

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



– ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ –

ΔΙΑΜΟΡΦΩΣΗ ΣΤΡΑΤΗΓΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ
ΚΑΙ Ο ΡΟΛΟΣ ΤΗΣ ΕΝΗΜΕΡΟΤΗΤΑΣ ΣΕ ΑΥΤΟ

ΑΙΜΙΛΙΑ ΖΜΠΗΤΑ

ΕΠΙΒΛΕΠΟΥΣΑ: –ΑΓΓΕΛΙΚΗ ΤΣΩΧΟΥ–

27 Ιανουαρίου 2022

Επιβλέπουσα

Αγγελική Τσώχου, Επίκουρη Καθηγήτρια ,
Ιόνιο Πανεπιστήμιο

Διμελής Επιτροπή

Στεφανιδάκης Μιχαήλ, Επίκουρος Καθηγητής,
Ιόνιο Πανεπιστήμιο

Κουρουθανάσης Παναγιώτης, Αναπληρωτής Καθηγητής,
Ιόνιο Πανεπιστήμιο

Αυτή η προσπάθεια αφιερώνεται στη μνήμη της μητέρας μου και στα παιδιά μου

Περίληψη

Το θέμα με το οποίο ασχολείται η συγκεκριμένη πτυχιακή εργασία είναι το Cloud Computing και ειδικότερα ο νευραλγικός τομέας της ασφάλειας. Το θέμα της εργασίας είναι η ανάπτυξη των στρατηγικών ασφάλειας όσον αφορά στο Cloud Computing αλλά θα γίνει και αναφορά στον ρόλο που διαδραματίζει η ενημερότητα σε αυτό. Αρχικά, με την βιβλιογραφική επισκόπηση γίνεται σύντομη αναφορά στην δομή και αρχιτεκτονική του Cloud Computing, στην συνέχεια ακολουθεί ανάλυση της ασφάλειας, των ευπαθειών και των απειλών αναφέρεται ποιες είναι και σε ποιο στάδιο βρίσκονται. Ιδιαίτερα ενδιαφέρον είναι να εξετάσουμε τις εξελίξεις και τις δυνατότητες που υπάρχουν για την θωράκιση της χρήσης του Cloud Computing αλλά και να εξετασθεί ποιες στρατηγικές ασφάλειας μπορούν να εφαρμοσθούν και τελικά τι επίπεδο ασφαλείας μπορούμε να επιδιώξουμε ώστε να διασφαλισθεί η ιδιωτικότητα των χρηστών αλλά και ποιος είναι ο ρόλος της ενημερότητας σε αυτό. Ακολουθεί το ερευνητικό κομμάτι μέσα από το οποίο γίνεται προσπάθεια μέσω των ερωτημάτων που τίθενται, να διαπιστωθεί πόσο σημαντική και ωφέλιμη είναι η υιοθέτηση του Υπολογιστικού Νέφους, και να μελετηθεί ο ρόλος της ενημερότητας. Το ερωτηματολόγιο στοχεύει όχι στον απλό χρήστη αλλά στον επιχειρηματικό χώρο, αφού εκεί η ασφάλεια αποτελεί κρίσιμο παράγοντα. Επιδιώκεται μέσα από την έρευνα να διαπιστωθεί ο βαθμός ενημερότητας των χρηστών για τους κινδύνους υιοθέτησης του Υπολογιστικού Νέφους, για τα κριτήρια επιλογής παρόχου, για τα στοιχεία που πρέπει να διέπουν τις συμφωνίες παροχής υπηρεσιών (Service Level Agreement) μεταξύ του χρήστη και του παρόχου και βέβαια τι ενέργειες μπορεί να κάνει ο ίδιος για να ενισχύσει την ασφάλεια.

Λέξεις κλειδιά: Cloud Computing, Security, Cloud Computing, Cloud Security, Cloud Threats, Cloud Vulnerabilities

Περιεχόμενα

1	Εισαγωγή στο Cloud Computing	1
1.1	Ιστορική αναδρομή στο Cloud Computing	1
1.2	Ορισμός του Cloud Computing	2
1.3	Χαρακτηριστικά του Cloud Computing	4
1.4	Αρχιτεκτονική του Υπολογιστικού Νέφους	5
1.5	Υπηρεσίες παρεχόμενες από το Υπολογιστικό Νέφος	7
1.5.1	Software as a Service (SaaS)	8
1.5.2	Platform as a Service (PaaS)	9
1.5.3	Infrastructure as a Service (IaaS)	10
1.5.4	Επιπρόσθετες Υπηρεσίες (Anything as a Service (XaaS)	11
1.6	Μοντέλα ανάπτυξης του Υπολογιστικού Νέφους	12
1.6.1	Δημόσιο Νέφος (Public Cloud)	13
1.6.2	Ιδιωτικό Νέφος (Private Cloud)	13
1.6.3	Υβριδικό Νέφος (Hybrid Cloud)	14
2	Ασφάλεια και Υπολογιστικό Νέφος	15
2.1	Ζητήματα Ασφάλειας στο Υπολογιστικό Νέφος	16
2.2	Ζητήματα ασφάλειας του μοντέλου <i>SaaS</i>	18
2.3	Ζητήματα ασφάλειας του μοντέλου <i>PaaS</i>	19
2.4	Ζητήματα ασφάλειας του μοντέλου <i>IaaS</i>	20
2.5	Ασφάλεια Δεδομένων	21
2.6	Ασφάλεια Δικτύου	23
2.7	Διαχείριση Ταυτότητας (Identity Management)	24
2.8	Web Application Security	25
2.9	Ευπάθειες του Υπολογιστικού Νέφους	25

2.10	Απειλές στο Υπολογιστικό Νέφος	27
3	Στρατηγικές Ασφάλειας Υπολογιστικού Νέφους	34
3.1	Στρατηγικές Ασφάλειας των Δεδομένων	34
3.2	Κεντριοποίηση	35
3.3	Προτυποποίηση	36
3.4	Αυτοματοποίηση	43
3.5	Στρατηγικές Προστασίας των Δεδομένων	45
4	Ενημερότητα ασφάλειας των χρηστών	46
5	Μεθοδολογία Έρευνας	48
5.1	Ερευνητικά Ερωτήματα	48
5.2	Ερευνητική προσέγγιση	49
5.3	Δείγμα Έρευνας	50
5.4	Μέσα συλλογής Δεδομένων	50
5.5	Σχεδίαση Ερωτηματολογίου	52
5.6	Εργαλεία Πληροφορικής για τη συλλογή και ανάλυση των δεδομένων της έρευνας	55
5.6.1	Google Forms	55
5.6.2	SPSS	56
6	Υλοποίηση Έρευνας	58
6.1	Πιλοτικές Δοκιμές	58
6.2	Πραγματοποίηση έρευνας	59
6.3	Δημογραφικά Στοιχεία	60
6.4	Έλεγχος Αξιοπιστίας	61
6.5	Αποτελέσματα Έρευνας	61
6.6	Συμπεράσματα	70
	Παράρτημα Α'	73
	Βιβλιογραφία	79
	Συντομεύσεις	88
	Γλωσσάρι Ξενικών Όρων	92

ΠΕΡΙΕΧΟΜΕΝΑ

iv

Ευρετήριο

96

Κατάλογος Σχημάτων

1.1	Η αρχιτεκτονική του Υπολογιστικού Νέφους	6
1.2	Μοντέλα Υπηρεσιών	7
1.3	Μοντέλα Ανάπτυξης	12
6.1	Μορφή εισαγωγικού σημειώματος ερωτηματολογίου έρευνας	59
6.2	Μεταβολές στο κόστος λειτουργίας και συντήρησης μετά την υιοθέτηση του Υπολογιστικού Νέφους	62
6.3	Διαλειτουργικότητα-Χρήση-Αξιοπιστία υπολογιστικών πόρων με την υιοθέτηση του Υπολογιστικού Νέφους	63
6.4	Διαθεσιμότητα-Φορητότητα Δεδομένων και Υπηρεσιών μετά την υιοθέτηση του Υπολογιστικού Νέφους	64
6.5	Απόδοση των παρεχόμενων υπηρεσιών με την υιοθέτηση του Υπολογιστικού Νέφους	65
6.6	Ασφάλεια χρήσης του Υπολογιστικού Νέφους	66
6.7	Ασφάλεια Δεδομένων μετά την υιοθέτηση του Υπολογιστικού Νέφους	67
6.8	Υποχρεώσεις παρόχου του Υπολογιστικού Νέφους	68
6.9	Δικαιώματα παρόχου του Υπολογιστικού Νέφους	69

Κατάλογος Πινάκων

1.1	Επικαιροποιημένο μοντέλο του cloud computing βασιζόμενο στο μοντέλο του Johan den Hann	3
5.1	Ερμηνεία απαντήσεων κλίμακας Likert	53

Κεφάλαιο 1

Εισαγωγή στο Cloud Computing



ΥΝΗΘΙΖΟΥΜΕ να λέμε πως αν δεν γνωρίζεις το παρελθόν κάποιου δεν μπορείς να προσδιορίσεις το μέλλον του. Έτσι λοιπόν για να κατανοήσουμε την εξέλιξη του Cloud Computing θα κάνουμε μια σύντομη ιστορική αναδρομή.

1.1 Ιστορική αναδρομή στο Cloud Computing

Η αρχική ιδέα ήταν η δημιουργία ενός συστήματος στο οποίο θα υπήρχε απομακρυσμένη πρόσβαση στην πληροφορία μέσω συνδέσεων υπολογιστή με υπολογιστή. Έτσι αναπτύχθηκε το *ARPANET* το 1969, το οποίο χρησιμοποιήθηκε για την επικοινωνία και τον διαμοιρασμό πόρων μεταξύ ερευνητών αρχικά, με την σύνδεση τεσσάρων πανεπιστημίων. Το επόμενο στάδιο ήταν στις αρχές της δεκαετίας του '80 με την εμφάνιση των υπερυπολογιστικών κέντρων που βασίζονταν στην δημιουργία ενός εθνικού κεντρικού δικτύου το οποίο έκανε χρήση του πρωτοκόλου *TCIP/IP*. Ενώ προς το τέλος της δεκαετίας εμφανίστηκε το *ISP* (Internet Service Provider). Φθάνουμε στο τέλος της δεκαετίας του '90 με κομβικό σημείο για την έναρξη της κυριαρχίας του **Cloud Computing** την εμφάνιση του *Salesforce.com*, δηλαδή του γνωστού *SaaS* (*Software-as-a-Service*). Την δεκαετία του 2000 εμφανίστηκε η πλατφόρμα *AWS* (*Amazon Web Services*) με την οποία παρέχονται υπηρεσίες *on-line* σε άλλους δικτυακούς τόπους ή πελάτες. Το 2006 έχουμε το *EC2* (*Elastic Compute Cloud*) μία κατ'ά βάση εμπορική υπηρεσία που παρέχεται μέσω του ιστού σε μικρές εταιρίες και χρήστες δίνοντας τους την δυνατότητα να νοικιάσουν *H/Y* ώστε να τρέξουν τις δικές τους εφαρμογές. Πολύ σύντομα το 2008 παρουσιάζεται το *Google App Engine* όπου οι προγραμματιστές

έχουν την δυνατότητα να έχουν εφαρμογές σε διαχειριζόμενα κέντρα δεδομένων, το γνωστό *PaaS (Platform-as-a-Service)*. Το 2010 έχουμε την εμφάνιση της πλατφόρμας *Azure* η οποία στήριξε την ανάπτυξη των εφαρμογών του ιστού αλλά και των κινητών, μέσω βέβαια του ιστού. Παράλληλα έχουμε την εμφάνιση της πλατφόρμας ανοικτού κώδικα *Rackspace OpenStack*. Ακολουθεί το *SmartCloud* από την *IBM* με μια σειρά από *Cloud Computing* τεχνολογίες για την δημιουργία των *public, private* και *hybrid clouds*. Όσπου το 2013 έχουμε την *Google Cloud Platform* το οποίο αποτελεί την πλατφόρμα *IaaS (Internet-as-a-Service)*. [1]

1.2 Ορισμός του Cloud Computing

Όσον αφορά στον ορισμό του Υπολογιστικού Νέφους ο επικρατέστερος δίνεται από το **NIST** (*National Institute of Standards and Technology*), σύμφωνα με το οποίο το Υπολογιστικό Νέφος (*Cloud computing*) παρέχει σε οποιαδήποτε χρονική στιγμή, με ευκολία και κατ' απαίτηση πρόσβαση σε ένα σύνολο διαμοιραζόμενων ρυθμιζόμενων υπολογιστικών πόρων (π.χ. δίκτυα, εξυπηρετητές, αποθήκευση, εφαρμογές και υπηρεσίες) τα οποία είναι διαθέσιμα και αποδεσμεύονται γρήγορα, με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης του παρόχου δηλαδή με υψηλό επίπεδο αυτοματοποίησης. [2]

Ο παραπάνω ορισμός δόθηκε πριν επτά χρόνια, και με τους ξέφρενους ρυθμούς εξέλιξης της τεχνολογίας, λογικό είναι να τίθεται θέμα επαναπροσδιορισμού του *Cloud Computing*. Προτείνεται ένα πιο λεπτομερές και επικαιροποιημένο πλαίσιο για τον ορισμό του *Cloud Computing* από τον *Johan Den Haan*, το οποίο βασίζεται στον ορισμό του **NIST** και στο οποίο περιλαμβάνονται όλες οι τεχνολογίες που προσφέρονται σήμερα. [3, 4]

Σε αυτό το μοντέλο περιγράφεται πως από το φυσικό επίπεδο περνάμε στο επίπεδο των εφαρμογών. Φαίνεται στον πίνακα 1.1 πως το φυσικό επίπεδο περιλαμβάνει τον υλικό εξοπλισμό όπως Switches, Routers. Στη συνέχεια έχουμε στο επόμενο επίπεδο την χρήση των Ειχονικών Μηχανών, με τις οποίες επιτυγχάνεται ο διαμοιρασμός των υπολογιστικών πόρων μεταξύ πολλαπλών χρηστών. Γίνεται χρήση τεχνολογιών όπως Software Defined Networking (SDN)(π.χ. OpenStack Neutron) και Software Defined Storage(SDS)(π.χ. OpenStack Cinder) οπότε τα δίκτυα δημιουργούνται μέσω προγραμματισμού, εικονικά, όπως και η αποθήκευση. Στη συνέχεια έχουμε το Foundational PaaS το οποίο είναι το επίπεδο των εφαρμογών που εστιάζει στην ανάπτυξη εφαρμογών και βάσεων δεδομένων αλλά και στην επικοινωνία μεταξύ των εφαρμογών (π.χ. Amazon S3). Το επόμενο επίπεδο είναι το PaaS με το οποίο περνάμε στον προγραμματισμό (π.χ. Google App Engine, Windows Azure SQL Database). Ακολουθεί

Πίνακας 1.1: Επικαιροποιημένο μοντέλο του cloud computing βασισμένο στο μοντέλο του Johan den Hann

6	SaaS	Applications			End Users
5	App Services	App Services	Communication and social Services	DaaS (Data as a Service)	Citizen Developers
4	Model-Driven PaaS	Model-Driven a PaaS	Model-Driven i PaaS	Data Analytics	Rapid Developers
3	PaaS	a PaaS	i PaaS	db PaaS	Developers Coders
2	Foundational PaaS	Application Containers	Routing Messaging Orchestration	Object Storage	Developers
1	Software Defined Datacenter	Virtual Machines	Software Defined Networking (SDN)	Software Defined Storage (SDS)	Infrastructure Engineers
0	Hardware	Servers	Switches Routers	Storage	
		Compute	Communicate	Store	

το επίπεδο Model-Driven PaaS το οποίο είναι πιο εξελιγμένο προγραμματιστικά χρησιμοποιώντας ανώτερου επιπέδου προγραμματιστικές γλώσσες, με αποτέλεσμα να παρέχει εφαρμογές ως υπηρεσίες αλλά και εργαλεία διαχείρισης των δεδομένων (αποθήκευση, ανάκτηση κ.τ.λ.). Στο επίπεδο App Services έχουμε πλατφόρμες οι οποίες παρέχουν τις εφαρμογές ως υπηρεσίες (π.χ. Data-as-a-Service (DaaS), Communications-as-a-Service (CaaS)) που διατίθενται μέσω των API και υπάρχει η δυνατότητα επαναχρησιμοποίησης τους (π.χ. Google Prediction API, Microsoft Azure Machine Learning Services, Amazon Simple Email Service). Και τέλος το επίπεδο SaaS που αφορά στην χρήση των εφαρμογών από τον τελικό χρήστη.

1.3 Χαρακτηριστικά του Cloud Computing

Με το Cloud Computing ουσιαστικά οι υπηρεσίες και οι εφαρμογές (π.χ. εφαρμογές εμπορικές, κοινωνικής δικτύωσης, πληροφορικής κ.τ.λ.) βρίσκονται σε συστήματα έξω από τον φυσικό χώρο του χρήστη, και του προσφέρονται ως λογισμικό, ως αποθήκευση αλλά και ως διαδικτυακές υποδομές, με χρέωση ανάλογη με την χρήση που κάνει. Σύμφωνα με το NIST το Υπολογιστικό Νέφος έχει πέντε βασικά χαρακτηριστικά:

- Κατ' απαίτηση υπηρεσία – Ο χρήστης έχει στην διάθεση του, ανάλογα με τις ανάγκες του και χωρίς να απαιτείται να προμηθευτεί τον απαραίτητο εξοπλισμό, υπολογιστικές δυνατότητες όπως χρόνο στον διακομιστή, δικτυακή αποθήκευση αλλά και εφαρμογές και υπηρεσίες χωρίς να απαιτείται η παρέμβαση του παρόχου ή η συμβολή ενός προγραμματιστή. Λόγω της ικανότητας κατανομής των πόρων ανάλογα με τις απαιτήσεις χρήσης παρατηρούμε ότι κατά περιόδους που υπάρχει μεγάλη ζήτηση χρησιμοποιούνται μεγάλοι διακομιστές, ή ανάλογα με το φορτίο εργασίας ενεργοποιούνται κάθε φορά διαφορετικά κέντρα δεδομένων. Εδώ βέβαια υπάρχει περιορισμός στην χρήση του υλικού ώστε να βρίσκεται σε χώρες που πληρούν τις προϋποθέσεις ιδιωτικότητας, έστω κατ' ελάχιστο.
- Ευρεία πρόσβαση στο δίκτυο – Οι πληροφορίες και οι υπηρεσίες που είναι διαθέσιμες από το Νέφος δεν ανήκουν μεμονωμένα σε κάποιον ή δεν βρίσκονται σε κάποιο φυσική συσκευή αλλά βρίσκονται στο Υπολογιστικό Νέφος. Επομένως ο χρήστης έχει τη δυνατότητα πρόσβασης σε πληροφορίες ή υπηρεσίες μέσω του Ιντερνετ, από οποιαδήποτε συσκευή (π.χ. κινητά τηλέφωνα, τάμπλετ και Η/Υ), οποιαδήποτε χρονική στιγμή και φυσικά από οποιαδήποτε τοποθεσία αρκεί βέβαια να υπάρχει σύνδεση στο διαδίκτυο.
- Συγκέντρωση πόρων και Πολλαπλή Εξυπηρέτηση *Multitenancy* – Οι διαφορετικοί φυσικοί και εικονικοί πόροι (διακομιστές, εικονικές μηχανές, αποθήκευση, μνήμη, επεξεργασία και εύρος δικτύου) που είναι διαθέσιμοι από τον πάροχο, διατίθενται δυναμικά ξανά και ξανά ανάλογα με τις απαιτήσεις των χρηστών. Ο χρήστης δεν έχει τον έλεγχο τους, ούτε γνωρίζει που βρίσκονται παρά μόνο ίσως μία γενική εικόνα (π.χ. χώρα). Το Υπολογιστικό Νέφος δίνει τη δυνατότητα οι φυσικοί και οι εικονικοί υπολογιστικοί πόροι, μέσω της εικονοποίησης, να χρησιμοποιηθούν παράλληλα από πολλούς χρήστες σύμφωνα με το μοντέλο της πολλαπλής μίσθωσης (*Multitenancy*).
- Μεγάλη ελαστικότητα και κλιμάκωση – Το Υπολογιστικό Νέφος έχει τη δυνατότητα κλιμάκωσης δηλαδή διαχείρισης των υπολογιστικών πόρων ανάλογα με τις απαιτήσεις

και ανάγκες του χρήστη. Η κλιμάκωση αφορά στην διάθεση της απαιτούμενης υποδομής είτε εξασφαλίζοντας περισσότερους υπολογιστικούς πόρους ίδιων χαρακτηριστικών (πχ περισσότεροι διακομιστές σε χρήση) το οποίο έχει χαμηλό κόστος, αλλά επίσης μπορεί να αφορά και στην αναβάθμιση των διαθέσιμων υπολογιστικών πόρων αυξάνοντας έτσι τις δυνατότητες σε υπολογιστική ισχύ για παράδειγμα, το οποίο όμως είναι πιο κοστοβόρο. Ο χρήστης δεν χρειάζεται να έχει ιδιαίτερες προγραμματιστικές γνώσεις και ταυτόχρονα του δημιουργείται η αίσθηση πως οι δυνατότητες σε υπολογιστικούς πόρους, σε σχέση με τις υπηρεσίες και τις εφαρμογές, που του παρέχονται είναι απεριόριστες οποιαδήποτε χρονική στιγμή. Ένα λοιπόν από τα χαρακτηριστικά του Cloud Computing, είναι η αίσθηση ευελιξίας δηλαδή η ικανότητα του να αναθέτει και να αποδεσμεύει τους πόρους, ακόμα και αυτόματα κάποιες φορές, αλλά και ταχύτητα ανάλογα με την ζήτηση.

- Μετρήσιμα επίπεδα παροχής υπηρεσιών (*Measured Service*) – Υπάρχει η δυνατότητα εποπτείας, ελέγχου και βελτιστοποίησης της χρήσης των πόρων, και τα αποτελέσματα παριστάνονται με αναφορές απεικόνισης όπου αποτυπώνεται η χρήση των υπολογιστικών πόρων αλλά και η απόδοση των υπηρεσιών, για παράδειγμα σχετικά με τον αριθμό των εξυπηρετητών που κατανέμονται, την χρονική περίοδο χρήσης της *CPU* (*Central Processing Unit*) δηλαδή του κεντρικού επεξεργαστή, της χρήσης αποθήκευσης και τέλος του εύρους του δικτύου που χρησιμοποιήθηκε για την μετακίνηση των δεδομένων από και προς το *Cloud*. Η αξιοποίηση αυτών των μετρήσεων οδηγεί στην ορθότερη τιμολόγηση αλλά και στην αξιολόγηση της παροχής των προσφερόμενων υπηρεσιών. Αυτό κατ' επέκταση συμβάλλει στην ορθότερη χρήση των πόρων, στην εξακρίβωση της ανάγκης αναβάθμισης των υποδομών και επομένως στην μείωση του κόστους παροχής των υπολογιστικών πόρων. [2, 6, 11]

1.4 Αρχιτεκτονική του Υπολογιστικού Νέφους

Το Υπολογιστικό Νέφος έχει μία φιλοσοφία αρχιτεκτονικής που στηρίζεται στη διάθεση και δημιουργία εφαρμογών ευρείας χρήσης μέσω του διαδικτύου. Καλύπτει τις απαιτήσεις σε υπολογιστικούς πόρους παρέχοντας τους απαραίτητους πόρους κάθε φορά για την εκτέλεση των εφαρμογών, τη χρήση ή την αποδέσμευση τους ανάλογα με τις ανάγκες του χρήστη. Έχει δηλαδή υψηλό βαθμό κλιμάκωσης ώστε να εξασφαλισθεί η απρόσκοπτη εκτέλεση των απαιτούμενων διεργασιών, ικανοποιώντας τις απαιτήσεις χρήσης του σύμφωνα με τα χαρακτηριστικά και τα πρότυπα που ακολουθεί, καθώς επίσης και με τον καθορισμό των κύριων συντελεστών,

των δραστηριοτήτων αλλά και των λειτουργιών τους όπως φαίνεται στο παρακάτω σχήμα.[10] Διακρίνουμε στο σχήμα που ακολουθεί, την τεχνολογία που χρησιμοποιείται και χωρίζεται σε



Σχήμα 1.1: Η αρχιτεκτονική του Υπολογιστικού Νέφους

τέσσερα επίπεδα σε σχέση με την πρόσβαση στο Νέφος από το χρήστη. Στο πρώτο επίπεδο έχουμε την σύνδεση του χρήστη με το Νέφος μέσω οποιασδήποτε συσκευής διαθέτει. Ακολουθεί το επίπεδο Δικτύου όπου ο χρήστης για να συνδεθεί πρέπει να έχει σύνδεση μέσω διαδικτύου. Στη συνέχεια υπάρχει το επίπεδο που παρέχει το απαραίτητο λογισμικό το οποίο μπορεί να είναι το λειτουργικό, λογισμικό που εξασφαλίζει την διασύνδεση του χρήστη με το κέντρο δεδομένων αλλά και τη διαχείριση των υπολογιστικών πόρων. Στο τέταρτο επίπεδο βρίσκονται οι διαθέσιμοι υπολογιστικοί πόροι.[10] Η τεχνολογία πάνω στην οποία βασίζεται το Νέφος περιλαμβάνει τις εξής συνιστώσες:

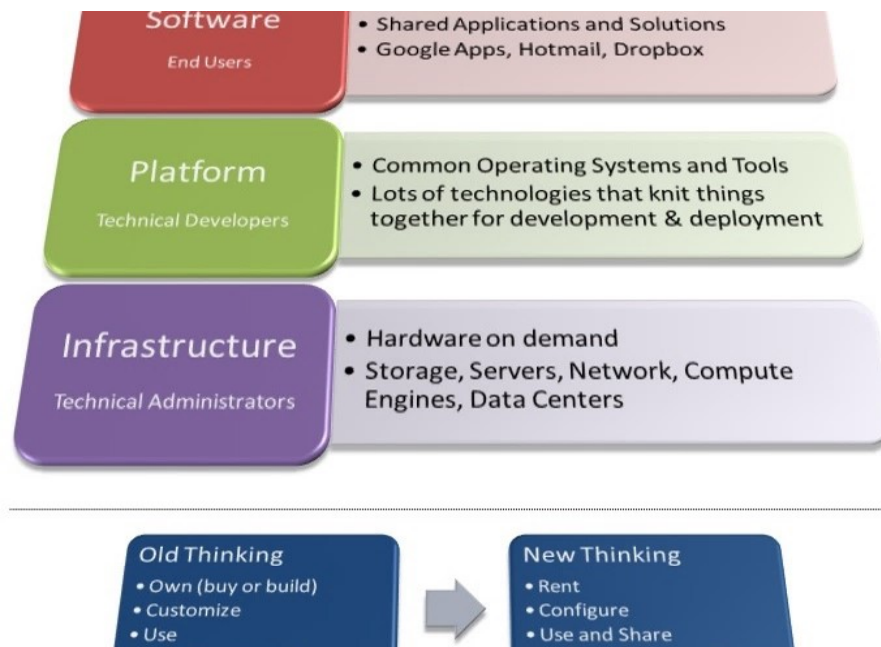
- Εφαρμογές
- Πλατφόρμα δηλαδή το περιβάλλον όπου εκτελούνται οι εφαρμογές
- Δομή, το σύνολο των υπολογιστικών πόρων
- Εικονοποίηση, η οποία είναι η βασική τεχνολογία που χρησιμοποιείται στο Υπολογιστικό Νέφος. Η φιλοσοφία της εικονοποίησης είναι η δημιουργία ανεξάρτητων και

απομονωμένων λογικών διασυνδέσεων από ένα φυσικό πόρο. Η κάθε μία λογική σύνδεση συμπεριφέρεται σαν ένας ανεξάρτητος φυσικός πόρος, ο οποίος έχει το δικό του λειτουργικό σύστημα και τρέχει τις δικές του εφαρμογές.

Το Υπολογιστικό Νέφος δίνει τη δυνατότητα στον χρήστη να έχει στη διάθεση του υπολογιστικές πλατφόρμες σε χαμηλό κόστος οι οποίες του παρέχουν ένα περιβάλλον μεγάλης κλιμάκωσης, με δυνατότητα διαμόρφωσης του με τρόπο που να εξυπηρετεί τις εξατομικευμένες ανάγκες του χρήστη, δυνατότητα χρήσης πολύπλοκων υπολογιστικών δομών, και χρήση δικτυακών υπηρεσιών. [3, 10, 11]

1.5 Υπηρεσίες παρεχόμενες από το Υπολογιστικό Νέφος

Το Υπολογιστικό Νέφος διαθέτει τρεις βασικούς τύπους υπηρεσιών, σύμφωνα με το *NIST* την *Software as a Service (SaaS)*, την *Platform as a Service (PaaS)* και την *Infrastructure as a Service (IaaS)*.



Σχήμα 1.2: Μοντέλα Υπηρεσιών

Εκτός από τα κλασικά μοντέλα υπηρεσιών πλέον οι πάροχοι προσφέρουν και άλλες υπηρεσίες οι οποίες χαρακτηρίζονται ως XaaS όπου το X αναφέρεται σε διάφορες τεχνολογίες οι οποίες παρέχονται ως υπηρεσίες όπως το Data as a Service (DaaS), Communications as a service (CaaS), Network as a service (NaaS) κτλ.[9]

1.5.1 Software as a Service (SaaS)

Σύμφωνα με το NIST, η διάθεση του λογισμικού κατ' απαίτηση του χρήστη ως υπηρεσία αναφέρεται στο μοντέλο Λογισμικό ως Υπηρεσία (*Software as a Service (SaaS)*). Ο χρήστης μέσω του διαδικτύου έχει πρόσβαση στις εφαρμογές και στο λογισμικό που διατίθενται από τον πάροχο, δίχως να απαιτείται η απόκτηση των αδειών χρήσης του λογισμικού, αλλά και χωρίς να έχει τον έλεγχο ή τη διαχείριση των υπολογιστικών πόρων (π.χ. διακομιστές, αποθηκευτικά μέσα κτλ.)[2]

Τη διαχείριση των υπολογιστικών πόρων αλλά και την ευθύνη για την εγκατάσταση, τη συντήρηση, την αναβάθμιση αλλά και την εγκατάσταση πρόσθετων αλλά και οτιδήποτε απαιτείται για την ολοκλήρωση των παρεχόμενων εφαρμογών προς το χρήστη, έχει ο πάροχος απαλάσσοντας έτσι τον χρήστη από τις σύνθετες και πολλές φορές δύσκολες για αυτόν διαδικασίες παραμετροποίησης και διαχείρισης του λογισμικού, απλοποιώντας πολύ με αυτό τον τρόπο τη χρήση του λογισμικού. Ουσιαστικά ο χρήστης νοικιάζει το λογισμικό από τον πάροχο όποτε το χρειάζεται και χρεώνεται για τις υπηρεσίες που χρησιμοποιεί είτε ανάλογα με τον αριθμό των χρηστών, είτε για το χρόνο χρήσης των υπηρεσιών, ή για τον αποθηκευτικό χώρο που χρησιμοποιεί ή ακόμα και για το εύρος ζώνης που χρειάζεται ανάλογα με τον τύπο των αρχείων που διαχειρίζεται ο χρήστης. Ο πάροχος έχει τον απόλυτο έλεγχο των υποδομών, της απόδοσης, της ασφάλειας, της κλιμάκωσης, της ιδιωτικότητας. Επίσης διαχειρίζεται τους υπολογιστικούς πόρους, την προγραμματιστική λογική και το μοντέλο ανάπτυξης μιας εφαρμογής και οτιδήποτε άλλο είναι απαραίτητο για να ολοκληρωθεί η εφαρμογή και να είναι διαθέσιμη να τη χρησιμοποιήσει ο χρήστης. Η εφαρμογή είναι διαθέσιμη στο χρήστη ως προσωπική διεργασία, θα μπορούσαμε να πούμε σαν ένα παράθυρο της πλατφόρμας του παρόχου, στο οποίο ο χρήστης θέτει τις επιθυμητές ρυθμίσεις, χωρίς όμως να τον απασχολεί η εξασφάλιση ή η διαχείριση των υπολογιστικών πόρων. Η πρόσβαση στην εφαρμογή-υπηρεσία γίνεται πολύ απλά συνήθως με την χρήση ενός *Web Browser*, από οποιαδήποτε συσκευή διαθέτει ο χρήστης αρκεί να υπάρχει σύνδεση με το διαδίκτυο. Επίσης, πολλοί πάροχοι δίνουν πρόσβαση στις εφαρμογές μέσω διαθέσιμων APIs ώστε να μπορούν εύκολα οι χρήστες να ορίσουν διάφορες παραμέτρους στις εφαρμογές. [6, 9]

Όσον αφορά στα δεδομένα ο πάροχος προσφέρει τη δημιουργία αντιγράφου ασφαλείας (backup) αλλά ο χρήστης έχει την ευθύνη για την διαχείριση των δεδομένων του, δηλαδή ποιος έχει δικαιώματα πρόσβασης, δυνατότητα διαγραφής, επεξεργασίας, αποθήκευσης και διάθεσης των δεδομένων. Οι θέσεις αποθήκευσης των δεδομένων είναι ευθύνη του παρόχου, οπότε αντίστοιχα είναι και υπεύθυνος για την διασφάλιση των δεδομένων (ασφάλεια, ακεραιότητα, εμπιστευτικότητα) επιλέγοντας ασφαλείς τοποθεσίες αποθήκευσης των δεδομένων, επιλέγοντας το κατάλληλο εμπλεκόμενο προσωπικό αλλά και εφαρμόζοντας τις ανάλογες πολιτικές ασφαλείας ώστε να πετύχει τα απαιτούμενα επίπεδα ασφαλείας στα δίκτυα, στη δομή, και στις εφαρμογές. Γνωστές εφαρμογές του μοντέλου *SaaS* είναι το Google Gmail, Microsoft 365, Salesforce, CRM (Customer Relationship Management), το ERP (Enterprise Resource Planning), καθώς επίσης και πολλές άλλες εταιρικές εφαρμογές.[8]

1.5.2 Platform as a Service (PaaS)

Το μοντέλο “Πλατφόρμα ως υπηρεσία” (*Platform as a service (PaaS)*) αποτελεί ένα πιο εξειδικευμένο μοντέλο, το οποίο απευθύνεται κυρίως σε προγραμματιστές. Ο πάροχος υποστηρίζει την διαδικασία ανάπτυξης των εφαρμογών (σχεδίαση, έλεγχος, παρακολούθηση, ανάπτυξη) διαθέτοντας τα εργαλεία ανάπτυξης εφαρμογών (π.χ. *Eclipse*, *Microsoft Access*, *Google Web Toolkit*, *Google Gears* κτλ) αλλά και τον τρόπο με τον οποίο θα γίνει η διάθεση αλλά και η διανομή των εφαρμογών όπως και η ανάλογη χρέωση των παροχών του. Ο χρήστης έχει τη δυνατότητα να χρησιμοποιήσει τις διαθέσιμες εφαρμογές αλλά και να αναπτύξει τις δικές του, χρησιμοποιώντας διάφορα εργαλεία ανάπτυξης λογισμικού, προγραμματιστικές γλώσσες, βιβλιοθήκες και οτιδήποτε άλλο απαιτείται για την ολοκλήρωση μιας εφαρμογής. Όλα αυτά διατίθενται από τον πάροχο καθώς επίσης και οι απαιτούμενοι δίαυλοι διανομής και πώλησης των αναπτυσσόμενων εφαρμογών, μέσω της δικιάς του πλατφόρμας ανάπτυξης εφαρμογών η οποία πλέον είναι διαθέσιμη με την ανάλογη χρέωση ως υπηρεσία . Τα εργαλεία ανάπτυξης εφαρμογών είναι διαθέσιμα μέσω ενός API και συνήθως είναι αποθηκευμένα στο Νέφος και πολύ εύκολα προσβάσιμα μέσω ενός *Web Browser*. Οπότε χωρίς ιδιαίτερες ικανότητες διαχειριστή ενός συστήματος αλλά και χωρίς να απαιτείται εξειδικευμένο προσωπικό με προγραμματιστικές γνώσεις ή γνώσεις για τον ορισμό των παραμέτρων του εξυπηρετητή δίνεται η δυνατότητα χρήσης των εφαρμογών με χαμηλότερο κόστος και πολυπλοκότητα. Παραδείγματα αυτού του μοντέλου υπηρεσιών (Platform as a service (PaaS)) είναι τα App Engine, Engine Yard, Heroku, Microsoft Azure κ.α. [7, 8]

Ο πάροχος διαθέτει και διαχειρίζεται ένα ενιαίο περιβάλλον πλατφόρμας, ώστε αυτοματοποιη-

μένα να πραγματοποιείται κλιμάκωση, διαχείριση και συντήρηση των πόρων και να προσδίδεται στο περιβάλλον πλατφόρμας υψηλού βαθμού διαθεσιμότητα, ελαστικότητα και ευελιξία. Ο χρήστης έχει τον έλεγχο των αναπτυσσόμενων εφαρμογών, δεν έχει όμως τον έλεγχο της υποδομής αλλά ούτε και την ευθύνη παραμετροποίησης, συντήρησης και διαχείρισης των υπολογιστικών πόρων (πχ. διακομιστές, βάση δεδομένων) οι οποίοι διατίθενται δυναμικά από τον πάροχο. Να σημειωθεί ότι το μοντέλο αυτό δεν δίνει τη δυνατότητα στον χρήστη να αλλάξει με ευκολία τον πάροχο, καθώς οι εφαρμογές αναπτύσσονται στην πλατφόρμα του με την χρήση των διαθέσιμων εργαλείων. τα οποία μπορεί να μην υπάρχουν σε άλλη πλατφόρμα, οπότε είναι περιορισμένη η φορητότητα των εφαρμογών από το ένα περιβάλλον στο άλλο.[22]

1.5.3 Infrastructure as a Service (IaaS)

Στο μοντέλο Δομή ως Υπηρεσία (*Infrastructure as a Service (IaaS)*) ο πάροχος έχει τον έλεγχο της εικονοποίησης, των αποθηκευτικών χώρων, του δικτύου και των διακομιστών (Server) ενώ ο χρήστης έχει τη δυνατότητα δέσμευσης και δυναμικής χρήσης της υλικοτεχνικής υποδομής του παρόχου (επεξεργαστική ισχύ, βάσεις δεδομένων, υπηρεσίες αυθεντικοποίησης κτλ), καθώς επίσης και του διαθέσιμου λογισμικού δηλαδή λειτουργικά συστήματα και εφαρμογές, κάνοντας χρήση των διαθέσιμων *APIs* και του γραφικού περιβάλλοντος της πλατφόρμας του παρόχου. Ακριβώς λόγω της δυναμικής χρήσης των υπολογιστικών και δικτυακών πόρων έχουμε αυξομείωση του εύρους ζώνης της μνήμης αλλά και του αποθηκευτικού χώρου, οπότε κρίνεται αναγκαία η εφαρμογή των ελέγχων και μετρήσεων της χρήσης, σε πραγματικό χρόνο, ώστε να εφαρμοσθεί η κλιμάκωση και ελαστικότητα όσον αφορά στην διάθεση και αποδέσμευση των υπολογιστικών πόρων για την ικανοποίηση των απαιτήσεων. Η υπενοικίαση των υπολογιστικών πόρων γίνεται βάσει των απαιτήσεων χρήσης, οπότε η ζήτηση αποτελεί και το κριτήριο χρέωσης. Η χρήση των εικονικών μηχανών στο *Cloud*, η πρόσβαση στο διαδίκτυο αλλά και στις υπηρεσίες δρομολόγησης και αποθήκευσης των δεδομένων σε υποδομές του Νέφους δίνουν τη δυνατότητα στο χρήστη να χρησιμοποιήσει οποιαδήποτε εφαρμογή πολύ εύκολα. Ο πάροχος είναι υπεύθυνος μόνο για την συντήρηση των υποδομών, για τη διαχείριση των υπηρεσιών που αφορούν στην λειτουργία του λογισμικού και για τις βάσεις δεδομένων ώστε να φαίνεται ότι οι υπολογιστικοί πόροι είναι ανεξάντλητοι. Ο πάροχος με την χρήση των εικονικών μηχανών (VM) διαχειρίζεται επαρκώς τους φυσικούς πόρους που διαθέτει. Έτσι, οι εφαρμογές είναι διαθέσιμες στο περιβάλλον του παρόχου με ελάχιστες αλλαγές στο λογισμικό. Έχοντας ως βάση τον ίδιο φυσικό εξοπλισμό, δημιουργούνται στιγμιότυπα εικονικών μηχανών τα οποία περιλαμβάνουν συγκεκριμένο λογισμικό όπως λειτουργικό σύστημα,

διακομιστές, βάσεις δεδομένων κτλ, ώστε να αποτελέσουν μια ειδική πλατφόρμα ή ίσως θα μπορούσαμε να τα χαρακτηρίσουμε ως εφαρμογές, που έχουν σχεδιαστεί για να ικανοποιήσουν την ανάγκη εξυπηρέτησης συγκεκριμένων απαιτήσεων του χρήστη. Ο χρήστης έχει τον έλεγχο των αποθηκευτικών μέσων και των εφαρμογών που έχουν αναπτυχθεί, και συνήθως έχει και τον έλεγχο του εξοπλισμού δικτύωσης σε περιορισμένο βαθμό (π.χ. firewalls). Επομένως, ο χρήστης δημιουργεί το δικό του κέντρο εικονικών μηχανών, και είναι υπεύθυνος για τη συντήρηση και ενημέρωση του λογισμικού που αφορά στις εικονικές μηχανές. Παραδείγματα του μοντέλου αυτού είναι το *Amazon Web Services (AWS)*, *Amazon Elastic Compute Cloud (Amazon EC2)*, *Microsoft Windows Azure* και το *Google Cloud Platform (GCP)*. [7, 12, 22]

1.5.4 Επιπρόσθετες Υπηρεσίες (Anything as a Service (XaaS))

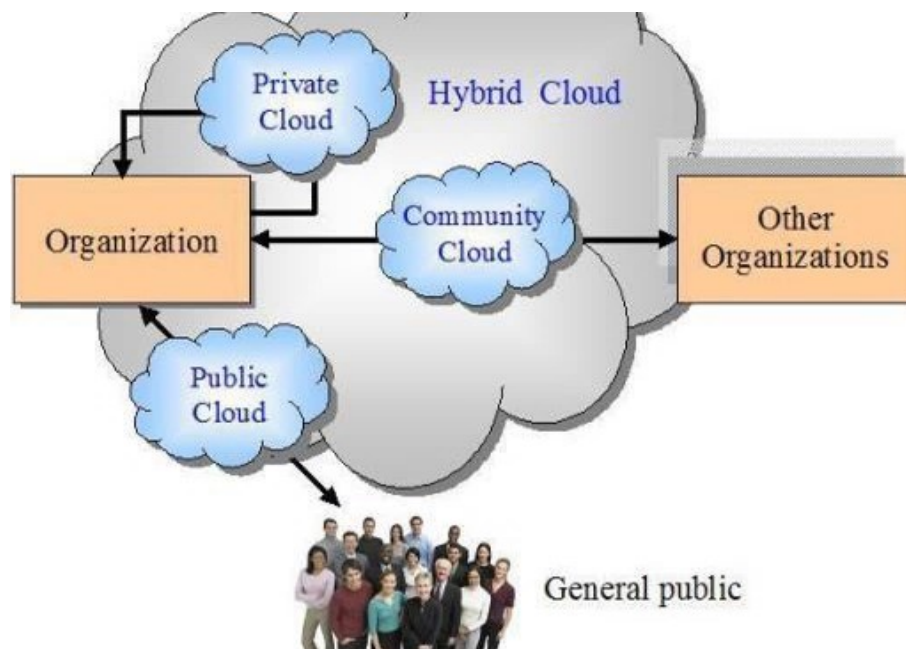
) Η φιλοσοφία του μοντέλου αυτού είναι η προσφορά όλων των διαθέσιμων από το διαδίκτυο τεχνολογιών ως υπηρεσίες. Χαρακτηρίζεται από υψηλού βαθμού κλιμάκωση και δυνατότητα διαθεσιμότητας περιβαλλόντων και υπηρεσιών μεγάλης επεξεργαστικής ισχύος. Μερικά παραδείγματα τέτοιων μοντέλων είναι:

- Hardware ως Υπηρεσία(HaaS) – Αφορά στην αγορά του υλικού (Hardware) ή βάσεων δεδομένων(π.χ. το Amazon EC2).[13]
- Business Process ως Υπηρεσία(BpaaS) – παροχή μέσω των τεχνολογιών του διαδικτύου από το Νέφος επαγγελματικών διαδικασιών ως υπηρεσίες, που εξυπηρετούν την πολυ χρηστικότητα και είναι συνήθως αυτοματοποιημένες.[3]
- Database ως Υπηρεσία (DbaaS) – Ένα νέο μοντέλο στο οποίο ως υπηρεσία παρέχεται η Βάση Δεδομένων (Database as a Service (DbaaS)). Αυτή η υπηρεσία καλύπτει την ανάγκη χρήσης κάποιας βάσης δεδομένων, χωρίς όμως την υποχρέωση παραμετροποίησης των απαιτούμενων φυσικών πόρων ή την εγκατάσταση λογισμικού, δίνοντας τη δυνατότητα της αποδοτικότερης και ευκολότερης χρήσης της βάσης από τον χρήστη. Ο πάροχος είναι υπεύθυνος για τη διαχείριση και την συντήρηση, ενώ ο χρήστης έχει τη δυνατότητα να ενημερώνει και να δημιουργεί ερωτήματα σε μία βάση δεδομένων που βρίσκεται στο Νέφος και να χρεώνεται ανάλογα με τη χρήση. [7]
- Κακόβουλο Λογισμικό ως Υπηρεσία – Η αγορά λογισμικού με σκοπό να δυσλειτουργήσει το υλικό ενός ανταγωνιστή και να τρωθεί έτσι η αξιοπιστία του.[3]

- Αποθηκευτικός χώρος ως Υπηρεσία (StaaS) – Στο μοντέλο αυτό έχουμε τη διάθεση από τον πάροχο αποθηκευτικού χώρου, με την ανάλογη χρέωση (πχ το Dropbox).
- Δικτύωση Νέφους ως Υπηρεσία (CloudNaaS) – Παρέχει διάφορες δικτυακές υπηρεσίες ώστε οι χρήστες να έχουν στη διάθεση τους διάφορες εικονικές δικτυακές λειτουργίες όπως απομόνωση δικτύου, ανίχνευση επίθεσης και πρόληψη, εύρος ζώνης κατ' απαίτηση, παρακολούθηση και φιλτράρισμα της κίνησης του δικτύου κτλ. Είναι διαθέσιμα με την υποδομή του Νέφους οπότε αποτελούν επαρκή, προσιτή λύση και με χαμηλό κόστος για τους χρήστες σε σχέση με αυτό που ίσχυε δηλαδή την διάθεση των δικτυακών υπηρεσιών από τον πάροχο μέσω τρίτου μέρους. [24]

1.6 Μοντέλα ανάπτυξης του Υπολογιστικού Νέφους

Το Υπολογιστικό Νέφος πρωτοεμφανίστηκε ως Δημόσιο Νέφος (Public Cloud) κατά την διάρκεια της εξέλιξης όμως δημιουργήθηκαν και άλλα δύο βασικά μοντέλα ανάπτυξης το Private Cloud και το Hybrid Cloud.



Σχήμα 1.3: Μοντέλα Ανάπτυξης

1.6.1 Δημόσιο Νέφος (Public Cloud)

Σε αυτό το μοντέλο παρέχονται υπολογιστικές και αποθηκευτικές υπηρεσίες μέσω του Internet, μέσω Web εφαρμογών ή υπηρεσιών από τον πάροχο. Ο χρήστης μέσω της αξιοποίησης των διαθέσιμων από τον πάροχο APIs χρησιμοποιεί τους πόρους που χρειάζεται, χωρίς να τον απασχολεί η φυσική τους θέση και χωρίς να χρειάζεται να επενδύσει στην απόκτηση πιο σύγχρονου υλικού ή λογισμικού. Το πλεονέκτημα χρήσης του δημοσίου νέφους για τους επαγγελματίες είναι ότι δεν απαιτείται καταβολή προκαταβολικών εξόδων, ενώ για τους χρήστες ισχύει η πληρωμή ανάλογα με την χρήση των πόρων, οι οποίοι να σημειωθεί ότι είναι διαχειρίσιμοι και ανεξάντλητοι. Μειονέκτημα κυρίως για τους επιχειρηματίες είναι η εξάρτησή τους από την βιωσιμότητα και αξιοπιστία του παρόχου καθώς επίσης και η πιθανή οικονομική επιβάρυνση που αφορά στην ταχύτερη μεταφορά των δεδομένων από και προς το Νέφος. Ένα άλλο μειονέκτημα έχει σχέση με την ασφάλεια, μιας και αποτελεί ευθύνη του παρόχου, ενώ ο χρήστης συμβάλλει ελάχιστα στον έλεγχο και επίβλεψη των θεμάτων ασφαλείας. [12]

1.6.2 Ιδιωτικό Νέφος (Private Cloud)

Αυτό το μοντέλο ανάπτυξης αναφέρεται σε ένα χρήστη, ο οποίος μπορεί να είναι ιδιώτης ή κάποια επιχείρηση. Χρησιμοποιείται κυρίως από επιχειρήσεις οι οποίες είναι υπεύθυνες για την λειτουργία του, αφού το δίκτυο, η επεξεργαστική ισχύς και η δομή αποθήκευσης είναι αφιερωμένα αποκλειστικά σε αυτόν που μισθώνει το Ιδιωτικό Νέφος χωρίς όμως να είναι απαραίτητο οι πόροι να βρίσκονται στις εγκαταστάσεις του. Πλεονέκτημα του Ιδιωτικού Νέφους είναι ότι αυτός που το χρησιμοποιεί έχει τον έλεγχο, έχει την δυνατότητα χαμηλής χρέωσης με την χρήση εικονικών μηχανών, καθορίζει τις πολιτικές, και τον έλεγχο πρόσβασης και εξασφαλίζει μεγάλο βαθμό ασφάλειας των υπολογιστικών πόρων που χρησιμοποιεί. Η πρόσβαση στα δεδομένα γίνεται μόνο από το μισθωτή του Ιδιωτικού Νέφους, ο οποίος μπορεί να επιλέξει αν θα χρησιμοποιήσει δικό του κέντρο δεδομένων και η διαχείριση θα γίνει από δικό του ειδικευμένο προσωπικό (Αφιερωμένο Ιδιωτικό Νέφος) ή αν θα χρησιμοποιήσει ότι του διαθέτει ο πάροχος με τις ανάλογες όμως διασφαλίσεις όσον αφορά στην εφαρμογή των κανονισμών και των πολιτικών ασφαλείας. Σύμφωνα με τα παραπάνω η χρήση του Ιδιωτικού Νέφους αποτελεί μία εξαιρετική λύση κυρίως για τις επιχειρήσεις ή τους οργανισμούς που διαχειρίζονται ευαίσθητα δεδομένα.[5, 7]

Στο Private cloud τα δεδομένα φιλοξενούνται σε κέντρα που ανήκουν στον χρήστη και με τη χρήση των τεχνολογιών πληροφορικής τα διαχειρίζεται ο ίδιος. Υπάρχει όμως και η δυνατότητα

τα δεδομένα να βρίσκονται στις εγκαταστάσεις ενός τρίτου μέρους, και η διαχείριση να πλαισιώνεται από συμφωνητικά που αποσαφηνίζουν το επίπεδο υπηρεσιών (service-level-agreement SLAs), αλλά και καθορίζουν τις απαιτήσεις ασφαλείας θέτοντας δεσμευτικές ρήτρες. Μία άλλη παραλλαγή του Ιδιωτικού Νέφους είναι το Κοινοτικό Νέφος (Community cloud) το οποίο και απευθύνεται σε ομάδες (πχ τράπεζες, στελέχη οργανισμών ή εμπορικών καταστημάτων κτλ.), οι οποίες συνεργάζονται σε έργα, εφαρμογές ή ακόμα και σε ερευνητικό πεδίο, έχουν κοινές απαιτήσεις και ανησυχίες (όπως απαιτήσεις ασφάλειας, ιδιωτικότητας, όμοιες θεωρήσεις πολιτικής και συμβατότητας κτλ.) και χρειάζονται τη διάθεση από το Νέφος ενός κέντρου ανάπτυξης, διαχείρισης και εκτέλεσης των εργασιών τους. Αυτό το κέντρο μπορεί να ανήκει, να έχει τη διαχείριση και τη λειτουργία του ή κάποιο από τα μέλη της ομάδας ή ένα τρίτο μέρος ή ακόμα και συνδυασμός αυτών. [2]

1.6.3 Υβριδικό Νέφος (Hybrid Cloud)

Αποτελεί τον συνδυασμό του Δημόσιου και Ιδιωτικού Cloud, τα οποία είναι διαθέσιμα στο ίδιο περιβάλλον. Στο Δημόσιο Νέφος είναι διαθέσιμο το λογισμικό, οι πλατφόρμες ανάπτυξης εφαρμογών καθώς επίσης και οι διαθέσιμες εφαρμογές και υπηρεσίες. Το Ιδιωτικό Νέφος το χρησιμοποιεί για την μεταφορά και την αποθήκευση των δεδομένων στο κέντρο δεδομένων που έχει δημιουργηθεί στο Ιδιωτικό Νέφος ή ακόμα και σε τοπικό κέντρο δεδομένων, ώστε να διασφαλιστούν τα δεδομένα καλύπτοντας έτσι την αδυναμία του Δημοσίου Νέφους όσον αφορά στην ασφάλεια τους. Γίνεται χρήση του Δημόσιου Νέφους για την ανάπτυξη των εφαρμογών ώστε να γίνει εκμετάλλευση της ευελιξίας που παρέχει αλλά και του χαμηλού κόστους αφού δεν απαιτείται η αγορά υλικού και λογισμικού αλλά ούτε και συντήρησης των υποδομών. Το Υβριδικό Cloud είναι λοιπόν πιο ευέλικτο, διακρίνεται από το χαρακτηριστικό της φορητότητας και της κλιμάκωσης, του χαμηλότερου κόστους και της ασφάλειας των δεδομένων, χαρακτηριστικά που αποτελούν πόλο έλξης κυρίως για τις επιχειρήσεις.[5, 7]

Κεφάλαιο 2

Ασφάλεια και Υπολογιστικό Νέφος

ΤΟ Υπολογιστικό Νέφος χρησιμοποιείται πλέον από απλούς χρήστες μέχρι εταιρείες και οργανισμούς. Το Υπολογιστικό Νέφος λόγω της φύσης του, που χαρακτηρίζεται από τον διαμοιρασμό κατ' απαίτηση πόρων, εφαρμογών αλλά και την εκτεταμένη χρήση εικονικού περιβάλλοντος, ακόμα διχάζει και τρομάζει κάποιους όσον αφορά στην ασφάλεια των δεδομένων και όχι μόνο. Μερικές από τις απειλές είναι η καταχρηστική και παράνομη χρήση του Υπολογιστικού Νέφους, μη ασφαλείς προγραμματιστικές διεπαφές των εφαρμογών (APIs), εισβολείς εκ των έσω, ευπάθειες διαμοιρασμού τεχνολογικού, απώλεια ή διαρροή των δεδομένων, υποκλοπή λογαριασμού, υπηρεσιών και κινήσεως και άγνωστο προφίλ κινδύνου. Εγείρονται επίσης θέματα αποθήκευσης των δεδομένων αφού ο χρήστης δε γνωρίζει την ακριβή τοποθεσία που βρίσκονται τα δεδομένα του αλλά και ποια άλλα δεδομένα είναι αποθηκευμένα στο ίδιο αποθηκευτικό χώρο με τα δικά του. Η ικανότητα ελέγχου της πληροφορίας αλλά και ελέγχου πρόσβασης σε αυτή καθορίζει σε ποιο βαθμό εξασφαλίζεται η Ιδιωτικότητα σε ένα σύστημα Νέφους. Υπάρχει λοιπόν εξάρτηση από τις προθέσεις και ενέργειες του παρόχου όσον αφορά στην ασφάλεια των δεδομένων αλλά και των εικονικών μηχανών, καθώς επίσης και ζητημάτων που εγείρονται είτε νομικών είτε συμβατότητας. Φυσικά έχουν γίνει τρομερά βήματα στον τομέα αυτό, όμως ακόμα υπάρχουν ευπάθειες και απειλές εναντίον της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας σε ένα σύστημα Νέφους.

2.1 Ζητήματα Ασφάλειας στο Υπολογιστικό Νέφος

Τα ζητήματα ασφάλειας που εγείρονται στο Υπολογιστικό Νέφος διαφέρουν για κάθε μοντέλο ανάπτυξης. Από όλα τα μοντέλα ανάπτυξης λιγότερο ασφαλές θεωρείται ότι είναι το Δημόσιο Νέφος. Σύμφωνα με το NIST στο Δημόσιο Νέφος, οι υποδομές είναι διαθέσιμες σε όλους τους χρήστες αλλά ανήκουν στον πάροχο.

Οι βασικότερες απειλές για την ασφάλεια σε αυτό το μοντέλο είναι:

- Απώλεια δεδομένων - Υπάρχει η περίπτωση της απώλειας των δεδομένων είτε λόγω βλάβης του εξοπλισμού, είτε λόγω στοχευμένης επίθεσης όπου ο επιτιθέμενος κρυπτογραφεί τα δεδομένα και αφαιρεί τη δυνατότητα πρόσβασης του χρήστη σε αυτά επιδιώκοντας να του δημιουργήσει συνήθως οικονομική ζημιά. Η δημιουργία αντιγράφων ασφαλείας αποδεικνύεται η σωτήρια λύση οδηγώντας στην επαρκή ανάκτηση των δεδομένων.[34]
- Παραβίαση των δεδομένων - Κυρίως αφορά στα ευαίσθητα δεδομένα στα οποία μπορεί να αποκτήσουν πρόσβαση άτομα τα οποία δεν είναι εξουσιοδοτημένα. [32]
- Επίθεση εκ των έσω - Μία από τις μεγαλύτερες αδυναμίες ασφαλείας είναι η επιλογή του προσωπικού καθώς επίσης και η συμμόρφωση του με τους κανονισμούς ασφαλείας που πρέπει να ισχύουν. Αν δεν εφαρμόζονται οι κανονισμοί ασφαλείας είτε από αμέλεια, είτε από λάθος ή και από σκοπιμότητα όπως πχ έχοντας πρόσβαση στα συστήματα από ίδια μέσα, το αποτέλεσμα είναι το ίδιο υπάρχει έκθεση των δεδομένων σε κίνδυνο.[34]
- Ευπάθειες του συστήματος : Το Δημόσιο Νέφος επειδή χρησιμοποιεί το Διαδίκτυο είναι εκτεθειμένο σε επιθέσεις, οι οποίες προκαλούν είτε Διακοπή Παροχής Υπηρεσιών (Denial-of-Service) είτε παραβίαση εμπιστευτικών δεδομένων όπως υποκλοπή κωδικών πρόσβασης.[7]

Από την άλλη στο Ιδιωτικό Νέφος θεωρείται ότι υπάρχει μεγαλύτερη ασφάλεια αφού η υποδομή είναι αφιερωμένη μόνο σε ένα χρήστη και ελέγχεται από τον ίδιο ή από τρίτο μέρος με προϋποθέσεις. Ο χρήστης έχει μεγαλύτερο έλεγχο των δεδομένων. Το Κοινοτικό Νέφος είναι λιγότερο ασφαλές σε σχέση με το Ιδιωτικό Νέφος αφού υπάρχει διαμοιρασμός της υποδομής μεταξύ μίας κοινότητας ή μίας ομάδας και η ασφάλεια εξαρτάται από τη σχέση εμπιστοσύνης που υπάρχει μεταξύ των μελών. Το Υβριδικό νέφος σύμφωνα με το NIST αποτελεί το συνδυασμό δύο ή περισσότερων μοντέλων ανάπτυξης, και αυτός ο συνδυασμός ενεργοποιεί την

φορητότητα των δεδομένων και των εφαρμογών. Η ασφάλεια στο Υβριδικό Νέφος εξαρτάται από την παραμετροποίηση που θα γίνει, αφού αυτό το μοντέλο αποτελεί κυρίως το συνδυασμό του Δημόσιου και Ιδιωτικού μοντέλου, οπότε υπάρχει η δυνατότητα χρήσης του Ιδιωτικού Νέφους για την διαχείριση των δεδομένων.

Τα ζητήματα ασφαλείας αφορούν είτε τον πάροχο ο οποίος οφείλει να διασφαλίσει τις υπηρεσίες που παρέχει καθώς και τα δεδομένα που αφορούν στο χρήστη, είτε τον χρήστη ο οποίος οφείλει να ελέγξει την ασφάλεια όσων του παρέχονται αλλά και το βαθμό έκθεσης των ευαίσθητων δεδομένων του σε κίνδυνο. Γενικά, λόγω του διαμοιρασμού των πόρων, των εφαρμογών, των παρεχόμενων υπηρεσιών αλλά και των αποθηκευτικών δομών μεταξύ των χρηστών, καθώς επίσης και της δυνατότητας κλιμάκωσης όσον αφορά στην χρήση των πόρων υπάρχει ο κίνδυνος της προσβολής της εμπιστευτικότητας των δεδομένων ή ακόμα και της απώλειας τους.[12]

Το *Cloud Computing* χρησιμοποιεί νέες τεχνολογίες όπως η Εικονοποίηση (εικονοποίηση διακομιστή, δικτύου, αποθήκευσης), Web τεχνολογίες (όπως XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP) κτλ) οι οποίες χρησιμοποιούνται με τη λογική της παροχής υπηρεσιών οπότε συνδυάζονται ώστε να εκτελεσθεί μία διεργασία, και βέβαια τα APIs (Application Programming Interface) με τα οποία ο χρήστης αποκτά ένα φιλικόν περιβάλλον διαχείρισης των εφαρμογών και των υπηρεσιών διαδικτύου αλλά ταυτόχρονα δίνεται η ευκαιρία στους κακόβουλους χρήστες να εντοπίσουν αδυναμίες και να επιτεθούν. Η χρήση όλων αυτών των τεχνολογιών πρέπει να συνοδεύεται και από ένα ικανοποιητικό επίπεδο ασφαλείας. Το μεγαλύτερο κενό ασφαλείας εντοπίζεται στο Δημόσιο Νέφος όπου η χρήση των εικονικών μηχανών, της παρακολούθησής τους, της υποστήριξης του ενδιάμεσου εξοπλισμού κτλ., ενέχει κινδύνους που αφορούν στην αλληλεπίδραση μεταξύ τους αλλά και στο καθένα ξεχωριστά όσον αφορά στην ασφάλεια της χρήσης του. Το γεγονός ότι το Υπολογιστικό Νέφος είναι ένα περιβάλλον που δύναται να εξυπηρετήσει πολλούς χρήστες παράλληλα, το καθιστά τρομερά ευάλωτο σε επιθέσεις κάνοντας επιτακτική την ανάγκη της αναγνώρισης του πλαισίου επιθέσεων και της εφαρμογής αποτελεσματικών μηχανισμών ασφαλείας.

2.2 Ζητήματα ασφάλειας του μοντέλου *SaaS*

Το μοντέλο SaaS παρέχει στο χρήστη τη δυνατότητα να χρησιμοποιεί απομακρυσμένα εφαρμογές, και να έχει πρόσβαση στο κέντρο δεδομένων ενός τρίτου μέρους. Σε αυτό το μοντέλο ο πάροχος έχει τον απόλυτο έλεγχο και του λογισμικού αλλά και του υλικού τμήματος. Ο πάροχος λοιπόν έχει την ευθύνη να εξασφαλίσει την ασφάλεια και την ιδιωτικότητα των χρηστών. Στο επίπεδο SaaS οι εφαρμογές ελκύουν τους υποψήφιους κακόβουλους χρήστες ώστε να εκδηλώσουν επίθεση αφού είναι διαχειρίσιμες μέσω του Διαδικτύου και επίσης χρησιμοποιούνται από πολλούς χρήστες. Πιθανές επιθέσεις που μπορεί να εκδηλωθούν σε αυτό το μοντέλο ανάπτυξης είναι :

- Injection Επιθέσεις όπως SQL injection (SQLi) Cross-site Scripting (XSS) την εισαγωγή δηλαδή ενός κακόβουλου προγράμματος.
- Broken authentication and session management όπου έχουμε παραβίαση των κωδικών πρόσβασης ή παράκαμψη τους με αποτέλεσμα να παραβιάζεται ο λογαριασμός του χρήστη και να αποκτάται ο έλεγχος από τον κακόβουλο χρήστη.
- Sensitive data exposure το οποίο αφορά στην διαρροή των ευαίσθητων δεδομένων.
- Χρήση εργαλείων αλλά και APIs των οποίων οι ευπάθειες είναι γνωστές επομένως δεν είναι ασφαλής η χρήση τους με αποτέλεσμα να μην είναι ασφαλής ούτε η χρήση των εφαρμογών.[27]

Σίγουρα θα πρέπει να ληφθούν μέτρα από τον πάροχο ώστε να εξασφαλισθεί η ακεραιότητα και διαθεσιμότητα των εφαρμογών αλλά και των δεδομένων των χρηστών. Η χρήση κρυπτογραφικών μεθόδων, διαπιστευτηρίων, τείχους προστασίας κ.α. αποτελούν τρόπους ενίσχυσης της ασφάλειας του επιπέδου αυτού. Φυσικά πολύ σημαντικό κομμάτι αποτελεί η προστασία των δεδομένων. Και βέβαια η ασφάλεια αποτελεί ευθύνη του παρόχου αλλά πως μπορεί ο χρήστης να εμπιστευτεί τον πάροχο από τη στιγμή που δεν γνωρίζει π.χ. τις εγκαταστάσεις και φυσικά την τοποθεσία τους, την υλική υποδομή, αλλά και την τοποθεσία των βάσεων δεδομένων. Ζητήματα τρωτότητας προκύπτουν και με τα κέντρα δεδομένων του παρόχου, τα οποία για μείωση του κόστους βρίσκονται συνήθως σε τοποθεσίες οι οποίες δεν παρέχουν ασφάλεια, αλλά και λόγω του γεγονότος ότι αποθηκεύονται τα δεδομένα όλων των χρηστών ανεξάρτητα από το αν είναι ευαίσθητα ή όχι, στην ίδια βάση δεδομένων, με αποτέλεσμα να καθίσταται εύκολη η παραβίαση τους. Η εφαρμογή των κατάλληλων μέτρων ασφάλειας είναι

αποκλειστική ευθύνη του παρόχου. Ενώ ο χρήστης δεν είναι σε θέση ούτε να πραγματοποιήσει οποιαδήποτε ενέργεια, αλλά ούτε και γνωρίζει τις ενέργειες του παρόχου όσον αφορά στην ασφάλεια. Ο χρήστης ευθύνεται κυρίως για την ασφάλεια του περιηγητή (Browser), για την αυθεντικοποίηση και την εξουσιοδότηση. Για να προστατευθεί ο χρήστης εφαρμόζονται κανονισμοί με τους οποίους ο πάροχος είναι υποχρεωμένος να αποθηκεύει τα δεδομένα σε τοποθεσίες οι οποίες διέπονται από νομικό πλαίσιο, ώστε να διασφαλίζεται ένα ελάχιστο επίπεδο ιδιωτικότητας. Επίσης υπάρχει κανονισμός που διασφαλίζει με χρηματική εγγύηση ότι σε περίπτωση οποιασδήποτε δυσλειτουργίας με ευθύνη του παρόχου τα δεδομένα δεν θα απωλεσθούν αλλά θα είναι στη διάθεση του χρήστη (ISO 27001, SSAE-16, Directive 95/46/ec κτλ.). Για να γνωρίζει ο χρήστης λοιπόν το επίπεδο ασφάλειας που του προσφέρεται, είναι απαραίτητη η σύναψη Συμφωνιών Επιπέδου Παροχής Υπηρεσιών (SLA). [15, 16]

2.3 Ζητήματα ασφάλειας του μοντέλου *PaaS*

Το μοντέλο *PaaS* δίνει τη δυνατότητα χρήσης αλλά και ανάπτυξης εφαρμογών από τον ίδιο το χρήστη μέσω της πλατφόρμας που διαθέτει ο πάροχος και χωρίς να απαιτείται να αποκτήσει και να παραμετροποιήσει τους απαιτούμενους πόρους είτε δικτυακούς είτε αποθηκευτικούς. Ο πάροχος είναι υπεύθυνος για το λογισμικό που διατίθεται στο χρήστη αλλά και για το λογισμικό που είναι απαραίτητο για την πραγματοποίηση της διασύνδεσης των εφαρμογών, των βάσεων δεδομένων και του λειτουργικού συστήματος καθώς επίσης και για την εικονοποίηση (Virtualization). Η χρήση των εικονικών μηχανών αποτελεί ένα σημαντικό παράγοντα για την ανάπτυξη των εφαρμογών, αλλά και ιδιαίτερα ευαίσθητο σε κακόβουλες επιθέσεις. Δίνεται η δυνατότητα στους χάκερ να δημιουργήσουν κακόβουλο λογισμικό και να επηρεάσουν τις εφαρμογές. Επομένως προκύπτει η ανάγκη προστασίας αυτών των εφαρμογών από οποιαδήποτε παράνομη ενέργεια (όπως αναδρομολόγηση, παραχώρηση δικαιωμάτων, προστασία κωδικών και προσωπικών στοιχείων του χρήστη κτλ) ώστε να εξασφαλιστεί η αδιάκοπη παροχή των υπηρεσιών και φυσικά να προστατευθούν και τα δεδομένα. Αφού λοιπόν τον έλεγχο τον έχει ο πάροχος, από αυτόν εξαρτάται να εξασφαλίσει αξιόπιστες και ασφαλείς συνδέσεις, καθώς επίσης και να διατηρήσει την απομόνωση μεταξύ των εφαρμογών, των δεδομένων και των λογισμικών διαφορετικών χρηστών. Ο πάροχος οφείλει να εφαρμόζει διεργασίες ελέγχου όπως ελέγχους παραβίασης του συστήματος, ελέγχους διαχείρισης της βάσης δεδομένων κτλ. Όπως και να προσφέρει υπηρεσίες διαχείρισης λογισμικού, ελέγχους συντήρησης σε όλο το κύκλο ανάπτυξης των εφαρμογών δηλαδή το πλαίσιο των εργασιών που πρέπει να ολοκληρωθούν σε

κάθε στάδιο ανάπτυξης των εφαρμογών και αυτό να παραμετροποιείται ανάλογα με τις ανάγκες που προκύπτουν. Σε αυτό το μοντέλο σημαντικό ρόλο για την ασφάλεια κατέχει η κρυπτογράφηση των επικοινωνιών. Επίσης πολύ σημαντικός είναι ο έλεγχος αυθεντικοποίησης και ταυτοποίησης.[20]

2.4 Ζητήματα ασφάλειας του μοντέλου *IaaS*

Σε αυτό το μοντέλο έχουμε τη διάθεση των υπολογιστικών πόρων στον χρήστη (διακομιστές, δικτυακό εξοπλισμό, αποθήκευση και εικονικές μηχανές) από τον πάροχο, ο οποίος ουσιαστικά ελέγχει και διαμοιράζει τους πόρους σε πολλούς χρήστες. Ο χρήστης χρησιμοποιεί τους διαθέσιμους πόρους για την εκτέλεση των εφαρμογών, έχοντας την δυνατότητα να επιλέξει το λειτουργικό σύστημα που επιθυμεί, τις βάσεις δεδομένων, το ενδιάμεσο λογισμικό (middleware) κ.τ.λ. Παρέχεται βασική ασφάλεια σε αυτό το μοντέλο όπως τείχος προστασίας, αλλά αυτό δεν είναι αρκετό για την ασφάλεια των εφαρμογών. Σημαντικό κομμάτι είναι η προστασία της φυσικής ασφάλειας των υποδομών, από βλάβη ή δολιοφθορά, που αφορά όχι μόνο στον εξοπλισμό αλλά και στο κανάλι διακίνησης των δεδομένων και των εντολών. Ο πάροχος έχει τους δικούς του μηχανισμούς επίβλεψης των διαδικασιών και των ελέγχων που αφορούν στις τεχνολογίες που παρέχονται ώστε να παρακολουθεί οποιαδήποτε μη εξουσιοδοτημένη αλλαγή ή ενέργεια.. Δεν έχει την ίδια δυνατότητα εφαρμογής ελέγχων ο χρήστης, ο οποίος δεν γνωρίζει άλλωστε την υποδομή που διαθέτει ο πάροχος, και περιορίζεται στο να λάβει γνώση των αναφορών ελέγχου του παρόχου με εξαίρεση τα ιδιωτικά κέντρα δεδομένων. Οι ευπάθειες εδώ αφορούν κυρίως στην ασφάλεια των εικονικών μηχανών. Η ασφάλεια των εικονικών μηχανών αναφέρεται στην ασφάλεια των στιγμιotypών των εικονικών μηχανών, τα οποία να σημειωθεί ότι ακόμα και όταν είναι κλειστά (Offline) υπάρχει κίνδυνος να εισαχθεί σε αυτά κακόβουλο λογισμικό ή να κλαπεί το VM αρχείο. Ευπάθειες εμφανίζονται στο εικονικό δίκτυο αφού κατά την επικοινωνία του κεντρικού VM(Hypervisor) με τις υπόλοιπες εικονικές μηχανές, μπορεί να εισαχθεί κακόβουλο λογισμικό, για αυτό είναι πολύ σημαντική η ασφάλεια του Hypervisor ο οποίος ελέγχει την πρόσβαση των εικονικών μηχανών στους φυσικούς πόρους. Άλλη ευπάθεια είναι η αξιοπιστία των δεδομένων που είναι αποθηκευμένα στις υποδομές του παρόχου, το δικτυακό κομμάτι, τη χρήση των εικονικών μηχανών, την ανάκτηση των δεδομένων και τις εφαρμογές (Cross-Site Scripting (XSS), SQL injections, Dos επιθέσεις) επομένως είναι απαραίτητο να υπάρχει προστασία με ευθύνη του παρόχου, ο οποίος θα πρέπει να ελέγχει τη δημιουργία και χρήση των εικονικών μηχανών διασφαλίζοντας έτσι

την αποφυγή της μη επιθυμητής πρόσβασης σε ευαίσθητα δεδομένα, επίθεση από κακόβουλο λογισμικό ή ακόμα και την διακίνηση των δεδομένων μέσω κακόβουλου καναλιού. [14, 16]

2.5 Ασφάλεια Δεδομένων

Η ασφάλεια των δεδομένων είναι ένα πολυσύνθετο ζήτημα, αφού αφορά σε όλες τις διαδικασίες χειρισμού τους όπως την προέλευση, την αποθήκευση, την χρήση, την αρχειοθέτηση, την ανάκτηση ακόμα και την καταστροφή τους. Για αυτό το λόγο δεν αρκεί μόνο να εφοδιαστούμε με προϊόντα λογισμικού που προστατεύουν τα δεδομένα αλλά κρίνεται απαραίτητο να εφαρμοσθεί και μία πολιτική ασφάλειας των δεδομένων, ώστε να καλύψει τις ανάγκες ασφαλείας κυρίως κατά τη μεταφορά και την αποθήκευση των δεδομένων. Τα δεδομένα αποτελούν το βασικό στοιχείο για το οποίο ο χρήστης επιθυμεί να εξασφαλίσει ότι δεν θα απολέσει την *Εμπιστευτικότητα*, την *Ακεραιότητα* και τη *Διαθεσιμότητα* των δεδομένων. Οι τρεις αυτές αρχές αφορούν στα εξής :

Ακεραιότητα των δεδομένων σημαίνει ότι η πληροφορία δεν έχει παραποιηθεί, δεν έχει διαγραφεί ή δεν είναι προσβάσιμη από κανένα μη εξουσιοδοτημένο χρήστη.

Η *Εμπιστευτικότητα* των δεδομένων αναφέρεται στην εξασφάλιση της ιδιωτικότητας δηλαδή την βεβαιότητα ότι κανείς δεν έχει μη εξουσιοδοτημένη πρόσβαση στα ευαίσθητα δεδομένα του χρήστη. Τα προβλήματα έγκειται κυρίως στην μη επαρκή κρυπτογράφηση τους πχ στα επίπεδα SaaS και PaaS στα οποία πολλές φορές δεν γίνεται κρυπτογράφηση των δεδομένων, με την οποία μεν διασφαλίζεται η των δεδομένων, αλλά αυξάνει το κόστος χρήσης του Νέφους και καθιστά αδύνατη την επεξεργασία, δεικτοδότηση ή την ταξινόμηση τους. Βέβαια, σημαντικό ρόλο έχει και το πρωτόκολλο που χρησιμοποιείται ειδικά για τη μετακίνηση των δεδομένων αφού ένα μη ασφαλές πρωτόκολλο θέτει σε κίνδυνο την των δεδομένων, δηλαδή την παραποίηση ή ακόμα και την περίπτωση της απώλειας των δεδομένων χωρίς να υπάρχει η δυνατότητα ανάκτησης τους. Η απώλεια δεδομένων μπορεί να είναι είτε εσκεμμένη στην περίπτωση της κακόβουλης πράξης είτε να οφείλεται σε μη σκόπιμη ενέργεια όπως στην περίπτωση διαγραφής δεδομένων από λάθος ή λόγω βλάβης σε κάποιο υλικό (π.χ. σε διακομιστή). Θέματα ασφαλείας των δεδομένων εγείρονται όσον αφορά και στην τοποθεσία αποθήκευσης τους, αλλά και στο ποιος έχει τον έλεγχο των δεδομένων και βέβαια πόσο ασφαλής είναι η διακίνηση τους. [28]

Η τοποθεσία αποθήκευσης των δεδομένων είναι καταληκτικός παράγοντας για την ασφάλεια των δεδομένων λόγω του διαφορετικού νομικού πλαισίου που ισχύει από χώρα σε χώρα, το

οποίο έχει άμεση επίπτωση στους μηχανισμούς ασφαλείας που εφαρμόζονται αν εφαρμόζονται. Μη γνωρίζοντας λοιπόν που είναι αποθηκευμένα τα δεδομένα, εγείρονται πολλά ερωτήματα σχετικά με το αν είναι κρυπτογραφημένα ή όχι, στην περίπτωση που είναι κρυπτογραφημένα ποιος αλγόριθμος κρυπτογράφησης έχει εφαρμοσθεί, πόσο αποτελεσματικός είναι, ποιος διαχειρίζεται τα κλειδιά κρυπτογράφησης, και βέβαια αν είναι ασφαλές το κανάλι μεταφοράς των δεδομένων. Βέβαια θα πρέπει να επισημανθεί ότι λόγω της χρήσης της τεχνολογίας της ει-κονοποίησης πολλές φορές και ο ίδιος ο πάροχος δεν γνωρίζει που βρίσκονται τα δεδομένα κάποια δεδομένη στιγμή, και φυσικά αναφερόμαστε και στην τοποθεσία αλλά και όσον αφο-ρά στο φυσικό μέρος (μηχάνημα). Πρόβλημα για την ασφάλεια αποτελεί και το γεγονός ότι τα δεδομένα δεν είναι απομονωμένα δηλαδή ο πάροχος στην ίδια βάση δεδομένων αποθηκε-ύει τα δεδομένα διαφορετικών χρηστών, γεγονός που εκθέτει σε κίνδυνο όλα τα δεδομένα που βρίσκονται στην ίδια βάση δεδομένων, στην περίπτωση που υπάρξει στόχευση κάποιων δεδομένων από κακόβουλη επίθεση. Στο επίπεδο SaaS η απομόνωση λαμβάνει χώρα για μετα-φορές που γίνονται στην ίδια διεργασία από διαφορετικούς χρήστες με διαφορετικά δεδομένα. Στο επίπεδο PaaS η απομόνωση αφορά στις εκτελέσιμες υπηρεσίες και στα API. Στο επίπε-δο IaaS η απομόνωση αφορά στις διαδικασίες των εικονικών μηχανών επεξεργασίας, μνήμης, αποθήκευσης και στα δίκτυα. Επειδή ο πάροχος διαχειρίζεται τα δεδομένα, επίθεση μπορεί να εκδηλωθεί και από εσωτερικούς παράγοντες πχ από το προσωπικό, αφού συνήθως δεν υπάρχουν προϋποθέσεις επιλογής του από τον πάροχο, οπότε είναι εύκολο κάποιος από το προσωπικό να πραγματοποιήσει δολιοφθορά είτε μεταποιώντας τα δεδομένα , σβήνοντας τα ή ακόμα και πουλώντας τα σε ανταγωνιστές. Επικίνδυνη είναι επίσης η δυνατότητα ανάκτησης δεδομένων που σβήστηκαν αλλά και η χρήση των μεταδاتا από τον πάροχο ή από τρίτο μέρος που διαχειρίζεται τα δεδομένα, κυρίως στο δημόσιο Νέφος. Είναι πολύ σημαντικό όσον αφορά στα metadata να γνωρίζει ο χρήστης ποια είναι η πολιτική διαχείρισης τους από τον πάροχο δηλαδή ποια metadata διατηρεί ο πάροχος ή το τρίτο μέρος, πως τα ασφαρίζει και τι πρόσβαση σε αυτά έχει ο ίδιος ο χρήστης. Είναι σημαντικό να διασφαλίζεται η προστασία της ακεραι-ότητας, της αξιοπιστίας και της εμπιστευτικότητας των δεδομένων προστατεύοντας τα από μη εξουσιοδοτημένη πρόσβαση. Ο χρήστης μπορεί να εκτιμήσει το επίπεδο ασφάλειας που του παρέχεται ελέγχοντας την πολιτική διαχείρισης των δεδομένων, τα εργαλεία που χρησιμοποιο-ύνται από τον πάροχο ή και τα σχόλια που γίνονται σχετικά με το επίπεδο ασφάλειας. [31, 43] Η χρήση των εικονικών ιδιωτικών δικτύων (VPN) μπορεί να συμβάλλει στην ασφάλεια των δεδομένων, κυρίως κατά τη διαδικασία της μετακίνησης τους, χρησιμοποιώντας το δημόσιο δίκτυο για τη δημιουργία, μέσα σε αυτό, μίας ασφαλούς σύνδεσης με κρυπτογράφηση και τε-ίχος προστασίας. Υπάρχουν βέβαια αδυναμίες που μπορεί να εκμεταλλευτεί ο κακόβουλος

επιτιθέμενος. Μία αδυναμία είναι ο αριθμός των host διακομιστών που χρησιμοποιούνται, όσο πιο μεγάλος είναι ο αριθμός τόσο πιο ευάλωτο είναι το δίκτυο στην μη εξουσιοδοτημένη πρόσβαση και έλεγχο των δεδομένων. Ουσιαστικά, υπάρχει παρακολούθηση της κίνησης των δεδομένων αλλά μετά την αποκρυπτογράφηση τους και όχι σε όλη τη διαδρομή τους, με αποτέλεσμα αν σε κάποιο σημείο του δικτύου γίνει παρέμβαση κακόβουλης κίνησης τότε όλο το δίκτυο έχει ουσιαστικά παραβιαστεί. Κάτι αντίστοιχο αποτελεί και η σύνδεση δύο δικτύων τα οποία δεν έχουν το ίδιο επίπεδο ασφαλείας. Με τη χρήση του πρωτοκόλου (service-to-host SSH, SSL) γίνεται εφαρμογή της παρακολούθησης του δικτύου και των ελέγχων ασφαλείας σε όλη την έκταση του περιορίζοντας αρκετά τις ευπάθειες.[33]

2.6 Ασφάλεια Δικτύου

Σημαντικό κομμάτι το οποίο είναι ευθύνη του παρόχου είναι η ασφάλεια του δικτύου. Μέσω του ίδιου δικτύου μετακινούνται τα πακέτα δεδομένων που αφορούν σε ευαίσθητα δεδομένα αλλά και πακέτα με λιγότερο σημαντικά δεδομένα. Αυτό έχει σαν αποτέλεσμα δεδομένα από ασφαλή σημεία να αναμιγνύονται με δεδομένα από μη ασφαλείς εφαρμογές και βέβαια ο διαχωρισμός των πακέτων γίνεται εικονικά αλλά πρακτικά αυτά κινούνται μέσω του ίδιου φυσικού καναλιού. Φυσικά, είναι δύσκολο να δημιουργηθεί ένα ιδιωτικό φυσικό δίκτυο όπως επίσης παρακινδυνευμένο να υπάρχει εμπιστοσύνη στον διαχειριστή του εικονικού δικτύου. Ίσως η λύση να υπάρχει στην κρυπτογράφηση των πακέτων σε όλη τη διαδρομή τους, αλλά και πάλι υπάρχει πρόβλημα γιατί θα πρέπει να υπάρχει και μισθωμένη γραμμή οπότε πλέον η δομή του παίρνει την κλασική μορφή ενός παραδοσιακού δικτύου. Ο πάροχος οφείλει να πραγματοποιεί ελέγχους διεύθυνσης στο δίκτυο, να πραγματοποιεί ανάλυση πακέτων, να αναγνωρίζει αδυναμίες διαχείρισης κτλ. Υποχρεούται για να υπάρχει ένα ικανοποιητικό επίπεδο ασφαλείας να χρησιμοποιεί τεχνικές κρυπτογράφησης της κίνησης του δικτύου (Secure Socket layer (SSL)) και ροής των δεδομένων (Transport Layer Security (TLS)), να χρησιμοποιεί ασφαλή πρωτόκολλα, να ελέγχει την εγκυρότητα των διαπιστευτηρίων και να διασφαλίσει ότι θα υπάρχει απομόνωση μεταξύ των διεργασιών των διαφορετικών χρηστών. Μία απειλή που αφορά στο δίκτυο είναι η Man in middle επίθεση όπου ο επιτιθέμενος επικοινωνεί με τον χρήστη μέσω μιας ανεξάρτητης σύνδεσης την οποία και ελέγχει έχοντας μη εξουσιοδοτημένη πρόσβαση σε VLANs και υποδίκτυα που μοιράζονται το ίδιο φυσικό εξοπλισμό [7]

Μία σύνηθης απειλή που αφορά στο δίκτυο είναι η XML Signature (Wrapping) Επίθεση, με την οποία ο επιτιθέμενος εισάγει κακόβουλο λογισμικό στη δομή των ανταλλασόμενων

μηνυμάτων SOAP (Simple Object Access Protocol) χωρίς να επιδρά στην υπογραφή του μηνύματος, με αποτέλεσμα να φαίνονται σαν αυθεντικά αφού διατηρούν την ίδια υπογραφή αλλά έχει παραποιηθεί το περιεχόμενο του μηνύματος. [25]

Μία ακόμη απειλή η οποία στοχεύει να πλήξει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων είναι το IP ,ARP Spoofing, το οποίο αποτελεί το έναυσμα για διάφορες επιθέσεις όπως man-in-the-middle (MitM), distributed denial of service (DDoS), ARP and DNS poisoning επιθέσεις. Η επίθεση αυτή εκδηλώνεται με την παραποίηση της διεύθυνσης πηγής του IP πακέτου. Είναι δύσκολο να γίνει αντιληπτή γιατί πολλές φορές η διαδικασία παραποίησης της διεύθυνσης πηγής χρησιμοποιείται π.χ. από διαγνωστικά εργαλεία δικτύου, έλεγχος φορτίου κ.τ.λ. , τα οποία και αποτελούν νόμιμες διαδικασίες. Οπότε συνήθως η επίθεση αυτή γίνεται αντιληπτή εκ του αποτελέσματος. [26]

Άλλη επίθεση είναι το Flooding, η οποία ουσιαστικά οδηγεί σε επίθεση DDoS (Distributed Denial of Service) αφού με την αποστολή μεγάλου αριθμού πακέτων στο δίκτυο οι πόροι δεν επαρκούν οπότε δεν είναι διαθέσιμες οι εφαρμογές ή τα δίκτυα. Πολλή κρίσιμη επίθεση είναι η Malware Injection, με την οποία ο επιτιθέμενος δημιουργεί το δικό του μοντέλο εφαρμογής υπηρεσιών, με στόχο να ξεγελάσει το χρήστη ώστε να χρησιμοποιήσει το κακόβουλο μοντέλο και είτε να υποκλέψει ή να παραποιήσει τα δεδομένα, ή να αποκτήσει πρόσβαση στους λογαριασμούς του χρήστη, είτε να του μπλοκάρει την παροχή υπηρεσιών. [18]

2.7 Διαχείριση Ταυτότητας (Identity Management)

Η Διαχείριση ταυτότητας (Identity Management) ουσιαστικά αναλαμβάνει να ελέγξει την πρόσβαση στα δεδομένα και στις εφαρμογές μέσω της ταυτοποίησης και αυθεντικοποίησης. Στην περίπτωση που η διαχείριση ταυτοποίησης και αυθεντικοποίησης είναι αδύναμη είναι πολύ εύκολο να παραβιαστούν οι κωδικοί του χρήστη με αποτέλεσμα να μην προστατεύεται αποτελεσματικά ο λογαριασμός του. Αφού υπάρχει αλληλεπίδραση μεταξύ διαφορετικών συσκευών, εφαρμογών, υπηρεσιών αλλά και ιδιοκτητών είναι απαραίτητο η διαχείριση ταυτοποίησης και αυθεντικοποίησης να περιλαμβάνει διαδικασίες κωδικοποίησης και κρυπτογράφησης για την πρόσβαση. Η ασφάλεια του λειτουργικού συστήματος στο επίπεδο IaaS δεν είναι ευθύνη του παρόχου αλλά του χρήστη, ενώ στο PaaS έχει ευθύνη ο πάροχος να φροντίσει για την ασφάλεια του λειτουργικού συστήματος και της πλατφόρμας ενώ στο επίπεδο των εφαρμογών η ασφάλεια είναι ευθύνη του χρήστη. Βέβαια αυτό έχει σαν αποτέλεσμα ο χρήστης για κάθε υπηρεσία που χρησιμοποιεί να έχει διαφορετικούς κωδικούς πρόσβασης, το οποίο φυ-

σικά εγχυμονεί κινδύνους διαρροής. Αυτό λύνεται με τη διαχείριση ταυτότητας με την οποία απλοποιείται η διαδικασία πρόσβασης, δίνοντας τη δυνατότητα στο χρήστη με τη χρήση ενός κωδικού να είναι δυνατή η πρόσβαση του σε μια σειρά από υπηρεσίες (Single sign-on (SSO)). Με μία αποτελεσματική διαχείριση ταυτότητας διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων ενώ απώλεια της διαθεσιμότητας έχουμε μόνο στην περίπτωση που έχουμε απώλεια των δεδομένων ή δεν είναι δυνατή η προσπέλαση τους. Άλλα ζητήματα που σχετίζονται με την μη αποτελεσματική Διαχείριση Ταυτότητας είναι οι επιθέσεις DoS (Denial of Service), XML επιθέσεις σε ιστοσελίδες κ.α.[7]

2.8 Web Application Security

Στο Υπολογιστικό Νέφος οι υπολογιστικοί πόροι βρίσκονται σε απομακρυσμένη τοποθεσία και ο χρήστης τους χειρίζεται απομακρυσμένα μέσω του διαδικτύου και απομακρυσμένα έχει πρόσβαση στις εφαρμογές. Οι εφαρμογές είναι ουσιαστικά προγράμματα τα οποία απαιτούν σύνδεση με το διαδίκτυο και τη χρήση κάποιου Web Browser για την διαχείριση και την εκτέλεση τους. Οι εφαρμογές είναι ευπαθείς γιατί ο ρυθμός ανάπτυξης τους είναι πολύ ταχύς ώστε να είναι δύσκολο να αντιμετωπισθούν και κυρίως να εντοπισθούν τα κενά ασφαλείας που τυχόν υπάρχουν. Κενά ασφαλείας που στοχεύουν να πλήξουν την αρχή της Αυθεντικοποίησης με την παραβίαση των διαπιστευτηρίων του χρήστη, και αποκτώντας μη εξουσιοδοτημένη πρόσβαση. Οι συνηθέστερες επιθέσεις είναι οι εξής Cross-Site Scripting, SQL Injection, Insufficient Transport Layer Protection, Fingerprinting και HTTP Response Splitting και αφορούν ουσιαστικά στην εισαγωγή κακόβουλου λογισμικού σε Ιστοσελίδες οι οποίες δεν είναι ύποπτες ή σε βάσεις δεδομένων με στόχο την πρόσβαση, την παραποίηση ή τη διαγραφή των δεδομένων του χρήστη.[44, 41]

Οι ευπάθειες των εφαρμογών αφορούν κυρίως στο επίπεδο SaaS, και επειδή υπάρχει πολυμορφία στον καθορισμό των παραμέτρων ασφαλείας λόγω των πολλών χρηστών, ενδείκνυται ο πάροχος να διεξάγει τακτικούς ελέγχους για την αξιολόγηση των επιθέσεων, και στη συνέχεια της διαχείρισης και εφαρμογής κανόνων ασφαλείας. [16]

2.9 Ευπάθειες του Υπολογιστικού Νέφους

Ευπάθεια είναι μία αδυναμία του συστήματος την οποία εκμεταλεύεται ο κακόβουλος χρήστης ώστε να εκδηλώσει επίθεση. Τα Cloud Computing συστήματα όπως έχει αναφερθεί χαρα-

κτηρίζονται από την πολυχρηστικότητα (multi-tenancy), των διαμοιρασμού των πόρων μέσα σε ένα εικονικό περιβάλλον στοιχεία που το κάνουν αρκετά ελκυστικό για την εκδήλωση επιθέσεων. Βασικός άξονας για την υιοθέτηση του Cloud Computing είναι η ασφάλεια και η ιδιωτικότητα που κυρίως οφείλει ο πάροχος να προσφέρει στους χρήστες, ώστε να αποφευχθεί η περίπτωση της απώλειας των δεδομένων κ.α. Βέβαια και οι χρήστες έχουν το δικό τους μερίδιο ευθύνης στη διατήρηση της ασφάλειας και της ιδιωτικότητας. Καθίσταται λοιπόν απαραίτητο να υπάρχει μεταξύ παρόχου και χρήστη μια συμφωνία για το επίπεδο των παρεχόμενων υπηρεσιών ώστε να είναι σαφές στο χρήστη τι ενέργειες πραγματοποιεί ο πάροχος, τι μπορεί να κάνει ο χρήστης για να επιδιώξει το επιθυμητό επίπεδο ασφάλειας.[5, 30]

Οι περισσότερες ευπάθειες οφείλονται σε τρύπες ασφαλείας που δημιουργούνται λόγω των πολλών και διαφορετικών τεχνολογιών που χρησιμοποιούνται, σε ανθρώπινα λάθη, και εφαρμογή μη επαρκών πολιτικών ασφαλείας. Οι ευπάθειες στο επίπεδο SaaS σχετίζονται με τα δεδομένα των χρηστών, τις Web εφαρμογές αλλά και τις Service-Oriented Architecture (SOA) εφαρμογές. Η ασφάλεια σε αυτό το επίπεδο είναι αποκλειστικά ευθύνη του παρόχου, ο οποίος θα πρέπει να διεξάγει ελέγχους των βάσεων δεδομένων, αλλά και να φροντίσει να υπάρχουν αντίγραφα ασφαλείας των δεδομένων.[27]

Οι ευπάθειες που σχετίζονται με την απώλεια των δεδομένων, συνήθως επηρεάζουν το επίπεδο IaaS, και μπορεί να είναι είτε φυσικές καταστροφές, ανθρώπινο λάθος, αστοχία εξοπλισμού ή και κακόβουλη επίθεση. Ευπάθεια θεωρείται και η επιλογή του προσωπικού του παρόχου αφού τα κριτήρια επιλογής του συνήθως είναι αμφίβολα. Είναι δύσκολο να αποκαλυφθεί ότι γίνεται επίθεση εκ των έσω, αφού το προσωπικό διατηρεί αυξημένα δικαιώματα πρόσβασης οπότε είναι πολύ εύκολο να πραγματοποιήσει την επίθεση. Η επίθεση εκ των έσω επηρεάζει και τα τρία επίπεδα SaaS, PaaS, και IaaS, και μπορεί να προκληθεί από προσωπικό το οποίο δεν εργάζεται πλέον σε αυτό τον πάροχο, ή από προσωπικό που έχει αυξημένα δικαιώματα πρόσβασης (πχ διαχειριστής), ή από τρίτο μέρος που συνεργάζεται με τον πάροχο. Ευπάθειες στη διαχείριση κλειδιού, σε ιούς του λειτουργικού συστήματος, μη ασφαλή δικτυακά πρωτόκολλα, μη ενημερωμένο λογισμικό επηρεάζουν και τα τρία επίπεδα. Μόνο τα επίπεδα PaaS και IaaS επηρεάζονται από τις ευπάθειες της εικονοποίησης και του λογισμικού που παρέχεται από τρίτο μέρος. Μία συνηθισμένη ευπάθεια είναι το δικαίωμα πρόσβασης, δηλαδή η δημιουργία λογαριασμού και η απόκτηση κωδικών. Βέβαια στο Cloud υπάρχει η περίπτωση να εκδηλωθεί παραβίαση ασφαλείας εκ των έσω αφού πολλές φορές παρατηρείται υπάλληλοι να έχουν δικαιώματα νόμιμης πρόσβασης σε ευαίσθητα δεδομένα, οπότε δεν είναι εύκολος ο εντοπισμός τους. Άλλη μία ευπάθεια είναι η ευρεία χρήση της τεχνολογίας της εικονοποίησης, η οποία να μεν προσφέρει πολλά στην παροχή υπηρεσιών αλλά ταυτόχρονα αποτελεί πονοκέφαλο όσον αφορά

στην ασφάλεια αφού διακομιστές, δικτυακός και αποθηκευτικός εξοπλισμός λειτουργούν σε ει-
κονικό περιβάλλον, οπότε είναι αρκετό κάποιος έχοντας πρόσβαση στο επίπεδο εικονοποίησης
να ελέγξει αρκετούς υπολογιστικούς πόρους ώστε να δημιουργήσει μια χαοτική κατάσταση
στην ασφάλεια. Το χαρακτηριστικό της πολυχρηστικότητας που διακρίνει το Cloud αποτελεί
άλλο ένα παράγοντα ευπάθειας για παραβίαση. Η απεικόνιση της διακίνησης των δεδομένων
γίνεται στο σημείο πρόσβασης και όχι καταγραφή των εισερχομένων και εξερχομένων όπως
συμβαίνει στα παραδοσιακά συστήματα. Αυτό αποτελεί πρόβλημα γιατί μία κίνηση μπορεί να
καταγραφεί ως εχθρική ενώ δεν είναι, επομένως είναι σημαντικό το σύστημα να είναι ασφαλές
στο σημείο πρόσβασης. Επίσης λόγω του διαμοιρασμού των υπολογιστικών πόρων μεταξύ
πολλών διαφορετικών χρηστών, υπάρχουν και διαφορετικές απαιτήσεις σε υποδομή αλλά και
σε υπηρεσίες και κατ' επέκταση διαφορετικές απαιτήσεις στο επιθυμητό επίπεδο ασφαλείας
επομένως δύσκολα ο πάροχος να ικανοποιήσει τις απαιτήσεις ασφαλείας μεμονωμένα του κάθε
χρήστη. Επομένως είναι χρήσιμο να υπάρχουν μηχανισμοί απομόνωσης ώστε να μην αφορά
όλους τους χρήστες η οποιαδήποτε αστοχία ορθής λειτουργίας.[21]

Η απώλεια διακυβέρνησης αποτελεί άλλη μία ευπάθεια. Η κατάσταση είναι περίπλοκη γιατί
ο πάροχος είναι επιφορτισμένος με κάποιες αρμοδιότητες όσον αφορά στην ασφάλεια αλλά
πολλές φορές δεν είναι σαφές ποιες είναι ακριβώς αυτές οι αρμοδιότητες. Έτσι κρίνεται απα-
ραίτητο να υπάρξει ένα συμφωνητικό παροχής υπηρεσιών (Service-Level Agreements (SLA))
με το οποίο θα αντιμετωπισθεί ως ένα βαθμό αυτό το πρόβλημα. Άλλο ένα πρόβλημα είναι
η δυσκολία του χρήστη να αλλάξει τον πάροχο, δεν υπάρχει δηλαδή φορητότητα. Επειδή ο
κάθε πάροχος διαθέτει τη δική του πλατφόρμα και τα δικά του API αφού δεν υπάρχουν
κοινά πρότυπα και πρωτόκολλα ανάπτυξης τους, πολλές φορές είναι δύσκολο ο χρήστης να
αλλάξει πάροχο και να μπορεί να μεταφέρει τα δεδομένα του από τον ένα πάροχο στον άλλο.
Και φυσικά υπάρχει το ενδεχόμενο ο πάροχος να διακόψει τη διάθεση των υπηρεσιών του με
αποτέλεσμα να χαθούν τα δεδομένα.[27, 30, 34]

2.10 Απειλές στο Υπολογιστικό Νέφος

Οι ευπάθειες των μηχανισμών πρόσβασης, οι ευπάθειες του τείχους προστασίας ή των διακομι-
στών που σχετίζονται με την διαχείριση ταυτοποίησης, η υποκλοπή των κωδικών πρόσβασης
του χρήστη επιτρέπουν την εκδήλωση απειλών στο Υπολογιστικό Νέφος. Εξετάζοντας το
Υπολογιστικό Νέφος από τη σκοπιά της Ασφάλειας, θα μπορούσαμε να παρατηρήσουμε ότι
η σχεδίαση του ελκύει την παραβατικότητα. Τα ζητήματα ασφαλείας που απορρέουν από τις

υπηρεσίες του Cloud, και η περίπτωση που η υποδομή δεν είναι αρκετά ασφαλής, δημιουργούν ευπάθειες που μεταφέρονται στο Υπολογιστικό Νέφος. Την ευθύνη αντιμετώπισης των ζητημάτων ασφαλείας την έχει κατά κύριο λόγο ο πάροχος, ο οποίος αποφασίζει με ποιον τρόπο θα τα αντιμετωπίσει. Επειδή ακόμα η ανάπτυξη του είναι σε εξέλιξη και δεν έχουν ορισθεί τα κατάλληλα πρότυπα, πολλές παρεχόμενες υπηρεσίες δεν συνοδεύονται από το αναγκαίο πλαίσιο ασφάλειας και ελέγχου, με αποτέλεσμα να έχουν υψηλό βαθμό ευπάθειας σε όλων των ειδών τις επιθέσεις και παραβιάσεις. Άλλος ένας λόγος είναι πως ενώ οι πάροχοι συνήθως παρέχουν υψηλού επιπέδου περιμετρική ασφάλεια, εναπόκεινται στους δημιουργούς του λογισμικού να εφαρμόσουν την πολιτική ασφαλείας που υπάρχει διαθέσιμη για την θωράκιση των εφαρμογών και υπηρεσιών όπως να κρυπτογραφήσουν τα δεδομένα, να διαχειριστούν τα κλειδιά, να εφαρμόσουν κωδικούς πρόσβασης ασφαλείς κτλ.[6]

Γενικά τα θέματα που εγείρονται αφορούν στην διατήρηση της Εμπιστευτικότητας για τα ευαίσθητα δεδομένα (ιατρικά στοιχεία, οικονομικά στοιχεία, προσωπικά στοιχεία, εταιρικά στοιχεία κτλ), στην προστασία από επιθέσεις εκ των έσω, η επίτευξη απομόνωσης μέσα στο πολυχρηστικό περιβάλλον του Cloud, η παρουσία μηχανισμών ασφαλείας για τους διακομιστές. Οι απειλές σχετίζονται με τις παραβιάσεις ή την απώλεια των δεδομένων, την επίθεση εκ των έσω, DoS, ευπαθή συστήματα και APIs, μη επαρκής διαχείριση ταυτοποίησης και αυθεντικοποίησης κτλ. Ας δούμε όμως αναλυτικά τις απειλές που υπάρχουν σήμερα:

- Παραβιάσεις ή Απώλεια δεδομένων: Η παραβίαση των δεδομένων αποτελεί την πρώτη απειλή και τον μεγαλύτερο πονοκέφαλο για τους παρόχους, αφού μία μη εξουσιοδοτημένη οντότητα αποκτά πρόσβαση σε ευαίσθητα δεδομένα τα οποία και μπορεί να διαχειριστεί όπως επιθυμεί (αντιγραφή, διαγραφή, παραποίηση). Πολλοί είναι αυτοί που επιθυμούν να παραβιάσουν ευαίσθητα δεδομένα όπως εμπορικοί ανταγωνιστές, άλλοι που επιθυμούν να πλήξουν σε προσωπικό επίπεδο ή εταιρικό κτλ. Οι παραβιάσεις δεδομένων μπορεί να γίνουν είτε από σκόπιμη ενέργεια, λόγω ευπαθειών των εφαρμογών, από κάποιο λάθος αλλά και από ελλιπή εφαρμογή κανόνων ασφαλείας. Η πιθανότητα να γίνει παραβίαση των δεδομένων αυξάνει ανάλογα με το βαθμό εξάρτησης της ασφαλείας από τον πάροχο. Όταν έχουμε απώλεια δεδομένων, τότε τα δεδομένα δεν είναι διαθέσιμα ή είναι παραποιημένα. Αιτίες που μπορεί να συμβεί αυτό είναι από αστοχία-βλάβη του εξοπλισμού, από σκόπιμη κακόβουλη ενέργεια ή από λανθασμένη ενέργεια που οδήγησε στη διαγραφή τους. [32]
- Εσωτερικοί εχθροί: Ίσως θα μπορούσε να χαρακτηριστεί ως καταστροφική απειλή. Μία εσωτερική απειλή μπορεί να επιφέρει καταστροφικό πλήγμα, αφού πλήττει την Ακεραι-

ότητα, την Εμπιστευτικότητα και την Διαθεσιμότητα των πληροφοριών των χρηστών. Συνήθως η επίθεση γίνεται από κάποιον υπάλληλο ή κάποιο συνétaίρο ο οποίος έχει πρόσβαση στα φυσικά μηχανήματα. Βέβαια ποιο εύκολο είναι η επίθεση να γίνει από το διαχειριστή του συστήματος ο οποίος γνωρίζει την τοπολογία του συστήματος, έχει πρόσβαση στον εξοπλισμό (πχ διακομιστές κτλ.) του κέντρου δεδομένων και συνεπώς έχει τη δυνατότητα πρόσβασης σε ευαίσθητες πληροφορίες . Είναι πολύ δύσκολο να ανιχνευθεί αυτή η επίθεση κι αυτό γιατί ο εισβολέας εγκαθιστά ένα ροοτκιτ σε έναν υπολογιστή μόλις αποκτήσει πρόσβαση σε επίπεδο διαχειριστή, το οποίο δεν ανιχνεύεται με τις τυπικές σαρώσεις αφού αυτές πραγματοποιούνται σε σύστημα το οποίο είναι διαμορφωμένο από το ροοτκιτ, το οποίο έχει τη δυνατότητα να παραπλανά τα αντιϊικά προγράμματα.[35]

- Άρνηση Υπηρεσίας (Denial of Service): Οι επιθέσεις αυτές είναι πολύ διαδεδομένες λόγω των πολλών συσκευών και υπολογιστικών συστημάτων με τα οποία κάποιος μπορεί να συνδεθεί, οπότε δημιουργούνται είτε δυσλειτουργίες στο σύστημα είτε δεν λειτουργεί καθόλου. Η επίθεση αυτή στοχεύει στην μείωση της Διαθεσιμότητας δηλαδή ο χρήστης χάνει τη δυνατότητα πρόσβασης είτε στα δεδομένα του είτε στις εφαρμογές. Η επίθεση αυτή επιτυγχάνεται προκαλώντας μεγάλη κατανάλωση των υπολογιστικών πόρων(πχ. Ισχύ επεξεργαστή, μνήμη, αποθηκευτικό χώρο και εύρος δικτύου) με αποτέλεσμα το σύστημα να γίνεται αργό και να μην ανταπεξέρχεται στις απαιτήσεις των χρηστών. Άλλη μία μορφή αυτής της επίθεσης είναι η κατανεμημένη άρνηση υπηρεσίας (DDoS) με την οποία ουσιαστικά γίνεται επίθεση σε υπηρεσία του Νέφους, κερδίζοντας τον έλεγχο κάποιων συστημάτων τα οποία χρησιμοποιούνται ως ζόμπι (botnet) και στέλνουν ψεύτικα μηνύματα φορτώνοντας την κίνηση του δικτύου, δημιουργώντας κομπούζιο αφού οι διακομιστές και το δίκτυο δεν λειτουργούν και κατ' επέκταση προκαλώντας άρνηση της πρόσβασης σε υπηρεσίες, και τη μη διαθεσιμότητα των δεδομένων, ή ακόμα και των πόρων στους χρήστες. [18]
- Ευαίσθητα συστήματα και APIs: Το λειτουργικό σύστημα και κυρίως τα στοιχεία του όπως τα εργαλεία εφαρμογών, το επίπεδο PaaS αλλά και στο επίπεδο IaaS παρουσιάζουν πολλές ευπάθειες τις οποίες εκμεταλλεύονται οι κακόβουλοι χρήστες. Πολύ συχνά οι πάροχοι για να μην επιβαρύνονται τα ίδια μηχανήματα αλλά και για να γίνεται καλύτερη κατανομή του φορτίου αντιγράφουν τη μνήμη των εικονικών μηχανών αλλά και το λειτουργικό και τα μεταφέρουν σε άλλα μηχανήματα. Κατά τη διάρκεια αυτής της μεταφοράς είναι ευάλωτο το σύστημα και το εκμεταλλεύεται ένας κακόβουλος χρήστης.

Επίσης ευπάθειες παρουσιάζουν τα APIs (Application Programming Interfaces) τα οποία αποτελούν τον τρόπο επικοινωνίας του χρήστη με την πλατφόρμα του παρόχου, και μέσω της αλληλεπίδρασης με αυτά ο χρήστης διαχειρίζεται τις υπηρεσίες του Νέφους. Ο κακόβουλος χρήστης μπορεί να κλέψει και να χρησιμοποιήσει τα διαπιστευτήρια του χρήστη ή να παραπλανήσει το χρήστη να χρησιμοποιήσει μια κακόβουλη εφαρμογή. Επειδή λοιπόν αποτελούν το δίαυλο επικοινωνίας με τις υπηρεσίες του Νέφους, είναι πολύ σημαντικός παράγοντας η ασφάλεια και επομένως ο σχεδιασμός τους πρέπει να περιλαμβάνει την προστασία από κακόβουλες πράξεις ή ακόμα και από λάθη.

- **Αδύναμη Διαχείριση Ταυτοποίησης και Αυθεντικοποίησης:** Σημαντικός παράγοντας ενίσχυσης της ασφάλειας είναι ο έλεγχος πρόσβασης. Ένας αδύναμος έλεγχος πρόσβασης όπως χρήση συνθηματικού πολύ απλού, ή η χρήση του ίδιου κλειδιού κρυπτογράφησης χωρίς να εφαρμόζεται η ανανέωση του, ή ακόμα και η διάθεση των κρυπτογραφικών κλειδιών μέσω δημοσίων αποθετηρίων, υποδηλώνει ότι τα συστήματα διαχείρισης πρόσβασης δεν είναι αποτελεσματικά και επομένως το σύστημα είναι ευαίσθητο σε επιθέσεις όπως η παραβίαση δεδομένων. Σε περιπτώσεις που η διαχείριση ταυτότητας και αυθεντικοποίησης δεν είναι ισχυρή είναι πολύ εύκολο οι κακόβουλοι χρήστες να αποκτήσουν πρόσβαση στο σύστημα και να έχουν πρόσβαση στα δεδομένα του χρήστη και να τα διαχειριστούν όπως επιθυμούν δηλαδή να τα διαβάσουν, να τα τροποποιήσουν ή ακόμα και να τα διαγράψουν, να υποκλέψουν τα δεδομένα κατά τη μεταφορά τους και φυσικά να εισχωρήσουν στο σύστημα κακόβουλο λογισμικό, τα οποία βέβαια μπορούν να αποβούν καταστροφικά για το χρήστη.
- **Απώλεια ελέγχου του λογαριασμού:** Στην περίπτωση που ο κακόβουλος χρήστης κλέψει τα διαπιστευτήρια ενός λογαριασμού, αποκτά πλέον τον έλεγχο του και μπορεί να παρακολουθεί την κίνηση του, να χειρίζεται τα δεδομένα οπότε πολύ πιθανόν να τα παραποιήσει, να επηρεάζει τις παρεχόμενες υπηρεσίες και όλα αυτά με στόχο να πλήξει κυρίως την εικόνα ενός χρήστη. Πλήττεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των προσφερόμενων υπηρεσιών.
- **Διαμοιρασμός Τεχνολογιών:** Ένα χαρακτηριστικό του Υπολογιστικού Νέφους είναι ο διαμοιρασμός των υπολογιστικών πόρων, των πλατφορμών και των υπηρεσιών. Η πολυποικιλότητα που διακρίνει το Υπολογιστικό Νέφος στο διαμοιρασμό πόρων, εφαρμογών και συστημάτων τα οποία έχουν διαφορετικό επίπεδο και διαφορετικές απαιτήσεις ασφάλειας, έχει σαν αποτέλεσμα να επηρεάζονται όλοι οι χρήστες από την αδυναμία α-

σφάλειας. Οι πάροχοι έχουν επενδύσει στο διαμοιρασμό αλλά δεν το έχουν σχεδιάσει με τέτοιο τρόπο ώστε να υπάρχει απομόνωση μεταξύ των συστατικών με αποτέλεσμα να δημιουργούνται ευπάθειες. Ο κακόβουλος χρήστης έχει τη δυνατότητα να πλήξει την ασφάλεια περισσότερων χρηστών αν όχι όλων, λόγω ακριβώς των τεχνολογιών που χρησιμοποιούνται όπως η εικονοποίηση αλλά και της φιλοσοφίας του διαμοιρασμού των τεχνολογιών.

- Έλλειψη λήψης μέτρων: Κατά την υιοθέτηση του Υπολογιστικού Νέφους ίσως το κρίσιμότερο σημείο είναι η σωστή επιλογή του παρόχου. Τα κριτήρια έχουν να κάνουν με το επίπεδο των παρεχόμενων υπηρεσιών και φυσικά με τις τεχνολογίες που διαθέτει αλλά και με την ασφάλεια, δηλαδή αν εφαρμόζει τις σωστές πολιτικές (πχ ISO 9001, DCS, PCI, HIPAA), αν διαθέτει τις κατάλληλες τεχνικές και εργαλεία για την ενίσχυση της ασφάλειας και τον έλεγχο της κατάστασης των πόρων και τους ελέγχους ασφαλείας που απαιτούνται ώστε να περιοριστεί η επικινδυνότητα στο μικρότερο δυνατό βαθμό.
- Δικτυακές επιθέσεις μέσω λογισμικού (APT): Στις δικτυακές επιθέσεις μέσω λογισμικού, ο επιτιθέμενος γίνεται κομμάτι του συστήματος είτε με υποκλοπή των κωδικών πρόσβασης ή έχοντας δικούς του κωδικούς. Στη συνέχεια αποκτώντας πρόσβαση σε κόμβους του δικτύου γίνεται στόχευση των βασικών εικονικών μηχανών του δικτύου ώστε να αποκτηθεί ο έλεγχος του λογισμικού εικονοποίησης του Hypervisor και πλέον ο κακόβουλος χρήστης αποκτά πληροφορίες που του δίνουν τη δυνατότητα να ελέγξει όλο το δίκτυο (φυσικά και εικονικά μηχανήματα). Λόγω ακριβώς της φύσης αυτής της επίθεσης είναι πολύ δύσκολο να ανιχνευθεί. Επηρεάζεται η δρομολόγηση των πακέτων δεδομένων ώστε αυτά να αντιγραφούν και να δρομολογηθούν εκεί που επιθυμεί ο εισβολέας. Οι εισβολείς εισχωρούν στις υπηρεσίες με τεχνικές όπως το phishing, το direct hacking, με κακόβουλο λογισμικό μέσω USB συσκευών, μέσω του δικτύου αλλά και μέσω της χρήσης ευάλωτων APIs.
- Μη ενημερωμένοι χρήστες: Πολλές φορές οι χρήστες θεωρούν ότι η ασφάλεια αποτελεί υποχρέωση του παρόχου και μόνο, με αποτέλεσμα οι ίδιοι να μην κάνουν τίποτα. Ουσιαστικά ο πάροχος ευθύνεται για την ασφάλεια των δεδομένων και γενικά για οτιδήποτε σε σχέση με τις υπηρεσίες για τις οποίες έχει γίνει συμφωνία (Service Level Agreement (SLA)). Οι χρήστες δεν εξετάζουν πως και πόσο μπορούν και οι ίδιοι να συμβάλλουν στην ενίσχυση της ασφάλειας. Ο χρήστης όμως ευθύνεται για την ασφάλεια του περιηγητή (Browser) , για την Αυθεντικοποίηση και την Εξουσιοδότηση.

- Ανθρώπινο λάθος: Ο πιο απρόβλεπτος παράγοντας για την ασφάλεια είναι ο ανθρώπινος παράγοντας, το ανθρώπινο λάθος. Για αυτό θα πρέπει να γίνεται εκπαίδευση και να πιστοποιείται σχετικά με την ασφάλεια ώστε να εφαρμόζονται οι απαραίτητες πολιτικές και πρότυπα.
- Ransomware : Μία άλλη απειλή είναι το ransomware, κατά την οποία κλειδώνονται τα αρχεία και οι πόροι στο σύστημα του χρήστη και δεν μπορεί να τα χρησιμοποιήσει. Ο χρήστης βρίσκεται στο έλεος του επιτιθέμενου να του δώσει τον κωδικό έναντι βέβαια κάποιας αμοιβής. Αυτός ο ιός μπορεί να εισέλθει μέσω των email, μέσω video, μέσω αρχείου PDF ή μέσω κάποιας ιστοσελίδας, μέσω μιας άλλης συσκευής.
- Επίθεση μονόπλευρου καναλιού: Αυτή η επίθεση εκμεταλλεύεται τις ευπάθειες από τη χρήση της εικονοποίησης, δηλαδή την ανυπαρξία απομόνωσης μεταξύ των εφαρμογών. Ο εισβολέας δημιουργεί ένα εικονικό μηχανήμα μέσα στο φυσικό μηχανήμα του χρήστη και μέσω του διαμοιρασμού του συστήματος αποσπά τα δεδομένα του χρήστη. Οπότε έχοντας και τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης στο σύστημα μέσω κακόβουλου λογισμικού, ο επιτιθέμενος μπορεί να έχει πρόσβαση στις πληροφορίες του συστήματος του χρήστη, όπως πληροφορίες που αφορούν τους διακομιστές, αλλά και στα δεδομένα του.
- Φωλιασμένη εικονοποίηση: Σε αυτή την επίθεση ουσιαστικά ανάμεσα στον Hypervisor του συστήματος και τον φυσικό εξοπλισμό ο εισβολέας παρεμβάλλει ένα μη εξουσιοδοτημένο Hypervisor ώστε να παραβιάσει τα ευαίσθητα δεδομένα και κωδικούς πρόσβασης. Ο Hypervisor είναι υπεύθυνος να παρέχει για τις εικονικές μηχανές την εικονική μνήμη όπως και τις πολιτικές που αφορούν στη CPU, επομένως στην περίπτωση που αυτή η επίθεση είναι πετυχημένη ο εισβολέας έχει πρόσβαση και στο σύστημα δηλαδή στη μνήμη ή σε άλλους υπολογιστικούς πόρους, χωρίς αυτό να προκαλεί δυσλειτουργία στο σύστημα οπότε και δεν γίνεται αντιληπτό από τον Hypervisor. Εκμεταλλεύεται την απουσία αμοιβαίων μηχανισμών αυθεντικοποίησης των δύο μερών δηλαδή του παρόχου και του χρήστη.[27, 29, 33, 36, 37]
- Καταχρηστική και παράνομη χρήση του Υπολογιστικού Νέφους: Χαρακτηριστικό του Υπολογιστικού Νέφους είναι η ψευδαίσθηση των ανεξάντλητων πόρων , που πολλές φορές συνοδεύεται από μία απλή διαδικασία καταχώρησης ώστε να μπορεί ο χρήστης να χρησιμοποιήσει τις υπηρεσίες του Νέφους. Πάνω σε αυτή την απλοϊκή καταχώρηση βρίσκουν καταφύγιο οι αποστολές ανεπιθύμητης αλληλογραφίας, οι δημιουργοί κα-

κόβουλου λογισμικού και άλλοι κακόβουλοι. Τα προβλήματα αυτά υπήρχαν παραδοσιακά στο μοντέλο PaaS, αλλά τώρα φαίνεται πως επεκτείνονται και στο μοντέλο IaaS, δημιουργώντας θέματα όπως σπάσιμο του κωδικού πρόσβασης, DDoS, εκκίνηση δυναμικών σημείων επίθεσης, φιλοξενία μολυσμένων δεδομένων, εντολή και έλεγχος βοτνετ. Τα παραπάνω μπορούν να περιοριστούν ή και να εξαλειφθούν με την εφαρμογή αυστηρότερης καταχώρησης και επικύρωσης εγγραφής των χρηστών, με ενίσχυση της παρακολούθησης πληρωμής με πιστωτικές κάρτες, με παρακολούθηση της κίνησης του δικτύου.[8]

Κεφάλαιο 3

Στρατηγικές Ασφάλειας Υπολογιστικού Νέφους

3.1 Στρατηγικές Ασφάλειας των Δεδομένων

ΓΙΑ την αντιμετώπιση των ζητημάτων ασφαλείας του περιβάλλοντος του Υπολογιστικού Νέφους είναι απαραίτητη η ανάπτυξη μηχανισμών προστασίας των φυσικών εγκαταστάσεων, του δικτύου, των υπολογιστικών πόρων αλλά και του λογισμικού. Αρχικά σημαντικό βήμα αποτελεί η ασφάλεια των δεδομένων. Φυσικά θα πρέπει να ακολουθούνται τα πρότυπα προστασίας των δεδομένων όπως το ISO27001 και ειδικότερα για την παροχή και χρήση των Υπηρεσιών του Υπολογιστικού Νέφους ισχύει το ISO27017, το οποίο ουσιαστικά προσθέτει τριάντα επτά ελέγχους ασφαλείας και επτά πρόσθετους ελέγχους που αφορούν στις υπηρεσίες του Νέφους, ενδεικτικά αναφέρονται ο διαχωρισμός αρμοδιοτήτων και υποχρεώσεων για το χρήστη και τον πάροχο, παρακολούθηση των υπηρεσιών Νέφους, διαχωρισμός και ενίσχυση της ασφαλείας των εικονικών μηχανών.[76] Το Υπολογιστικό Νέφος χρησιμοποιεί πολλές τεχνολογίες και η σημαντικότερη από αυτές είναι η εικονοποίηση. Για να είναι ασφαλής η χρήση των εικονικών μηχανών και να αντιμετωπιστούν οι ευπάθειες από τη χρήση τους, απαιτείται η προμήθεια και των απαραίτητων πρόσθετων εργαλείων. Επίσης άλλοι παράγοντες που πρέπει να ληφθούν υπόψη είναι η δυνατότητα φορητότητας αλλά και η ανάκτηση δεδομένων. Η φορητότητα αποτελεί ένα παράγοντα που ενισχύει την ασφάλεια αφού ο χρήστης μπορεί να αλλάξει πάροχο χωρίς να κινδυνεύει να χάσει τα δεδομένα του. Και η ανάκτηση δεδομένων επίσης αποτελεί ένα πολύ σημαντικό παράγοντα ενίσχυσης της

ασφάλειας του Υπολογιστικού Νέφους αφού εξασφαλίζεται η απρόσκοπτη λειτουργία του συστήματος γεγονός που εξασφαλίζει την αξιοπιστία του συστήματος και επομένως τη συνεχή διάθεση των υπηρεσιών και των δεδομένων στο χρήστη. Σημαντικό επίσης είναι να υπάρχουν μηχανισμοί παρακολούθησης του δικτύου ώστε σε περίπτωση που υπάρχει εισβολέας να γίνει αντιληπτό. Οι πάροχοι βέβαια θα πρέπει να ενημερώνουν τους χρήστες στην περίπτωση που υπάρξει κάποιο συμβάν παραβίασης ώστε να ληφθούν πιο εντατικά μέτρα όπως ενεργοποίηση τείχους προστασίας, η υιοθέτηση εργαλείων εισαγωγής στις εφαρμογές (application logging tools) κλπ. Επομένως οφείλει ο πάροχος να έχει μηχανισμούς επαρκούς ανταπόκρισης σε περιπτώσεις παραβίασης αλλά και να εφαρμόζει τεχνικές ελέγχου των περιστατικών παραβίασης ώστε να διαπιστωθεί γιατί συνέβησαν και να αντιμετωπισθούν οι αδυναμίες. Η υιοθέτηση του Υπολογιστικού Νέφους απαιτεί την εφαρμογή μιας καλά ορισμένης στρατηγικής. Οι βασικές στρατηγικές ασφάλειας στο Υπολογιστικό Νέφος βασίζονται στην κεντριοποίηση, στην εφαρμογή προτύπων και στην αυτοματοποίηση.

3.2 Κεντριοποίηση

Η φιλοσοφία της Κεντριοποίησης ουσιαστικά είναι ότι υπάρχει ένας κεντρικός διακομιστής ο οποίος έχει περισσότερους υπολογιστικούς πόρους από τους εξυπηρετούμενους χρήστες, και μέσω αυτού γίνονται όλες οι ενέργειες που αφορούν στην ασφάλεια. Από ένα κεντρικό σημείο λοιπόν ενεργοποιούνται οι μηχανισμοί ασφαλείας και ξεκινάνε οι έλεγχοι ασφαλείας, οι διαδικασίες, οι υπηρεσίες και οι πολιτικές που θα εφαρμοσθούν και βέβαια με αυτή την αρχιτεκτονική παρακολουθείται όλο το δίκτυο. Αυτό είναι και το πλεονέκτημα όσον αφορά στην ασφάλεια, αλλά και πάλι πρέπει να επισημανθεί ότι στη διαχείριση της ασφάλειας υπάρχουν πρόβλήματα πχ. στο διαμοιρασμό των κλειδιών στους χρήστες ώστε να γίνει η ταυτοποίηση και αυθεντικοποίηση τους για να έχουν πρόσβαση στις υπηρεσίες και τις εφαρμογές του Νέφους. Επιπρόσθετα, υπάρχουν κάποιες ενέργειες βασικές που σαν σύνολο αποτελούν στρατηγική, οι η προστασία, ο εντοπισμός και η πρόληψη. Η προστασία περιλαμβάνει τους ελέγχους ασφαλείας, τις πολιτικές ασφαλείας και τις διαδικασίες που απαιτούνται για την προστασία από παραβιάσεις. Ο εντοπισμός αφορά σε μια προληπτική διαδικασία μελέτης του συστήματος ενεργοποιώντας γεγονότα, μελετώντας τα μητρώα κινήσεων και ανακαλύπτοντας πιθανές ευπάθειες του συστήματος. Στην περίπτωση που κατά τη διαδικασία του εντοπισμού υπάρχει ένδειξη ευπάθειας ή παραβίασης τότε λαμβάνονται μέτρα ώστε να περιοριστεί το πρόβλημα. Αυτό αποτελεί πολύ σημαντικό βήμα διατήρησης της ασφάλειας αρκεί να γίνουν οι απαραίτητοι

έλεγχοι σε καίρια σημεία όπως η κρυπτογράφηση, τα API, η ασφάλεια του Ιστού, η διαχείριση των κλειδιών ασφάλειας, τα μητρώα κινήσεων, η εφαρμογή των πολιτικών.[6, 38]

3.3 Προτυποποίηση

Η Προτυποποίηση αφορά σίγουρα στην εφαρμογή λύσεων σχετικών με την ασφάλεια, βελτιώνει την απόδοση, ενισχύει την συμβατότητα όπου ο χρήστης θα μπορεί με ευκολία να συνεργάζεται με διαφορετικούς παρόχους αφού διασφαλίζεται η συμβατότητα των προϊόντων, των υπηρεσιών αλλά και των διαφόρων στοιχείων που είναι διαθέσιμα και βελτιώνει την διαχείριση των δεδομένων του καθώς και την αξιοπιστία και τη σταθερότητα αφού θα καθορίζεται το νομικό πλαίσιο που θα τον καλύπτει. Σκοπός είναι μέσω της εφαρμογής των προτύπων να διασφαλίζεται η διαθεσιμότητα των υπηρεσιών. Έτσι το 2009 δημιουργήθηκε ο Διεθνής Οργανισμός Προτυποποίησης (International Organization for Standardization (ISO)) ο οποίος έχει την ευθύνη για την ανάπτυξη διαφόρων προτύπων για τη διευκόλυνση των συναλλαγών μεταξύ των κρατών της Ευρωπαϊκής Ένωσης. Κάθε πάροχος στην Ευρωπαϊκή Ένωση πιστοποιείται μέσω αυτού του οργανισμού ότι ακολουθεί την προτυποποίηση σχετικά με τη διαχείριση των δεδομένων και την ασφάλεια τους. Με την προτυποποίηση έχει δημιουργηθεί ένα κλίμα ομαλής συνεργασίας αφού έχει διευκολυνθεί η επικοινωνία, το εμπόριο αλλά και η εμπιστοσύνη μεταξύ όλων των παραγόντων (χρηστών, παρόχων, κράτους). Έχει δημιουργηθεί η υποεπιτροπή προτυποποίησης ISO/IEC JTC 1/SC 38 Cloud Computing and Distributed Platforms η οποία αφορά στο Υπολογιστικό Νέφος, και προωθεί την προτυποποίηση σε τρεις τομείς :

- Βασικές έννοιες και τεχνολογίες
- Λειτουργικά Θέματα και
- Αλληλεπιδράσεις μεταξύ των συστημάτων Υπολογιστικού Νέφους και άλλων καταναμεμένων συστημάτων

Ειδικά αφορά στην Υπηρεσιοκεντρική Αρχιτεκτονική (Service Oriented Architecture (SOA)) , στις Συμφωνίες Επιπέδου Υπηρεσιών (SLA), στη Λειτουργικότητα και Φορητότητα αλλά και στα δεδομένα και στην διακίνηση τους. [46][47] [48] Τα πρότυπα ISO/IEC 18384 του 2016 αφορούν στην Αρχιτεκτονική του SOA. Το ISO/IEC 18384-1 αναφέρεται στους όρους και έννοιες του SOA, το ISO/IEC 18384-2 αναφέρεται στην αντιμετώπιση των προβλημάτων

του, και τέλος το ISO/IEC 18384-3 αναφέρεται στην υπόσταση του SOA. Για τις Συμφωνίες Επιπέδου Υπηρεσιών (SLA) στο Υπολογιστικό Νέφος υπάρχει το πρότυπο ISO/IEC 19086. Οι Συμφωνίες Επιπέδου Υπηρεσιών του Νέφους (Service Level Agreements (SLAs)) αποτελούν μία σημαντική συνιστώσα του συμβολαίου για τις παρεχόμενες υπηρεσίες με σκοπό να πραγματοποιηθεί μία συμφωνία της οποίας οι όροι θα είναι εφικτοί, μετρήσιμοι, ουσιαστικοί και φυσικά αποδεκτοί και από τα δύο μέρη δηλαδή τον πάροχο και το χρήστη. Το SLA είναι μία συμφωνία μεταξύ του παρόχου και του χρήστη με την οποία ορίζεται το επίπεδο υπηρεσιών που επιθυμεί ο χρήστης και που παρέχει ο πάροχος. Τα SLA στο Νέφος είναι περίπλοκα ειδικά στην περίπτωση που σε μία υπηρεσία εμπλέκονται πολλοί πάροχοι. Το πρώτο βήμα για τη σύνταξη του SLA είναι ο καθορισμός των προσδοκιών του χρήστη. Όσο πιο δυνατό είναι το SLA, τόσο μεγαλύτερο είναι το κόστος της διαχείρισης και συντήρησης του. Η κρισιμότητα της υπηρεσίας είναι ο παράγοντας που καθορίζει τα SLA δηλαδή για υπηρεσίες όπως e-banking οι κακές υπηρεσίες είναι πρόβλημα γιατί απαιτούνται δυνατά SLA. Το Νέφος παρέχει πολλές διαφορετικές υπηρεσίες, διαφορετικά μοντέλα ανάπτυξης επομένως διαφορετικές απαιτήσεις σε κάθε Συμφωνία Επιπέδου Υπηρεσιών (SLA) άρα περίπλοκος τρόπος ολοκλήρωσης των συμφωνιών. Η ορολογία που διέπει τις συμφωνίες διαφέρει μεταξύ των παρόχων και φυσικά δεν έχει ο χρήστης τη δυνατότητα σύγκρισης του παρεχόμενου επιπέδου υπηρεσιών των παρόχων. Με τη δημιουργία των προτύπων αντιμετωπίζονται τα ζητήματα που αφορούν στα SLA, επιτυγχάνεται η σαφήνεια και ορίζεται το πλαίσιο των SLA που αφορά στις υπηρεσίες του Υπολογιστικού Νέφους και πώς αναπτύσσονται και ποια είναι τα δομικά στοιχεία των Συμφωνιών Επιπέδου Υπηρεσιών. Επίσης στο πρότυπο αποσαφηνίζονται οι όροι που χρησιμοποιούνται στις συμφωνίες ορίζονται οι μετρήσεις αλλά και οι απαιτήσεις που σχετίζονται με τις συμφωνίες των υπηρεσιών του Νέφους. Το πρότυπο ISO/IEC 19086 του 2016 περιλάμβανε τρία μέρη μέχρι το 2019, οπότε και εκδόθηκε το τέταρτο μέρος. Στο πρώτο μέρος γίνεται μια γενική ανασκόπηση και αναφέρονται οι βασικές έννοιες (ορολογία, ορισμοί, έννοιες) του Service Level Agreement (SLA). Ο στόχος είναι να υπάρχει ευελιξία στους όρους του συμβολαίου μεταξύ παρόχου και χρήστη, ώστε η συμφωνία να ικανοποιεί κάθε φορά τις διαφορετικές απαιτήσεις από τις παρεχόμενες υπηρεσίες. Στο δεύτερο μέρος, το οποίο ενημερώθηκε το 2018, αναπτύσσεται το μετρικό μοντέλο, όπου καθιερώνεται η σχετική ορολογία, ορίζεται ένα μοντέλο μετρήσεων και αναφέρονται εφαρμογές του. Ορίζοντας σαφέστερα το μετρικό μοντέλο επιτυγχάνεται η σαφήνεια στην ισχύουσα ορολογία, η δυνατότητα σύγκρισης μεταξύ διαφορετικών μετρικών μοντέλων και η ανάπτυξη μετρικών εργαλείων ώστε να διευκολυνθεί η εφαρμογή των μετρήσεων. Το τρίτο μέρος, το οποίο ενημερώθηκε το 2017, αναφέρεται στην ορολογία και το πλαίσιο που διέπει τις συμφωνίες υπηρεσιών (Service Level

Agreement (SLA)). Ορίζει τις βασικές απαιτήσεις των συμφωνιών επιπέδου υπηρεσιών, με τη μορφή κυρίως οδηγιών και όχι παρέχοντας μία συγκεκριμένη δομή. Το τέταρτο μέρος, το οποίο εκδόθηκε τον Ιανουάριο του 2019, αφορά στην προστασία των ευαίσθητων προσωπικών δεδομένων (Personally Identifiable Information (PII)). Για την εξασφάλιση της αδιάλειπτης διάθεσης των υπηρεσιών καθορίζονται οι στόχοι και τα όρια που πρέπει να πληρεί το επίπεδο υπηρεσιών μέσω των Αντικειμένων Επιπέδου Υπηρεσιών (Service Level Objectives (SLO)) τα οποία είναι σύνολα μεθόδων μετρήσεως και μετρικής κλίμακας, τα οποία σε συνδυασμό με τα Αντικείμενα Ποιότητας Υπηρεσιών (Service Qualitative Objectives (SQO)), καταγράφουν τα μετρήσιμα χαρακτηριστικά που αφορούν στην απόδοση, στην ασφάλεια, στην διαχείριση δεδομένων και τέλος στην προστασία των ευαίσθητων προσωπικών δεδομένων. Δημιουργούνται (Service Level Objectives (SLO)) για κάθε μετρήσιμη παράμετρο όπως την διαθεσιμότητα, το χρόνο απόκρισης, υποστήριξη από τον πάροχο, τη δυνατότητα μετάβασης σε διαφορετικό πάροχο κτλ. Ειδικά για την ασφάλεια, οι μετρήσεις αφορούν στο επίπεδο ασφάλειας που επιθυμεί να έχει ο χρήστης και αυτό που διαθέτει ο πάροχος. Έτσι έχουμε SLO σχετικά με τις εξής παραμέτρους τη Διαθεσιμότητα, Αυθεντικοποίηση και Εξουσιοδότηση, Αναφορά και Διαχείριση των συμβάντων ασφαλείας, Κρυπτογραφία, λογικιν και Παρακολούθηση, Έλεγχος και Επιβεβαίωση ασφαλείας, Διαχείριση Ευπαθειών και τέλος η Διοίκηση. Για κάθε μία από τις παραπάνω παραμέτρους με τα SLO έχουμε τα παρακάτω στοιχεία τα οποία βοηθούν τον χρήστη να επιλέξει τον κατάλληλο πάροχο:

- Διαθεσιμότητα Υπηρεσιών: Αναφέρεται στην Διαθεσιμότητα των Υπηρεσιών, δηλαδή στην απρόσκοπτη διάθεση των υπηρεσιών αλλά και των δεδομένων, το οποίο αποτελεί κομμάτι του ελέγχου ασφαλείας. Είναι χρήσιμο για τον χρήστη να γνωρίζει αυτό το στοιχείο για να επιλέξει τον πάροχο που πληρεί τις απαιτήσεις του.
- Αυθεντικοποίηση και Εξουσιοδότηση: Πολύ σημαντικό στοιχείο για την ασφάλεια αποτελεί ο έλεγχος πρόσβασης ώστε να διασφαλιστεί ότι δεν θα υπάρχει παραβίαση των πληροφοριών του χρήστη από μη εξουσιοδοτημένο άτομο. Βεβαιώνεται ότι μηχανισμοί αυθεντικοποίησης και εξουσιοδότησης διατίθενται από τον πάροχο, διαπιστώνεται το επίπεδο αξιοπιστίας των μηχανισμών αυθεντικοποίησης, περιγράφονται οι μηχανισμοί με τους οποίους προστατεύονται οι κωδικοί του χρήστη και βέβαια αναφέρεται αν η αυθεντικοποίηση πραγματοποιείται και με ποιες τεχνολογίες από τρίτο μέρος για τον πάροχο. Μηχανισμοί πιστοποίησης, εξουσιοδότησης και ασφαλείας που χρησιμοποιούνται συνήθως είναι η εφαρμογή του Συστήματος Ενιαίας Πρόσβασης (single-sign-on(SSO)), η Βιομετρική αυθεντικοποίηση, η πολυπαραμετρική αυθεντικοποίηση, η ανίχνευση ει-

σβολής κτλ. Για την αντιμετώπιση κακόβουλων επιθέσεων πχ. SQL injection. Να επισημανθεί όμως ότι δεν δίνονται πληροφορίες για τον τρόπο που διατίθενται οι μηχανισμοί αυθεντικοποίησης στο χρήστη.[42, 33]

- Αναφορά και Διαχείριση των συμβάντων ασφαλείας: Η δημιουργία ιστορικού συμβάντων παραβίασης, αποτελεί μία πολύ χρήσιμη βάση με την οποία μπορούν να αντιμετωπιστούν οι ευπάθειες. Η ανίχνευση, αναφορά και η διαχείριση των περιστατικών ασφαλείας είναι ευθύνη αποκλειστικά του παρόχου. Βάσει αυτού του ιστορικού γίνονται μετρήσεις για τον αριθμό των περιστατικών παραβίασης που έχουν αναφερθεί στο χρήστη, τον αριθμό των περιστατικών που αξιολογήθηκαν από τον πάροχο και τον χρόνο που απαιτήθηκε από τη στιγμή που έγινε γνωστό το περιστατικό μέχρι την επίλυσή του. Τα αποτελέσματα αποτυπώνονται σε ποσοστιαία κλίμακα, σε αναλογία προς το σύνολο των περιστατικών που λαμβάνουν χώρα σε καθορισμένο χρονικό διάστημα. Τα συμπεράσματα από αυτό το SLO, αποτελούν ένα καλό δείκτη του επιπέδου ασφαλείας που παρέχει ο πάροχος και δίνουν τη δυνατότητα στο χρήστη να κάνει μία καλή συμφωνία με όρους που θα του διασφαλίσουν ότι και θα έχει ενημέρωση αλλά και θα είναι έγκαιρη για τα περιστατικά παραβίασης.[42]
- Κρυπτογράφηση : Για την προστασία των δεδομένων κρίνεται απαραίτητη η κρυπτογράφηση τους, δηλαδή η μεταποίηση τους μέσω ενός αλγορίθμου με στόχο να φαίνεται αλλοιωμένο το περιεχόμενό τους και να αποφευχθεί η παραβίασή τους. Ως ευαίσθητα δεδομένα (personally identifiable information (PII)) θεωρούνται τα προσωπικά στοιχεία, τα ιατρικά δεδομένα, τα οικονομικά δεδομένα. Τα ευαίσθητα δεδομένα πρέπει πάντα να είναι κρυπτογραφημένα, και να χρησιμοποιείται ένα ασφαλές πρωτόκολλο όπως https, sFTP, ή SSL. Βέβαια τα δεδομένα για να είναι ασφαλή πρέπει να είναι κρυπτογραφημένα όχι μόνο κατά τη διακίνηση τους αλλά και κατά την αποθήκευσή τους. Υπάρχουν διάφοροι αλγόριθμοι οι οποίοι δεν είναι όλοι το ίδιο αποτελεσματικοί. Με την πιστοποίηση ελέγχεται πόσο ισχυρός είναι ο αλγόριθμος, πόσο αποτελεσματικό είναι το κρυπτογραφικό υλικό που χρησιμοποιείται και πόσο δυνατό είναι το κλειδί του αλγορίθμου. Τα κλειδιά θα πρέπει να κρυπτογραφούνται πριν την αποθήκευσή τους και σε ένα ασφαλές μέρος με περιορισμένη πρόσβαση. Πολύ σημαντικό για να μην υπάρξει παραβίαση των κλειδιών είναι ανά τακτά χρονικά διαστήματα και με αυτοματοποιημένη διαδικασία να γίνεται αλλαγή τους.[42]
- Σύνδεση και Παρακολούθηση: Η καταγραφή αλλά και η παρακολούθηση κατά τη σύνδε-

ση, της κατάστασης των διακομιστών, των εφαρμογών, του δικτύου, των υπηρεσιών (τα Log Files) κατά τη λειτουργία και χρήση τους αποτελεί ευθύνη του παρόχου. Τα αρχεία Λογ περιέχουν χρήσιμες πληροφορίες για την δραστηριότητα της βάσης δεδομένων, της πρόσβασης του χρήστη, λάθη, πληροφορίες αποσφαλμάτωσης κτλ. Σημαντική είναι η παρακολούθηση και καταγραφή των ενεργειών μέσω των Log αρχείων που σχετίζονται με την ασφάλεια αλλά και την απόδοση των συστημάτων στην πλατφόρμα που διαθέτει ο πάροχος και δρα περισσότερο προληπτικά παρακολουθώντας για ύποπτα μοτίβα που υποδηλώνουν τη πιθανότητα προσπάθειας εισβολής. Υπάρχουν διαθέσιμα εργαλεία ασφάλειας όπως διάφορα API που διαθέτει ο πάροχος (στο μοντέλο PaaS γιατί στο IaaS την ευθύνη για την εγκατάσταση και τον έλεγχο των εργαλείων την έχει ο χρήστης) και τα οποία σχετίζονται με τον εντοπισμό ζητημάτων ασφάλειας όπως την προσπάθεια εισβολής ή την ύπαρξη κακόβουλου λογισμικού στο σύστημα και η παρακολούθηση μέσω αυτών των εργαλείων δίνει πληροφορίες σχετικές με τη δραστηριότητα και επικινδυνότητα του συστήματος. Οι δραστηριότητες που παρακολουθούνται είναι ενδεικτικά η αποτυχημένη σύνδεση επαναλαμβανόμενα, μη εξουσιοδοτημένη σύνδεση, κινήσεις των λογαριασμών, δραστηριότητες σχετικά με ενέργειες που αφορούν στα δεδομένα (διαγραφή, αντιγραφή, προσπέλαση κτλ.), διαθεσιμότητα εφαρμογών κτλ. Οι εγγραφές στα αρχεία καταγραφής Log Files καταδεικνύουν τη χρήση μιας υπηρεσίας από το χρήστη και συμβάλλουν στην ανάλυση των περιστατικών παραβίασης καθώς και μη εύρυθμης λειτουργίας του συστήματος.[42, 46]

- Έλεγχος και Επιβεβαίωση ασφάλειας: Ο έλεγχος είναι η διαδικασία ανασκόπησης των διαδικασιών και ελέγχων ασφαλείας ώστε να υπάρξει διαβεβαίωση ότι το σύστημα είναι συμβατό με τις απαιτήσεις ασφαλείας και τα SLA. Το σχετικό SLO αποτελεί τη πιστοποίηση ότι τα πρότυπα και οι σχετικές οδηγίες έχουν υιοθετηθεί από τον πάροχο, ότι τα πιστοποιητικά που διαθέτει ο πάροχος για τις υπηρεσίες είναι σε ισχύ καθώς και ότι το επίπεδο της αποτελεσματικότητας και της επάρκειας πληρούν τις απαιτήσεις του χρήστη. Αυτοί οι έλεγχοι συμβάλλουν στην ενίσχυση της ασφάλειας.[42]
- Διαχείριση Ευπαθειών: Η Διαχείριση των ευπαθειών είναι μία επαναλαμβανόμενη διαδικασία, με την οποία διαρκώς γίνεται έλεγχος των διαδικασιών με τις οποίες σχετίζεται η επικινδυνότητα ασφάλειας αφού το πεδίο των ευπαθειών και των αδυναμιών είναι τόσο ευμετάβλητο. Οι πληροφορίες σχετικά με τις ευπάθειες πρέπει να λαμβάνονται έγκαιρα ώστε να γίνει η αξιολόγηση των ευπαθειών και να ληφθούν μέτρα για την αντιμετώπιση των κινδύνων. Τα σχετικά με τη Διαχείριση Ευπαθειών SLO δίνουν το ποσοστό

επί τις εκατό των έγκαιρα αντιμετωπίσιμων ευπαθειών, το ποσοστό επί τις εκατό των έγκαιρων αναφορών ευπαθειών για την ενημέρωση του χρήστη και στοιχεία σχετικά με τις αναφορές για την αντιμετώπιση των ευπαθειών όπως το μηχανισμό που χρησιμοποιεί ο πάροχος για να ενημερώσει το χρήστη αλλά και τη συχνότητα των αναφορών.

- **Διοίκηση:** Ουσιαστικά αφορά στη διαχείριση των αλλαγών που λαμβάνουν χώρα στις υπηρεσίες όπως η λειτουργικότητα, οι διεπαφές και οι ενημερώσεις λογισμικού. Πρέπει να υπάρχει μηχανισμός ενημέρωσης του χρήστη για τις επικείμενες αλλαγές και φυσικά η ενημέρωση να γίνεται μέσα σε ένα εύλογο χρονικό διάστημα. Ο χρήστης θα πρέπει να ενημερωθεί σε τι αφορούν αυτές οι αλλαγές πχ. αν είναι λειτουργικές και να υπάρχει και το ποσοστό επί τις εκατό των αναφορών σχετικών με τις έγκαιρες αλλαγές των Υπηρεσιών του Νέφους.[42]

Το πρότυπο που ασχολείται με την διαλειτουργικότητα και τη φορητότητα είναι το ISO/IEC 19941 το οποίο ενημερώθηκε το 2017. Διαλειτουργικότητα είναι η ικανότητα συνεργασίας διαφορετικών συστημάτων ή εφαρμογών, δηλαδή η ανταλλαγή πληροφοριών μεταξύ τους. Πιο ειδικά στο Νέφος η διαλειτουργικότητα είναι περίπλοκη διαδικασία αφού θα πρέπει τα μοντέλα Υπηρεσιών (Δημόσιο, Ιδιωτικό και Υβριδικό) να συνεργαστούν μεταξύ τους παρόλο που έχουν διαφορετικές διεπαφές, τρόπους αυθεντικοποίησης και εξουσιοδότησης, διαμόρφωση κτλ. Η φορητότητα είναι η δυνατότητα μεταφοράς των δεδομένων του χρήστη ή και των εφαρμογών του μεταξύ δύο διαφορετικών Υπηρεσιών αλλά και μεταξύ διαφορετικών παρόχων. Πολύ σημαντική δυνατότητα γιατί δεν δεσμεύεται ο χρήστης να παραμένει σε ένα πάροχο ο οποίος δεν πληρεί τις απαιτήσεις του. Με αυτό το πρότυπο γίνεται προσπάθεια να καθιερωθεί η ορολογία που αφορά στις βασικές έννοιες της διαλειτουργικότητας και της φορητότητας στο Νέφος και ειδικότερα στις υπηρεσίες του Νέφους ώστε ο πάροχος και ο χρήστης να έχουν κοινή βάση αφετηρίας όπου ο ένας θα ορίζει τι προσφέρει και ο άλλος τι ζητά. Προσδιορίζεται η σχέση και η αλληλεπίδραση μεταξύ της διαλειτουργικότητας και της φορητότητας γιατί ενώ αποτελούν δύο διαφορετικούς τομείς ο ένας επηρεάζει τον άλλο. Επίσης να αποσαφηνιστούν ποιες είναι οι ανάγκες των χρηστών, ποια τα ζητήματα που σχετίζονται με τη διαλειτουργικότητα και τη φορητότητα στο Υπολογιστικό Νέφος αλλά και ποια η σχέση με τα άλλα πρότυπα (πχ. το πρότυπο ISO/IEC 19086 (SLA)). [42]

Όπως αναφέρθηκε παραπάνω άλλο ένα βασικό ζήτημα είναι τα δεδομένα και η διακίνηση τους, στο οποίο αναφέρεται το πρότυπο ISO/IEC 19944, το οποίο ενημερώθηκε το 2017. Ο χρήστης πρέπει να γνωρίζει αν ο πάροχος εφαρμόζει τους νόμους και τους κανονισμούς που ισχύουν σχετικά με τη χρήση των διαφόρων τύπων δεδομένων, όπως τα ευαίσθητα προσωπικά

δεδομένα που σχετίζονται άμεσα με το χρήστη αλλά και τα metadata τα οποία σχετίζονται έμμεσα με το χρήστη. Το πρότυπο αυτό ασχολείται με τον ορισμό των βασικών εννοιών και την κατάταξη των δεδομένων σε κατηγορίες, καθώς επίσης και τη μετακίνηση όλων των τύπων δεδομένων μεταξύ των συσκευών, των υπηρεσιών και των χρηστών. Αρχικά, γίνεται μία ανακεφαλαίωση και ορισμός των τύπων σύνδεσης των υπηρεσιών στο Νέφος και των χρηστών μέσω φορητών συσκευών. Αναφέρονται οι συνέπειες της χρήσης των φορητών συσκευών και όχι μόνο. Επίσης επισημαίνεται η σπουδαιότητα της τοποθεσίας που είναι τα δεδομένα, των ζητημάτων των φορητών συσκευών, της ταυτοποίησης, αποσαφηνίζονται οι τύποι των δεδομένων που διακινούνται στο Νέφος έτσι επιδιώκεται να γίνει καλύτερα αντιληπτό στο χρήστη τι σημαίνει η ιδιωτικότητα και εμπιστευτικότητα των δεδομένων του ώστε να κατανοήσει και την αναγκαιότητα της προστασίας τους. Για την ενίσχυση της ασφάλειας εφαρμόζονται μέθοδοι όπως η κρυπτογράφηση, η ταυτοποίηση κτλ. Επίσης πλέον η ασφάλεια παρέχεται ως υπηρεσία και μάλιστα υπάρχουν διαθέσιμα σύνολα υπηρεσιών ασφαλείας τα οποία μπορούν να χρησιμοποιηθούν στις εφαρμογές. Και φυσικά υπάρχουν πολλές μετρήσεις σχετικές με την ασφάλεια (καταχώρηση μητρώου κινήσεων, λαθών, επισημάνσεων, απασφαλμάτωσης δεδομένων κτλ). Τα παραπάνω πρότυπα έχουν εκδοθεί το 2016 και βέβαια είναι σημαντικό να είναι ενημερωμένα σε σχέση με τις ανάγκες και τις συνθήκες που διαμορφώνονται στην αγορά. Να επισημανθεί ότι το 2012 είχε εκδοθεί μόλις ένα πρότυπο ενώ το 2016 πέντε πρότυπα, γεγονός που αποδεικνύει την ανάγκη και την σπουδαιότητα των προτύπων.[42]

Το πρότυπο ISO/IEC TR 23186 του 2018 αναφέρεται στο πλαίσιο επεξεργασίας δεδομένων από πολλαπλές πηγές (multi-sourced δεδομένα) και περιλαμβάνει υποχρεώσεις και ελέγχους σχετικά με τη χρήση των δεδομένων, την προέλευση τους και την ασφάλεια. Το πρότυπο ISO/IEC TR 22678 του 2019 αφορά στις οδηγίες ανάπτυξης πολιτικών. Οι πολιτικές είναι κανόνες που χρησιμοποιούνται για τη διαχείριση της ασφάλειας του συστήματος. Το Υπολογιστικό Νέφος παρέχει στους χρήστες μία πληθώρα υπηρεσιών διαφορετικής βαρύτητας πχ. απλές υπηρεσίες όπως email μέχρι πιο σύνθετες όπως τα κοινωνικά δίκτυα, η μηχανική μάθηση κτλ, επίσης διατίθενται διάφορα κέντρα δεδομένων διαφορετικής αποθηκευτικής χωρητικότητας και ποικίλα τηλεπικοινωνιακά δίκτυα. Επομένως μέσα σε αυτό το πολύμορφο περιβάλλον είναι απαραίτητο να αναπτυχθούν πολιτικές σχετικές με την ανάπτυξη και χρήση όλων των προσφερόμενων συστημάτων και υπηρεσιών. Ορίζονται λοιπόν οι βασικές έννοιες που αφορούν στις πολιτικές και πρακτικές που διαμορφώνονται σύμφωνα με τα διεθνή πρότυπα και ποια είναι αυτά. Οι πολιτικές αποτελούν διαδικασίες οι οποίες μπορούν να αυτοματοποιηθούν ώστε να εξαλειφθεί η πιθανότητα ανθρώπινου λάθους.[42]

Στην Ευρωπαϊκή Ένωση τα προσωπικά δεδομένα σύμφωνα με τον Γενικό Κανονισμό Προ-

στασίας των Δεδομένων (άρθρο 17) δεν απαιτείται να παραμένουν αποθηκευμένα συνεχώς, δίνοντας το δικαίωμα στο χρήστη να τα διαγράψει εφόσον το επιθυμεί. Βέβαια προκύπτει ένα θέμα σχετικά με τα blockchain. Το Blockchain είναι μια νέα τεχνολογία με την οποία μία σειρά δεδομένων ομαδοποιούνται σε χρονικά αριθμημένες συστοιχίες, όπως τα δεδομένα των ιατρικών εξετάσεων. Το ζήτημα είναι πόσο ασφαλής είναι η αποθήκευση αυτών των δεδομένων και των metadata. Για αυτό προτείνεται να αποθηκεύονται σε μία κατακευματισμένη βάση δεδομένων κι όχι μέσα στο blockchain.[19]

Έχουν δημιουργηθεί πρότυπα ασφαλείας τα οποία ενισχύουν την ιδιωτικότητα και την ασφάλεια και είναι εύκολο να εφαρμοσθούν. Το SAML (Security Assertion Markup Language) χρησιμοποιείται κυρίως για την αυθεντικοποίηση, και εξουσιοδότηση ασφαρίζοντας την επικοινωνία μεταξύ δύο μερών. Κάνει χρήση της τεχνολογίας ανταλλαγής δεδομένων XML για να ολοκληρώσει ερωτοαποκρίσεις μέσω των οποίων γίνεται η αυθεντικοποίηση. Άλλη μία μέθοδος είναι το OpenIDOpenID, το οποίο βασίζεται στο σύστημα ενιαίας πρόσβασης single-sign-on (SSO) δηλαδή με τη χρήση ενός κωδικού έχει πρόσβαση σε ένα σύνολο υπηρεσιών. Για την ασφάλεια των επικοινωνιών χρησιμοποιούνται τα πρωτόκολλα SSL/TLS, τα οποία αρχικά κάνουν τη διαδικασία της χειραψίας δηλαδή κανονίζουν τις λεπτομέρειες της σύνδεσης. Στη συνέχεια γίνεται ανταλλαγή των δημόσιων κλειδιών κρυπτογράφησης και τέλος γίνεται η μετάδοση των κρυπτογραφημένων δεδομένων.[33]

3.4 Αυτοματοποίηση

Η επόμενη βασική στρατηγική είναι η αυτοματοποίηση. Βασική στρατηγική αφού με την αυτοματοποίηση πολλές ενέργειες ελέγχου που χρειάζεται να επαναλαμβάνονται γίνονται ρουτίνα που αυτόματα ενεργοποιούνται κάθε φορά. Στο επίπεδο των εφαρμογών το κλειδί της εφαρμογής πολιτικών είναι η αυτοματοποίηση. Στο περιβάλλον IaaS επιτυγχάνεται με скриπτάκια τα οποία περιέχουν συγκεντρωτικά όλες τις πολιτικές ασφαλείας που αφορούν στην πρόσβαση, στην κρυπτογράφηση κτλ. και τα οποία ενημερώνονται για οποιαδήποτε αλλαγή και την εφαρμόζουν με αυτοματοποιημένο τρόπο. Επίσης και οι αναφορές ελέγχου μπορούν να αυτοματοποιηθούν. Η αυτοματοποίηση των ελέγχων είναι μία διαδικασία που ευνοεί και τον πάροχο αλλά και τον χρήστη. Ο πάροχος επωφελείται από αυτή την διαδικασία ώστε να γνωρίζει την απόδοση του συστήματος του και να το βελτιώσει όπου χρειάζεται, και όλο αυτό έχει την ευκαιρία να το κοινωνήσει στους χρήστες ώστε να τον επιλέξουν. Από την άλλη μεριά ο χρήστης, επωφελείται αφού ενώ τον έλεγχο των υπηρεσιών τον έχει ο πάροχος,

με την αυτοματοποίηση των ελέγχων έχει στην διάθεση του την ακτινογραφία των παροχών και εμμέσως υπάρχει διαφάνεια στη σχέση μεταξύ του παρόχου και του χρήστη άρα και μεγαλύτερη εμπιστοσύνη. Με την αυτοματοποίηση των ελέγχων διαπιστώνεται κατά πόσο οι υπηρεσίες που παρέχονται πληρούν τις προϋποθέσεις ασφαλείας που έχουν συμφωνηθεί μεταξύ του χρήστη και του παρόχου. Την αυτοματοποίηση των ελέγχων την αναλαμβάνουν εταιρείες, οι οποίες θέτουν τα κριτήρια που θα εφαρμόσουν για την διεξαγωγή των ελέγχων στο Υπολογιστικό Νέφος. Με τα κριτήρια γίνεται αξιολόγηση της αντιμετώπισης των μειονεκτημάτων του Υπολογιστικού Νέφους, αφού τα κριτήρια εξετάζουν αν εφαρμόζονται τεχνικές σε τακτά διαστήματα που να αντιμετωπίζουν αυτά τα μειονεκτήματα. Ένα τέτοιο παράδειγμα αποτελούν οι συνεχείς ανασκοπήσεις του πηγαίου κώδικα οι οποίες πρέπει να εφαρμόζονται ανά τακτά χρονικά διαστήματα, ώστε να εντοπισθούν πιθανά τρωτά σημεία και ευπάθειες. Θα πρέπει λοιπόν να γίνει έλεγχος αν ο πάροχος εφαρμόζει τις συνεχείς ανασκοπήσεις, γιατί υπάρχει ο κίνδυνος να μην ακολουθεί την διαδικασία προσπαθώντας να αυξήσει το κέρδος του. Με την εφαρμογή ανάλογων κριτηρίων μέσω αυτοματοποιημένης διαδικασίας πραγματοποιείται συνεχής έλεγχος της διαθεσιμότητας και ακεραιότητας των δεδομένων, της τοποθεσίας τους, της ασφαλούς διαχείρισης πρόσβασης και της κρυπτογράφησης των δεδομένων.[46]

Άλλος ένας αυτοματοποιημένος έλεγχος είναι η χρήση αισθητήρα IDS (intrusion detection system) ανίχνευσης εισβολής, το οποίο είναι μία εφαρμογή ή ακόμα και μία φυσική συσκευή η οποία παρακολουθεί τα δίκτυα, τους διακομιστές ή και τα δύο ώστε να διαπιστωθεί αν υπάρχει εισβολή στο σύστημα. Στην ουσία καταχωρεί τα γεγονότα που λαμβάνουν χώρα, ουσιαστικά τα αναγνωρίζει τους δίνει μία ταυτότητα, χωρίς να έχει διαπιστώσει αν αυτά αποτελούν απειλή ή όχι. Γίνεται συλλογή και επεξεργασία των σχετικών με την ασφάλεια πληροφοριών (τύπος απειλής, πηγή, συνέπειες), οι οποίες στη συνέχεια αξιολογούνται και αυτό το υλικό αποτελεί τη βάση για την αναγνώριση και αντιμετώπιση των απειλών και των ευπαθειών.[47]

Η στρατηγική της ανάκτησης των δεδομένων είναι πολύ κρίσιμο σημείο για την αξιοπιστία του συστήματος. Το αντίγραφο ασφαλείας μπορεί να αποθηκευτεί είτε τοπικά το οποίο έχει χαμηλό κόστος και ο χρόνος προσπέλασης είναι μικρός είτε στο Νέφος το οποίο έχει το πλεονέκτημα ότι στη περίπτωση προβλήματος του τοπικού υλικού τα δεδομένα δεν επηρεάζονται. Σημαντική παράμετρος είναι ο χρόνος ανάκτησης (RTO) δηλαδή ο χρόνος που απαιτείται για να επανέλθει το σύστημα στην κανονική λειτουργία του. Η δεύτερη παράμετρος είναι το σημείο ανάκτησης (RPO) δηλαδή το ποσοστό δεδομένων που μπορεί να απωλεσθεί χωρίς να προκληθεί πρόβλημα. Η τρίτη παράμετρος είναι ο υπολογισμός του κόστους αντιμετώπισης μίας τέτοιας κατάστασης καταστροφής. Στο μοντέλο IaaS υπεύθυνος για την αντιμετώπιση μίας κατάστασης καταστροφής είναι ο χρήστης. Μερικές τεχνικές ανάκτησης είναι η δια-

τήρηση αντιγράφων σε ημερήσια βάση σε μία βάση δεδομένων αλλά και σε μία δεύτερη βάση δεδομένων σε διαφορετικό σημείο. Ειδικά για τα ευαίσθητα δεδομένα πρέπει να γίνεται πολύ συχνά η ενημέρωση του αντιγράφου ασφαλείας, και μάλιστα να υποστηρίζεται και από κρυπτογράφηση ώστε να μην υπάρχει κίνδυνος παραβίασης. Μία άλλη τεχνική είναι η χρήση των αυτοματοποιημένων σενιπς με τα οποία δημιουργούνται διακομιστές βάσεων δεδομένων και επιτυγχάνεται η επαναφορά των αντιγράφων. Άλλη μέθοδος είναι να βρίσκεται ο διακομιστής της βάσης δεδομένων πάντα σε λειτουργία παράλληλα με τη κύρια βάση δεδομένων και οι υπόλοιποι διακομιστές είναι απενεργοποιημένοι. Στην περίπτωση προβλήματος ενεργοποιούνται οι υπόλοιποι διακομιστές. Το πλεονέκτημα είναι ότι ο χρόνος ανάκτησης είναι μειωμένος αφού δεν απαιτείται ανάκτηση της βάσης δεδομένων.[6]

3.5 Στρατηγικές Προστασίας των Δεδομένων

Η προστασία των δεδομένων αλλά και των εφαρμογών θα πρέπει να οχυρωθεί πολύπλευρα. Το περιβάλλον της εικονοποίησης σίγουρα είναι ευάλωτο, και θα πρέπει να εφαρμοσθούν κάποια μέτρα όπως η χρήση τείχους προστασίας. Επίσης σημαντική είναι και η αυθεντικοποίηση πρόσβασης που εδώ μπορεί να χρησιμοποιηθεί η Ψηφιακή Υπογραφή, το SSO(Single Sign-on) μεταξύ του χρήστη και του παρόχου αλλά και το Security Assertion Markup Language(SAML) που χρησιμοποιείται κυρίως για την πρόσβαση στα δεδομένα και τις εφαρμογές των διαχειριστών αλλά και των χρηστών. Εκτός από τους ελέγχους πρόσβασης για την προστασία των δεδομένων χρησιμοποιείται και η κρυπτογράφηση. Η διαχείριση των κρυπτογραφικών κλειδιών είναι ευθύνη κυρίως του χρήστη αφού η διαδικασία παραγωγής κρυπτογραφικών κλειδιών και η αποθήκευσή τους γίνεται έξω από το Νέφος. Είναι σημαντική η διαχείριση των δεδομένων και των Metadata ώστε να υποστηρίζεται η φορητότητα και η διαλειτουργικότητα μεταξύ των εφαρμογών. Η ασφάλεια δεν αποτελεί αρμοδιότητα και ευθύνη μόνο του παρόχου ή του χρήστη. Πρέπει σίγουρα να υπάρξει συνεργασία μεταξύ τους ώστε να εφαρμοσθούν οι πολιτικές, οι διαδικασίες και οι απαιτούμενοι τεχνικοί έλεγχοι ώστε να υποστηριχθεί ο έλεγχος ασφαλείας με την εφαρμογή των απαιτούμενων κανονισμών και νομικών κανόνων.[39]

Κεφάλαιο 4

Ενημερότητα ασφάλειας των χρηστών

ΣΤΟ ΓΟΤΡΑ η υιοθέτηση του Υπολογιστικού Νέφους έχει μία συνεχή ανοδική πορεία. Παράγοντες που έχουν συμβάλει σε αυτό είναι αδιαμφισβήτητα το οικονομικό όφελος λόγω χαμηλού κόστους, οι σημαντικές βελτιώσεις που έχουν γίνει στο επίπεδο ασφαλείας καθώς επίσης και το αυξημένο επίπεδο αξιοπιστίας που παρέχει. Έτσι λοιπόν, οι μικρές και μεσαίες κυρίως επιχειρήσεις για να μειώσουν τα έξοδα που αφορούν στην αγορά, εγκατάσταση και συντήρηση του απαραίτητου τεχνολογικού εξοπλισμού, αρχίζουν να στρέφονται προς το Υπολογιστικό Νέφος, το οποίο διαθέτει στον χρήστη τον εξοπλισμό που χρειάζεται, αναλαμβάνοντας επίσης την εγκατάσταση και συντήρηση του. Επίσης και η ασφάλεια του συστήματος αλλά και του δικτύου είναι σχεδόν αποκλειστικά ευθύνη του παρόχου. Για την ασφαλή υιοθέτηση του Υπολογιστικού Νέφους είναι απαραίτητο να καθιερωθεί μία επιτυχής στρατηγική ασφαλείας, η οποία να προκύπτει μέσω της ανάλυσης των προτεραιοτήτων ασφαλείας αλλά και των αντίμετρων που θα πρέπει να εφαρμοσθούν. Για την ολοκλήρωση της ανάλυσης σημαντική μεταβλητή είναι το επίπεδο ενημερότητας (Awareness) και του παρόχου αλλά και του χρήστη. Η ενημερότητα είναι ένας πολύπλευρος παράγοντας αφού εξαρτάται από διαφορετικές συνιστώσες. Μία βασική συνιστώσα είναι ποιός χρησιμοποιεί τις υπηρεσίες του Υπολογιστικού Νέφους. Ο απλός χρήστης του διαδικτύου μπορεί να χρησιμοποιεί το Υπολογιστικό Νέφος και να μη το γνωρίζει, για παράδειγμα το ηλεκτρονικό ταχυδρομείο, τα κοινωνικά δίκτυα, και άλλες υπηρεσίες. Η ενημερότητα σίγουρα λοιπόν δεν αφορά τον απλό χρήστη, αλλά κυρίως τον επαγγελματία χρήστη ο οποίος συνειδητά χρησι-

μπορεί το Υπολογιστικό Νέφος ώστε να επωφεληθεί από τον περιορισμό εξόδων για αγορά λογισμικού αλλά και εξοπλισμού, προσαρμογή των διαθέσιμων υπολογιστικών πόρων ανάλογα με τις απαιτήσεις και γενικά από τις τεχνολογίες που προσφέρονται. Σύμφωνα με τα παραπάνω για τον επαγγελματία χρήστη σημαντική συνιστώσα είναι σίγουρα η γνώση γενικά των χαρακτηριστικών του Υπολογιστικού Νέφους, το επίπεδο γνώσεων του σχετικά με τις παρεχόμενες τεχνολογίες καθώς επίσης και το επίπεδο της γνώσης των υπηρεσιών αλλά και των ευκαιριών που παρέχονται κατά την υιοθέτηση του Υπολογιστικού Νέφους. Οι γνώσεις αυτές προκύπτουν μέσω της μάθησης από διάφορες πηγές όπως βιβλία, ιστοσελίδες κ.τ.λ., μέσω της εκπαίδευσης πάνω στο Υπολογιστικό Νέφος και για το λόγο αυτό συμπεραίνουμε ότι είναι υποκειμενικό το επίπεδο γνώσης του κάθε χρήστη. Η ενημέρωση κατάστασης (Situation Awareness) είναι ο όρος που περιγράφει την επίγνωση των χαρακτηριστικών που επικρατούν στο περιβάλλον Υπολογιστικού Νέφους του χρήστη αλλά και τη δυνατότητα αντίληψης της εξέλιξής τους. Δηλαδή ο χρήστης θα πρέπει να αντιληφθεί τι συμβαίνει στο περιβάλλον στο οποίο βρίσκεται, το οποίο είναι πολύ βασικό βήμα το οποίο θα οδηγήσει στην κατανόηση και αναγνώριση των ευπαθειών του συστήματος και στη συνέχεια στη σωστή αντίδραση αντιμετώπισης τους. Συγκεντρώνονται λοιπόν στοιχεία σχετικά με τους κινδύνους που ελοχεύουν με τη χρήση του Υπολογιστικού Νέφους, ακολουθεί η ανάλυση τους η οποία συμβάλλει στο να αναγνωρίζονται οι κίνδυνοι αρκετά γρήγορα, και να αντιμετωπίζονται σχεδόν την στιγμή που συμβαίνουν.[45]

Όσον αφορά την ασφάλεια δεν πρέπει να παραβλέπουμε και να υποτιμούμε τον πιο απρόβλεπτο παράγοντα από τον οποίο εξαρτάται και αυτός είναι ο ανθρώπινος παράγοντας. Επομένως ποιος είναι ο ρόλος του χρήστη και η συνεισφορά του στην ασφάλεια ενός συστήματος του Υπολογιστικού Νέφους; Ποιος είναι ο ρόλος και η συμβολή της ενημερότητας του χρήστη στην ενίσχυση της ασφάλειας; Όταν ο χρήστης γνωρίζει τι είναι Υπολογιστικό Νέφος και έχει εξοικειωθεί με τις τεχνολογίες που θα χρησιμοποιήσει θα είναι σε θέση να χρησιμοποιήσει τους διαθέσιμους μηχανισμούς ασφάλειας προς όφελος του. Θα είναι σε θέση να απαιτήσει ή καλύτερα να εξασφαλίσει ένα πολύ καλό επίπεδο ασφάλειας κατά την υιοθέτηση του Υπολογιστικού Νέφους, επιλέγοντας πιο συνειδητά τον καλύτερο πάροχο με την κατάρτηση πληρέστερων όσον αφορά στις απαιτήσεις που έχει ανάλογα με τις ανάγκες του, Συμφωνιών Επιπέδου Υπηρεσιών (SLA) με τους παρόχους όπως έχει αναφερθεί παραπάνω. Η ενημερότητα λοιπόν τι ρόλο διαδραματίζει στην υιοθέτηση του Νέφους αλλά και στην ενίσχυση της ασφαλούς χρήσης του. Αυτά τα ερωτήματα ευελπιστούμε να απαντηθούν στην έρευνα που ακολουθεί.

Κεφάλαιο 5

Μεθοδολογία Έρευνας

5.1 Ερευνητικά Ερωτήματα

ΕΡΕΥΝΗΤΙΚΑ ερωτήματα που η παρούσα μελέτη ευελπιστεί να απαντήσει είναι τα εξής:

- Ποια οφέλη έχουν αποκομίσει οι επιχειρήσεις στην Ελλάδα που έχουν υιοθετήσει υπηρεσίες υπολογιστικού νέφους·
- Ποιος ο βαθμός ενημερότητας των κινδύνων που συνεπάγεται η χρήση υπηρεσιών υπολογιστικού νέφους εκ μέρους των επιχειρήσεις στη χώρα που έχουν υιοθετήσει υπηρεσίες υπολογιστικής νέφους·
- Ποιος ο βαθμός ενημερότητας των χαρακτηριστικών που διέπουν τη συμφωνία παροχής υπηρεσιών υπολογιστικού νέφους (Service Level Agreement) που έχουν συνάψει επιχειρήσεων στη χώρα με παρόχους υπηρεσιών υπολογιστικού νέφους·
- Υπάρχει διαφοροποίηση του βαθμού ενημερότητας των κινδύνων που συνεπάγεται η χρήση υπηρεσιών υπολογιστικού νέφους σε σχέση με το μέγεθος μιας αντίστοιχης επιχείρησης στην Ελλάδα·
- Υπάρχει διαφοροποίηση του βαθμού ενημερότητας των κινδύνων που συνεπάγεται η χρήση υπηρεσιών υπολογιστικού νέφους σε σχέση με τον τομέα που δραστηριοποιείται μια επιχείρηση στην Ελλάδα·

- Υπάρχει διαφοροποίηση του βαθμού ενημερότητας των χαρακτηριστικών που διέπουν τη συμφωνία SLA με παρόχους υπηρεσιών υπολογιστικού νέφους σε σχέση με το μέγεθος μιας αντίστοιχης επιχείρησης στην Ελλάδα.
- Υπάρχει διαφοροποίηση του βαθμού ενημερότητας των χαρακτηριστικών που διέπουν τη συμφωνία SLA με παρόχους υπηρεσιών υπολογιστικού νέφους σε σχέση με τον τομέα που δραστηριοποιείται μια επιχείρηση στην Ελλάδα.

5.2 Ερευνητική προσέγγιση

Για την απάντηση στα παραπάνω ερευνητικά ερωτήματα επιλέγεται η εφαρμογή ποσοτικής ερευνητικής προσέγγισης με τη χρήση ερωτηματολογίου ως μέσου συλλογής πρωτογενών δεδομένων από επιχειρήσεις που έχουν υιοθετήσει τη χρήση υπηρεσιών υπολογιστικού νέφους στη χώρα.

Μια ποσοτική ερευνητική προσέγγιση επιλέγεται όταν επιδιώκεται η έκφραση με αριθμητικά στοιχεία, ποσοστού ή μερίδας οντοτήτων που ακολουθεί μια στάση ή έχει υιοθετήσει μια πρακτική στη λειτουργία του.[50]

Αντίστοιχα, για αρκετά από τα παραπάνω αναφερθέντα ερευνητικά ερωτήματα επιδιώκεται η έκφραση με αριθμητικά στοιχεία του ποσοστού μεταξύ των επιχειρήσεων που έχουν υιοθετήσει τη χρήση υπηρεσιών υπολογιστικού νέφους, του επιπέδου ενημερότητας των κινδύνων χρήσης σχετικών υπηρεσιών αλλά και σε ποιο ποσοστό γνωρίζουν με λεπτομέρεια τους όρους του συμβολαίου που έχουν υπογράψει με παρόχους υπηρεσιών υπολογιστικού νέφους.

Επιπροσθέτως, μια ποσοτική ερευνητική προσέγγιση είναι περισσότερο κατάλληλη όταν πριν την υλοποίηση της έρευνας έχει προηγηθεί βιβλιογραφική ανασκόπηση επί του αντικειμένου μελέτης, όπως συνέβει και στην περίπτωση της παρούσας μελέτης. Αντίθετα, μια ποιοτική ερευνητική προσέγγιση είναι περισσότερο κατάλληλη όταν ο ερευνητής δεν διαθέτει επαρκείς γνώσεις σχετικά με το αντικείμενο μελέτης.[51]

Επιπλέον, αξίζει να αναφερθεί πως η εφαρμογή ποσοτικής ερευνητικής προσέγγισης αποτελεί την πλέον δημοφιλή ερευνητική προσέγγιση που εφαρμόζεται στην πλειονότητα των ερευνών που υλοποιούνται σε παγκόσμιο επίπεδο.[52]

Τέλος, σε σχετικές έρευνες που υλοποιήθηκαν στο παρελθόν εφαρμόστηκε ανάλογη ερευνητική προσέγγιση. Ανάλογα και για την παρούσα ερευνητική προσέγγιση θα εφαρμοσθεί η ποσοτική ερευνητική προσέγγιση και η χρήση ερωτηματολογίου για τη συλλογή δεδομένων από τους συμμετέχοντες (που αφορά σε επιχειρήσεις) στην έρευνα. [53, 54, 55, 56]

5.3 Δείγμα Έρευνας

Ως δείγμα της έρευνας έχει επιλεγθεί η χρήση εγχώριων επιχειρήσεων που έχουν υιοθετήσει τη χρήση υπηρεσιών Υπολογιστικού Νέφους. Για την προσέλκυση συμμετεχόντων στην έρευνα στάλθηκαν ατομικές προσκλήσεις συμμετοχής με βάση τα στοιχεία επικοινωνίας των επιχειρήσεων, όπως εκείνα εμφανίζονται στη σελίδα επικοινωνίας στους ιστοτόπους των διαφόρων επιχειρήσεων. Επιπλέον, στάλθηκαν σχετικές προσκλήσεις σε ομάδες επιχειρήσεων σε κοινωνικά δίκτυα, καθώς επίσης και σε περιοχές συζητήσεων (forum) σχετικά με την υιοθέτηση υπηρεσιών υπολογιστικού νέφους. Το δείγμα της έρευνας μπορεί να χαρακτηριστεί έως ευκαιριακό, καθώς δεν απαιτούνται κάποια ειδικά κριτήρια για την αποδοχή της συμμετοχής στην έρευνα μιας επιχείρησης αλλά το μόνο κριτήριο που πρέπει να πληρείται από την επιχείρηση, είναι να έχει γίνει υιοθέτηση της χρήσης υπηρεσιών υπολογιστικού νέφους. Επομένως συμμετέχουν στην έρευνα επιχειρήσεις τις οποίες η ερευνήτρια κατάφερε να προσεγγίσει ευκολότερα και να τις πείσει να συμμετέχουν στην έρευνα.

5.4 Μέσα συλλογής Δεδομένων

Όπως αναφέρθηκε παραπάνω ως μέσο συλλογής δεδομένων στην έρευνα έχει επιλεγθεί η χρήση ερωτηματολογίου από τις επιχειρήσεις που έχουν υιοθετήσει τη χρήση υπηρεσιών υπολογιστικού νέφους στη χώρα. Όπως αναφέρουν σχετικά οι [57], το ερωτηματολόγιο αποτελεί το δημοφιλέστερο μέσο συλλογής δεδομένων σε μία έρευνα. Κύριοι λόγοι υπέρ της αντίστοιχης απόφασης αποτέλεσαν οι εξής :

- ενίσχυση αξιοπιστίας των δεδομένων συλλογής, εξαιτίας της ανωνυμίας που συνοδεύει το ερωτηματολόγιο ως εργαλείο συλλογής δεδομένων
- ταχύτητα στη συλλογή των δεδομένων
- χαμηλό κόστος συλλογής δεδομένων
- μεγάλη γεωγραφική κάλυψη
- οικειότητα των περισσότερων ανθρώπων με τη διαδικασία συμπλήρωσης ενός ερωτηματολογίου
- δυσκολία άμεσης επίδρασης του ερευνητή στην επιλογή απαντήσεων κατά τη συμπλήρωση του ερωτηματολογίου από τους συμμετέχοντες σε μια έρευνα

- ευκολία στατιστικής ανάλυσης ερωτηματολογίων που περιλαμβάνουν αποκλειστικά κλειστού τύπου ερωτήσεις[58]

Ωστόσο, θα πρέπει να επισημανθεί πως η χρήση ερωτηματολογίου ως μέσου συλλογής δεδομένων σε μια έρευνα συνοδεύεται από ορισμένους περιορισμούς, όπως :

- αδυναμία τεκμηρίωσης απάντησης εκ μέρους των συμμετεχόντων στην έρευνα
- αδυναμία υποβολής συμπληρωματικών ερωτήσεων στους συμμετέχοντες σε μια έρευνα, με βάση τις απαντήσεις που έδωσαν στο ερωτηματολόγιο
- πιθανότητα λανθασμένης ερμηνείας των ερωτήσεων
- αδυναμία παροχής διευκρινίσεων εκ μέρους του ερευνητή, εφόσον το ζητήσουν οι συμμετέχοντες σε μια έρευνα[59]

Για την μείωση των παραπάνω περιορισμών σχετικά με τη χρήση ενός ερωτηματολογίου σε μια έρευνα κρίνεται ωφέλιμη και ουσιαστική η χρήση αποκλειστικά ερωτήσεων τύπου Likert που είναι ευκολότερες στην κατανόηση, καθώς επίσης και η διενέργεια πιλοτικών δοκιμών του ερωτηματολογίου με στελέχη άλλων επιχειρήσεων, οι οποίοι δεν συμμετείχαν στην έρευνα με σκοπό τη διασφάλιση της ορθής κατανόησης των ερωτήσεων. Επιπλέον, να σημειωθεί ότι η διάθεση του ερωτηματολογίου προς συμπλήρωση στις συμμετέχουσες επιχειρήσεις στην έρευνα πραγματοποιήθηκε ηλεκτρονικά. Οφέλη από την επιλογή χρήσης ενός ηλεκτρονικού ερωτηματολογίου, έναντι ενός παραδοσιακού έντυπου ερωτηματολογίου αποτελούν:

- περιορισμός κόστους συλλογής δεδομένων
- διασφάλιση ανωνυμίας στους συμμετέχοντες
- αυτοματοποιημένος έλεγχος ορθότητας συμπλήρωσης ερωτήσεων εκ μέρους της εφαρμογής φιλοξενίας του ερωτηματολογίου
- μεγαλύτερη ταχύτητα στη συμπλήρωση του ερωτηματολογίου
- λιγότερο παρεμβατικό στη ζωή των ατόμων που συμμετέχουν σε μια έρευνα, καθώς οι συμμετέχοντες σε μια έρευνα μπορούν να συμπληρώσουν το ερωτηματολόγιο το χρονικό διάστημα που τους εξυπηρετεί καλύτερα
- εύκολη και χωρίς σφάλματα μεταφορά των απαντήσεων που έχουν δοθεί σε ένα ερωτηματολόγιο σε προγράμματα στατιστικής ανάλυσης[60]

5.5 Σχεδίαση Ερωτηματολογίου

Στο ερωτηματολόγιο της έρευνας περιλαμβάνονται αποκλειστικά ερωτήσεις τύπου Likert με πέντε (-5-) πιθανές απαντήσεις (1, 2, 3, 4, 5). Στο σημείο αυτό θα πρέπει να επισημανθεί πως οι ερωτήσεις τύπου Likert αποτελούν την κυρίαρχη μορφή ερωτήσεων που περιλαμβάνονται σε όλες τις έρευνες που χρησιμοποιούν το ερωτηματολόγιο ως εργαλείο συλλογής δεδομένων [61]. Οι ερωτήσεις κλίμακας Likert είναι κατάλληλες για την αποτίμηση στάσεων ή απόψεων μεταξύ του δείγματος μιας έρευνας, στοιχείο που βρίσκεται σε αναλογία με τους στόχους της παρούσας μελέτης. [62]

Η χρήση αντίστοιχων ερωτήσεων – προτάσεων σε ένα ερωτηματολόγιο πρακτικά αξιολογούν το επίπεδο συμφωνίας ή διαφωνίας των συμμετεχόντων σε μια έρευνα, με το περιεχόμενο κάθε ερώτησης – πρότασης που περιλαμβάνεται σε ένα ερωτηματολόγιο.

Επιλέγεται η χρήση κλίμακας Likert με πέντε πιθανές απαντήσεις δηλαδή με περιττό αριθμό πιθανών αποκρίσεων στις ερωτήσεις του ερωτηματολογίου, με σκοπό την παροχή της δυνατότητας στους συμμετέχοντες στην έρευνα να εκφράσουν καθαρά αν συμφωνούν ή διαφωνούν με μια πρόταση, καθώς κάτι ανάλογο είναι πιθανό να ισχύει κατά τη συμπλήρωση ενός ερωτηματολογίου. Σε διαφορετική περίπτωση οι συμμετέχοντες στην έρευνα θα αναγκαστούν να απαντήσουν θετικά ή αρνητικά σε μια ερώτηση – πρόταση, για την οποία πιθανόν να μη διαθέτουν ξεκάθαρη προτίμηση. Όταν σε ένα ερωτηματολόγιο δεν παρέχεται η επιλογή ούτε διαφωνώ – ούτε συμφωνώ, οι συμμετέχοντες σε αντίστοιχες έρευνες, τείνουν να απαντούν τυχαία μια από τις επιλογές που βρίσκονται κοντά στη μέση επιλογή, χωρίς να μπορούν να δηλώσουν την πραγματική τους πεποίθηση ή στάση. [72]

Κατά την εφαρμογή ανάλογης πρακτικής εγκυμονεί ο κίνδυνος προκατάληψης στις αποκρίσεις του ερωτηματολογίου μιας έρευνας. [73]

Το ερωτηματολόγιο της έρευνας περιλαμβάνει συνολικά 48 ερωτήσεις, οι οποίες προέρχονται από σχετικές ερωτήσεις που χρησιμοποιήθηκαν σε άλλες αντίστοιχες έρευνες. Όλες οι ερωτήσεις είναι σε κλίμακα Likert, με πιθανές τιμές από ένα (1) μέχρι και πέντε (5). Πιο συγκεκριμένα στον παρακάτω πίνακα απεικονίζεται η αντιστοίχιση μεταξύ των πιθανών απαντήσεων της κλίμακας Likert που χρησιμοποιήθηκε στις ερωτήσεις του ερωτηματολογίου της παρούσας μελέτης και της σχετικής ερμηνείας των απαντήσεων:

Πίνακας 5.1: Ερμηνεία απαντήσεων κλίμακας Likert

Απάντηση στην ερώτηση	Ερμηνεία απάντησης
1	Διαφωνώ απόλυτα
2	Διαφωνώ
3	Ούτε Διαφωνώ - Ούτε Συμφωνώ
4	Συμφωνώ
5	Συμφωνώ απόλυτα

Η επιλογή πέντε και όχι περισσότερων, περιπτώσεων στο σύνολο, επιλογών απάντησης έγινε με γνώμονα την ευκολία στη συμπλήρωση το ερωτηματολογίου, καθώς παρέχοντας όχι περισσότερες από πέντε πιθανές απαντήσεις προς επιλογή, διασφαλίζει πως τα άτομα που θα συμπληρώσουν το ερωτηματολόγιο θα διαβάσουν και θα κατανοήσουν ευκολότερα τις πιθανές επιλογές απάντησης στο ερωτηματολόγιο . [74] Επιπλέον, όπως αναφέρουν σχετικά οι Sachdev & Verma, η χρήση κλίμακας Likert πέντε (5) πιθανών απαντήσεων μειώνει τη δυσκολία στη συμπλήρωση ενός ερωτηματολογίου, αυξάνει το ποσοστό ανταπόκρισης σε προκλήσεις συμμετοχής σε μια έρευνα και τείνει να ενισχύει την αξιοπιστία των αποκρίσεων. [75] Βασικά οφέλη που προκύπτουν από την επιλογή αποκλειστικά ερωτήσεων τύπου Likert σε ένα ερωτηματολόγιο είναι τα εξής:

- ευκολία εφαρμογής στατιστικής ανάλυσης των απαντήσεων στο ερωτηματολόγιο
- ευκολία και ταχύτητα στη σχεδίαση του ερωτηματολογίου εκ μέρους του ερευνητή
- ευκολία στην κατανόηση των ερωτήσεων και ταχύτητα κατά την συμπλήρωση του ερωτηματολογίου εκ μέρους των συμμετεχόντων σε μια έρευνα
- ευκολία στη διατύπωση συμπερασμάτων, σχεδίασης αναφορών και διαγραμματικής απεικόνισης των αποκρίσεων σε ένα ερωτηματολόγιο [70]

Οι ερωτήσεις που συμπεριλήφθησαν στο ερωτηματολόγιο της παρούσας έρευνας προέρχονται από σχετικές ερωτήσεις που χρησιμοποιήθηκαν σε άλλες αντίστοιχες έρευνες [53, 54], καθώς επίσης και στα συμπεράσματα άλλων σχετικών ερευνών [63, 64, 65].

Πιο συγκεκριμένα, για την πρώτη κατηγορία ερευνητικών ερωτημάτων χρησιμοποιήθηκαν οι

ερωτήσεις (15 πρώτες ερωτήσεις) που περιλαμβάνονται σε έρευνα των Chen et al. με αντικείμενο την αποτίμηση οφελειών που έχουν αποκομίσει επιχειρήσεις στην Ταϊβάν από την υιοθέτηση χρήσης υπηρεσιών υπολογιστικής νέφους. [54]

Τα οφέλη που αποτιμά η συγκεκριμένη έρευνα σχετίζονται με οικονομικά οφέλη, καθώς επίσης και οφέλη στην ικανότητα λειτουργίας και προσαρμογής των οργανισμών.

Όσον αφορά στην δεύτερη κατηγορία των ερευνητικών ερωτημάτων σχετικά με την ενημερότητα των κινδύνων χρήσης υπηρεσιών υπολογιστικού νέφους εκ μέρους των επιχειρήσεων στη χώρα θα χρησιμοποιηθούν ως βάση τα συμπεράσματα έρευνας των Dutta et al.[53]

Μία αντίστοιχη έρευνα είχε ως δείγμα 295 ειδικούς επιστήμονες πληροφορικής οι οποίοι είχαν υψηλή τεχνογνωσία και εμπειρία στο Υπολογιστικό Νέφος από τη Μεγάλη Βρετανία και ως αντικείμενο τη διαπίστωση των σημαντικότερων κινδύνων που ενέχει η υιοθέτηση υπηρεσιών υπολογιστικού νέφους εκ μέρους διαφόρων επιχειρήσεων και οργανισμών. Πιο συγκεκριμένα στο ερωτηματολόγιο της παρούσας μελέτης ενσωματώνονται δέκα (-10-) ερωτήσεις που ζητάνε από τις συμμετέχουσες επιχειρήσεις στην έρευνα να αξιολογήσουν το επίπεδο σημαντικότητας των δέκα (-10-) κινδύνων με τη μεγαλύτερη σημαντικότητα κατά την υιοθέτηση χρήσης των υπηρεσιών Υπολογιστικού Νέφους, όπως εκείνοι διαπιστώθηκαν στην αντίστοιχη έρευνα των Dutta et al. [53]

Η ενημερότητα ή μη της σημαντικότητας των αντίστοιχων κινδύνων εκ μέρους των επιχειρήσεων στη χώρα θα αποτελεί στοιχείο υπέρ της ενημερότητας ή μη των κινδύνων υιοθέτησης υπηρεσιών Υπολογιστικού Νέφους εκ μέρους επιχειρήσεων και οργανισμών στην Ελλάδα.

Τέλος, σχετικά με την τρίτη κατηγορία ερευνητικών ερωτημάτων σχετικά με την ενημερότητα των λεπτομερειών της συμφωνίας (SLA) που έχουν συνάψει επιχειρήσεις στη χώρα με τους παρόχους υπηρεσιών υπολογιστικού νέφους χρησιμοποιήθηκαν 23 σχετικές ερωτήσεις, που βασίστηκαν στην αποτύπωση των στοιχείων που περιλαμβάνονται σε συμφωνίες επιπέδου παροχής υπηρεσιών (SLA) υπολογιστικού νέφους σε έρευνες των Saravanan & Rajaram, Amazonas et al., και Terfas. [63, 64, 65]

Οι αντίστοιχες ερωτήσεις ομαδοποιήθηκαν σε πέντε (-5-) συνιστώσες στοιχείων που περιλαμβάνονται σε συμφωνίες SLA:

1. Απόδοση (4 ερωτήσεις)
2. Ασφάλεια (6 ερωτήσεις)
3. Δεδομένα (5 ερωτήσεις)
4. Δικαιώματα παρόχου (4 ερωτήσεις)

5. Υποχρεώσεις παρόχου (4 ερωτήσεις)

Η ομαδοποίηση των συνιστωσών στοιχείων που περιλαμβάνονται στις συμφωνίες SLA που έχουν συνάψει επιχειρήσεις στη χώρα με παρόχους υπηρεσιών υπολογιστικού νέφους, μας επιτρέπει τη διαπίστωση τυχόν διαφοροποιήσεων ενημερότητας των όρων συμφωνίας με παρόχους υπηρεσιών υπολογιστικού νέφους με βάση το αντικείμενο (συνιστώσα) των σχετικών όρων συμφωνίας. Οι απαντήσεις στα επόμενα τέσσερα ερωτήματα προκύπτουν από την εφαρμογή ελέγχων συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις σχετικά με τη δεύτερη και τρίτη κατηγορία ερευνητικών ερωτημάτων και σε δημογραφικά χαρακτηριστικά των επιχειρήσεων που θα συμμετέχουν στην έρευνα (εισαγωγικές ερωτήσεις στο ερωτηματολόγιο).

5.6 Εργαλεία Πληροφορικής για τη συλλογή και ανάλυση των δεδομένων της έρευνας

Στο πλαίσιο υλοποίησης της παρούσας έρευνας θα χρησιμοποιηθεί η εφαρμογή Google Forms με σκοπό τη δημοσίευση του ερωτηματολογίου στο διαδίκτυο και η εφαρμογή SPSS με σκοπό τη στατιστική ανάλυση των απαντήσεων που θα δοθούν στο ερωτηματολόγιο της παρούσας μελέτης.

5.6.1 Google Forms

Όσον αφορά στην δημοσίευση του ερωτηματολογίου στο διαδίκτυο, αυτή θα γίνει μέσω της εφαρμογής Google Forms. Η αντίστοιχη εφαρμογή είναι δωρεάν στη χρήση και διατίθεται από τη Google προς τους εγγεγραμμένους χρήστες του αντίστοιχου ιστότοπου. Ο αριθμός των διαθέσιμων εφαρμογών με σκοπό τη δημοσίευση ερωτηματολογίων στο διαδίκτυο είναι μεγαλύτερος από τριακόσια (-300-) προγράμματα. [66]

Σε έρευνα των Milliner & Flowers που σχετίζεται με τις διαθέσιμες εφαρμογές δημοσίευσης ερωτηματολογίων στο διαδίκτυο κρίθηκαν ως καλύτερες και περισσότερο δημοφιλείς οι εξής : η εφαρμογή Google Forms και η εφαρμογή Survey Monkeys.[67]

Μεταξύ των δύο επιλέχτηκε η εφαρμογή Google Forms διότι σε εκείνη δεν περιλαμβάνεται κάποιος περιορισμός σχετικά με τον αριθμό των ερωτήσεων που μπορεί να περιλαμβάνει ένα ηλεκτρονικό ερωτηματολόγιο και σχετικά με τον μέγιστο αριθμό χρηστών που μπορεί να απαντήσει κάποιο ερωτηματολόγιο, όπως ισχύει με την δωρεάν έκδοση της εφαρμογής Survey

Monkeys.[67]

Αναλυτικότερα, βασικά πλεονεκτήματα της επιλογής του Google Forms για τη δημοσίευση ενός ερωτηματολογίου στο διαδίκτυο αποτελούν [68]:

- Το εύκολο στη χρήση περιβάλλον της εφαρμογής
- Η ταχύτατη δημιουργία ενός ερωτηματολογίου
- Η δυνατότητα συμπλήρωσης του ερωτηματολογίου με τη χρήση κινητού τηλεφώνου
- Η δυνατότητα εξαγωγής των απαντήσεων σε διάφορες μορφές (όπως xls, csv) που επιτρέπουν την άμεση εισαγωγή των δεδομένων σε στατιστικά προγράμματα με σκοπό την περαιτέρω ανάλυση των αποκρίσεων σε ένα ερωτηματολόγιο
- Η διαγραμματική απεικόνιση των απαντήσεων για κάθε ερώτηση ξεχωριστά
- Η δυνατότητα διαμοίρασης των προσκλήσεων συμπλήρωσης ενός ερωτηματολογίου σε κοινωνικά δίκτυα και τέλος
- Η δυνατότητα της αυτοματοποιημένης αποστολής προσκλήσεων προς συμπλήρωση ενός ερωτηματολογίου μέσω μηνύματος ηλεκτρονικού ταχυδρομείου

Τέλος, για την επιλογή του συγκεκριμένου εργαλείου δημοσίευσης ερωτηματολογίων μέσω διαδικτύου συνέβαλε και η κατοχή σχετικής πρότερης εμπειρίας εκ μέρους της ερευνήτριας, η οποία δεν διαθέτει εμπειρία χρήσης κάποιας άλλης εφαρμογής δημοσίευσης ερωτηματολογίων στο διαδίκτυο.

5.6.2 SPSS

Η στατιστική ανάλυση των αποκρίσεων στο ερωτηματολόγιο της έρευνας θα πραγματοποιηθεί μέσω της εφαρμογής SPSS (Statistical Package for the Social Sciences) της IBM. Η χρήση εφαρμογής για την στατιστική ανάλυση των απαντήσεων σε ένα ερωτηματολόγιο στο πλαίσιο υλοποίησης μιας έρευνας είναι σε συμφωνία με την ποσοτική ερευνητική προσέγγιση που έχει επιλεγεί για την παρούσα έρευνα. Η χρήση ενός στατιστικού πακέτου λογισμικού επιτρέπει την εξαγωγή συμπερασμάτων, χωρίς τη δυνατότητα επίδρασης εκ μέρους της ερευνήτριας.[69] Πιο συγκεκριμένα, η εφαρμογή SPSS θα χρησιμοποιηθεί για τον υπολογισμό περιγραφικών στατιστικών δεικτών, για την εφαρμογή ελέγχων συσχέτισης, καθώς επίσης για την εφαρμογή

ελέγχου της αξιοπιστίας και της εσωτερικής συνοχής των απαντήσεων που θα δοθούν στο ερωτηματολόγιο. Ο έλεγχος αξιοπιστίας βασίζεται στη χρήση του δείκτη Cronbach alpha. Ο δείκτης αυτός θεωρείται ο πιο αξιόπιστος και δημοφιλής δείκτης που αφορά στην αξιολόγηση της αξιοπιστίας και της εσωτερικής συνοχής των απαντήσεων ενός ερωτηματολογίου που περιλαμβάνει ερωτήσεις του τύπου Likert.[71]

Αναφορικά με τους στατιστικούς δείκτες που θα χρησιμοποιηθούν για την στατιστική ανάλυση των απαντήσεων, αναφέρεται ότι θα χρησιμοποιηθούν οι τιμές των δεικτών: μέγιστο, ελάχιστο, τυπική απόκλιση και μέση τιμή. Οι τιμές των δεικτών μέγιστο και ελάχιστο επιτρέπουν τη διαπίστωση πιθανών ακραίων αντιλήψεων και στάσεων μεταξύ των συμμετεχόντων σε μια έρευνα. Αντίστοιχα, ο δείκτης τυπικής απόκλισης επιτρέπει τον έλεγχο της ομοιομορφίας μεταξύ των απαντήσεων στις ερωτήσεις ενός ερωτηματολογίου. Τέλος, ο δείκτης μέσης τιμής επιτρέπει τη σύγκριση των απαντήσεων στις ερωτήσεις του ερωτηματολογίου και τη διαπίστωση των παραγόντων που οι συμμετέχοντες σε μια έρευνα αποδίδουν μεγαλύτερη σημασία.

Τέλος, η εφαρμογή SPSS θα χρησιμοποιηθεί για τον έλεγχο της ύπαρξης στατιστικά σημαντικής ή μη συσχέτισης μεταξύ του βαθμού ενημερότητας των κινδύνων που συνεπάγεται η χρήση υπηρεσιών του υπολογιστικού νέφους και

1. Του μεγέθους μιας επιχείρησης, καθώς επίσης
2. Του τομέα που εκείνη δραστηριοποιείται.

Αντίστοιχα, η εφαρμογή SPSS θα χρησιμοποιηθεί και για τον έλεγχο της ύπαρξης στατιστικά σημαντικής ή μη συσχέτισης μεταξύ του βαθμού ενημερότητας των χαρακτηριστικών που διέπουν τη συμφωνία SLA με τους παρόχους των υπηρεσιών υπολογιστικού νέφους και

1. Του μεγέθους μιας επιχείρησης, καθώς επίσης και
2. Του τομέα που εκείνη δραστηριοποιείται.

Κεφάλαιο 6

Υλοποίηση Έρευνας

ΠΙΝ την πραγματοποίηση της έρευνας πραγματοποιήθηκαν πιλοτικές δοκιμές συμπλήρωσης του ερωτηματολογίου από στελέχη επιχειρήσεων που είναι υπεύθυνοι διαχείρισης υπηρεσιών υπολογιστικής νέφους στις επιχειρήσεις που εργάζονται.

6.1 Πιλοτικές Δοκιμές

Πιο συγκεκριμένα πραγματοποιήθηκαν δυο επαναλήψεις πιλοτικών δοκιμών συμπλήρωσης του ερωτηματολογίου με διαφορετικά στελέχη επιχειρήσεων σε κάθε επανάληψη πιλοτικής δοκιμής. Οι σχετικές πιλοτικές δοκιμές έλαβαν τόπο τον Ιούνιο του 2020. Μέσω των πιλοτικών δοκιμών παρέχεται η δυνατότητα αξιολόγησης της εγκυρότητας των ερωτήσεων συμπερίληψης σε ένα ερωτηματολόγιο, δηλαδή εάν εκείνες γίνονται ορθά κατανοητές από τους συμμετέχοντες σε μια έρευνα, καθώς επίσης και της αξιοπιστίας των απαντήσεων, δηλαδή εάν οι απαντήσεις σε ένα ερωτηματολόγιο είναι ανάλογες κατά την επανάληψη συμπλήρωσης ενός ερωτηματολογίου. Κατά την πρώτη πιλοτική δοκιμή εκτέλεσης του ερωτηματολογίου υπήρξαν συστάσεις σχετικά με τη σειρά και τη διατύπωση ορισμένων ερωτήσεων, στοιχείο το οποίο ελήφθη υπόψη και προσαρμόστηκε ανάλογα το ερωτηματολόγιο της έρευνας. Κατά τη δεύτερη πιλοτική δοκιμή δεν υπήρξαν κάποιες επιπρόσθετες παρατηρήσεις σχετικά με τη δομή ή τη διατύπωση των ερωτήσεων του ερωτηματολογίου της έρευνας αλλά στην πλατφόρμα του Google Forms είχε ενεργοποιηθεί η ενημέρωση της ερευνήτριας μέσω ηλεκτρονικού ταχυδρομείου σε κάθε συμπλήρωση του ερωτηματολογίου, ώστε να υπάρχει καλύτερος έλεγχος των αναμενόμενων αποκρίσεων. Επιπλέον, υπήρξαν πιλοτικές δοκιμές συμπλήρωσης του ερωτηματολογίου της

έρευνας με τη χρήση προσωπικού υπολογιστή, φορητού υπολογιστή, τηλεφώνου και tablet, χωρίς να διαπιστωθεί κάποια δυσκολία κατά τη συμπλήρωση του ερωτηματολογίου με κάποια συσκευή χρήσης. Τέλος, από τις πιλοτικές δοκιμές διαπιστώθηκε πως ο μέσος χρόνος συμπλήρωσης του ερωτηματολογίου κυμαίνονταν περί των οχτώ (8) λεπτών, χρόνος μη αποτρεπτικός για τη συμπλήρωση εκείνου.

6.2 Πραγματοποίηση έρευνας

Η έρευνα πραγματοποιήθηκε τον Ιούνιο του 2020. Πιο συγκεκριμένα οι προσκλήσεις συμμετοχής στην έρευνα στάλθηκαν προς υποψήφιους συμμετέχοντες στην έρευνα το πρώτο δεκαήμερο του Ιουνίου του 2020 και στη συνέχεια το ερωτηματολόγιο ήταν διαθέσιμο προς συμπλήρωση ηλεκτρονικά για περίπου δεκαπέντε μέρες. Το ερωτηματολόγιο συνοδευόταν από ένα εισαγωγικό σημείωμα όπου αναφερόταν ο σκοπός διεξαγωγής αυτής της έρευνας, καθώς επίσης και την διαβεβαίωση για την διασφάλιση της ανωνυμίας των συμμετεχόντων στην έρευνα. Στην παρακάτω εικόνα παρουσιάζεται η μορφή και το περιεχόμενο του εισαγωγικού σημειώματος του ηλεκτρονικού ερωτηματολογίου που στάλθηκε για την έρευνα:



Σχήμα 6.1: Μορφή εισαγωγικού σημειώματος ερωτηματολογίου έρευνας

Συνολικά στάλθηκαν 127 προσκλήσεις συμμετοχής στην έρευνα και ανταποκρίθηκαν στην έρευνα 11 στελέχη επιχειρήσεων της χώρας, αντιστοιχώντας σε ποσοστό ανταπόκρισης 0,085. Πολύ χαμηλό ποσοστό ανταπόκρισης παρόλο που το ερωτηματολόγιο δεν απαιτούσε πολύ χρόνο για τη συμπλήρωση του, και οι ερωτήσεις ήταν αρκετά σαφείς.

6.3 Δημογραφικά Στοιχεία

Όπως αναφέρθηκε παραπάνω το δείγμα της έρευνας αποτελείται από 11 στελέχη επιχειρήσεων

- με γνώση των λόγων που έχουν καθορίσει την απόφαση χρήσης υπηρεσιών υπολογιστικού Νέφους στον οργανισμό που εργάζονται και
- γνωρίζουν πως έχουν διαμορφωθεί οι σχετικές υπηρεσίες χρήσης

Αναφορικά με τον κλάδο δραστηριοποίησης των σχετικών οργανισμών, και οι 11 δραστηριοποιούνται στον τομέα Πληροφορικής, και μάλιστα έχουν ήδη υιοθετήσει το Υπολογιστικό Νέφος και παρέχουν υπηρεσίες που σχετίζονται με το Υπολογιστικό Νέφος. Το προφίλ των επιχειρήσεων των οποίων τα στελέχη συμμετείχαν στην έρευνα απασχολούν 1-10 υπαλλήλους. Για την υλοποίηση της παραπάνω αξιολόγησης λαμβάνεται τυχαίο δείγμα 120 πελατών και καταγράφονται οι απόψεις τους. Η απόκριση στις ερωτήσεις σημειώνεται σε μία κλίμακα 5 χαρακτηρισμών τα οποία αποτυπώνονται με βάση την ονοματολογία μιας παραδοσιακής ή μη κλίμακας μέτρησης. Η κλίμακα, γνωστή ως Likert (διατυπωμένη από τον Αμερικανό ψυχολόγο Rensis Likert), με διεθνή απήχηση, συγκροτείται από συγκεκριμένη έκφραση του λόγου στους επιμέρους χαρακτηρισμούς οι οποίοι συντίθενται από δύο αντίρροπες κατευθύνσεις μεταβολής (αρνητική – θετική εξέλιξη): 1= έντονα διαφωνώ, 2= διαφωνώ, 3= αδιάφορο, 4= συμφωνώ, 5= συμφωνώ απόλυτα. Προτού όμως επιχειρηθεί οποιαδήποτε σε βάθος στατιστική ανάλυση των ερωτήσεων, προηγείται η ανάλυση των υποθέσεων ώστε να διαπιστωθεί αν οι ερωτήσεις εκφράζουν την προτίμηση υιοθέτησης του υπολογιστικού νέφους. Η αξιοπιστία κάθε ερώτησης προσμετράται με τη βοήθεια ειδικών στατιστικών παραμέτρων όπως:

- Ο δείκτης α του Cronbach ο οποίος μετρά το βαθμό της εσωτερικής συνάφειας όλων των ερωτήσεων (ενδοσυνέπεια – internal consistency)।

- Ο πίνακας των ενδοσυσχετίσεων μας δείχνει τη σχέση κάθε ζεύγους ερωτήσεων πόσο δηλαδή η μία συμπληρώνει την άλλη, αλλά και πόσο σαφής είναι ώστε να γίνει αντιληπτή από τον ερωτώμενο.

Τα στατιστικά αποτελέσματα για να έχουν θεωρηθούν έγκυρα έχει διαπιστωθεί ότι ο συντελεστής συσχέτισης πρέπει να έχει τιμή μεγαλύτερη από 0,7 ενώ στην περίπτωση που η τιμή είναι μικρότερη η ερώτηση είναι σκόπιμο να μη λαμβάνεται υπόψη κατά την ανάλυση των αποτελεσμάτων.

6.4 Έλεγχος Αξιοπιστίας

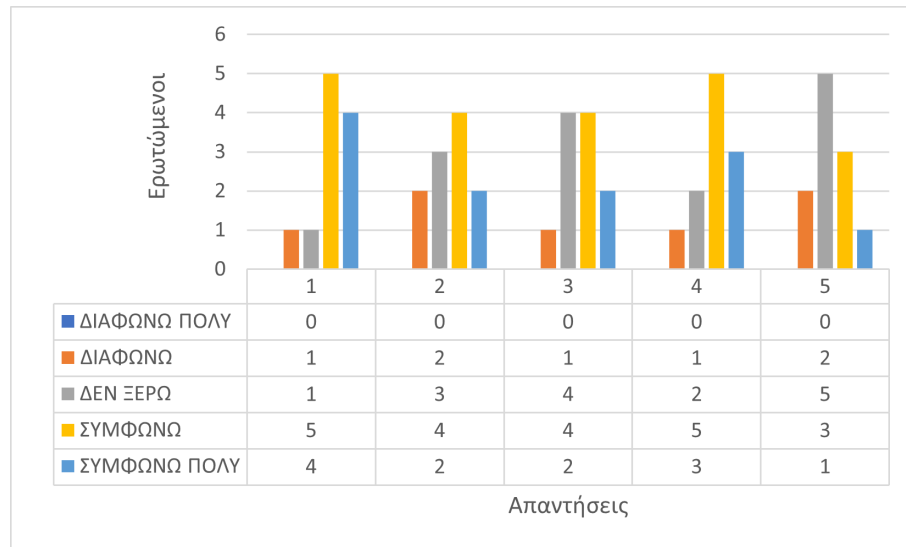
Ο δείκτης Cronbach α θεωρείτε ως ένας αξιόπιστος δείκτης για χρήση, σχετικά με την ύπαρξη εσωτερικής συνοχής και αξιοπιστίας στις απαντήσεις που έχουν δοθεί σε ένα ερωτηματολόγιο που περιλαμβάνει αποκλειστικά ερωτήσεις τύπου Likert. Πιο συγκεκριμένα προκειμένου να θεωρηθούν αξιόπιστες οι απαντήσεις που έχουν δοθεί σε ένα ερωτηματολόγιο που περιλαμβάνει ερωτήσεις τύπου Likert, θα πρέπει η τιμή του αντίστοιχου δείκτη να κυμαίνεται μεταξύ 0,7 και 1% (Τααχολ Δεννισκ, 2011). Το ποσοστό ανταπόκρισης που αναφέρθηκε παραπάνω, είναι εξαιρετικά χαμηλό και πιθανόν να οφείλεται και λόγω των ειδικών συνθηκών που επικράτησαν με την εξάπλωση του Covid-19.

Παρόλα αυτά για την παρούσα έρευνα η ανάλυση των αποτελεσμάτων δεν αποσκοπεί στην εκμαίευση έγκυρων αποτελεσμάτων αλλά περισσότερο για την αποτύπωση της τάσης που επικρατεί. Για το λόγο αυτό δεν έχει αξία να υπολογιστεί ο δείκτης Cronbach α αφού το ποσοστό συμμετοχής στην έρευνα είναι χαμηλό. Η στατιστική ανάλυση των απαντήσεων των ερωτηματολογίων έγινε χρησιμοποιώντας περιγραφική στατιστική. Σε κάθε τομέα που ερευνάται είναι σημαντικό να εξεταστούν και να αναλυθούν οι μεταβλητές δηλαδή οι ερωτήσεις. Για το λόγο αυτό έχει τρομερή αξία για την αξιοπιστία να γίνει σωστή επιλογή των ερωτήσεων.

6.5 Αποτελέσματα Έρευνας

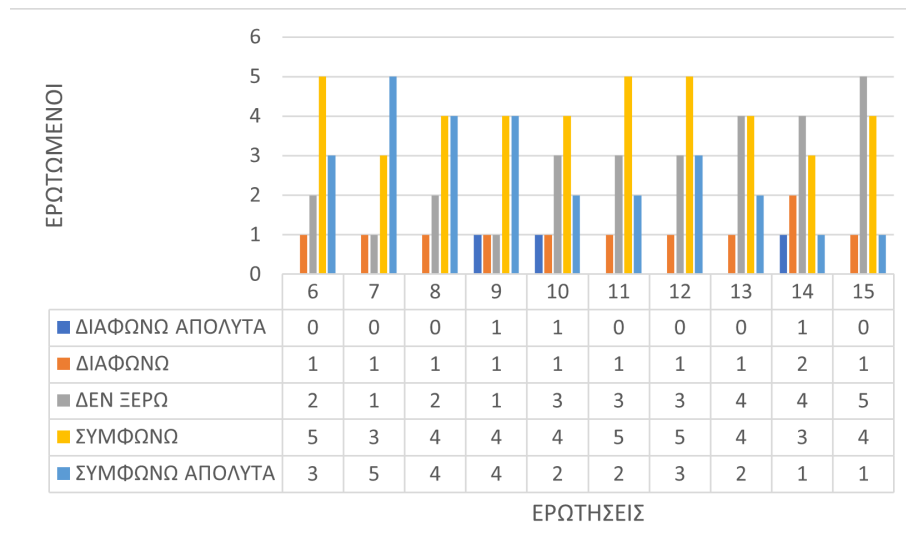
Αρχικά τέθηκαν 15 ερωτήσεις οι οποίες αφορούν στα οφέλη του υπολογιστικού νέφους. Οι παράγοντες που εξετάζονται είναι το κόστος, η εύκολη προσαρμογή και χρήση νέων υπηρεσιών αλλά και το ποσοστό αξιοποίησης των υπολογιστικών πόρων. Όσον αφορά στο κόστος οι ερωτήσεις αναφέρονται στη μείωση του κόστους ανάπτυξης νέων υπηρεσιών, συντήρησης και

ανανέωσης του υλικού και του λογισμικού καθώς και το λειτουργικό κόστος. Στο παρακάτω σχήμα φαίνονται οι απαντήσεις στις πέντε πρώτες ερωτήσεις που αφορούν στο κόστος



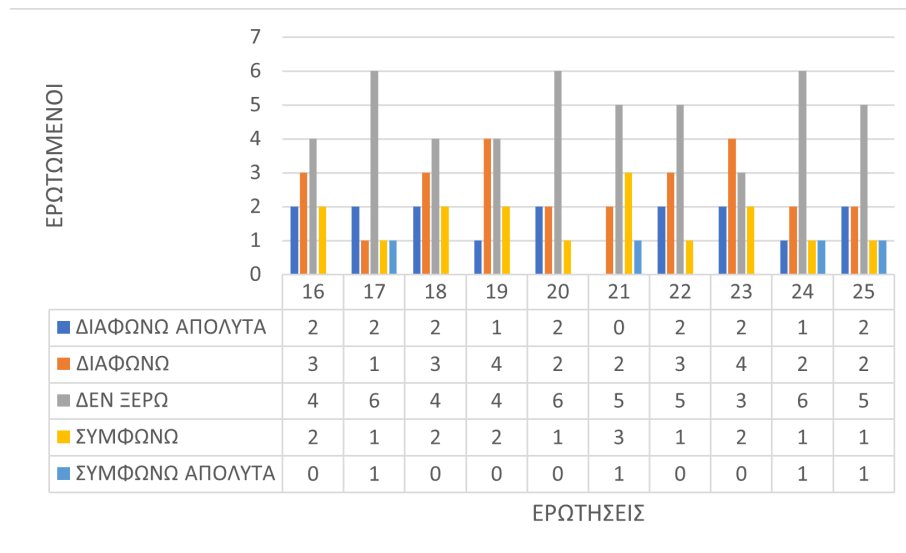
Σχήμα 6.2: Μεταβολές στο κόστος λειτουργίας και συντήρησης μετά την υιοθέτηση του Υπολογιστικού Νέφους

Από τους ερωτώμενους σε ποσοστό 81,8% περίπου, συμφωνούν/ συμφωνούν απόλυτα ότι μειώνεται το κόστος ανάπτυξης νέων υπηρεσιών καθώς και οι δαπάνες ανανέωσης λογισμικού. Ενώ περίπου το 70% συμφωνεί ότι το λειτουργικό κόστος μειώνεται με την υιοθέτηση του Υπολογιστικού Νέφους. Όσον αφορά στο συνολικό κόστος συντήρησης υλικού και λογισμικού φαίνεται ότι οι μισοί περίπου (45,4%) από τους ερωτώμενους συμφωνούν ενώ το 36,3% δεν έχει σχηματίσει γνώμη ακόμα αν μειώνεται όντως το συνολικό κόστος συντήρησης. Επομένως φαίνεται πως η πλειοψηφία των επιχειρήσεων (70-80%) αναγνωρίζει σε οποιονδήποτε βαθμό πως η υιοθέτηση του Υπολογιστικού Νέφους θα μειώσει το κόστος δαπανών για την επιχείρησή τους και το σημαντικότερο είναι πως υπολογίζουν πως η ανάπτυξη των υπηρεσιών στο Νέφος θα έχει πολύ μικρότερο κόστος από τις αντίστοιχες παραδοσιακές υπηρεσίες.



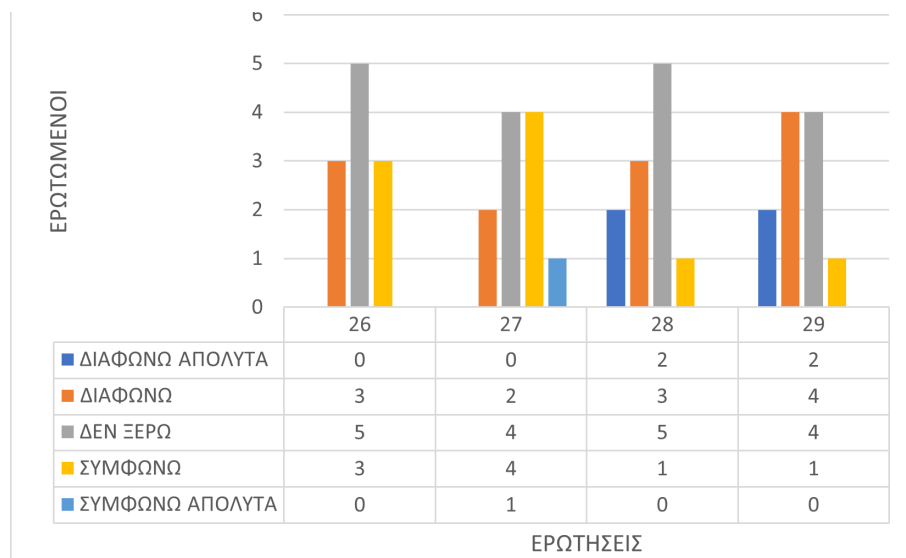
Σχήμα 6.3: Διαλειτουργικότητα-Χρήση-Αξιοπιστία υπολογιστικών πόρων με την υιοθέτηση του Υπολογιστικού Νέφους

Στο σχήμα 6.3 παρατηρούμε πως στις ερωτήσεις που αφορούν στην βελτίωση της ταχύτητας εφαρμογής και χρήσης των νέων πόρων αλλά και στη βελτίωση της διαλειτουργικότητας μεταξύ διαφορετικών υπολογιστικών πόρων και εφαρμογών, σε ποσοστό 72,7% απάντησαν ότι συμφωνούν/ συμφωνούν απόλυτα. Για την ικανότητα προσαρμογής των υπολογιστικών πόρων από τις απαντήσεις διαφαίνεται πως το 67% περίπου συμφωνεί/ συμφωνεί απόλυτα. Αλλά φαίνεται από τη διασπορά των απαντήσεων πως το 45% περίπου δεν είναι σίγουρο πως έχει περιοριστεί η ανάγκη προσαρμογής των υπολογιστικών πόρων ενώ για τη δυνατότητα ανταλλαγής υπολογιστικών πόρων και δεδομένων με άλλες επιχειρήσεις η διασπορά των απαντήσεων δείχνει πως το 63% αμφιβάλλει ότι υπάρχει αυτή η δυνατότητα. Όσον αφορά στην αξιοπιστία των υπολογιστικών πόρων αλλά και στην βελτίωση του χρόνου επαναφοράς των υπολογιστικών πόρων σε κανονική λειτουργία βλέπουμε πως το ποσοστό που συμφωνεί / συμφωνεί απόλυτα κυμαίνεται από 54,5%- 63,63%.



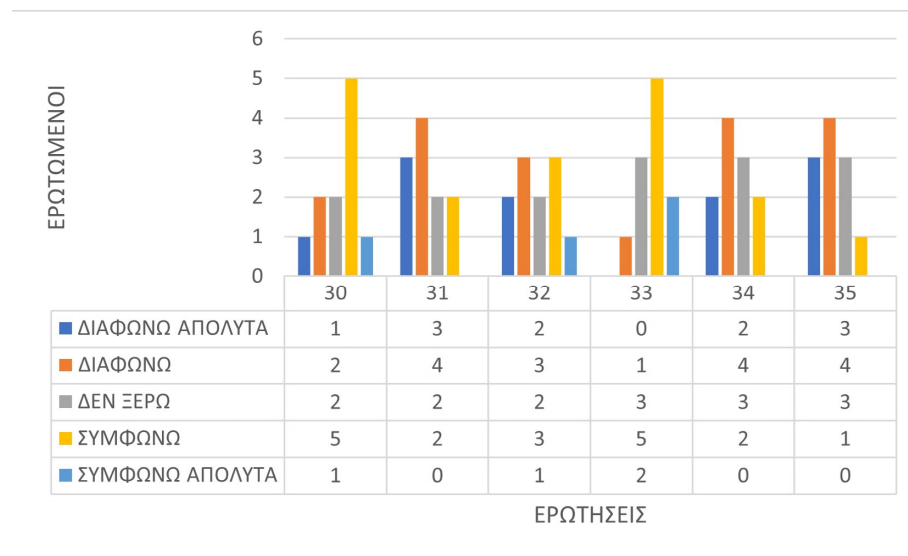
Σχήμα 6.4: Διαθεσιμότητα-Φορητότητα Δεδομένων και Υπηρεσιών μετά την υιοθέτηση του Υπολογιστικού Νέφους

Στο σχήμα 6.4 σε ποσοστό 36,3 % οι χρήστες φαίνεται να μην είναι σίγουροι αν υπάρχει κίνδυνος για τα αποθηκευμένα δεδομένα, ενώ το 45,45% θεωρεί πως είναι ασφαλή τα δεδομένα. Βέβαια στην ερώτηση που αφορά στους νόμους περί προστασίας των δεδομένων σε χώρες που φιλοξενούν υπηρεσίες υπολογιστικού νέφους, το 54,5% δεν γνωρίζει αν υπάρχει ασυνέπεια στους νόμους από χώρα σε χώρα, ενώ μόνο το 18% βλέπει ότι υπάρχει κίνδυνος από την ασυνέπεια των νόμων το οποίο ποσοστό είναι το ίδιο που θεωρεί πως απειλείται το απόρρητο των αποθηκευμένων δεδομένων στο Νέφος. Γενικά σε ποσοστό από 36,3- 54,5% δεν γνωρίζουν αν η αλλαγή παρόχου είναι εφικτή ή αν μπορεί να φέρει δυσκολίες στη μεταφορά-διασύνδεση των δεδομένων. Όσον αφορά στην αποκατάσταση καταστροφών το 36,3% δεν είναι σίγουροι αν υπάρχει έλλειψη στην αντιμετώπιση κρίσιμων καταστάσεων.



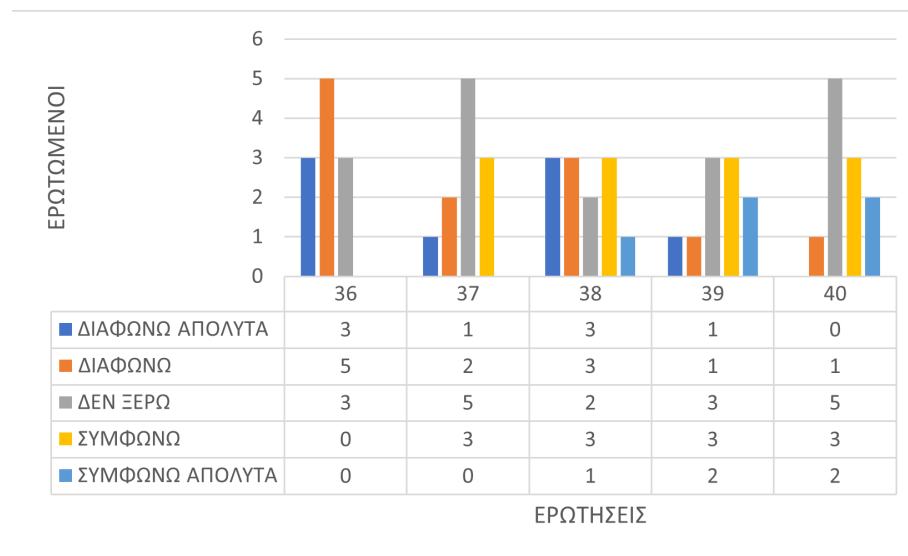
Σχήμα 6.5: Απόδοση των παρεχόμενων υπηρεσιών με την υιοθέτηση του Υπολογιστικού Νέφους

Εξετάζοντας αν οι ερωτώμενοι γνωρίζουν το επίπεδο της απόδοσης των υπηρεσιών, ερωτήθηκαν για το χρόνο διαθεσιμότητας, καθώς και για το χρόνο που απαιτείται μέχρι τη διάθεση μιας υπηρεσίας, επίσης για τον αριθμό των ενεργών συνδέσεων αλλά και τον αριθμό των αιτημάτων που δύναται να εξυπηρετηθούν συγκεκριμένη χρονική περίοδο. Παρατηρούμε στο σχήμα 6.5 ότι κυριαρχεί η απάντηση Ούτε Συμφωνώ/Ούτε Διαφωνώ σε ποσοστό 36,3- 45,5%, οπότε συμπεραίνουμε ότι οι ερωτηθέντες δεν είναι σίγουροι για το τι ισχύει.



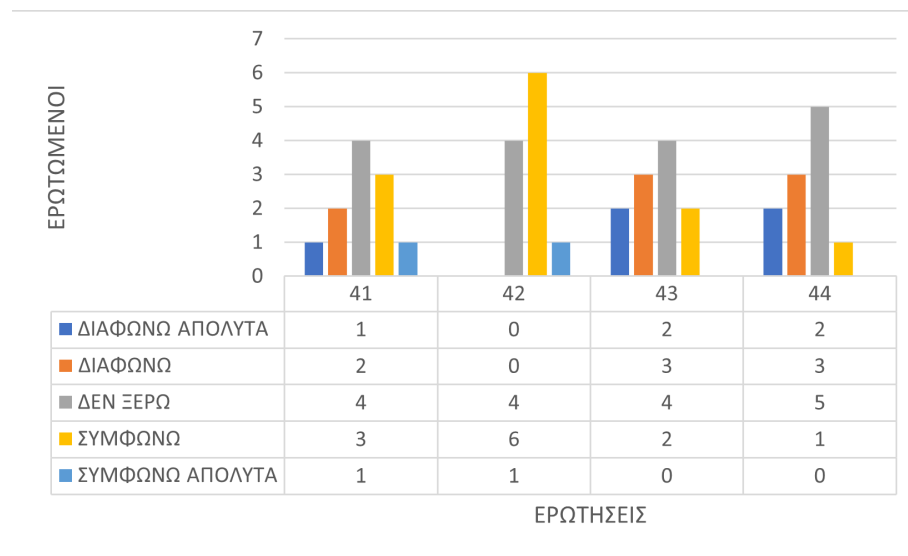
Σχήμα 6.6: Ασφάλεια χρήσης του Υπολογιστικού Νέφους

Στο σχήμα 6.6 οι ερωτήσεις αφορούν στην ασφάλεια, και συγκεκριμένα ερωτήθηκαν σχετικά με το αν γνωρίζουν τις τεχνικές κρυπτογράφησης που εφαρμόζει ο πάροχος όπου το 54,5/% απάντησε πως γνωρίζει, ενώ από τη διασπορά των απαντήσεων φαίνεται πως το 45,4% δεν γνωρίζει ή δεν είναι σίγουρο ότι ξέρει. Επίσης όσον αφορά στην διασφάλιση της ακεραιότητας των δεδομένων, φαίνεται ότι το 54,5% νοιώθει ότι είναι ικανοποιημένο. Αντίθετα σε ποσοστό περίπου 86% δεν έχει μελετήσει την πολιτική πρόσβασης του προσωπικού ή πρόσβασης στις εγκαταστάσεις.



Σχήμα 6.7: Ασφάλεια Δεδομένων μετά την υιοθέτηση του Υπολογιστικού Νέφους

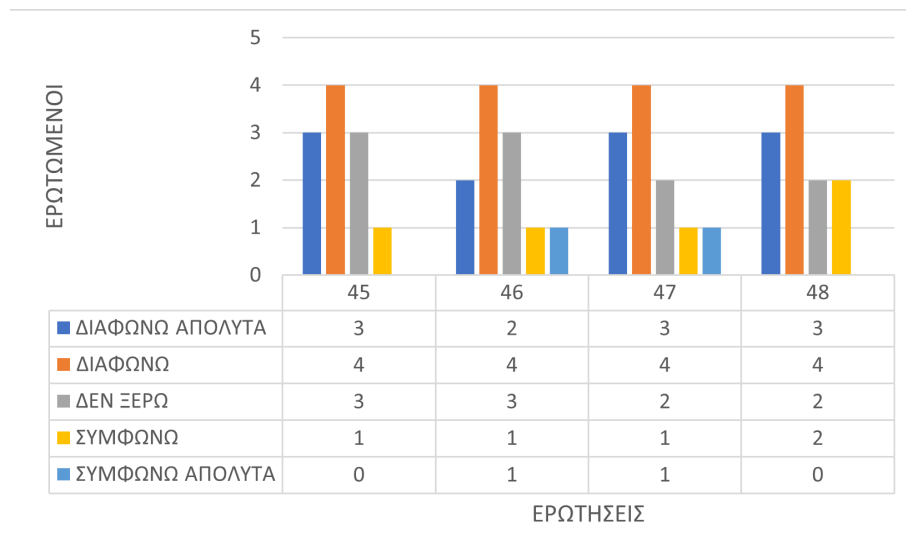
Το σχήμα 6.7 αναφέρεται στα δεδομένα. Παρατηρούμε ότι σε ποσοστό 54,5% δεν γνωρίζουν τη φυσική τοποθεσία των δεδομένων, και σε ποσοστό 54,5% περίπου δεν είναι σίγουροι ότι διατηρούν τη νομική ιδιοκτησία των δεδομένων τους. Σε ποσοστό 54,5% φαίνεται να μην γνωρίζουν την τύχη των δεδομένων στην περίπτωση που λήξει το συμβόλαιο με το πάροχο και σε ποσοστό 18% δεν είναι σίγουροι για το ποια θα είναι η τύχη των δεδομένων τους, Το 45,4% θεωρεί ότι είναι εύκολο να μεταφέρει τα δεδομένα σε άλλο πάροχο ενώ το ίδιο ποσοστό φαίνεται να μην είναι σίγουρο για το ποια είναι η πολιτική προστασίας της ιδιωτικότητας του παρόχου.



Σχήμα 6.8: Υποχρεώσεις παρόχου του Υπολογιστικού Νέφους

Για να διαπιστώσουμε το επίπεδο ενημερότητας των όρων των συμφωνιών επιπέδου υπηρεσιών (SLAs) θέσαμε ερωτήματα που αφορούν στο ύψος της αποζημίωσης που δικαιούται ο χρήστης στη περίπτωση που ο πάροχος δεν είναι συνεπής με τους όρους των (SLAs), και αφορά στη διαδικασία εξόδου από τη συμφωνία, στη συγκατάθεση μεταφοράς των δεδομένων σε άλλη τοποθεσία και τέλος για το χρονικό διάστημα που ο πάροχος διατηρεί αντίγραφα ασφαλείας των δεδομένων. Όπως βλέπουμε στο σχήμα 6.8, σε ποσοστό 27,7 % φαίνεται να γνωρίζουν το ποσό της αποζημίωσης που μπορούν να διεκδικήσουν, ενώ από τη διασπορά των απαντήσεων φαίνεται πως το 63,6% είτε δε γνωρίζουν είτε δεν είναι σίγουροι για το ποσό αποζημίωσης που δικαιούνται. Αντίθετα φαίνεται πως στο ερώτημα εάν γνωρίζουν τη διαδικασία εξόδου από τη συμφωνία το 54,5% έχει ενημερωθεί. Σε ποσοστό 36,3% δεν είναι σίγουροι ότι απαιτείται η συγκατάθεση τους για τη μεταφορά των δεδομένων σε άλλη τοποθεσία. Επίσης σε ποσοστό

45,4 % φαίνεται να μην είναι σίγουροι ότι γνωρίζουν το χρονικό διάστημα που διατηρούνται αντίγραφα ασφαλείας των δεδομένων από τον πάροχο.



Σχήμα 6.9: Δικαιώματα παρόχου του Υπολογιστικού Νέφους

Το σχήμα 6.9 αποτυπώνει τις απαντήσεις στα ερωτήματα αν ο πάροχος έχει το δικαίωμα μονομερούς απενεργοποίησης του λογαριασμού χρήστη, όπου το 90% είτε δε γνωρίζει είτε δεν ξέρει αν είναι εφικτό. Γενικά στις ερωτήσεις που αφορούν στα δικαιώματα του παρόχου και αφορούν το εφαρμοστέο δίκαιο κυριαρχεί η απάντηση διαφωνώ δηλαδή δεν γνωρίζουν σε ποσοστό 36,3%.

6.6 Συμπεράσματα

Το Υπολογιστικό Νέφος πρέπει να περιβληθεί από την ασπίδα της εμπιστοσύνης, ακεραιότητας και διαφάνειας μεταξύ του χρήστη και του παρόχου για να ενισχυθεί η υιοθέτηση και ανάπτυξη του. Οι Υπηρεσίες Υπολογιστικού Νέφους πέρα από τη μείωση του κόστους ή τις ευκολίες που παρέχουν τεχνολογικά, θα πρέπει να προσδίδουν ποιότητα στους παράγοντες που πλαισιώνουν τις παρεχόμενες υπηρεσίες όπως την εμπιστοσύνη, ασφάλεια αλλά και διαχείριση και διάθεση των πόρων. Με την έρευνα αυτής της εργασίας επιδιώχθηκε να βγει συμπέρασμα για το βαθμό ενημερότητας των χρηστών που έχουν υιοθετήσει τις Υπηρεσίες Υπολογιστικού Νέφους. Αρχικά ρωτήθηκαν για τα οφέλη του Υπολογιστικού Νέφους. Ένα από τα οφέλη του Υπολογιστικού Νέφους είναι η μείωση του κόστους που αφορά στην ανάπτυξη Υπηρεσιών, στην ανανέωση λογισμικού, στη συντήρηση είτε του λογισμικού είτε του υλικού και στο λειτουργικό κόστος. Φαίνεται πως μεγάλο ποσοστό των ερωτηθέντων περίπου το 70 - 80% συμφωνεί ότι έχει μειωθεί γενικά το κόστος ενώ σε ποσοστό περίπου 35% φαίνεται να μην είναι σίγουροι για τη μείωση του κόστους συντήρησης. Η ελαστικότητα, προσαρμοστικότητα είναι οφέλη του Υπολογιστικού Νέφους. Σε ποσοστό περίπου 70% φαίνεται ότι οι χρήστες συμφωνούν σε αυτό. Οι χρήστες λοιπόν δέχονται την ικανότητα προσαρμογής των υπολογιστικών πόρων στις ανάγκες τους, καθώς και την βελτίωση της διαχείρισης και διαθεσής τους μάλιστα με αρκετά καλή ανταπόκριση. Πολλή θετική είναι και η άποψη τους για την αξιοπιστία των υπολογιστικών πόρων, όπου το 60% θεωρεί ότι η αξιοπιστία των υπολογιστικών πόρων είναι μεγαλύτερη από αυτή των παραδοσιακών συστημάτων. Μελετήθηκε η ενημερότητα των χρηστών όσον αφορά στο τομέα της επίγνωσης των κινδύνων που απορρέουν από την υιοθέτηση του Υπολογιστικού Νέφους, όπως η προσωρινή μη διαθεσιμότητα των υπηρεσιών, η εξασφάλιση της ακεραιότητας, εμπιστευτικότητας και ιδιωτικότητας των δεδομένων, αλλά και η αποκατάσταση τους σε περίπτωση καταστροφών, είτε σε περίπτωση αλλαγής παρόχου αν εξασφαλίζεται η μεταφορά των δεδομένων αλλά και αν γενικά είναι ευάλωτο σε επιθέσεις όπως DoS. Τα συμπεράσματα στα οποία καταλήξαμε είναι ότι περίπου οι μισοί θεωρούν πως είναι ασφαλή τα δεδομένα τους αλλά σε ποσοστό 54,5%, δηλαδή οι μισοί περίπου φαίνεται να μην έχουν δώσει ιδιαίτερη βαρύτητα στο γεγονός ότι υπάρχει ασυνέπεια στους νόμους περί προστασίας των δεδομένων από χώρα σε χώρα. Άρα συμπεραίνουμε ότι η εντύπωση που έχουν για την ασφάλεια των δεδομένων είναι επίπλαστη. Επομένως πρέπει να ενισχυθεί η ενημερότητα όσον αφορά στη γνώση που αφορά στις χώρες που έχει επιλέξει ο πάροχος να συνεργάζεται και ποιο είναι το πλαίσιο που ισχύει για τις υπηρεσίες Υπολογιστικού Νέφους σε αυτές. Ένα έλλειμμα ενημερότητας φαίνεται να υπάρχει και όσον αφορά στην μεταφορά των δεδομένων

στην περίπτωση της αλλαγής παρόχου, αφού περίπου το 45% δε γνωρίζει τι συμβαίνει σε αυτή την περίπτωση. Και για τις επιθέσεις αλλά και για την αποκατάσταση ή διάθεση των υπηρεσιών φαίνεται να είναι μεγάλο το ποσοστό (περίπου 40%) αυτών που ούτε συμφωνούν ούτε διαφωνούν, δηλαδή δεν είναι σίγουροι για το τι ισχύει. Συμπεραίνουμε λοιπόν ότι η ενημερότητα των χρηστών όσον αφορά στους κινδύνους χρήσης του Υπολογιστικού Νέφους πρέπει να ενισχυθεί, ώστε να μπορούν οι χρήστες να προφυλαχθούν από τους κινδύνους και να μη χρησιμοποιούν διστακτικά τις υπηρεσίες Υπολογιστικού Νέφους. Αντίστοιχο έλλειμμα ενημερότητας φαίνεται να υπάρχει και στο τομέα της απόδοσης των υπηρεσιών, αφού περίπου το 40%, δε γνωρίζει το χρόνο διάθεσης των υπηρεσιών ή τον αριθμό των ενεργών συνδέσεων που μπορεί να εξυπηρετηθούν μια συγκεκριμένη χρονική στιγμή. Σημαντικός τομέας για να ερευνηθεί είναι η ενημερότητα που αφορά στην ασφάλεια. Γενικά, μπορούμε να συμπεράνουμε ότι περίπου οι μισοί έχουν ενημερωθεί για τις τεχνικές κρυπτογράφησης που εφαρμόζει ο πάροχος, και το ίδιο ποσοστό θεωρεί ότι είναι ασφαλή τα δεδομένα του. Βέβαια από την έρευνα προκύπτει ότι σε ποσοστό 86%, το οποίο είναι πολύ υψηλό, δεν είναι ενημερωμένοι για τη πολιτική πρόσβασης του προσωπικού αλλά και πρόσβασης στις εγκαταστάσεις. Συμπεραίνουμε ότι οι χρήστες δεν γνωρίζουν, δεν είναι ενημερωμένοι για το πόσο σημαντική είναι η πολιτική πρόσβασης που εφαρμόζει ο πάροχος για την ασφάλεια. Όσον αφορά στα δεδομένα τα συμπεράσματα είναι πως σε ποσοστό 55% περίπου δεν γνωρίζουν τη φυσική τοποθεσία αποθήκευσης των δεδομένων, γεγονός που μας κάνει να οδηγηθούμε στο συμπέρασμα ότι δεν είναι ενημερωμένοι για το πόσο σημαντικό είναι να γνωρίζει ο χρήστης τις χώρες στις οποίες αποθηκεύει τα δεδομένα ο πάροχος γιατί θα είναι πραγματικά σε θέση να ξέρει πόσο ασφαλή είναι τα δεδομένα του αφού θα ξέρει το νομικό πλαίσιο που ισχύει. Κι εδώ βλέπουμε πόσο σημαντική είναι η ενημερότητα για το χρήστη. Εξετάστηκε το επίπεδο επίγνωσης των όρων των συμφωνιών επιπέδου υπηρεσιών (SLAs) σχετικά με τις υποχρεώσεις και τα δικαιώματα του παρόχου ως προς το χρήστη. Τα συμπεράσματα που εξήχθησαν από τις απαντήσεις σχετικά είναι ότι σε ποσοστό 60% περίπου δε γνωρίζουν το ύψος της αποζημίωσης που δικαιούνται από το πάροχο. Φαίνεται επίσης πως οι χρήστες σε ποσοστό περίπου 40% δεν έχουν ξεκάθαρη εικόνα αν χρειάζεται η συγκατάθεση τους για τη μεταφορά των δεδομένων σε άλλη τοποθεσία ή το διάστημα που διατηρούνται αντίγραφα ασφαλείας των δεδομένων από το πάροχο. Από την έρευνα σχετικά με τα δικαιώματα του παρόχου καταλήγουμε πως σε ποσοστό 36% δε γνωρίζουν τι ισχύει, ποιο είναι δηλαδή το εφαρμοστέο δίκαιο. Πολύ σημαντικός ο ρόλος της ενημερότητας, αφού αν ο χρήστης είναι ενήμερος τότε θα εξετάσει προσεκτικά τους όρους των συμφωνιών επιπέδου υπηρεσιών (SLAs), ώστε να μην έρχονται σε αντίθεση με τις παρεχόμενες υπηρεσίες προς το χρήστη. Από την έρευνα προκύπτει πως οι επιχειρήσεις στον

μεγαλύτερο τους αριθμό γνωρίζουν τα οφέλη των υπηρεσιών του Υπολογιστικού Νέφους, αλλά παράλληλα υπάρχει προβληματισμός αφού απάντησαν πως δε γνωρίζουν για θέματα που αφορούν στην ασφάλεια των δεδομένων και την εμπιστοσύνη ως προς των πάροχο των υπηρεσιών αυτών. Καταλήγουμε στο συμπέρασμα πως ο ρόλος της ενημερότητας των χρηστών είναι κομβικός και μπορεί να αποτελέσει το μοχλό πίεσης προς τους παρόχους υπηρεσιών Υπολογιστικού Νέφους ώστε να δώσουν την αρμόζουσα βαρύτητα στην ασφάλεια και αξιοπιστία των παρεχόμενων υπηρεσιών τους.. Η ενημερότητα μπορεί να βοηθήσει το χρήστη να εμπιστευθεί και να κατανοήσει ότι μπορεί να χρησιμοποιήσει τις υπηρεσίες του Υπολογιστικού Νέφους με ασφάλεια, καλή απόδοση, προστασία της ιδιωτικότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων. Ο ενήμερος χρήστης θα απαιτήσει να υπάρξει διαφάνεια ως προς το τόπο αποθήκευσης των δεδομένων ώστε να εξασφαλισθεί ότι θα υπάρχει νομικό πλαίσιο που θα προστατεύει τα δεδομένα του. Κατά την επιλογή παρόχου θα εξετάσει το ενδεχόμενο αποζημίωσης από το πάροχο στην περίπτωση που δεν τηρηθούν τα συμφωνηθέντα σχετικά με τις παρεχόμενες υπηρεσίες. Ο ενήμερος χρήστης θα εξετάσει με προσοχή τους όρους των συμφωνιών επιπέδου υπηρεσιών ώστε να επιλέξει τον καλύτερο πάροχο για να εξασφαλίσει τη καλύτερη δυνατή παροχή υπηρεσιών.

Παράρτημα Α΄

Παράρτημα 1: Ερωτηματολόγιο έρευνας

Αγαπητοί Κυρίες και Κύριοι,

Ονομάζομαι Αμιλία Ζμπήτα και στο πλαίσιο υλοποίησης της πτυχιακής μου εργασίας στο Τμήμα Πληροφορικής του Ιόνιου Πανεπιστημίου, πραγματοποιώ έρευνα σχετικά με τη χρήση των υπηρεσιών Υπολογιστικού Νέφους από επιχειρήσεις στη χώρα.

Η συμμετοχή σας στην έρευνα είναι ανώνυμη. Όλα τα στοιχεία που θα συγκεντρωθούν στο πλαίσιο της έρευνας είναι εμπιστευτικά και θα χρησιμοποιηθούν αποκλειστικά για ερευνητικούς σκοπούς.

Το ερωτηματολόγιο περιλαμβάνει συνολικά 48 ερωτήσεις – προτάσεις. Για κάθε ερώτηση- πρόταση επιλέξτε την απάντηση που σας αντιπροσωπεύει καλύτερα (1: Διαφωνώ απόλυτα, 2: Διαφωνώ, 3: Ούτε Διαφωνώ Ούτε Συμφωνώ, 4: Συμφωνώ, 5: Συμφωνώ απόλυτα).

Σας ευχαριστώ προκαταβολικά για το χρόνο σας και τη βοήθεια σας στην υλοποίηση της εργασίας μου.

Με εκτίμηση, Αμιλία Ζμπήτα

Δημογραφικά χαρακτηριστικά επιχείρησης 1. Αντικείμενο ενασχόλησης επιχείρησης: ☐ Α-κίνητα, ☐ Ασφαλιστικές υπηρεσίες, ☐ Εκπαίδευση, ☐ Μέσα ενημέρωσης, ☐ Πληροφορική, ☐ Τηλεπικοινωνίες, ☐ Τουρισμός, ☐ Υγεία, ☐ Χρηματοπιστωτικές υπηρεσίες, ☐ Άλλο

2. Αριθμός υπαλλήλων: ☐ 1-10 υπάλληλοι, ☐ 11-50 υπάλληλοι, ☐ 51-100 υπάλληλοι, ☐ πάνω από 100 υπάλληλοι

Ερωτηματολόγιο

Οφέλη Υπολογιστικού Νέφους

- Αξιολογήστε τους παρακάτω παράγοντες στην επιχείρησή σας μετά την υιοθέτηση χρήσης υπηρεσιών Υπολογιστικού Νέφους, σε σχέση με το παρελθόν
1. Το αρχικό κόστος ανάπτυξης νέων υπηρεσιών πληροφορικής (νέες εγκαταστάσεις, εκπαίδευση) είναι χαμηλότερο
 2. Το συνολικό λειτουργικό κόστος του τομέα πληροφορικής, συμπεριλαμβανομένου του χρόνου, του εργατικού δυναμικού και των εγκαταστάσεων είναι χαμηλότερο
 3. Το συνολικό κόστος συντήρησης του υλικού και λογισμικού πληροφορικής, συμπεριλαμβανομένου του χρόνου, του ανθρώπινου δυναμικού και των εγκαταστάσεων είναι χαμηλότερο
 4. Η δαπάνη ανανέωσης λογισμικού, υλικού, εγκαταστάσεων και τεχνικών είναι χαμηλότερη
 5. Το λειτουργικό κόστος της επιχείρησης (μάρκετινγκ, παραγωγή, πωλήσεις και υπηρεσίες μετά πώλησης) είναι χαμηλότερο
 6. Η ταχύτητα εφαρμογής και χρήσης νέων πόρων πληροφορικής έχει βελτιωθεί σημαντικά
 7. Έχει βελτιωθεί σημαντικά η διαλειτουργικότητα μεταξύ διαφορετικών υπολογιστικών πόρων και εφαρμογών
 8. Η επεξεργασία πληροφοριών είναι αποτελεσματικότερη
 9. Ο χρόνος ανταπόκρισης προς τον πελάτη έχει βελτιωθεί σημαντικά
 10. Έχει περιοριστεί η ανάγκη προσαρμογής (customization) των υπολογιστικών πόρων χρήσης
 11. Έχει βελτιωθεί η ικανότητα προσαρμογής των υπολογιστικών πόρων χρήσης
 12. Έχει αυξηθεί η ικανότητα της επιχείρησης να προσαρμόζει τις διάφορες λειτουργίες της με βάση τις ανάγκες της αγοράς
 13. Έχει βελτιωθεί ο χρόνος επαναφοράς σε κανονική λειτουργία κατά την εμφάνιση προβλημάτων στη λειτουργία υπολογιστικών πόρων

14. Η δυνατότητα ανταλλαγής υπολογιστικών πόρων και δεδομένων με άλλες επιχειρήσεις είναι μεγαλύτερη
15. Η αξιοπιστία των υπολογιστικών πόρων είναι μεγαλύτερη
16. Διασφαλίζεται το απόρρητο των δεδομένων που βρίσκονται αποθηκευμένα στο σύννεφο
17. Ασυνεπείς νόμοι περί προστασίας δεδομένων μεταξύ των χωρών που φιλοξενούν τις υπηρεσίες Υπολογιστικού Νέφους
18. Δυσκολία αλλαγής παρόχου υπηρεσιών Υπολογιστικού Νέφους
19. Έλλειψη εφαρμογής προγραμμάτων αποκατάστασης των καταστροφών και των σχεδίων αντιμετώπισης έκτακτης ανάγκης σε περιβάλλον Υπολογιστικού Νέφους εκ μέρους των χρηστών ή των επιχειρήσεων
20. Δυσκολία μεταφοράς – διασύνδεσης δεδομένων μετά το πέρας του συμβολαίου με κάποιον πάροχο υπηρεσιών Υπολογιστικού Νέφους
21. Ανεπαρκής κατάρτιση σχετικά με τις υπηρεσίες και τη χρήση της Υπολογιστικού Νέφους εκ μέρους των χρηστών
22. Προσωρινή μη διαθεσιμότητα υπηρεσιών Υπολογιστικού Νέφους
23. Κρυμμένα κόστη χρήσης υπηρεσιών του Υπολογιστικού Νέφους λόγω μη διαφανών μοντέλων λειτουργίας στο σύννεφο
24. Κίνδυνος επιθέσεων άρνησης εξυπηρέτησης (DoS) σε περιβάλλον Υπολογιστικού Νέφους
25. Μη εξουσιοδοτημένη πρόσβαση σε επιχειρηματικά δεδομένα ή εφαρμογές στο σύννεφο

Επίγνωση στοιχείων συμφωνίας επιπέδου υπηρεσία (Service Level Agreement)

- Πόσο καλά γνωρίζεται τα παρακάτω χαρακτηριστικά – στοιχεία των υπηρεσιών Υπολογιστικού Νέφους που χρησιμοποιείται:

- **Απόδοση**

26. Γνωρίζω το ελάχιστο ποσοστό χρόνου (availability) που είναι διαθέσιμες οι υπηρεσίες Υπολογιστικού Νέφους εκ μέρους του παρόχου υπηρεσιών Υπολογιστικού Νέφους που συνεργάζομαι
27. Γνωρίζω ποιος ο χρόνος που απαιτείται προκειμένου να είναι διαθέσιμη μία υπηρεσία από τη στιγμή που θα την αιτηθώ (respond time)
28. Γνωρίζω τον μέγιστο αριθμό ταυτόχρονα ενεργών ατομικών συνδέσεων στις υπηρεσίες Υπολογιστικού Νέφους (simultaneous connections) που χρησιμοποιώ
29. Γνωρίζω τον αριθμό των αιτημάτων που μπορούν να εξυπηρετήσουν οι υπηρεσίες Υπολογιστικού Νέφους που χρησιμοποιώ σε συγκεκριμένη χρονική περίοδο (throughput)

- **Ασφάλεια**

30. Γνωρίζω σχετικά με τις τεχνικές κρυπτογράφησης που εφαρμόζει ο πάροχος υπηρεσιών Υπολογιστικού Νέφους
31. Έχω μελετήσει με λεπτομέρεια το σχέδιο αποκατάστασης καταστροφών του παρόχου υπηρεσιών Υπολογιστικού Νέφους
32. Γνωρίζω σχετικά με τα δεδομένα που μπορώ να λαμβάνω από τον πάροχο σχετικά με το ιστορικό πρόσβασης και χρήσης των υπηρεσιών Υπολογιστικού Νέφους
33. Έχω μελετήσει τις διασφαλίσεις ακεραιότητας των δεδομένων εκ μέρους του παρόχου υπηρεσιών Υπολογιστικού Νέφους
34. Έχω μελετήσει την πολιτική πρόσβασης του προσωπικού του παρόχου στα δεδομένα που βρίσκονται αποθηκευμένα στο σύννεφο

35. Γνωρίζω σχετικά με την πολιτική πρόσβασης στις εγκαταστάσεις του παρόχου από μη εξουσιοδοτημένη πρόσβαση, βλάβη ή υποκλοπή

• **Δεδομένα**

36. Γνωρίζω τη φυσική τοποθεσία αποθήκευσης των δεδομένων στο σύννεφο
37. Διατηρώ τη νομική ιδιοκτησία των δεδομένων που βρίσκονται αποθηκευμένα στο σύννεφο
38. Γνωρίζω ποια θα είναι η τύχη των δεδομένων που φιλοξενούνται στο σύννεφο κατά τη λήξη του συμβολαίου με τον πάροχο υπηρεσιών Υπολογιστικού Νέφους
39. Μπορώ εύκολα να μεταφέρω τα δεδομένα σε έναν άλλον πάροχο υπηρεσιών Υπολογιστικού Νέφους
40. Γνωρίζω την πολιτική προστασίας της ιδιωτικότητας των δεδομένων που εφαρμόζεται από τον πάροχο υπηρεσιών Υπολογιστικού Νέφους

• **Υποχρεώσεις παρόχου**

41. Γνωρίζω το ύψος της αποζημίωσης που θα λάβω εάν ο πάροχος υπηρεσιών Υπολογιστικού Νέφους δεν είναι συνεπής με τους όρους του SLA (Service Level Agreement)
42. Γνωρίζω εάν υπάρχει ή όχι τεκμηριωμένη διαδικασία εξόδου ως μέρος της συμφωνίας παροχής υπηρεσιών Υπολογιστικού Νέφους
43. Γνωρίζω εάν απαιτείται η συγκατάθεση μου για τη μεταφορά των δεδομένων μου σε άλλη τοποθεσία
44. Γνωρίζω το χρονικό διάστημα που είναι υποχρεωμένος ο πάροχος να διατηρεί αντίγραφα ασφαλείας των δεδομένων

- **Δικαιώματα παρόχου**

45. Γνωρίζω εάν κατέχει ο πάροχος το δικαίωμα μονομερώς να απενεργοποιήσει τον λογαριασμό μου
46. Γνωρίζω τις συνθήκες κάτω από τις οποίες είναι δυνατή η διάθεση των δεδομένων της επιχείρησής μου στο σύννεφο σε κάποια νομική υπηρεσία ή δικαστική αρχή
47. Γνωρίζω ποιο το εφαρμοστέο δίκαιο για την επίλυση πιθανών διαφορών με τον πάροχο υπηρεσιών Υπολογιστικού Νέφους
48. Γνωρίζω εάν στη συμφωνία καταγράφονται με λεπτομέρεια οι υπηρεσίες οι οποίες δεν παρέχονται από τον πάροχο στο πλαίσιο της συμφωνίας που έχω συνάψει μαζί του

Βιβλιογραφία

- [1] Keith D.Foote, *A Brief History of Cloud Computing*,url="<https://www.dataversity.net/brief-history-cloud-computing/>".
- [2] Mell Peter and Grance Tim and others, *The NIST definition of cloud computing*, Computer Security Division, Information Technology Laboratory, National.
- [3] C.Miyachi, *What is "Cloud"?It is time to update the NIST definition?*,year=2018,volume=5,number=3,pages=6-11.
- [4] Johan Den Haan, *The Cloud Landscape Described, Categorized, and Compared*,url="<http://www.theenterpriseearchitect.eu/blog/categorize-compare-cloud-vendors/>".
- [5] Tim Mather, Subra Kumaraswamy, and Shahed Latif , *Cloud Security and Privacy*, ISBN: 978-0-596-80276-9.
- [6] Kavis, Michael J, *Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS)*, ISBN: 9781118826461.
- [7] Hill Richard and Hirsch Laurie and Lake Peter and Moshiri Siavashi, *Guide to Cloud Computing Principles and Practice* , ISBN:447146034, 9781447146032 .
- [8] Antonopoulos Nick and Gillam Lee , *Cloud computing* , 2010,Springer, ISBN: 9783319546445.
- [9] Vacca John R, *Cloud computing security: foundations and challenges*, year=2016, publisher=CRC Press.

- [10] Liu Fang and Tong Jin and Mao Jian and Bohn Robert and Messina John and Badger Lee and Leaf Dawn, *NIST cloud computing reference architecture*, NIST special publication,year=2011, volume= 500,pages=1–28.
- [11] Chandrasekaran K, *Essentials of cloud computing*, year=2014,publisher= Chapman and Hall/CRC ,ISBN-13: 978-1-4822-0544-2 (eBook - PDF).
- [12] Jadeja Yashpalsinh and Modi Kirit, *Cloud computing-concepts, architecture and challenges*, 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET),pages=877–880.
- [13] Wang Lizhe and Tao Jie and Kunze Marcel and Castellanos Alvaro Canales and Kramer David and Karl Wolfgang, *Scientific cloud computing: Early definition and experience*,2008 10th ieee international conference on high performance computing and communications,pages=825–830.
- [14] Hussein Nidal Hassan and Khalid Ahmed, *A survey of Cloud Computing Security challenges and solutions* ,year=2016, journal=International Journal of Computer Science and Information Security,volume=14,number=1,pages=52,publisher=LJS Publishing.
- [15] Iqba Salman and Kiah Miss Laiha Mat and Anuar Nor Badrul and Daghighi Babak and Wahab Ainuddin Wahid Abdul and Khan Suleman, *Service delivery models of cloud computing: security issues and open challenges*, year=2016, journal=Security and Communication Networks, volume=9,number=17, pages=4726–4750, publisher=Wiley Online Library.
- [16] Almorsy Mohamed and Grundy John and Müller Ingo, *An analysis of the cloud computing security problem* ,year=2016, journal=arXiv preprint arXiv:1609.01107.
- [17] Chao Lee, *Cloud Computing Networking: Theory, Practice, and Development*, year=2015, publisher=Auerbach Publications.
- [18] Chouhan Priyanka and Singh Rajendra, *Security attacks on cloud computing with possible solution*,year=2016,journal=International Journal of Advanced Research in Computer Science and Software Engineering,volume=6,number=1.
- [19] Esposito Christian and De Santis Alfredo and Tortora Genny and Chang Henry and Choo Kim-Kwang Raymond , *Blockchain: A panacea for healthcare cloud-based data security and privacy?* , year=2018 , journal = IEEE Cloud Computing ,pages=31–37.

- [20] Badger Mark Lee and Grance Timothy and Patt-Corner Robert and Voas Jeffery M , *Cloud computing synopsis and recommendations*, year=2012, publisher=National Institute of Standards & Technology .
- [21] Ramachandra Gururaj and Iftikhar Mohsin and Khan Farrukh Aslam, *A comprehensive survey on security in cloud computing*, year=2017,journal=Procedia Computer Science,volume=110, pages=465–472, publisher=Elsevier.
- [22] Ashraf Imran , *An overview of service models of cloud computing* , year= 2014 , journal= International Journal of Multidisciplinary and Current Research,pages=779–783.
- [23] Lee Gary , *Cloud networking: understanding cloud-based data center networks*, 2014 , publisher= Morgan Kaufmann.
- [24] Benson Theophilus and Akella Aditya and Shaikh Anees and Sahu Sambit , *CloudNaaS: a cloud networking platform for enterprise applications* , 2011 ,booktitle= Proceedings of the 2nd ACM Symposium on Cloud Computing.
- [25] Gupta Abhinav Nath and Thilagam P Santhi, *Detection of XML signature wrapping attack using node counting*,year=2016, booktitle=Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC-16’), pages=57–63, organization = Springer.
- [26] Vljajic Natalija and Chowdhury Mashruf and Litoiu Marin, *IP Spoofing In and Out of the Public Cloud: From Policy to Practice*, year=2019, journal=Computers, volume=8, number=4, pages=81,publisher=Multidisciplinary Digital Publishing Institute.
- [27] Hashizume, Keiko and Rosado, David G and Fernández-Medina, Eduardo and Fernandez, Eduardo B, *An analysis of security issues for cloud computing*, year=2013, journal=Journal of internet services and applications, volume=4, number=1, pages=1–13, publisher=Springer.
- [28] Kumar P Ravi and Raj P Herbert and Jelciana P, *Exploring data security issues and solutions in cloud computing*,year=2018,journal=Procedia Computer Science, volume=125, pages=691–697, publisher=Elsevier.

- [29] AWS Security Whitepaper , *Amazon Web Services: Overview of Security Processes*, 2017 , url = <https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf> .
- [30] Sabir Sabiyyah , *Security Issues in Cloud Computing and their Solutions: A Review* , 2018 , journal= INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, volume=9, number=11,pages= 343–346 .
- [31] Vairagade Rupali Sachin and Vairagade Nitin Ashokrao, *Cloud Computing Data Storage and Security Enhancement* , 2012 , journal= International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, volume = 1.
- [32] Islam Tariqul and Manivannan D and Zeadally Sherali , *A classification and characterization of security threats in cloud computing* ,year=2016,journal=Int. J. Next-Gener. Comput, volume=7, number=1.
- [33] Sharma Shubhanjali and Gupta Garima and Laxmi PR, *A survey on cloud security issues and techniques*,2014, journal=arXiv preprint arXiv:1403.5627.
- [34] Zissis Dimitrios and Lekkas Dimitrios, *Addressing cloud computing security issues*,2012,journal=Future Generation computer systems ,volume=28,number=3,pages=583–592.
- [35] Hassan Wajid and Chou Te-Shun and Li Xiaoming and Appiah-Kubi Patrick and Tamer Omar, *Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks*, year=2019, journal=Int J Inf & Commun Technol ISSN,volume=2252,number=8776,pages=8776.
- [36] Top Threats Working Group and others, *The treacherous 12: cloud computing top threats in 2016*,year=2016,journal=Cloud Security Alliance,url="<https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf>".
- [37] Gonzales Dan and Kaplan Jeremy M and Saltzman Evan and Winkelman Zev and Woods Dulani, *Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds* ,year= 2015 , journal=IEEE Transactions on Cloud Computing, volume=5, number=3,pages=523–536.

- [38] Chiregi Matin and Navimipour Nima Jafari, *A comprehensive study of the trust evaluation mechanisms in the cloud computing*, year=2017, journal=Journal of Service Science Research, volume=9, number=1, pages=1–30, publisher=Springer.
- [39] Hogan Michael and Liu Fang and Soko, Annie and Tong Jin, *Nist cloud computing standards roadmap*, year=2011, journal=NIST Special Publication, volume=35, pages=6–11.
- [40] Loutas Nikolaos and Kamateri Eleni and Bos, Filippo and Tarabanis Konstantinos, *Cloud computing interoperability: the state of play*, booktitle=2011 IEEE Third International Conference on Cloud Computing Technology and Science, pages=752–757.
- [41] Alzahrani Abdulrahman and Alqazzaz Ali and Zhu Ye and Fu Huirong and Al-mashfi Nabil, *Web application security tools analysis*, year=2017, booktitle=2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids), pages=237–242, organization=IEEE.
- [42] IEC's members, *ISO/IEC JTC 1/SC 38 Cloud Computing and Distributed Platforms*, url="https://www.iec.ch/dyn/www/f?p=103:22:1849939180502:::FSP_ORG_ID,FSP_LANG_ID\mskip\medmuskip7608,25".
- [43] Angadi Abhinay B and Angadi Akshata B and Gull Karuna C, *Security Issues with Possible Solutions in Cloud Computing-A Survey*, year=2013, journal=International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), volume=2, number=2, pages=2278–1323.
- [44] Binu Sumitra and Misbahuddin Mohammed, *A survey of traditional and cloud specific security issues*, year=2013, booktitle=International Symposium on Security in Computing and Communication, pages=110–129.
- [45] Chen Jianfeng and Xu Rui and Li Chunlin, *Research of Security Situational Awareness and Visualization Approach in Cloud Computing*, year=2018, booktitle=2018 International Conference on Networking and Network Applications (NaNA), pages=201–205, organization=IEEE.

- [46] Lins Sebastian and Schneider Stephan and Sunyaev Ali, *Trust is good, control is better: Creating secure clouds by continuous auditing*, year=2016, journal=IEEE Transactions on Cloud Computing, volume=6, number=3, pages=890–903, publisher=IEEE.
- [47] HEİDARPOUR Mostafa and RASHİDİ Ali J and AHMADİ Kourosch D, *Cyber Situational Awareness using Intelligent Information Fusion Engine (IIFE)*, 2015, journal=Cumhuriyet Üniversitesi Fen-Edebiyat Fakültesi Fen Bilimleri Dergisi, volume=36, number=3,pages=3218–3229.
- [48] Kundra Vivek, *Federal cloud computing strategy* , year=2011, publisher=White House [Chief Information Officers Council].
- [49] Suzette Kent , *FEDERAL CLOUD COMPUTING STRATEGY*,year=2019,url="<https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf>."
- [50] Muijs Daniel, *Doing quantitative research in education with SPSS*, year=2010, publisher=Sage.
- [51] Creswell John W and Creswell J David, *Research design: Qualitative, quantitative, and mixed methods approaches*, year=2017, publisher=Sage publications.
- [52] Allen Mike and Titsworth Scott and Hunt Stephen K, *Quantitative research in communication*,year=2008, publisher=Sage Publications.
- [53] Dutta Amab and Peng Guo Chao Alex and Choudhary Alok, *Risks in enterprise cloud computing: the perspective of IT experts*,year=2013, journal=Journal of Computer Information Systems,volume=53, number=4, pages=39–48, publisher=Taylor & Francis.
- [54] Chen Thomas and Chuang Ta-Tao and Nakatani Kazuo, *The perceived business benefit of cloud computing: An exploratory study*,year=2016,journal=Journal of International Technology and Information Management, volume=25, number=4, pages=7.
- [55] Dr Gudapati Syam Prasad and Vidya S. Gaikwad, *A Survey on User Awareness of Cloud Security*,year = 2018,journal = International Journal of Engineering & Technology,volume = 7,number = 2.32.

- [56] Mijuskovic Adriana and Ferati Mexhid, *Cloud Storage Privacy and Security User Awareness: A Comparative Analysis between Dutch and Macedonian Users*, year=2018, booktitle=Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pages=1362–1383, publisher=IGI Global.
- [57] McMillan J and Schumacher S, *Research in Education (Seventh)*, year=2014, publisher=London: Pearson Education Limited.
- [58] Lewis Grace A, *Role of standards in cloud-computing interoperability*, year=2013, booktitle=2013 46th Hawaii International Conference on System Sciences, pages=1652–1661.
- [59] Rowley Jenny, *Designing and using research questionnaires*, year=2014, journal=Management Research Review, publisher=Emerald Group Publishing Limited.
- [60] Evans Joel R and Mathur Anil, *The value of online surveys*, year=2005, journal=Internet research, year=2005, publisher=Emerald Group Publishing Limited.
- [61] Roberts Margaret E and Stewart Brandon M and Tingley Dustin and Lucas Christopher and Leder-Luis Jetson and Gadarian Shana Kushner and Albertson Bethany and Rand David G, *Structural topic models for open-ended survey responses*, year=2014, journal=American Journal of Political Science, volume=58, number=4, pages=1064–1082, publisher=Wiley Online Library.
- [62] Bowling A, *Research Methods in Health: Investigating Health and Health Services* Open University Press: Buckingham, year=1997, publisher=Philadelphia.
- [63] Saravanan K and Rajaram M, *An Exploratory Study of Cloud Service Level Agreements-State of the Art Review*, year=2015, journal=INFOCOMP Journal of Computer Science, volume=18, number=1, pages=32–56.
- [64] Amazonas José Roberto and Akbari-Moghanjoughi Ayyoub and Santos-Boada Germán and Pareta Josep Solé, *Service Level Agreements for Communication Networks: A Survey*, year=2019, journal=International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), volume=2, number=2, pages=2278–1323.

- [65] Terfas Hebatalla, *The analysis of cloud computing service level agreement (SLA) to support cloud service consumers with the SLA creation process*,year=2019,school=École de technologie supérieure.
- [66] Fan Weimiao and Yan Zheng, *Factors affecting response rates of the web survey: A systematic review* , year=2010,journal=Computers in human behavior, volume=26, number=2, pages=132–139, publisher=Elsevier.
- [67] Milliner B and Flowers S, *Form technology for language teachers: How do you like your monkey*,year=2015, journal=The Language Teacher, volume=39, number=3, pages=24–27.
- [68] Haddad Rami J and Kalaani Youakim, *Google Forms: A Real-Time Formative Assessment Approach for Adaptive Learning*,year=2014,booktitle=Proceedings of the 2014 ASEE Annual Conference & Exposition, Indianapolis, IN. age, volume=26, number=11.
- [69] Myers Michael D and Avison David, *Qualitative research in information systems: a reader*,year=2002,publisher=Sage.
- [70] Brownell Peter, *Research methods in management accounting*,year=1995,publisher=Coopers and Lybrand and Accounting Association of Australia and New Zealand.
- [71] Open UK University, *Cronbach's Alpha*,year=2014,url="<https://www.open.ac.uk/socialsciences/spsstutorial/files/tutorials/cronbachs-alpha.pdf>".
- [72] Baumgartner Hans and Steenkamp Jan-Benedict EM, *Response styles in marketing research: A cross-national investigation*,year=2001,journal=Journal of marketing research, volume=38,number=2, pages=143–156,publisher=SAGE Publications Sage CA: Los Angeles, CA.
- [73] Bishop George F, *Experiments with the middle response alternative in survey questions*, year=1987, journal=Public Opinion Quarterly, volume=51, number=2, pages=220–232,publisher=Oxford University Press.
- [74] Dawes John, *Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales*,year=2008, jour-

- nal=International journal of market research,volume=50,number=1,pages=61–104,
publisher=SAGE Publications Sage UK: London, England.
- [75] Sachdev Sheetal B and Verma Harsh V, *Relative importance of service quality dimensions: A multisectoral study*,year=2004,journal=Journal of services research, volume=4, number=1.
- [76] Weil, Timothy R, *Standards for Cloud Risk Assessments-What's Missing?*,year=2020, booktitle=2020 IEEE Cloud Summit, pages=11–17, organization=IEEE.

Συντμήσεις

API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
AWS	Amazon Web Services
CPU	Central PProcessing Unit
CRM	Customer Relationship Management
CSS	Cascading Style Sheets
DaaS	Data as a Service
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service

EC2	Elastic Compute Cloud
ERP	Enterprise resource planning
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet service provider
NaaS	Network as a service
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SDN	Software Defined Networking
SDS	Software Defined Storage
SLA	Service-Level Agreement
SLO	Service Level Objective
SOA	Service-oriented architecture
SOAP	Simple Object Access Protocol
SQO	Service Qualitive Objective
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single sign-on
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

VM	Virtual Machine
VPN	Virtual Private Network
WSDL	Web Services Description Language
XaaS	Anything as a Service
XML	eXtensible Markup Language
XSS	Cross-site scripting

Γλωσσάρι Ξενικών Όρων

API	Διασύνδεση Προγραμματισμού Εφαρμογών
Browser	Φυλλομετρητής
CaaS	Επικοινωνίες ως Υπηρεσία
Cloud Computing	Υπολογιστικό Νέφος
CPU	Κεντρική Μονάδα Επεξεργασίας
CRM	Ο τρόπος διαχείρισης της σχέσης των διαφημιζόμενων με τη χρήση ειδικών εργαλείων προγραμματισμού
CSS	Αλληλουχία Φύλλων Στυλ
DaaS	Δεδομένα ως Υπηρεσία
ERP	Συστήματα Ενδοεπιχειρησιακού Προγραμματισμού
Firewall	Το σύνολο του τεχνικού εξοπλισμού που χρησιμοποιείται για την ασφάλεια των ιδιωτικών πληροφοριών
Hacker	Χρήστης που εισβάλλει παράνομα σε μια ιστοσελίδα

Host	Ο υπολογιστής που φιλοξενεί διαφόρου τύπου δεδομένα
HTTP	Πρωτόκολλο μεταφοράς υπερκειμένου
HTTPS	Ασφαλές Πρωτόκολλο μεταφοράς υπερκειμένου
Hybrid Cloud	Υβριδικό Νέφος
Hypervisor	Λογισμικό ελέγχου που δημιουργεί και εκτελεί Εικονικές Μηχανές
IaaS	Διαδίκτυο ως Υπηρεσία
ISO	Διεθνής Οργανισμός Τυποποίησης
ISP	Η εταιρεία παροχής σύνδεσης στο Διαδίκτυο
Log File1	Αρχείο στο οποίο καταχωρούνται όλες οι κινήσεις που γίνονται σε έναν Ιστότοπο
Middleware	Ενδιάμεσο Λογισμικό
Multitenancy	Πολλαπλή Χρήση Πόρων
PaaS	Πλατφόρμα ως Υπηρεσία
PII	Στοιχεία προσωπικής ταυτοποίησης
Public Cloud	Δημόσιο Νέφος

Private Cloud	Ιδιωτικό Νέφος
Router	Δρομολογητής
SaaS	Λογισμικό ως Υπηρεσία
SDN	Δίκτυο καθοριζόμενο από Λογισμικό
SDS	Πόροι αποθήκευσης καθοριζόμενοι από λογισμικό
Server	Ο κεντρικός υπολογιστής που εχυπηρετεί όλους τους υπόλοιπους υπολογιστές του δικτύου διατηρώντας αποθηκευμένα λογισμικό και δεδομένα
Session	Η πλήρης επίσκεψη σε μια τοποθεσία του Διαδικτύου που διέπει την μετάδοση και ροή των δεδομένων
SLA	Σύμβαση Επιπέδου Υπηρεσί'ν
SOA	Υπηρεσιοστρεφής Αρχιτεκτονική
SOAP	Απλό Πρωτόκολλο Προσπέλασης Αντικειμένων
SQO	Αντικείμενο Ποιότητας Υπηρεσίας
SSH	Ασφαλές Δικτυακό Πρωτόκολλο για τη μεταφορά των δεδομένων μεταθύ υπολογιστών
SSL	Κρυπτογραφημένη σύνδεση μεταξύ του διακομιστή και του φυλλομετρητή του χρήστη
SSO	Σύστημα Ενιαίας Πρόσβασης

Switch	Μεταγωγέας
TCP/IP	Βασικό πρωτόκολλο του Διαδικτύου
TLS	Πρωτόκολλο Κρυπτογράφησης μεταξύ του επιπέδου εφαρμογών και του επιπέδου μεταφοράς
Virtualization	Τεχνολογία Εικονοποίησης
VLAN	Εικονικό Τοπικό Δίκτυο
VM	Εικονική Μηχανή
VPN	Εικονικό Ιδιωτικό Δίκτυο
WSDL	Γλώσσα περιγραφής υπηρεσιών Ιστού
XaaS	Anything ως Υπηρεσία
XML	Είναι γλώσσα που χρησιμοποιείται για να καθορίσει νέες Markup γλώσσες

Ευρετήριο

- Multitenancy, 4
- Platform as a service (PaaS), 9
- Private Cloud, 13
- Public Cloud, 12
- Software as a Service (SaaS), 8
- single-sign-on (SSO), 43
- Anything as a Service (XaaS), 11
- Cloud computing, 2
- Hybrid Cloud, 14
- Infrastructure as a Service (IaaS), 10
- SAML (Security Assertion Markup Language), 43
- SLA, 37
- Service Level Objectives (SLO), 38
- Service Qualitative Objectives (SQO), 38
- Ακεραιότητα, 21
- Εικονοποίηση, 6
- Εμπιστευτικότητα, 21
- Ευπάθειες του συστήματος, 16
- Ιδιωτικό Νέφος, 13
- Προτυποποίηση, 36
- Αντικείμενα Ποιότητας Υπηρεσιών, 38
- Αντικειμένων Επιπέδου Υπηρεσιών, 38
- Απειλές, 16
- Απώλεια δεδομένων, 16
- Διαλειτουργικότητα, 41
- Δομή ως Υπηρεσία, 10
- Επίθεση εκ των έσω, 16
- Επιθέσεις, 18
- Κρυπτογράφηση, 39
- Λογισμικό ως Υπηρεσία, 8
- Μοντέλα Ανάπτυξης, 12
- Μοντέλα Υπηρεσιών, 8
- Παραβίαση των δεδομένων, 16
- Πλατφόρμα ως υπηρεσία, 9
- Συμφωνίες Επιπέδου Υπηρεσιών, 37
- Υβριδικό Νέφος, 14
- Φορητότητα, 41