έλεγχος, πιθανές χαμηλές ταχύτητες πρόσβασης κ.α.)[021]. Αξίζει να σημειωθεί ότι οι μεγάλες εταιρείες λογισμικού, όπως η Microsoft, η Oracle, η Sun κ.α., δημοσιεύουν αναλυτική βιβλιογραφία σχετικά με το πώς να γίνει με ασφάλεια η διαμόρφωση των προϊόντων τους[027].

Αντίστοιχα απαιτείται και η χρήση ασφαλών και δοκιμασμένων Διεπαφών Προγραμματισμού Εφαρμογών καθώς και κατανόηση της λειτουργίας τους και των αλληλεξαρτήσεων που αφορούν στη χρήση τους. Πολύ σημαντική είναι η υιοθέτηση αυστηρού ελέγχου πρόσβασης στις διεπαφές και η τήρηση διαδικασία ασφάλειας στη κλήση τους, που μπορεί να γίνεται με την χρήση μυστικών κλειδιών πρόσβασης ή και με κρυπτογράφηση από άκρη σε άκρη, χρησιμοποιώντας την τεχνολογία SSL[002].

5.3.3 Προστασία από Ιούς , Κακόβουλο λογισμικό

Η χρήση ειδικού λογισμικού κατά των ιών (Antivirus) και των κακόβουλων λογισμικών, το οποίο θα ενημερώνεται τακτικά είναι επιβεβλημένη τόσο από τη μεριά του παρόχου, όσο και από την πλευρά του χρήστη. Αυτό προβλέπεται και από τα καθιερωμένα πρότυπα ασφάλειας (για παράδειγμα από το PCIDSS) [046].

Μια συνηθισμένη τακτική για την χρήση τέτοιων λογισμικών στο περιβάλλον των εικονικών συσκευών, είναι αυτά να συμπεριλαμβάνονται στο πρότυπο δημιουργίας μιας εικονικής συσκευής. Έτσι κάθε φορά που γίνεται κλήση για δημιουργία μιας εικονικής συσκευής αυτή έχει προτοθετημένο και ενεργό λογισμικό κατά των ιών [087].

Από την άλλη το περιβάλλον του νέφους και των εικονικών συσκευών μπορεί να μειώσει αισθητά το κόστος επαναφορά του συστήματος μετά από «μόλυνση» με ιό γιατί συνήθως απαιτείται η κατάργηση των μολυσμένων εικονικών συσκευών και η αντικατάστασή τους με άλλες «καθαρές»[087].

5.3.4 Υποδομή δικτύου

Όλη η λειτουργία του νέφους βασίζεται στη γνωστή υποδομή δικτύου η σωστή ρύθμιση της οποίας είναι καθοριστική για την ασφάλεια. Έτσι οι δρομολογητές (routers) και οι μεταγωγείς (switches) πρέπει να είναι κατάλληλα ρυθμισμένοι. Οι πίνακες δρομολόγησης(routing tables) πρέπει να περιλαμβάνουν μόνο έγκυρες και εγκεκριμένες διαδρομές και όλη η κυκλοφορία που φεύγει από κάθε υποδίκτυο πρέπει να κατευθύνεται σε καθορισμένο προορισμό. Επίσης χρειάζονται διαδικασίες ισχυρής πιστοποίησης και εξουσιοδότησης για να μπορεί κάποιος να επέμβει στις ρυθμίσεις των συσκευών αυτών[087].

Επιπλέον στο επίπεδο της υποδομής του νέφους οι πάροχοι μπορούν να ενισχύσουν την ασφάλεια δικτύου με τη χρήση αναχωμάτων ασφάλειας (Firewalls) και συστημάτων ανίχνευσης/αντιμετώπισης εισβολών (Intrusion Detection/Prevention Systems(IDS/IPS)) [077].

Το ανάχωμα ασφάλειας είναι ένα σύστημα σχεδιασμένο να εμποδίζει τη μη εξουσιοδοτημένη πρόσβαση προς ή από ένα ιδιωτικό δίκτυο ή εικονικά ιδιωτικό δίκτυο. Μπορεί επίσης να βοηθήσει μειώνοντας την επιφάνεια επίθεσης των εικονικών εξυπηρετητών σε περιβάλλοντα νέφους, ενώ ελέγχει τόσο την εισερχόμενη όσο και την εξερχόμενη κυκλοφορία Με την ανάπτυξη αναχώματος ασφάλειας στις εικονικές συσκευές με ρυθμίσεις-πολιτικές που συμβαδίζουν την πολιτική ασφάλειας του οργανισμού, μπορεί κανείς να επιτύχει την επιλεκτική απομόνωση της εικονικής συσκευής, το φιλτράρισμα των δεδομένων σε επίπεδο ανοιχτών πορτών, το διαχωρισμό των δεδομένων για ανάλυση καλύπτοντας όλα τα πρωτόκολλα τύπου IP. Με τον τρόπο αυτό, μπορούν να προληφθούν επιθέσεις άρνηση παροχής υπηρεσιών (DoS). Επιπλέον, τα αναχώματα ασφάλειας επιτρέπουν τον καθορισμό διαφορετικών πολιτικών σε διαφορετικά τμήματα-διεπαφές του δικτύου [015].

Τα συστήματα ανίχνευσης/αντιμετώπισης εισβολών παρακολουθούν την κίνηση του δικτύου και την συγκρίνουν με γνωστά μοτίβα που θεωρούνται κανονική συμπεριφορά. Έτσι ανιχνεύουν «ανωμαλίες», δηλαδή συμπεριφορά που θεωρείται μη κανονική ή αναμενόμενη, που συνήθως σημαίνει κάποιο κίνδυνο για έναν οργανισμό και ανάλογα την καταγράφουν (τα συστήματα ανίχνευσης) ή επεμβαίνουν για τη διακοπή της(τα συστήματα αντιμετώπισης). Τα συστήματα αυτά μπορούν να προστατεύσουν από νέες τρωτότητες (για τις οποίες δεν έχουν εκδοθεί ακόμη ενημερώσεις ασφάλειας) τόσο τις εφαρμογές όσο και τα λειτουργικά συστήματα που τρέχουν σε εικονικές συσκευές. Εντός του νέφους τα συστήματα αυτά συχνά εστιάζουν στην εικονική υποδομή και στη δραστηριότητα μεταξύ των Hypervisors για την αντιμετώπιση συντονισμένων μαζικών επιθέσεων [015,021].

Επιπλέον ο σωστός συνδυασμός της χρήσης των αναχωμάτων ασφάλειας και των συστημάτων ανίχνευσης εισβολών μπορεί να ανακόψει και τυχόν επιθέσεις που ξεκινούν μέσα από το νέφος προς τα έξω λειτουργώντας ως ένα σύστημα ανίχνευσης εξερχόμενων επιθέσεων (extrusion detection system)[001].

5.3.5 Εικονικό Ιδιωτικό Νέφος

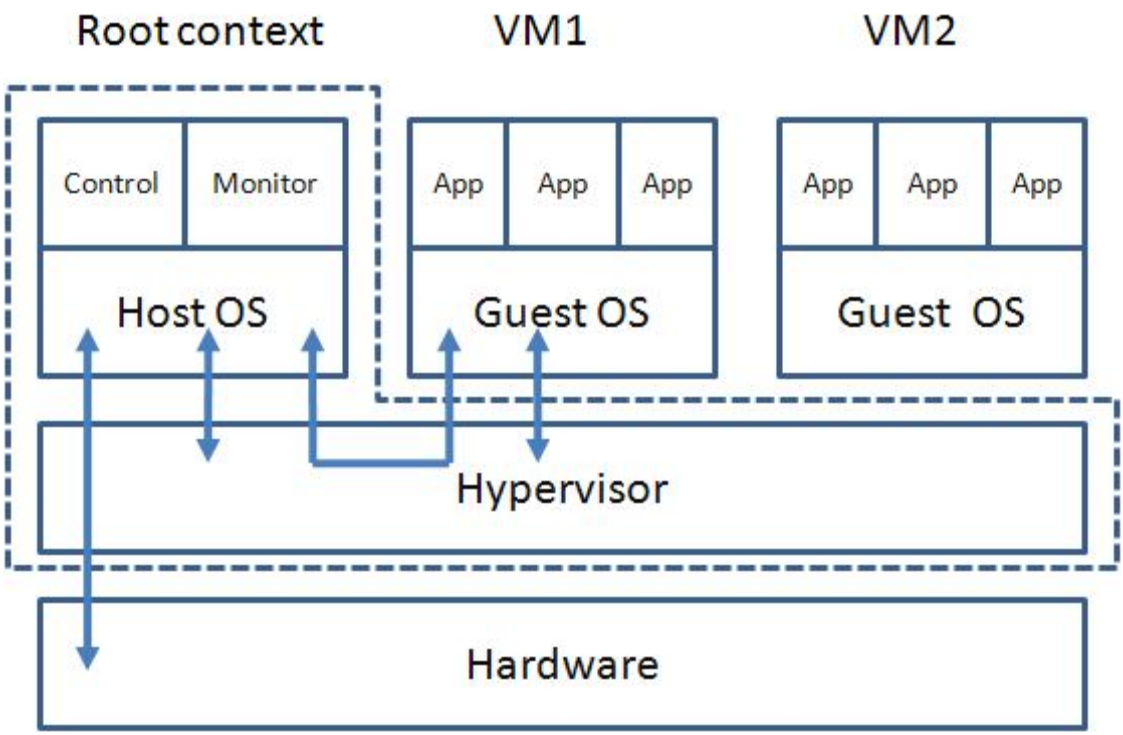
Στο μοντέλο του IaaS υπάρχουν πάροχοι (πχ η AMAZON) που κατ' αντιστοιχία με τα εικονικά ιδιωτικά δίκτυα, μπορούν να διαθέσουν εικονικό ιδιωτικό νέφος. Σε ένα τέτοιο εικονικό ιδιωτικό νέφος δίνεται η δυνατότητα για δέσμευση φυσικών υποδομών για αποκλειστική χρήση από έναν πελάτη-οργανισμό.

Κάθε εικονικό ιδιωτικό νέφος είναι ένα απομονωμένο δίκτυο εντός του νέφους με δικές του διευθύνσεις IP και χωρίς απευθείας εξωτερικές συνδέσεις. Ειδικές πύλες δικτύου (gateways) επιτρέπουν την σύνδεση του εικονικού ιδιωτικού νέφους με την υποδομή του πελάτη (VPN Gateway) ή και με το διαδίκτυο αν απαιτείται (Internet Gateway), ενώ και πάλι χρησιμοποιείται ανάχωμα ασφάλειας [002].

5.4 Ασφάλεια Εικονικοποίησης (Virtualization Security)

Όπως αναφέρθηκε ο Hypervisor είναι ένα λογισμικό το οποίο εγκαθίσταται στο υλικό (hardware) και δημιουργεί πολλαπλές εικονικές συσκευές, που τρέχουν πάνω στο υλικό. Με απλά λόγια αποτελεί την καρδιά της λειτουργίας της εικονικοποίησης, στα πλεονεκτήματα τις

οποίας στηρίχθηκε η ανάπτυξη του νέφους. Η τυπική διαμόρφωση εικονικοποίησης ενός διακομιστή με την χρήση Hypervisor φαίνεται στο σχήμα 5.2. Ο πιο συνηθισμένος τύπος Hypervisor που χρησιμοποιείται είναι ο Xen, που είναι προϊόν ανοιχτού κώδικα και συντηρείται από την κοινότητα του Xen υπό την άδεια GNU General Public License (GPL2)[020,089]. Άλλοι γνωστοί Hypervisors είναι οι VMware ESXi, Hyper-V, and KVM [074].



Σχήμα 5.2: Τυπική διαμόρφωση εικονικοποίησης ενός διακομιστή. Τα βέλη δείχνουν τις αλληλεπιδράσεις μεταξύ των εμπλεκομένων μερών[043].

Το National Institute of Standards and Technology έχει εκδώσει την οδηγία NIST Special Publication 800-125 «Guide to Security for Full Virtualization Technologies» όπου σχετικά με την ασφάλεια του Hypervisor δίνει τις ακόλουθες συστάσεις[057]:

- Εγκατάσταση όλων των ενημερώσεων του Hypervisor που δίνει ο κατασκευαστής. Οι περισσότεροι Hypervisors έχουν τη δυνατότητα αυτόματου ελέγχου και εγκατάστασης αναβαθμίσεων.

- Περιορισμός πρόσβασης των διαχειριστών στην διεπαφή του Hypervisor. Προστασία όλων των διαχειριστικών καναλιών επικοινωνίας, είτε χρησιμοποιώντας αποκλειστικό δίκτυο για διαχείριση ή χρησιμοποιώντας δοκιμασμένες τακτικές πιστοποίησης και κρυπτογράφησης.

- Συγχρονισμός όλων των στοιχείων της εικονικής υποδομής σε κάποιον αξιόπιστο εξυπηρετητή χρονισμού. Με τον τρόπο αυτό προστατεύεται το σύστημα από τις επιθέσεις χρονισμού(timing attacks) σε κρυπτογραφικές λειτουργίες [083].

- Αποσύνδεση μη χρησιμοποιούμενων συσκευών από το σύστημα.

- Απενεργοποίηση όλων των υπηρεσιών του Hypervisor που δεν χρειάζονται ή δεν χρησιμοποιούνται και αποτελούν πιθανά σημεία ευπαθειών (πχ διαμοιρασμός αρχείων).

- Χρήση δυνατοτήτων ενδοσκόπησης για την παρακολούθηση της ασφάλειας κάθε φιλοξενούμενου λειτουργικού συστήματος. Μια τέτοια τεχνική έχει παρουσιάσει η IBM, όπου εξετάζοντας τον πίνακα κλήσεων του συστήματος (System-Call Table) από το φιλοξενούμενο λειτουργικό και άλλες παραμέτρους στο βασικό υλικό (hardware) βγάζει συμπεράσματα για το φιλοξενούμενο λογισμικό [018].

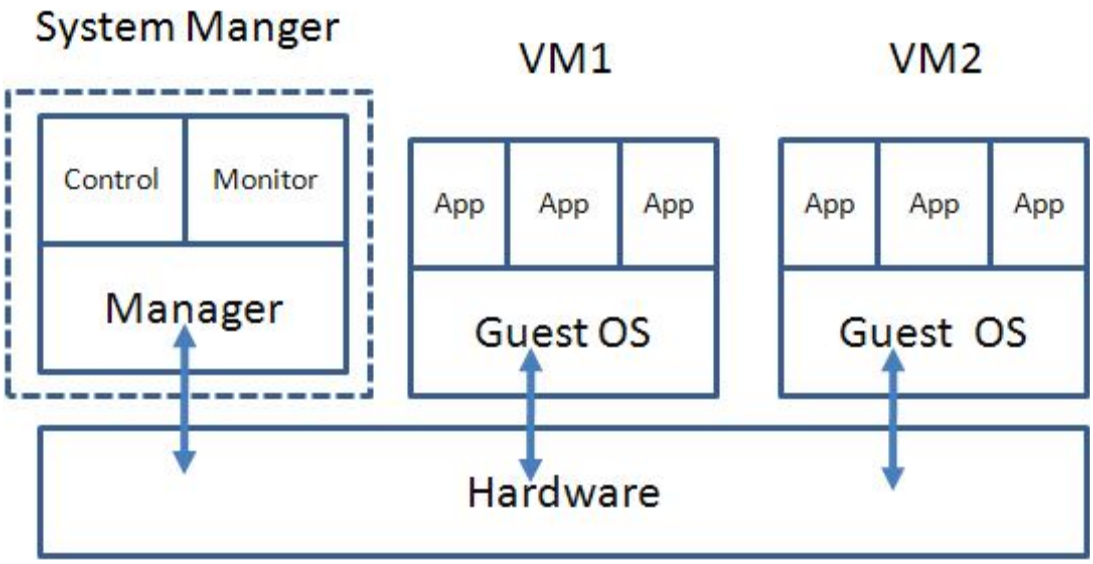
- Χρήση δυνατοτήτων ενδοσκόπησης για την παρακολούθηση της κίνησης μεταξύ των φιλοξενούμενων λειτουργικών συστημάτων, καθώς είναι πιθανό η κίνηση αυτή να μην ελέγχεται από άλλους μηχανισμούς που ελέγχουν την κίνηση στα κλασικά δίκτυα (όπως αναχώματα ασφάλειας κ.α.)

- Παρακολούθηση του ίδιου του Hypervisor για ύποπτες ενδείξεις, είτε μέσω αυτοματοποιημένων διαδικασιών αυτοελέγχου, είτε μέσω ανάλυσης καταγραφών.

Για τους πελάτες που χρησιμοποιούν LINUX ο XEN έχει και τη δυνατότητα του paravirtualization, που είναι μια τεχνική εικονικοποίησης κατά την οποία το φιλοξενούμενο λειτουργικό σύστημα βασίζεται στον Hypervisor και μέσω αυτού έχει πρόσβαση σε λειτουργίες που κανονικά θα απαιτούσαν αυξημένα προνόμια πρόσβασης στο υλικό. Με την τεχνική αυτή για την πρόσβαση στο υλικό υπάρχουν τέσσερα επίπεδα δικαιωμάτων από 0 έως 3 που λέγονται δακτύλιοι, με τον δακτύλιο 0 να έχει τα περισσότερα δικαιώματα. Το λειτουργικό σύστημα του οικοδεσπότη εκτελείται στον δακτύλιο 0, του φιλοξενούμενου στον δακτύλιο 1 και οι εφαρμογές

στο λιγότερο προνομιούχο δακτύλιο 3. Αυτός ο σαφής διαχωρισμός δικαιωμάτων παρέχει πρόσθετη ασφάλεια.[002, 083].

Μια άλλη αντιμετώπιση που προτάθηκε από τον E.Keller κ.α. [043] είναι η λύση noHype που προτείνει την κατάργηση του Hypervisor και απευθείας ανάπτυξη κάθε εικονικής μηχανής πάνω σε συγκεκριμένο τμήμα του υλικό (μνήμη, πυρήνα του επεξεργαστή κ.α.). Η πρόταση αυτή φαίνεται στο σχήμα 5.3.



Σχήμα 5.3: Προτεινόμενη διαμόρφωση εικονικοποίησης διακομιστή χωρίς χρήση Hypervisor[043].

5.5 Αρχιτεκτονική Έμπιστης Νεφοϋπολογιστικής (Trusted Cloud Computing)

Η κοινοπραξία Trusted Computing Group (TCG) έχει αναπτύξει προδιαγραφές προσπαθώντας να δημιουργήσει ένα περιβάλλον έμπιστου νέφους. Η αρχιτεκτονική που προτείνει, προστατεύει τα δεδομένα χρησιμοποιώντας ειδικές συσκευές ασφάλειας που «κλειδώνουν» τα κρυπτογραφημένα κλειδιά, τους κωδικούς πρόσβασης και άλλα τμήματα δεδομένων που απαιτούνται για τη λειτουργία του έμπιστου νέφους [080].

Για να παρέχει περισσότερη ασφάλεια από αυτή που μπορεί να παρέχει μόνο το λογισμικό, η TCG έχει καθορίσει τις προδιαγραφές της ειδικής συσκευής που καλείται Trusted Platform Module (TPM), και πάνω σε αυτή έχει στηριχθεί η συγκεκριμένη αρχιτεκτονική [080].

Η συσκευή TPM, που ενσωματώνεται πλέον σε πολλούς υπολογιστές, έχει δυνατότητες όπως πιστοποίηση του μηχανήματος που είναι τοποθετημένη, προστασία παραβίασης, μηχανικής κρυπτογράφησης(hardware encryption), αναγνωρισμένης υπογραφής, ασφαλής αποθήκευσης κλειδιών και μαρτυρίας. Με τον όρο μαρτυρίας εννοείται η δυνατότητα της συσκευής TPM να ελέγχει το λογισμικό καθώς αυτό φορτώνεται και να παρέχει ασφαλείς αναφορές (μαρτυρίες) σχετικά με το τι ακριβώς τρέχει στο σύστημα [080].

Το έμπιστο νέφος δημιουργείται καθώς όσοι συμμετέχουν σε αυτό (πάροχος, πελάτες) χρησιμοποιούν τις συγκεκριμένες έμπιστες μηχανές. Πέρα από τη συσκευή TPM το TCG παρέχει και προδιαγραφές για το Trusted Network Connect(TNC) (ένα πρότυπο για ασφάλεια των δικτύων και έλεγχο πρόσβασης) καθώς και προδιαγραφές για Trusted Storage (ένα πρότυπο για κρυπτογράφηση δεδομένων ολόκληρου δίσκου, χρησιμοποιώντας συσκευές που είναι ενσωματωμένες πάνω στους δίσκους)[070,080,].

Βέβαια η χρήση των TPM συνεπάγεται κάποιους περιορισμούς στην ευελιξία και συνήθως παρουσιάζονται προβλήματα όταν χρησιμοποιείται εικονικοποίηση και πολλές εικονικές συσκευές είναι στημένες πάνω σε μία φυσική πλατφόρμα (που έχει μία συσκευή TPM).

Μια λύση είναι η χρήση εικονικών συσκευών TPM (Virtual TPM) για κάθε εικονική συσκευή. Η λύση αυτή, καθώς το εικονικό TPM είναι κομμάτι λογισμικού δεν προσφέρει προστασία σε επιθέσεις υλικού(hardware), γι' αυτό απαιτούνται και μέτρα φυσικής προστασίας όταν χρησιμοποιείται[044,083].

5.6 Η Λύση του Υβριδικού Νέφους (Hybrid Cloud)

Όπως αναφέρθηκε, ένα από τα μοντέλα ανάπτυξης της νεφοϋπολογιστικής είναι το υβριδικό νέφος, το οποίο είναι ένα συνδυασμός ιδιόκτητων εσωτερικών υποδομών και εξωτερικών (του παρόχου) υποδομών του νέφους. Οι ξεχωριστές υποδομές συνδέονται μεταξύ τους με τεχνολογίες που επιτρέπουν ευελιξία στη μεταφορά των δεδομένων και των εφαρμογών μεταξύ των υποδομών, αναλόγως τις ανάγκες (για παράδειγμα ενεργοποίηση του εξωτερικού νέφους με σκοπό την εξισορρόπηση ξαφνικού φόρτου εργασίας –μια τεχνολογία που ονομάζεται «Cloud bursting») [012].

Η περίπτωση του υβριδικού νέφους παρέχει επιπλέον ασφάλεια σε έναν οργανισμό, καθώς τα κρίσιμα τμήματα των εφαρμογών και των δεδομένων για τη λειτουργία του μπορούν να παραμείνουν εντός του οργανισμού, ενώ τα υπόλοιπα μπορούν να μετακινηθούν στο νέφος. Με τον τρόπο αυτό εξασφαλίζονται οι ευαίσθητες πληροφορίες-δεδομένα καθώς παραμένουν στη διαχείριση του , ενώ εξασφαλίζεται και η δυνατότητα λειτουργίας του οργανισμού ακόμα και όταν για κάποιο λόγο χαθεί η σύνδεση με το εξωτερικό νέφος(off line) [012].

Οι πάροχοι παρέχουν λύσεις που επιτρέπουν την ανάπτυξη τέτοιων υβριδικών μοντέλων όπως για παράδειγμα το Amazon Virtual Private Cloud, το Skytap Virtual Lab και το CohesiveFT VPN-Cubed. Οι λύσεις αυτές χρησιμοποιούν την τεχνολογία IPsec και τις δυνατότητες διασύνδεσης Εικονικών Ιδιωτικών Δικτύων(Virtual Private Networks tunneling) για τη διασύνδεση του δημόσιου νέφους με τις ιδιόκτητες υποδομές. Επίσης η Eucalyptus και η Open-Nebula είναι δύο συμπληρωματικές τεχνολογίες που παρέχουν ελεύθερα εργαλεία για την ανάπτυξη και τον έλεγχο υβριδικών αρχιτεκτονικών νέφους[002,012,073].

Παράλληλα έχουν αναπτυχθεί και εφαρμογές που συνεργάζονται με το MapReduse(που είναι ένα προγραμματιστικό μοντέλο για επεξεργασία μεγάλων συνόλων δεδομένων σε κατανεμημένα συστήματα) με τις οποίες ο χρήστης επισημαίνει τα ευαίσθητα δεδομένα με χρήση μιας ετικέτας και κατόπιν αυτά, αυτόματα, παραμένουν εντός του ιδιωτικού νέφους ενώ τα υπόλοιπα κατευθύνονται στο δημόσιο νέφος[090].

Κεφάλαιο 6
Πλαίσιο Αξιολόγησης Ασφάλειας

Στο κεφάλαιο αυτό περιγράφεται η δουλειά που έχει γίνει από διάφορους οργανισμούς για τη δημιουργία πλαισίου, μέσα από το οποίο ο υποψήφιος πελάτης-χρήστης του νέφους θα μπορεί να αξιολογήσει το επίπεδο ασφάλειας που του παρέχει ο πάροχος που αξιολογείται. Επιπλέον θα παρουσιαστούν και τα προτεινόμενα βήματα, τα οποία πρέπει να συμπεριλαμβάνονται σε μία στρατηγική μετακίνησης στο νέφος.

6.1 Διαθέσιμες Εργασίες

Οι περισσότεροι χρήστες του νέφους, είτε πρόκειται για ιδιωτικό ή δημόσιο, έχουν συγκεκριμένες προσδοκίες για την ασφάλεια των δεδομένων τους. Αντίστοιχα, ο πάροχος που χειρίζεται το νέφος αναλαμβάνει ευθύνη για τη διασφάλιση ότι υπάρχουν μέτρα ασφάλειας και ακολουθούνται τα πρότυπα και οι διαδικασίες.

Κατ' αρχάς, υπάρχουν δύο πτυχές στους ελέγχους ασφάλειας για τις εφαρμογές νέφους. Η πρώτη έχει να κάνει με την παρουσία του ίδιου του ελέγχου. Η δεύτερη αφορά την αποτελεσματικότητα ή την ευρωστία του ελέγχου. Με άλλα λόγια, δεν είναι αρκετό ένας έλεγχος ασφάλειας να εκτελείται, αλλά πρέπει επίσης να είναι και αποτελεσματικός. Αυτό μπορεί να

εκφραστεί και ως ο βαθμός εμπιστοσύνης (ή αξιοπιστίας) που μπορεί να αναμένεται από τους ελέγχους αυτούς. Για παράδειγμα, ένα νέφος μπορεί να εφαρμόζει κρυπτογραφημένες επικοινωνίες μεταξύ του και ενός εξωτερικού χρήστη, αλλά αν γίνεται έλεγχος αξιολόγησης της αποτελεσματικότητα των κρυπτογραφημένων επικοινωνιών, τότε θα πρέπει κατά κάποιο τρόπο να βεβαιωθεί ότι και ο έλεγχος έχει σχεδιαστεί σωστά, εφαρμόστηκε και επαλήθευσε τα αποτελέσματα που αναμένονταν[087].

Με βάση την ευαισθησία των δεδομένων ή την αναμενόμενη επικινδυνότητα ενός συστήματος, θα πρέπει να υπάρξει μια αρχική φάση στην οποία εντοπίζονται οι απαιτήσεις για τους κατά περίπτωση ελέγχους ασφάλειας. Ακολουθεί αρχική αξιολόγηση της αποτελεσματικότητας των ελέγχων που τέθηκαν σε εφαρμογή και ανάλυση τυχών ενεργειών αποκατάστασης. Η διαδικασία αυτή επαναλαμβάνεται περιοδικά, ώστε να σχηματιστεί μία αρκετά καλή εικόνα του κατά πόσον οι υπηρεσίες του νέφους παρέχουν ασφάλεια έναντι στους κινδύνου που υπόκεινται. Συχνά οι πάροχοι δημοσιεύουν τα αποτελέσματα ενός τρίτου ανεξάρτητου φορέα αξιολόγησης ασφάλειας με σκοπό τη διαφήμιση, προώθηση των υπηρεσιών τους[087].

Μέχρι τώρα αρκετές προσπάθειες έχουν γίνει για να προφέρουν οδηγό ή πλαίσιο αξιολόγησης ασφάλειας του νέφους.

Η Cloud Security Alliance (CSA) έχει εκδώσει τα ακόλουθα:

- Τον Πίνακα Ελέγχων του Νέφους (Cloud Controls Matrix (CCM)): Ένας πίνακας σχεδιασμένος για να παρέχει θεμελιώδεις αρχές ασφάλειας για την καθοδήγηση των παρόχων και να βοηθήσει μελλοντικούς πελάτες νέφους στην εκτίμηση του συνολικού κινδύνου της ασφάλειας του παρόχου. Η έκδοση 1.4 (Μάρτιος 2013) του Πίνακα Ελέγχων του Νέφους παρέχει ένα πλαίσιο ελέγχου που δίνει λεπτομερείς επεξηγήσεις των εννοιών της ασφάλειας και των αρχών που είναι ευθυγραμμισμένες με τις κατευθύνσεις της Cloud Security Alliance σε 13 τομείς[022].

- Το Ερωτηματολόγιο της Πρωτοβουλίας Κοινών Εκτιμήσεων (Consensus Assessments Initiative Questionnaire), έκδοση 1.1 (Σεπτέμβριος 2011): που εστιάζει στο να προσφέρει στη βιομηχανία αποδεκτούς τρόπους για να τεκμηριώσει τι έλεγχοι ασφάλειας υπάρχουν σε προσφορές παροχών IaaS, PaaS και SaaS, παρέχοντας διαφάνεια των ελέγχων ασφάλειας[023].

- Τον Οδηγό Ασφάλειας για Κρίσιμους Τομείς Εστιασμένους στην Υπολογιστική Νέφους (Security Guidance for Critical Areas of Focus in Cloud Computing): η έκδοση 3.0 παρέχει οδηγίες ασφάλειας για το νέφος χωρισμένες σε τρία κύρια τμήματα (αρχιτεκτονική, διακυβέρνηση, λειτουργία νέφους) που καλύπτουν συνολικά 14 περιοχές[021].

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Network and Information Security Agency (ENISA)), που είναι επικεφαλής των προσπαθειών για θέσπιση οδηγιών ασφάλειας στην Ευρώπη, έχει παρουσιάσει αρκετές οδηγίες για την ασφαλή υιοθέτηση του νέφους, σε αυτά περιλαμβάνονται:

- Το «Νεφοϋπολογιστική: Πλαίσιο Διασφάλισης Πληροφοριών» (Cloud Computing: Information Assurance Framework):που εκδόθηκε το Νοέμβριο του 2009 και αποτελεί ένα πλαίσιο ασφάλειας και εργαλείο για τους υπεύθυνους ανάπτυξης δικτύων προκειμένου να εκτιμηθεί η ασφάλεια των παρόχων πριν πάρουν την απόφαση να κινηθούν προς το υπολογιστικό νέφος[027].

- Το «Νεφοϋπολογιστική: Οφέλη, Κίνδυνοι και Συστάσεις για την Ασφάλεια των Πληροφοριών» (Cloud Computing: Benefits, Risks and Recommendations for Information Security):μία μελέτη, που εκδόθηκε το Νοέμβριο του 2009 και επιτρέπει την εμπεριστατωμένη αξιολόγηση των κινδύνων για την ασφάλεια. Παρουσιάζει τα οφέλη από τη χρήση του νέφους και παρέχει καθοδήγηση ασφάλειας για τους πιθανούς και υπάρχοντες χρήστες του[031].

- Το «Ασφάλεια και ανθεκτικότητα σε Κυβερνητικά Νέφη» (Security and Resilience in Governmental Clouds):μία μελέτη του 2011, που παρέχει έναν οδηγό για δημόσιους φορείς στον ορισμό των απαιτήσεών τους για ασφάλεια, ανθεκτικότητα και πώς να αξιολογήσουν και να επιλέξουν από τα διάφορα μοντέλα παράδοσης υπηρεσιών του νέφους[030].

- Το «Ασφαλείς Προμήθειες» (Procure Secure): ένας λεπτομερής οδηγός του 2012, για την παρακολούθηση των επιπέδων ασφάλειας της παροχής υπηρεσιών σε συμβάσεις νέφους, σε όλη τη διάρκεια του έργου. Έχει στόχο να βελτιωθεί η κατανόηση των πελατών στον τομέα της ασφάλειας των υπηρεσιών νέφους και τους πιθανούς δείκτες και μεθόδους που μπορούν να χρησιμοποιηθούν για να παρέχουν την κατάλληλη διαφάνεια, κατά τη διάρκεια της παροχής υπηρεσιών. Ο νέος οδηγός αφορά στις προμήθειες του Δημοσίου, οι οποίες αντιστοιχούν σχεδόν στο 20% του ΑΕΠ της ΕΕ, περίπου 2,2 τρις (στοιχεία της Eurostat από

το 2009). Περιλαμβάνει μια λίστα ελέγχου για τις ομάδες προμηθειών, καθώς και μία σε βάθος περιγραφή της κάθε παραμέτρου ασφάλειας: τί πρέπει να μετρηθεί και πώς. Οι παράμετροι ασφάλειας που καλύπτει είναι οι εξής: αντιμετώπιση έκτακτων περιστατικών, ελαστικότητα υπηρεσιών και ανοχή φορτίου, διαχείριση του κύκλου ζωής των δεδομένων, τεχνική συμμόρφωση και διαχείριση ευπάθειας, διοίκηση αλλαγών, απομόνωση δεδομένων και διαχείριση καταγραφής και έρευνας[028].

- Η «Κρίσιμη Νεφοϋπολογιστική» (Critical Cloud Computing):μια μελέτη του 2012, με σκοπό την προστασία των Υποδομών Ζωτικής Πληροφορίας (Critical Information Infrastructure Protection (CIIP)) στις υπηρεσίες νεφοϋπολογιστικής, όπου στο κεφάλαιο 5 δίνεται η περίληψη των εισηγήσεων που εστιάζει στο τρίγωνο αξιολόγηση επικινδυνότητας, μέτρα ασφάλειας, αναφορές συμβάντων[026].

Το NIST έχει εκδώσει την οδηγία Special Publication 800-144: «Guidelines on Security and Privacy in Public Cloud Computing» που παρέχει μια επισκόπηση των προκλήσεων της ασφάλειας και της ιδιωτικότητας σχετικά με το νέφος και επισημαίνει εκτιμήσεις που πρέπει να λαμβάνουν υπόψη οι οργανισμοί κατά την εξωτερική ανάθεση δεδομένων, εφαρμογών και υποδομών σε ένα δημόσιο περιβάλλον νέφους[056].

Επιπλέον στις ΗΠΑ, το Federal Risk and Authorization Management Program (FedRAMP) είναι το πρόγραμμα για τις ομοσπονδιακές κυβερνητικές υπηρεσίες που πρέπει να τηρούν στην προμήθεια των υπηρεσιών νέφους. Παρέχει μια τυποποιημένη και κεντρική προσέγγιση για την αξιολόγηση ασφάλειας, την έγκριση και τη συνεχή παρακολούθηση των υπηρεσιών νέφους. Το πρόγραμμα όχι μόνο θέτει τις απαιτήσεις ασφάλειας, αλλά επίσης παρακολουθεί την εφαρμογή των μέτρων ασφάλειας, για παράδειγμα, με τριμηνιαίες περιοδικές εκθέσεις ελέγχου τρωτών σημείων. Μπορεί να αποτελέσει σημείο αναφοράς για τις δημόσιες συμβάσεις στις ΗΠΑ, απευθύνεται όμως και στους παρόχους που μπορούν να αποκτήσουν αντίστοιχη εξουσιοδότηση ασφάλειας αλλά και σε τρίτους ανεξάρτητους φορείς που κάνουν αντίστοιχες εκτιμήσεις[082].

Τα παραπάνω, καθώς και άλλες προσπάθειες που έχουν δημοσιευθεί για τον καθορισμό πλαισίου αξιολόγησης ασφάλειας του νέφους [049, 087] κάνουν ξεκάθαρο ότι, τόσο σε ευρωπαϊκό επίπεδο όσο και στις ΗΠΑ, γίνονται συνεχείς και σημαντικές προσπάθειες, τόσο για τη σωστή αξιολόγηση της ασφάλειας που παρέχουν οι υπηρεσίες νέφους, όσο και για τη βελτίωση της ίδιας αυτής της ασφάλειας.

6.2 Προτεινόμενα Βήματα

Συνδυάζοντας και συνοψίζοντας τις πληροφορίες από τις πηγές που αναφέρθηκαν στην προηγούμενη παράγραφο, προσδιορίστηκαν τα ακόλουθα προτεινόμενα βήματα που πρέπει να συμπεριλαμβάνονται σε μία στρατηγική ομαλής μετακίνησης στο νέφος.

6.2.1 Προκαταρκτικές ενέργειες

Πρόκειται για τις ενέργειες που θα εκτελεστούν πριν από κάποια μετακίνηση.

1. Προσδιορισμός απαιτήσεων ασφάλειας και ιδιωτικότητας του οργανισμού.

2. Ταξινόμηση των δεδομένων-διαβάθμιση της πληροφορίας.

3. Σύγκριση της Πολιτικής Ασφάλειας του οργανισμού με αυτή του παρόχου.

4. Εκτίμηση της συνολικής εικόνας του παρόχου, αξιολόγηση πιστοποιήσεων και προτύπων που πληρεί.

5. Αξιολόγηση επικινδυνότητας της μετάβασης.

6. Προσδιορισμός ελέγχων ασφάλειας και συνεργασία με ανεξάρτητους τρίτους φορείς.

7. Προσδιορισμός της νέας αρχιτεκτονικής υπηρεσιών και τεχνικών λύσεων ασφάλειας που εφαρμόζονται.

8. Προσδιορισμός του Συμφωνητικού Παροχής Υπηρεσιών.

9. Προσδιορισμός του τρόπου διαχείρισης συμβάντων- περιστατικών ασφάλειας.

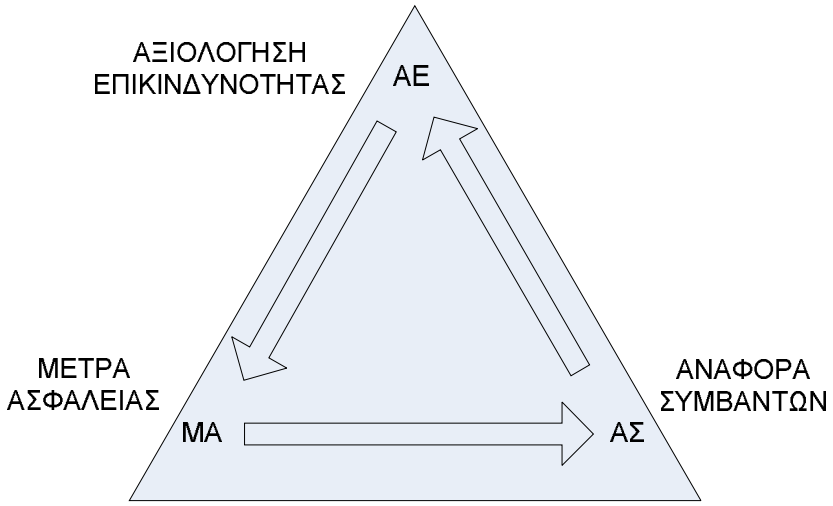
10. Προσδιορισμός του τρόπου παρακολούθησης εκτέλεσης συμβολαίων.

11. Καθορισμός διαδικασιών τερματισμού συμβολαίου.

6.2.2 Δοκιμαστική Χρήση-Σταδιακή Μετάπτωση

Ακολουθεί ο προσδιορισμός του τμήματος των υπηρεσιών που θα μεταβούν στο νέφος. Αρχικά προτείνεται η μετάβαση ενός «πιλοτικού» τμήματος[088], μέσα από το οποίο το προσωπικό του οργανισμού θα αποκτήσει εξοικείωση με την τεχνολογία και τις δυνατότητες του παρόχου, αλλά ταυτόχρονα θα δοκιμαστούν στην πράξη αυτά που συμφωνήθηκαν και προσδιορίστηκαν στις προκαταρκτικές ενέργειες.

Στη συνέχεια μπορεί να ακολουθήσει η σταδιακή μετάπτωση όλο και περισσότερων υπηρεσιών, ανάλογα και με τις απαιτήσεις του οργανισμού, μέσα από την επανάληψη των βημάτων του προτεινόμενου τριγώνου: αξιολόγηση επικινδυνότητας, μέτρα ασφάλειας, αναφορές συμβάντων που φαίνεται και στο σχήμα 6.1 [026].



Σχήμα 6.1: Βασικές διαδικασίες διαχείρισης της ασφάλειας κατά τη διαδικασία μετάπτωσης σε περιβάλλον νέφους.

Σε αυτό το σημείο, η διαδικασία εισέρχεται στο τελικό στάδιο, που στόχο έχει τη συνεχή βελτίωση των παρεχόμενων υπηρεσιών από το νέφος. Ο οργανισμός συνεχίζει να μεταφέρει κατάλληλα δεδομένα και εφαρμογές στο σύννεφο και ίσως ακόμη αντίστροφα, πίσω από το σύννεφο σε εσωτερική υποδομή, εάν είναι απαραίτητο, με βάση την ενδελεχή και συνεχή αξιολόγηση της καταλληλότητας και αποτελεσματικότητας χρήσης των τεχνολογιών νέφους για τον συγκεκριμένο οργανισμό [088].

Κεφάλαιο 7
Συμπεράσματα

Αναμφίβολα η τεχνολογία περιβάλλοντος νεφοϋπολογιστικής αποτελεί ένα νέο υπολογιστικό πρότυπο, που είναι υπό πλήρη άνθηση. Οι τελικοί χρήστες, μέσω του διαδικτύου, έχουν πρόσβαση στις υπηρεσίες που προσφέρονται από το νέφος και ουσιαστικά μπορούν να μοιράζονται υπολογιστικούς πόρους, πληροφορίες και λογισμικό.

Εξαιτίας των βασικών χαρακτηριστικών του νέφους προκύπτουν από τη χρήση του πολλά οφέλη. Το πιο σημαντικό, φαίνεται να είναι η μη απαίτηση για επένδυση και ανάπτυξη εσωτερικής υποδομής για μία εταιρεία. Ειδικά για καινούργιες και μικρές επιχειρήσεις οι λύσεις που προσφέρει η υπολογιστική νέφους μπορεί να είναι αρκετά φτηνότερες από την ανάπτυξη συστημάτων και υπηρεσιών εσωτερικά, ενώ η φύση του νέφους είναι τέτοια ώστε οι χρήστες να πληρώνουν μόνο για τις υπηρεσίες που χρειάζονται, όταν τις χρειάζονται.

Εκτός από το χαμηλότερο κόστος, άλλα οφέλη είναι η ταχύτητα με την οποία γίνεται η υλοποίηση, ανάπτυξη εφαρμογών-λύσεων, και η ταχύτερη εξαγωγή αποτελεσμάτων από προγράμματα μεγάλων υπολογιστικών απαιτήσεων δέσμης. Η δυνατότητα για προσήλωση του προσωπικού μια εταιρείας στο κυρίως έργο της και η αδιάλειπτη διαθεσιμότητα αποθηκευτικού χώρου αξίζουν επίσης να αναφερθούν.

Πέρα από τα οφέλη των επιχειρήσεων, το υπολογιστικό νέφος μπορεί να συμβάλει και στην προστασία του περιβάλλοντος, καθώς είναι ο καλύτερος τρόπος για τη βελτίωση της ενεργειακής απόδοσης κάνοντας χρήση εξυπηρετητών χαμηλής ενεργειακής κατανάλωσης και πράσινων πηγών παραγωγής ενέργειας, ενώ η χρήση του υλικού μπορεί να βελτιστοποιηθεί (και με χρήση τεχνολογιών εικονικοποίησης) μειώνοντας τον αριθμό των φυσικών μηχανών που απαιτούνται για να εκτελεσθεί συγκεκριμένη αλληλουχία εργασιών.

Ακόμη, οι υποδομές μεγάλης κλίμακας που χρησιμοποιούνται στο νέφος συνεπάγονται οφέλη στην ασφάλεια, που προκύπτουν από το εξειδικευμένο προσωπικό, τις μεγάλες δυνατότητες της υποδομής (που εγγυάται και μεγάλη διαθεσιμότητα), τις διαδικασίες δημιουργίας αντιγράφων ασφάλειας και τη συγκέντρωση των δεδομένων σε μεγάλα κέντρα δεδομένων που παρέχουν μεγάλη φυσική ασφάλεια. Έτσι για πολλές μικρές ή μεσαίες επιχειρήσεις, οι οποίες δε διαθέτουν την απαραίτητη τεχνογνωσία ή την υποδομή ασφάλειας, η μετακίνηση στο νέφος συνεπάγεται ενισχυμένη ασφάλεια.

Στο κεφάλαιο 2 παρουσιάστηκαν ενδεικτικά σενάρια που αφορούν στην επιλογή χρήσης υπηρεσιών του νέφους για τα μοντέλα υπηρεσίας του (SaaS, PaaS, IaaS) από ιδιώτες, μικρές ή μεγαλύτερες εταιρείες.

Βέβαια είναι ξεκάθαρο ότι με τη επιλογή χρήσης υπηρεσιών του νέφους, οι χρήστες χάνουν τον έλεγχο από τη μία των δεδομένων τους σε ότι αφορά το πώς αποθηκεύονται, πως μοιράζονται και χρησιμοποιούνται και από την άλλη των μέτρων ασφάλειας που χρησιμοποιούνται για την προστασία των δεδομένων αυτών. Οι έννοιες και οι όροι της ιδιωτικότητας, των ευαίσθητων προσωπικών δεδομένων, της εμπιστευτικότητας, της ακεραιτότητας και της διαθεσιμότητας έχουν σχέση με την ασφάλεια και επηρεάζονται από την αρχιτεκτονική και λειτουργία του νέφους.

Έτσι παρουσιάζονται μία σειρά από κινδύνους και ζητήματα ασφάλειας που σχετίζονται με τη χρήση και τη φύση του νέφους. Βέβαια καθώς όλη η αρχιτεκτονική της λειτουργίας του νέφους βασίζεται στο διαδίκτυο, συνεχίζουν να υφίστανται οι κίνδυνοι που σχετίζονται με τη λειτουργία του διαδικτύου. Κινδύνους συνεπάγεται και η χρήση της τεχνολογίας της εικονικοποίησης που είναι βασική για τη λειτουργία του νέφους. Παρουσιάζονται ακόμη και μία σειρά από νομικά θέματα, που αφορούν και τα Συμφωνητικά Παροχής Υπηρεσιών (ΣΠΥ) (Service Level Agreement(SLA)),που καθορίζουν τη συμφωνία παρόχου –πελάτη.

Σε κάθε περίπτωση τα αγαθά (οι πληροφορίες, τα δεδομένα, οι υπολογιστικοί πόροι κ.α.), τόσο των πελατών του νέφους όσο και των ίδιων των παρόχων πρέπει να προστατεύονται και να γίνονται προσπάθειες για τη διασφάλισή τους.

Για να επιτευχθεί η ασφάλεια στο «νεφελώδες» περιβάλλον της νεφοϋπολογιστικής, απαιτούνται διάφορα βήματα, στα οποία εμπλέκονται οι πάροχοι και οι πελάτες, που ξεκινούν από θέσπιση κατάλληλων διαδικασιών, πρακτικών, χρήση ειδικών τεχνικών εξασφάλισης των δεδομένων. Σε αυτές συμπεριλαμβάνεται η κρυπτογράφηση, η χρήση ψηφιακών υπογραφών και πιστοποιητικών και ο λεπτομερής έλεγχος πρόσβασης. Κύριο λόγο διαδραματίζουν και οι Αρχές Πιστοποίησης που αναλαμβάνουν την έκδοση αυτών των πιστοποιητικών.

Επιπλέον απαιτείται η εφαρμογή ρυθμίσεων, που συνεισφέρουν στην ασφάλεια σε βάθος, ενώ υπάρχουν λύσεις για την ασφαλή χρήση της εικονικοποίησης και προτεινόμενες εφαρμοσμένες επιλογές όπως αυτή του Trusted Cloud Computing και του υβριδικού νέφους.

Η πληθώρα παρόχων, προτεινόμενων λύσεων ασφάλειας και προτύπων κάνει ιδιαίτερα δύσκολη την απόφαση επιλογής παρόχου και μοντέλου χρήσης του νέφους, που να καλύπτει τις απαιτήσεις ενός πελάτη και τον βαθμό επικινδυνότητας στον οποίο θέλει να εκτεθεί. Για το λόγο αυτό, έχει γίνει από διάφορους οργανισμούς πολλή προσπάθεια για τη δημιουργία πλαισίου, μέσα από το οποίο ο υποψήφιος πελάτης-χρήστης του νέφους θα μπορεί να αξιολογήσει το επίπεδο ασφαλείας που του παρέχει ο πάροχος που αξιολογείται. Μία στρατηγική ομαλής μετακίνησης στο νέφος εκτιμάται ότι πρέπει να περιλαμβάνει συγκεκριμένες προκαταρκτικές ενέργειες, δοκιμαστική χρήση και σταδιακή μετάπτωση.

Είναι αντιληπτό ότι όσο μεγαλύτερη είναι η ιδιόκτητη υποδομή και άρα η επένδυση που έχει γίνει σε μία εταιρεία τόσο προσεκτικότερη πρέπει να είναι η μετάβαση, ενώ η επιλογή ακριβότερων και εξειδικευμένων λύσεων μπορεί να είναι επιβεβλημένη. Αυτό αφορά κυρίως τα μοντέλα του PaaS και IaaS, των οποίων η χρήση είναι πιο κρίσιμη και σαφώς η εμπλοκή του πελάτη περισσότερη.

Από την άλλη φαίνεται ότι οι ιδιώτες, οι μικρές, μεσαίες και νεοσύστατες επιχειρήσεις μπορούν πολύ πιο εύκολα να εκμεταλλευτούν τις υπηρεσίες του νέφους και πραγματικά οι ευκαιρίες που τους παρέχονται είναι πρωτόγνωρες και ουσιαστικά ανεξάντλητες.

Βιβλιογραφία

[001] Dr M.A.T.AlSudiari, Dr. TGK Vasista. «Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications».Advanced Computing: An International Journal (ACIJ), Vol.3, No.2,σελ 159-169,March 2012.

[002] Amazon Web Services. «Overview of Security Processes». URL:http://aws.amazon.com/security/,May 2011.

[003] Amazon Web Services. «Amazon Elastic Compute Cloud (Amazon EC2)». URL:http://aws.amazon.com/ec2/(accessed 26-3-13).

[004] American Institute of Certified Public Accountants (AICPA). «SAS 70 Overview».URL: http://sas70.com/sas70_overview.html(accessed 15-1-13).

[005] American Institute of Certified Public Accountants (AICPA). «SSAE 16 Overview».http://ssae16.com/SSAE16_overview.html(accessed 15-1-13).

[006] M.Armbrust, A. Fox, R. Griffith,A. D. Joseph, R. Katz, A.Konwinski, G.Lee, D. Patterson, A. Rabkin, I..Stoica, M.Zaharia. «A View of Cloud Computing». Communications of the ACM,Vol. 53, No. 4, σελ.50-58,April 2010.

[007] M.Armbrust,A. Fox, R. Griffith, A. D. Joseph, R. Katz,A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M.Zaharia. «Above the Clouds: A Berkeley View of Cloud Computing ».UC Berkeley Reliable Adaptive Distributed Systems Laboratory February 10, 2009.

[008] P.Arora, A. Singh, H.Tyagi. «Evaluation and Comparison of Security Issues on Cloud Computing Environment ».World of Computer Science and Information Technology Journal (WCSIT),Vol. 2, No. 5, σελ.179-183, 2012.

[009] V.Arraj. «ITIL®: The Basics». URL:http://www.best-management-practice.com /gempdf/ITIL_The_Basics.pdf White Paper, May 2010(accessed 15-1-13).

[010] A.Benlian,T. Hess. «Opportunities and risks of software-as-a-service: Findings from a survey of IT executives ».(ELSEVIER) Decision Support Systems(52) σελ.232-246, 2011.

[011] J.Brodkin. «Gartner: Seven cloud-computing security risks». Network World, URL:http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853,July 02, 2008.

[012] R.Buyya, J.Broberg, A.Goscinski(Editors). «Cloud Computing: Principles and Paradigms». Published by John Wiley & Sons, Inc., Hoboken, New Jersey, 2011.

[013] Capital.gr. «Παρουσίαση Μελέτης του ΙΟΒΕ σε Εκδήλωση της Microsoft». Capital.gr, 23/2/2012,13:47, URL http://www.capital.gr/news.asp?id=1420194 (accessed 27-3-13).

[014] CERT. «CERT Spotlight: Mitigating Threats from Within». URL: http://www.cert.org/ (accessed 12-3-13).

[015] K.Chadha,A. Bajpai. «Security Aspects of Cloud Computing». International Journal of Computer Applications (0975 – 8887),Vol.40,No.8,σελ.43-47,February 2012.

[016] F.Chang,P. S. Fales, M. Steiner, R. Viswanathan, T. J. Williams, T. L. Wood. «Mitigating High Latency Outliers for Cloud-Based Telecommunication Services». Bell Labs Technical Journal 17(2),Alcatel-Lucent, σελ.121–142, 2012.

[017] R.ChowP. Golle, M.Jakobsson, E. Shi, J. Staddon,R.Masuoka, J.Molina. «Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control». CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security, New York, NY, USA, σελ.85-90, 2009.

[018] M.Christodorescu, R. Sailer, D. Lee Schales, D.Sgandurra, D. Zamboni. «Cloud Security Is Not (Just) Virtualization Security». CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security, New York, NY, USA, σελ.97-102, 2009.

[019] Cloud Computing Use Case Discussion Group. «Cloud Computing Use Cases White Paper». Ver 4.0, July 2, 2010.

[020] Context Information Security. «Assessing Cloud Node Security». URL:http://www.contextis.com/files/Context-Assessing_Cloud_Node_Security-Whitepaper.pdf, March 2011.

[021] CSA(Cloud Security Alliance). «Security Guidance For Critical Areas of Focus in Cloud Computing V3.0». URL:http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[022] CSA(Cloud Security Alliance). «Cloud Controls Matrix». Ver 1.4, URL:https://cloudsecurityalliance.org/research/ccm/, March 8, 2013.

[023] CSA(Cloud Security Alliance) .«Consensus Assessments Initiative Questionnaire». Ver 1.1 https://cloudsecurityalliance.org/research/cai/, September 1, 2011.

[024] R.Curtmola, S.Kamara, J.Garay, R.Ostrovsky. «Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions». CCS '06 Proceedings of the 13th ACM conference on Computer and communications security, ACM New York, NY, USA, σελ.79-88, 2006.

[025] F.Doelitzscher,A.Sulistio, C. Reich, H. Kuijs, D. Wolf. «Private cloud for collaboration and e-Learning services: from IaaS to SaaS».Springer-Verlag 2010 Computing (2011),91, σελ.23–42, July 2010.

[026] ENISA(Europian Network and Information Security Agency)Dr. M.A.C. Dekker. «Critical Cloud Computing: A CIIP perspective on cloud computing services». Version 1,0,December 2012.

[027] ENISA(Europian Network and Information Security Agency)D. Catteddu, G.Hogben(editors). «Cloud Computing: Information Assurance Framework». URL:http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework, November 2009.

[028] ENISA(Europian Network and Information Security Agency), Δελτίο τύπου. «Ασφαλείς προμήθειες: Ο νέος οδηγός της ENISA για την παρακολούθηση των συμβάσεων Υπολογιστικού Νέφους (Cloud Computing)». URL:http://www.enisa.europa.eu/media/press-releases/asphaleis-prometheies/view, April 2, 2012.

[029] ENISA(Europian Network and Information Security Agency),Dr G. Hogben, Dr M.Dekker (editors). «Procure Secure:A guide to monitoring of security service levels in cloud

contracts». URL:http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts, 2012.

[030] ENISA(Europian Network and Information Security Agency),D. Catteddu(editor). «Security & Resilience in Governmental Clouds: Making an informed decision». URL: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds, January 2011.

[031] ENISA(Europian Network and Information Security Agency),D. Catteddu, G.Hogben(editors). «Cloud Computing: Benefits, Risks and Recommendations for Information Security». URL:http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment, November 2009.

[032] Ch.I.Fan,Shi-Yuan Huang. «Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage». (ELSEVIER)Future Generation Computer Systems,2012.05.005, 2012.

[033] Federal Financial Institutions Examination Council Information Technology Subcommittee. «Outsourced Cloud Computing». URL:http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf, July 10, 2012.

[034] Federal Financial Institutions Examination Council. «Outsourcing Technology Services». URL:http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf, June 2004.

[035] Google. «Πολιτική Απορρήτου». http://www.google.com/intl/el/policies/privacy/, Τελευταία τροποποίηση: 27 Ιουλίου 2012,(accessed 12-3-13).

[036] Google Developers. «Why App Engine». URL:https://developers.google.com/appengine/whyappengine, (accessed 25-3-13).

[037] International Organization for Standardization(ISO). «ISO/IEC 27000». URL: http://www.iso.org/iso/home/store/catalogue_tc.htm, (accessed 15-1-13).

[038] IT Governance Institute. «Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 Extract». URL :http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Val-IT-Framework-2.0-Extract-Jul-2008.pdf, (accessed 15-1-13).

[039] D.Jamil,H.Zaki. «Cloud Computing Security». International Journal of Engineering Science and Technology (IJEST),Vol. 3, No. 4, σελ 3478-2483, April 2011.

[040] W.Jie,J.Arshad, R.Sinnott, P. Townend, Z. Lei. «A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control». ACM Computing Surveys, Vol. 43, No. 2, Article 12, σελ.1–26, January 2011.

[041] S.K.Sood. «A combined approach to ensure data security in cloud computing». (ELSEVIER),Journal of Network and Computer Applications,35, σελ.1831-1838, 2012.

[042] K.D.Kadam,S. K. Gajre, R. L. Paikrao. «Security issues in Cloud Computing». National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012), Proceedings published by International Journal of Computer Applications® (IJCA),σελ.22-26, 2012.

[043] E.Keller,J. Szefer, J. Rexford, R. B. Lee. «NoHype: Virtualized Cloud Infrastructure without the Virtualization». Conference: ISCA '10 The 37th Annual International Symposium on Computer Architecture, Saint-Malo, France, June, 19 - 23,2010.

[044] F.J.Krautheim, D.S. Phatak, A. T. Sherman. «Introducing the Trusted Virtual Environment Module:A New Mechanism for Rooting Trust in Cloud Computing». Springer-Verlag Berlin Heidelberg 2010,TRUST 2010, LNCS 6101, σελ 211-227, 2010.

[045] V.Krishna Reddy,Dr. L.S.S.Reddy. «Security Architecture of Cloud Computing». International Journal of Engineering Science and Technology (IJEST),Vol. 3, No. 9, σελ.7149-7155, September 2011.

[046] R.Krutz, R.Dean Vines. «Cloud Security: A Comprehensive Guide to Secure Cloud Computing». Wiley Publishing, Inc, Indianapolis,2010.

[047] J.F.Kurose,K.W.Ross. «Computer Networking, a Top-Down Approach». Fifth Edition, Pearson Addison-Wesley, Boston 2010,

[048] G.Loveland. «Security Among the Clouds: Is Cloud Computing Safe Enough For Your Sensitive Data?(Knowledge Leadership)». Compliance Week, URL: http://www.highbeam.com/doc/1G1-243799959.html, December 1, 2010.

[049] A.Mathew. «Security and Privacy Issues of Cloud Computing; Solutions and Secure Framework». International Journal of Multidisciplinary Research,2(4), σελ.182-193, April 2012.

[050] [050]Microsoft. «HealthVault». URL: https://www.healthvault.com/gr/en/overview, (accessed 24-3-13).

[051] Y.G.Min,H.J.Shiv, Y.H.Bang. «Cloud Computing Security Issues and Access Control Solutions». Journal of Security Engineering,Vol.9, No.2, σελ 135-142, April 2012.

[052] D.Molnar,S.Schechter. «Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud». URL http://weis2010.econinfosec.org/papers/session5/weis2010_schechter.pdf, 2010.

[053] NetWeek Editor, Cloud computing conference: «Το σωστό SLA για το Cloud». URL:http://www.netweek.gr/default.asp?pid=9&la=1&arID=22766, 16 Μαρτίου 2012, 13:10,(accessed 20-2-13).

[054] NIST(National Institute of Standards and Technology) E.Chew, M.Swanson, K.Stine, N.Bartol, A.Brown, W Robinson. Special Publication 800-55 Rev1. «Performance Measurement Guide for Information Security». URL:http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf, July 2008.

[055] NIST(National Institute of Standards and Technology)P. Mell, T. Grance. Special Publication 800-145. «The NIST Definition of Cloud Computing». URL:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, September 2011.

[056] NIST(National Institute of Standards and Technology)W.Jansen, T. Grance,Special Publication 800-144. «Guidelines on Security and Privacy in Public Cloud Computing».

URL: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf, December 2011.

[057] NIST(National Institute of Standards and Technology)K.Scarfone, M.Souppaya, P.Hoffman,Special Publication 800-125. «Guide to Security for Full Virtualization Technologies». URL:http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf, January 2011.

[058] NIST(National Institute of Standards and Technology)Special Publication 800-39. «Managing Information Security Risk :Organization, Mission, and Information System View». URL:http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, March 2011.

[059] NIST(National Institute of Standards and Technology)Special Publication 800-53 Rev3. «Recommended Security Controls for Federal Information Systems and Organizations». URL:http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, August 2009.

[060] NIST(National Institute of Standards and Technology)R. Kissel, M.Scholl, S. Skolochenko, X. Li,Special Publication 800-88. «Guidelines for Media Sanitization». URL:http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf, September, 2006.

[061] D.Nomusa. «Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing». Report Information from ProQuest,03:00, November 05, 2012.

[062] S.Northcutt, L.Zeltser, S.Winters, K.Kent, R.W.Ritshey. «Inside Network Perimeter Security». Second Edition, Sams Publishing, Indianapolis, 2005.

[063] M.Okuhara,T. Shiozaki,T. Suzuki. «Security Architectures for Cloud Computing». FUJITSU Sci.Tech J., Vol. 46, No. 4, σελ.397–402, October 2010.

[064] S.Qaisar. «Cloud Computing: Network/Security Threats and Countermeasures». Interdisciplinary Journal Of Contemporary Research In Business, Vol.3, No.9, σελ.1323-1329, January 2012.

[065] J.Ribeiro. «Netflix DVD website down on Monday». URL: http://www.pcadvisor.co.uk/news/photo-video/3418062/netflix-faced-problems-relating-dvd-website/, January 2, 2013.

[066] S.Ristov,M.Gusev, M. Kostoska. «Cloud Computing Security in Business Information Systems». International Journal of Network Security & Its Applications (IJNSA),Vol.4, No.2, σελ.75-93, March 2012.

[067] J.W.Rittinghouse, J.F.Ransome. «Cloud Computing Implementation, Management, and Security». CRC Press,Taylor & Francis Group,Boca Raton,2010.

[068] C.Rong,S. T. Nguyen, M.G.Jaat. «Beyond lightning: A survey on security challenges in cloud computing».(ELSEVIER) Computers and Electrical Engineering,σελ.1-8,2012.

[069] SANS Institute, InfoSec Reading Room. «Security Policy Roadmap - Process for Creating Security Policies». URL:http://www.sans.org/reading_room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies_494, 2001

[070] R.Shaikh,M. Sasikumar. «Security Issues in Cloud Computing: A survey». International Journal of Computer Applications (0975 – 8887), Vol.44, No.19,σελ.4-10, April 2012.

[071] M.Sharma, H.Bansal, A. K. Sharma. «Cloud Computing: Different Approach & Security Challenge». I nternational Journal of Soft Computing and Engineering (IJSCE)Vol.2, Issue1, σελ.421-424, March 2012.

[072] T.Shekha Kar,M. A. Parvez Mahmud ,S. H. Farjana ,K. W. Nafi, B. C. Karmokar. «A Newer Secure Communication, File Encryption and User Identification based Cloud Security Architecture». International Journal of Computer Applications (0975 – 8887),Vol. 52, No. 4, σελ.26-30, August 2012.

[073] S.Singh, T.Jangwal. «Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues». International Journal of Computer Science & Information Technology (IJCSIT), Vol.4, No.2, σελ.17-31, April 2012.

[074] S.Spector,Xen.org Community. «Why Xen?». URL: http://www.xen.org/files/Marketing/WhyXen.pdf, (accessed 20-2-13).

[075] D.SvantessonR.Clarke. «Privacy and Consumer Risks in Cloud Computing». (ELSEVIER) Computer Law & Security Review 26, σελ 391-397,2010.

[076] M.Tebaa,S. EL Hajji, A.EL Ghazi. «Homomorphic Encryption Applied to the Cloud Computing Security» Proceedings of the World Congress on Engineering 2012, Vol I, WCE 2012, London, U.K, July 4 - 6, 2012.

[077] S.Thirukumaran,M.Sanjay Ram, A.Vijayraj. «Security Perspective Of Cloud Computing With Survey Of Security Issues». Journal of Global Research in Computer Science, Vol.3, No.1, σελ.77-82, January 2012.

[078] H.Tianfield. «Security Issues in Cloud Computing».2012 IEEE International Conference on Systems, Man, and Cybernetics, October 14-17,COEX,Seoul,Korea, σελ 1082-1089, 2012.

[079] A.Tripathi,P. Yadav. «Enhancing Security of Cloud Computing using Elliptic Curve Cryptography». International Journal of Computer Applications (0975 – 8887), Vol.57, No.1, σελ.26-30, November 2012.

[080] Trusted Computing Group. «Cloud Computing and Security –A Natural Match». URL: http://www.trustedcomputinggroup.org/resources/cloud_computing_and_security__a_natural_match, April 2010.

[081] Ch.Tsaravas, M.Themistocleous. «Cloud Computing And EGovernment: A Literature Review».European, Mediterranean & Middle Eastern Conference on Information Systems 2011, Athens, Greece, σελ 154-164, May 30-31 2011.

[082] U.S. General Services Administration(GSA). «About FedRAMP». URL: http://www.gsa.gov/portal/category/102375, (accessed 2-3-13).

[083] L.M.Vaquero,L. Rodero-Merino, D. Morán. «Locking the sky: a survey on IaaS cloud security». Computing (2011) 91,Springer-Verlag 2010,σελ 93-118, November 24, 2010.

[084] J.Weihua,S.Shibing. «Research on the Security Issues of Cloud Computing».Intelligence Computation and Evolutionary Computation, AISC 180, springerlink.com, σελ 845-848, 2013.

[085] WIKIPEDIA. «Federal Information Security Management Act of 2002». URL:http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002, (accessed 20-2-13).

[086] Wikipedia. «COBIT». URL:http://en.wikipedia.org/wiki/COBIT, (accessed 15-1-13).

[087] V.J.R.Winkler, B.Meine (Technical Editor). «Securing the Cloud: Cloud Computer Security Techniques and Tactics». Syngress is an imprint of Elsevier, Waltham, 2011.

[088] D.C.Wyld. «The Cloudy Future of Government IT:Cloud Computing and the Public Sector Around the World».I nternational Journal of Web & Semantic Technology (IJWesT), Vol 1, No1, σελ 1-20, January 2010.

[089] Xen.org. «Xen Hypervisor:The open source standard for hardware virtualization». URL:http://www.xen.org/products/xenhyp.html, (accessed 20-2-13)

[090] K.Zhang, X.Zhou, Y. Chen, X.Wang, Y. Ruan. «Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds». CCS'11, October 17–21, 2011, Chicago, Illinois, USA, σελ 515-525, October 2011.

[091] D.Zissis, D.Lekkas. «Addressing Cloud Computing Security Issues». Future Generation Computer Systems 28, σελ 583-592, 2012.

[092] ΒΙΚΙΠΑΙΔΕΙΑ. «Ασφάλεια Δικτύων Υπολογιστών». URL: http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD, (accessed 16-1-13).

[093] [093]ΒΙΚΙΠΑΙΔΕΙΑ. «Ψηφιακή υπογραφή». URL: http://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA

%CE%AE_%CF%85%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE, (accessed 15-2-13).

[094] Σ.Γκρίτζαλης, Σ.Κάτσικας, Δ.Γκρίτζαλης. «Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν και Ηλεκτρονικής Διακυβέρνησης». Εκδόσεις Παπασωτηρίου, Αθήνα, 2003.

[095] Σ.Γκρίτζαλης,. «Ψηφιακές Υπογραφές: Διεθνής εμπειρία, τάσεις και προοπτικές». Σημειώσεις, Πανεπιστήμιο Αιγαίου,2008.

[096] Π.Γκρουμούτης. «Πόλεμος για τον Έλεγχο του Ίντερνετ». Εφημερίδα Πρώτο Θέμα, σελ 18, 23 Δεκεμβρίου 2012.

[097] Ευρωπαϊκή Επιτροπή ,Ενημερωτικό Σημείωμα. «Εκμετάλλευση των δυνατοτήτων του υπολογιστικού νέφους (Cloud Computing) στην Ευρώπη – τι είναι και τι σημαίνει αυτό για μένα;». Reference: MEMO/12/713, URL:http://europa.eu/rapid/press-release_MEMO-12-713_el.htm, Βρυξέλλες, 27 Σεπτεμβρίου 2012.

[098] Μ.Καρύδα, «Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων». Σημειώσεις για Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου Μάιος 2010.

[099] Σ.Κατσικάς, Δ.Γκρίτζαλης, Σ.Γκρίτζαλης(Επιστημονική Επιμέλεια). «Ασφάλεια Πληροφοριακών Συστημάτων». Εκδόσεις Νέων Τεχνολογιών, Αθήνα2004.

[100] Θ.Κούτσης. «Ποιος θα ελέγξει το Διαδίκτυο;». Μετάφραση άρθρου Le Monde Diplomatique URL:http://jimmy278.blogspot.gr/2013/03/le-monde-diplomatique.html, (accessed 12-3-13).

[101] Κ.Λαμπρινουδάκης, Ε.Μήτρου, Σ.Γκρίτζαλης, Σ.Κάτσικας (Επιστημονική Επιμέλεια). «Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα». Εκδόσεις Παπασωτηρίου, Αθήνα, 2010.

[102] ΝΟΜΟΣ 2472/1997. «Προστασία του Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα με Ενσωματωμένες τις Τροποποιήσεις». URL:http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROS

OPIKA%20DEDOMENA/%CE%9DOMOTHESIA%20PROSOPIKA%20DEDOMENA_GREEK/2472_97_NOV2011_FINALVERSION.PDF, (accessed 16-1-13).

[103] Προσχέδιο Κοινής Υπουργικής Απόφασης με ΘΕΜΑ . « Ελάχιστες Υποχρεώσεις για τη Διασφάλιση της Ακεραιότητας Δημόσιων Τηλεφωνικών Δικτύων και Διαθεσιμότητας Δημόσιων Τηλεφωνικών Υπηρεσιών σε Σταθερές Θέσεις». URL:http://www.opengov.gr/yme/wp-content/uploads/downloads/2011/08/kya_akeraiotita.pdf, (accessed 18-2-13).

[104] Η.Τσίχλης. «Ποιά είναι τα ευαίσθητα προσωπικά δεδομένα και ποιά τα κατοχυρωμένα Δικαιώματά μας ».URL: http://www.inews.gr/96/poia-einai-ta-evaisthita-prosopika-dedomena-kai-poia-ta-katochyromena-dikaiomata-mas.htm, (accessed 13-1-13).

[105] Υπηρεσία Ανάπτυξης Πληροφορικής, Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης. «Αρχή Πιστοποίησης του Ελληνικού Δημοσίου». URL: http://www.yap.gov.gr/ ,(accessed 15-2-13).

[106] Ν.Φραγκούλη. «Ψάχνουν έσοδα στα... Σύννεφα οι Ελληνικές Εταιρείες Τηλεπικοινωνιών». Κέρδος 19/8/2012 06:00, URL: http://www.kerdos.gr/default.aspx?id=1785048&nt=103, (accessed 27-3-13).

Παράρτημα Α

Αντιστοίχηση Ελληνικών - Αγγλικών Όρων

Α	
Αγαθό	Asset
Ανάκαμψη	Failover
Αναφορά	Report
ανάχωμα ασφάλειας	Firewall
Απλό Κείμενο	Plaintext
Απόκρυψη Δεδομένων	Data Masking
Απώλεια Διακυβέρνησης	Loss Of Governance
Αρχείο Καταγραφής Ελέγχου	Audit log
Αρχές Πιστοποίησης	CA - Certification Authorities
Αρχή των Ελάχιστων Προνομίων	Least Privilege Principal (LPP)
Αρχιτεκτονικές Προσανατολισμένες στις Υπηρεσίες	Service Oriented Architectures
Ασφάλεια Φυλλομετρητή	Browser Security
Ασφάλεια σε Βάθος	Defense in Depth
Ασφάλεια Ταυτότητας	Identity Security
Β	
Βάσει Ρόλου Έλεγχος Πρόσβασης	Role-Based Access Controls RBAC
Βασίζονται στο Δίκτυο	Web Based
Βιωσιμότητα σε Βάθος Χρόνου	Long-term Viability

Δ	
Δεδομένα	Data
Δεδομένα για τα Δεδομένα	metadata
Δημόσιο Νέφος	Public cloud
Διακομιστής (ή εξυπηρετητής)	Server
Διακοπή Υπηρεσίας	Disruption of Service
Διαμοίραση Φόρτου Εργασίας	Load Balancing
Διασύνδεση Εικονικών Ιδιωτικών Δικτύων	Virtual Private Networks Tunneling
Διεπαφές Προγραμματισμού Εφαρμογών	Application Programming Interfaces (APIs)
Διεπαφή	Interface
Διεπαφή Χρήστη	User Interface
Δρομολογητής	Router
Ε	
Εικονικοποίηση	Virtualization
Εικονικό Ιδιωτικό Δίκτυο	Virtual Private Network
Ελάχιστο Προνόμιο	Least Privilege
Έμπιστη Νεφοϋπολογιστική	Trusted Cloud Computing
Εξάρτηση σε συγκεκριμένο πάροχο	Lock In
Εξουσιοδότηση	Authorization
Εξυπηρετητής (ή διακομιστής)	Server
Έξυπνο Κινητό	Smartphone
Εξωτερική Ανάθεση Υπηρεσιών Νέφους	Public Cloud Outsourcing
Επίθεση Άρνησης Παροχής Υπηρεσιών	Denial Of Service(D.O.S.) Attack
Επίθεση Ενδιάμεσου	Man in the Middle Attack
Επίθεση Παρακολούθησης Δικτύου	Network Sniffing Attack
Επίθεση Πλημμυρίδας	Flooding Attack
Επίθεση Στέρησης Πόρων	Resource Starvation Attack
Επίθεση Χρονισμού	Timing Attack
Επίθεση SQL	SQL Injection Attack
Επικινδυνότητα	Risk
Επίπτωση	Impact
Ερωτηματολόγιο της Πρωτοβουλίας Κοινών Εκτιμήσεων	Consensus Assessments Initiative Questionnaire
Ευρεία Πρόσβαση στο Δίκτυο	Broad Network Access
Εφαρμογή Ιστού	Web Application
Ι	
Ιδιοκτήτης (ή κάτοχος)	Owner
Ιδιωτικό Νέφος	Private Cloud
Ιδιωτικότητα του Ατόμου	Privacy of the Person
Ιός	Virus
Κ	
Κακόβουλο λογισμικό	Malware
Κατ' απαίτηση αυτοεξυπηρέτηση	On-demand Self-Service

Καταγραφή Ασφάλειας	Security Log
Κατανεμημένοι Εξυπηρετητές	Distributed Servers
Κάτοχος (ή Ιδιοκτήτης)	Owner
Κέντρο Δεδομένων	Datacenter
Κοινή Διάθεση Πόρων	Resource Pooling
Κόμβος του Νέφους	Cloud Host
Κρυπτογράφηση	Encryption
Κρυπτογράφηση Αναζήτησης	Searchable Encryption
Κρυπτογράφηση Κατηγορήματος	Predicate Encryption
Κρυπτογραφία	Cryptography
Κρυπτογραφική συνάρτηση Κατατεμαχισμού	Hash Function
Κωδικοποιημένο Κείμενο	Cyphertext
Κωδικός μιας Φοράς	One-Time Password (OTP)
Λ	
Λίστα Ελέγχου Προσπέλασης Δικτύου	Network Access Control List
Λογισμικό ως Υπηρεσία	Software as a Service (SaaS)
Λογισμικό	Software
Μ	
Μεταγωγέας	Switch
Μη Αποποίηση	Non-repudiation
Μηχανική Κρυπτογράφηση	Hardware Encryption
Μετρήσιμες Υπηρεσίες	Measured Services
Μισθωτής	Tenant
Ν	
Νέφος Κοινότητας	Community Cloud
Νεφοϋπολογιστική (ή Υπολογιστική Νέφους)	Cloud Computing
Ο	
Ομομορφική Κρυπτογράφηση	Homomorphic Encryption
Ομοσπονδιακή Πράξη Διαχείρισης Ασφάλειας Πληροφοριών	Federal Information Security Management Act (FISMA)
Ομοσπονδιακή Ταυτότητας	Federated Identity
Π	
Πακέτα Δεδομένων	Data Packets
Παρακολούθηση	Monitoring
Παραμετροποίηση	Configuration
Παροχή Υπηρεσιών Πραγματικού Χρόνου	Real Time Services Delivery
Πάροχος Υπηρεσιών Νέφους	Cloud Service Provider
Πελάτης	Client
Πίνακας Κλήσεων του Συστήματος	System-Call Table
Πίνακας Ελέγχων του Νέφους	Cloud Controls Matrix (CCM)
Πιστοποίηση ταυτότητας	Authentication
Πιστοποιητικό	Certificate
Πλατφόρμα ως Υπηρεσία	Platform as a Service (PaaS)

Πληροφορία	Information
Πληροφοριακή Ιδιωτικότητα	Informational Privacy
Πολλαπλών Μισθωτών	Multi-tenant
Πρόσβαση εκ των Έσω	Insider Access
Πρόσβαση κατ' Εξαίρεση	Privileged User Access
Πρότυπο	Standard
Πύλη Δικτύου	Gateway
Σ	
Σάρωση Θυρών	Port scanning
Συμμόρφωση στους Κανονισμούς	Regulatory Compliance
Συμφωνητικό Παροχής Υπηρεσιών	Service Level Agreement(SLA)
Σύνοψη	Digest
Συσκευή Αυξημένων Επεξεργαστικών Δυνατοτήτων	Thick Client
Συσκευή με Προστασία Παραβίασης	Tamperproof Device
Συσκευή Μειωμένων Επεξεργαστικών Δυνατοτήτων	Thin Client
Σύστημα Ανίχνευσης Εξερχόμενων Επιθέσεων	Extrusion Detection System
Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών	Information Security Management System(ISMS)
Σύστημα Ανίχνευσης/Αντιμετώπισης Εισβολών	Intrusion Detection/Prevention Systems(IDS/IPS)
Σχέδιο Επιχειρησιακής Συνέχειας	Business Continuity Plan
Τ	
Ταχεία Ελαστικότητα	Rapid Elasticity
Τεχνολογία Ενιαίου Σημείου Πρόσβασης	Single Sign-On
Τοπικό Δίκτυο Περιοχής	Local Area Network(LAN)
Τοποθεσία των Δεδομένων	Data Location
Υ	
Υβριδικό Νέφος	Hybrid Cloud
Υλικό	Hardware
Υποδομή Αποθήκευσης Δεδομένων	Storage
Υποδομή Αποκλειστικής Χρήσης	Single Tenant Hardware
Υποδομή Δημόσιου Κλειδιού	Public Key Infrastructure(PKI)
Υπολογιστική Νέφους	Cloud Computing
Υποστήριξη Έρευνας	Investigative Support
Φ	
Φυλλομετρητής Ιστοσελίδων	Web Browser
Χ	
Χρήστης	User
Χωρική Ιδιωτικότητα	Territorial Privacy
Ψ	
Ψηφιακή Υπογραφή	Digital Signature

Παράρτημα Β
Αντιστοίχηση Αγγλικών-Ελληνικών Όρων

A	
Application Programming Interfaces (APIs)	Διεπαφές Προγραμματισμού Εφαρμογών
Asset	Αγαθό
Audit log	Αρχείο Καταγραφής Ελέγχου
Authentication	Πιστοποίηση ταυτότητας
Authorization	Εξουσιοδότηση
B	
Broad Network Access	Ευρεία Πρόσβαση στο Δίκτυο
Browser Security	Ασφάλεια Φυλλομετρητή
Business Continuity Plan	Σχέδιο Επιχειρησιακής Συνέχειας
C	
CA - Certification Authorities	Αρχές Πιστοποίησης
Certificate	Πιστοποιητικό
Client	Πελάτης
Cloud Computing	Νεφοϋπολογιστική ή Υπολογιστική Νέφους
Cloud Controls Matrix (CCM)	Πίνακας Ελέγχων του Νέφους
Cloud Host	Κόμβος του Νέφους
Cloud Service Provider	Πάροχος Υπηρεσιών Νέφους
Community Cloud	Νέφος Κοινότητας
Configuration	Παραμετροποίηση

Consensus Assessments Initiative Questionnaire	Ερωτηματολόγιο της Πρωτοβουλίας Κοινών Εκτιμήσεων
Cryptography	Κρυπτογραφία
Cyphertext	Κωδικοποιημένο Κείμενο
D	
Data	Δεδομένα
Data Location	Τοποθεσία των Δεδομένων
Data Masking	Απόκρυψη Δεδομένων
Data Packets	Πακέτα δεδομένων
Datacenter	Κέντρο Δεδομένων
Defense in Depth	Ασφάλεια σε Βάθος
Denial Of Service(D.O.S.) Attack	Επίθεση Άρνησης Παροχής Υπηρεσιών
Digest	Σύνοψη
Digital Signature	Ψηφιακή Υπογραφή
Disruption of Service	Διακοπή Υπηρεσίας
Distributed Servers	Κατανεμημένοι Εξυπηρετητές
E	
Encryption	Κρυπτογράφηση
Extrusion Detection System	Σύστημα Ανίχνευσης Εξερχόμενων Επιθέσεων
F	
Failover	Ανάκαμψη
Federal Information Security Management Act (FISMA)	Ομοσπονδιακή Πράξη Διαχείρισης Ασφάλειας Πληροφοριών
Federated Identity	Ομοσπονδιακή Ταυτότητας
Firewall	ανάχωμα ασφάλειας
Flooding Attack	Επίθεση Πλημμυρίδας
G	
Gateway	Πύλη Δικτύου
H	
Hardware	Υλικό
Hardware Encryption	Μηχανική Κρυπτογράφηση
Hash Function	Κρυπτογραφική Συνάρτηση Κατατεμαχισμού
Homomorphic Encryption	Ομομορφική Κρυπτογράφηση
Hybrid Cloud	Υβριδικό Νέφος
I	
Identity Security	Ασφάλεια Ταυτότητας
Impact	Επίπτωση
Information	Πληροφορία
Information Security Management System(ISMS)	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
Informational Privacy	Πληροφοριακή Ιδιωτικότητα
Insider Access	Πρόσβαση εκ των Έσω
Interface	Διεπαφή
Intrusion Detection/Prevention Systems(IDS/IPS)	Σύστημα Ανίχνευσης/Αντιμετώπισης Εισβολών

Investigative Support	Υποστήριξη Έρευνας
L	
Least Privilege	Ελάχιστο Προνόμιο
Least Privilege Principal (LPP)	Αρχή των Ελάχιστων Προνομίων
Load Balancing	Διαμοίραση Φόρτου Εργασίας
Local Area Network(LAN)	Τοπικό Δίκτυο Περιοχής
Lock In	Εξάρτηση σε συγκεκριμένο πάροχο
Long-term Viability	Βιωσιμότητα σε Βάθος Χρόνου
Loss Of Governance	Απώλεια Διακυβέρνησης
M	
Malware	Κακόβουλο λογισμικό
Man in the Middle Attack	Επίθεση Ενδιάμεσου
Measured Services	Μετρήσιμες Υπηρεσίες
Metadata	Δεδομένα για τα Δεδομένα
Monitoring	Παρακολούθηση
Multi-tenant	Πολλαπλών Μισθωτών
N	
Network Access Control List	Λίστα Ελέγχου Προσπέλασης Δικτύου
Network Sniffing Attack	Επίθεση Παρακολούθησης Δικτύου
Non-repudiation	Μη Αποποίηση
O	
On-demand Self-Service	Κατ' απαίτηση αυτοεξυπηρέτηση
One-Time Password (OTP)	Κωδικός μιας Φοράς
Owner	Ιδιοκτήτης ή Κάτοχος
P	
Plaintext	Απλό Κείμενο
Platform as a Service (PaaS)	Πλατφόρμα ως Υπηρεσία
Port scanning	Σάρωση Θυρών
Predicate Encryption	Κρυπτογράφηση Κατηγορήματος
Privacy of the Person	Ιδιωτικότητα του Ατόμου
Private Cloud	Ιδιωτικό Νέφος
Privileged User Access	Πρόσβαση κατ' Εξαίρεση
Public Cloud Outsourcing	Εξωτερική Ανάθεση Υπηρεσιών Νέφους
Public cloud	Δημόσιο Νέφος
Public Key Infrastructure(PKI)	Υποδομή Δημόσιου Κλειδιού
R	
Rapid Elasticity	Ταχεία Ελαστικότητα
Real Time Services Delivery	Παροχή Υπηρεσιών Πραγματικού Χρόνου
Regulatory Compliance	Συμμόρφωση στους Κανονισμούς
Report	Αναφορά
Resource Pooling	Κοινή Διάθεση Πόρων
Resource Starvation Attack	Επίθεση Στέρησης Πόρων
Risk	Επικινδυνότητα
Role-Based Access Controls RBAC	Βάσει Ρόλου Έλεγχος Πρόσβασης
Router	Δρομολογητής
S	

Searchable Encryption	Κρυπτογράφηση Αναζήτησης
Security Log	Καταγραφή Ασφάλειας
Server	Διακομιστής ή Εξυπηρετητής
Service Level Agreement(SLA)	Συμφωνητικό Παροχής Υπηρεσιών
Service Oriented Architectures	Αρχιτεκτονικές Προσανατολισμένες στις Υπηρεσίες
Single Sign-On	Τεχνολογία Ενιαίου Σημείου Πρόσβασης
Single Tenant Hardware	Υποδομή Αποκλειστικής Χρήσης
Smartphone	Έξυπνο Κινητό
Software	Λογισμικό
Software as a Service (SaaS)	Λογισμικό ως Υπηρεσία
SQL Injection Attack	Επίθεση SQL
Standard	Πρότυπο
Storage	Υποδομή Αποθήκευσης Δεδομένων
Switch	Μεταγωγέας
System-Call Table	Πίνακας Κλήσεων του Συστήματος
T	
Tamperproof Device	Συσκευή με Προστασία Παραβίασης
Tenant	Μισθωτής
Territorial Privacy	Χωρική Ιδιωτικότητα
Thick Client	Συσκευή Αυξημένων Επεξεργαστικών Δυνατοτήτων
Thin Client	Συσκευή Μειωμένων Επεξεργαστικών Δυνατοτήτων
Timing Attack	Επίθεση Χρονισμού
Trusted Cloud Computing	Έμπιστη Νεφοϋπολογιστική
U	
User	Χρήστης
User Interface	Διεπαφή Χρήστη
V	
Virtual Private Network	Εικονικό Ιδιωτικό Δίκτυο
Virtual Private Networks Tunneling	Διασύνδεση Εικονικών Ιδιωτικών Δικτύων
Virtualization	Εικονικοποίηση
Virus	Ιός
W	
Web Application	Εφαρμογή Ιστού
Web Based	Βασίζονται στο Δίκτυο
Web Browser	Φυλλομετρητής Ιστοσελίδων