ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

"ΜΕΛΕΤΗ ΖΗΤΗΜΑΤΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΑ ΝΕΦΗ"

Διπλωματική Εργασία

του

Μήλιου Αθανάσιου

Θεσσαλονίκη, Νοέμβριος 2020

"ΜΕΛΕΤΗ ΖΗΤΗΜΑΤΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΑ ΝΕΦΗ"

Μήλιος Αθανάσιος

Πτυχίο Οικονομικών Επιστημών, ΑΠΘ 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Παπαδημητρίου Παναγιώτης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 4/11/2020

Παπαδημητρίου Παναγιώτης	Πετρίδου Σοφία	Σακελλαρίου Ηλίας
.....	.....	.....

Περίληψη

Ο σκοπός της έρευνας αυτής είναι να μελετήσει τα κύρια ζητήματα ιδιωτικότητας στα υπολογιστικά νέφη. Αρχικά, γίνεται μία εκτενής παρουσίαση της δομής, των υπηρεσιών και των μοντέλων ανάπτυξης των υπολογιστικών νεφών. Τα τελευταία περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα, πράγμα που σημαίνει ότι παραμονεύουν κίνδυνοι ως προς την προστασία τους. Για να ερευνηθεί διεξοδικά το θέμα των παραβιάσεων ιδιωτικότητας στο υπολογιστικό νέφος, έγινε εκτενής βιβλιογραφική έρευνα σε δύο κατηγορίες: τις παραβιάσεις ιδιωτικότητας από κακόβουλους χρήστες και τις παραβιάσεις ιδιωτικότητας από αναξιόπιστους παρόχους cloud. Πιο συγκεκριμένα, στις παραβιάσεις ιδιωτικότητας από κακόβουλους χρήστες παρουσιάζονται οι απειλές απορρήτου σε δύο περιπτώσεις: κατά τη μεταφορά δεδομένων από και προς τον διακομιστή του παρόχου, καθώς και κατά την αποθήκευση και επεξεργασία των δεδομένων εντός της υποδομής του cloud. Στην περίπτωση των παρόχων cloud παρουσιάστηκαν έμμεσοι και άμεσοι τρόποι, με τους οποίους τίθεται σε κίνδυνο η ιδιωτικότητα των χρηστών. Τέλος, μελετήθηκαν κάποιες τεχνικές, οι οποίες μπορούν να βοηθήσουν την διασφάλιση της ιδιωτικότητας στα υπολογιστικά νέφη.

Λέξεις Κλειδιά: Υπολογιστικό νέφος, ευαίσθητα δεδομένα, κακόβουλος χρήστης παραβίαση ιδιωτικότητας

Abstract

The goal of this thesis is to study the main issues of privacy in cloud computing. Firstly, there is an extensive presentation of the structure, services and development models of cloud computing. The latter contains sensitive personal information, which means that there are risks in terms of their protection. In order to thoroughly investigate the issue of privacy breaches in the cloud, extensive bibliographic research was conducted in two categories: privacy breaches by malicious users and privacy breaches by unreliable cloud providers. More specifically, privacy breaches by malicious users present privacy threats in two cases: against the transfer of data to and from the provider's server, as well as during the storage and processing of data within the cloud infrastructure. In the case of cloud providers, there are indirect and direct ways in which users' privacy is compromised. Finally, some techniques have been studied that can help ensure the privacy of cloud computing.

Keywords: Cloud computing, sensitive data, malicious user violating privacy

Πρόλογος – Ευχαριστίες

Η παρούσα Διπλωματική Εργασία, θέμα της οποίας είναι: «Μελέτη ζητημάτων ιδιωτικότητας σε υπολογιστικά νέφη», εκπονήθηκε κατά την περίοδο του ακαδημαϊκού έτους 2019-2020, στα πλαίσια του προγράμματος μεταπτυχιακών σπουδών στην Εφαρμοσμένη Πληροφορική του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας.

Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του κ. Παναγιώτη Παπαδημητρίου, Επίκουρου Καθηγητή του Τμήματος Εφαρμοσμένης Πληροφορικής.

Με την ολοκλήρωση του Μεταπτυχιακού Προγράμματος Σπουδών στο τμήμα της Εφαρμοσμένης Πληροφορικής, μου είναι απαραίτητο να ευχαριστήσω όλους εκείνους τους ανθρώπους που μου συμπαραστάθηκαν και με στήριξαν στην πορεία αυτή.

Κυρίως, θα ήθελα να ευχαριστήσω την γυναίκα μου, Νεφέλη, για την τεράστια ηθική και ψυχολογική συμπαράσταση, που μου προσέφερε κατά την διεκπεραίωση της διπλωματικής μου μελέτης.

Επίσης, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κύριο Παπαδημητρίου Παναγιώτη, για την άψογη συνεργασία και για τις εποικοδομητικές παρατηρήσεις του, που είχαν καθοριστικό ρόλο για την ολοκλήρωση της συγγραφής της εργασίας μου.

Τέλος, ευχαριστώ όλους όσοι με στήριξαν στην ολοκλήρωση της διπλωματικής μου εργασίας.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

1. Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Αναμφίβολα, η δημοτικότητα και η επιτυχία του υπολογιστικού νέφους έχουν εκτοξευθεί στα ύψη την τελευταία δεκαετία. Ωστόσο, το υπολογιστικό νέφος έχει αλλάξει δραματικά τον τρόπο διαχείρισης των πληροφοριών και ειδικά στην περίπτωση των προσωπικών δεδομένων. Το ζήτημα της ιδιωτικότητας και της ασφάλειας των δεδομένων υπήρξε σταθερά ένα σημαντικό ζήτημα στην τεχνολογία των πληροφοριών. Το ζήτημα αυτό στο περιβάλλον του υπολογιστικού νέφους γίνεται ιδιαίτερα σοβαρό, διότι τα δεδομένα καθίστανται περισσότερο ευάλωτα, καθώς βρίσκονται διασκορπισμένα σε διαφορετικά μέρη του πλανήτη ταυτόχρονα. Χωρίς γνώση της φυσικής θέσης του διακομιστή ή του τρόπου με τον οποίο γίνεται η επεξεργασία των προσωπικών δεδομένων, οι τελικοί χρήστες καταναλώνουν υπηρεσίες υπολογιστικού νέφους, χωρίς να έχουν πληροφορίες σχετικά με τις διαδικασίες που εκτελούνται. Τα δεδομένα στο cloud είναι ευκολότερο να τα διαχειριστούν, αλλά, επίσης, είναι και πιο εύκολο να χαθεί ο έλεγχος τους. Για παράδειγμα, η αποθήκευση ιδιωτικών δεδομένων σε έναν διακομιστή κάπου στον κυβερνοχώρο θα μπορούσε να αποτελέσει σημαντική απειλή για την ιδιωτική ζωή. Το υπολογιστικό νέφος, έτσι, διεγείρει μία σειρά ερωτήσεων σχετικά με το απόρρητο και την ασφάλεια των δεδομένων. Μπορούν οι χρήστες να εμπιστευτούν τον εκάστοτε πάροχο cloud; Είναι αρκετά αξιόπιστοι οι διακομιστές των παρόχων; Τί γίνεται αν κάποιος χρήστης θέλει να αλλάξει πάροχο αναφορικά με τα αρχεία που έχει αποθηκευμένα στον προηγούμενο;

Η ασφάλεια των δεδομένων και η προστασία της ιδιωτικής ζωής αποτελούν τις δύο μείζονος σημασίας ανησυχίες των χρηστών και παρόχων σχετικά με την τεχνολογία cloud.

1.2 Κίνητρα και στόχοι της διπλωματικής

Η παρούσα διπλωματική εργασία έχει ως στόχο να ερευνήσει και να μελετήσει τα ζητήματα ιδιωτικότητας στο υπολογιστικό νέφος, όπως, επίσης, και να προτείνει

κάποιες τεχνολογίες για την ενίσχυση της προστασίας των δεδομένων και την διασφάλισης της ιδιωτικότητας των χρηστών. Πιο συγκεκριμένα, μέσω της βιβλιογραφικής επισκόπησης που έγινε, εξετάστηκαν πολλά ζητήματα ιδιωτικότητας, που αφορούν στο υπολογιστικό νέφος, όπως αδυναμίες συστημάτων εικονικοποίησης εξυπηρετητών, πολιτικές παρόχων νεφών, που παραβιάζουν την ιδιωτικότητα, επιθέσεις κακόβουλων χρηστών με στόχο την πρόσβαση σε δεδομένα χρηστών.

Είναι γνωστό ότι η Ευρωπαϊκή Ένωση αντιλήφθηκε το μέγεθος του κινδύνου της παραβίασης προσωπικών δεδομένων με αποτέλεσμα να θεσπίσει και να βάλει σε εφαρμογή τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR). Αυτό ωθεί υποχρεωτικά τις νομικές οντότητες να ερευνούν αδιάκοπα και να αναπτύσσουν μοντέλα προστασίας της ιδιωτικότητας στις διάφορες πλατφόρμες – υπηρεσίες που παρέχουν στους διάφορους χρήστες, προκειμένου να αποφύγουν οικονομικά πρόστιμα και κακή δημοσιοποίηση των παρεχόμενων υπηρεσιών τους.

Η πολυπλοκότητα της υποδομής του υπολογιστικού νέφους δε γίνεται εύκολα κατανοητή από ένα άτομο με ελλιπείς γνώσεις πληροφορικής. Αυτό κατέστη ένα μεγάλο κίνητρο διεξαγωγής της παρούσας διπλωματικής εργασίας με σκοπό την κατανόηση των επιμέρους τρόπων υποκλοπής προσωπικών δεδομένων.

Παράλληλα, εφόσον ολοένα και περισσότεροι χρήστες εισέρχονται στον κόσμο του υπολογιστικού νέφους, αναδύεται η ανάγκη της επαγρύπνησης και της μέριμνας των τελευταίων αναφορικά με τους κινδύνους ιδιωτικότητας που παραμονεύουν. Οι περισσότεροι χρήστες σήμερα αδιαφορούν ή δεν είναι αρκετά ενημερωμένοι για το πως ένας κακόβουλος χρήστης ή ένας αναξιόπιστος πάροχος μπορεί να τους δημιουργήσει ποικίλα προβλήματα σε σχέση με την ιδιωτικότητα τους.

1.3 Διάρθρωση της μελέτης

Στο πρώτο κεφάλαιο, εμπεριέχεται η εισαγωγή της εργασίας, η παρουσίαση της σημαντικότητας του θέματος, η συνεισφορά στο ευρύτερο κοινωνικό σύνολο και, τέλος, η διάρθρωση της μελέτης.
Στο δεύτερο κεφάλαιο, αναπτύσσεται η έννοια του υπολογιστικού νέφους, παρατίθενται τα βασικά χαρακτηριστικά του, αριθμούνται και επεξηγούνται τα μοντέλα Νεφών και, τέλος, αναλύεται η δομή τους.

Εν συνεχεία, στο τρίτο μέρος της διπλωματικής, επεξηγείται ο βασικός άξονας του θέματος, δηλαδή η ιδιωτικότητα, παρουσιάζεται η ισχύουσα εγχώρια νομοθεσία περί προστασίας και επεξεργασίας προσωπικών δεδομένων και, καταλήγοντας, προβάλλονται συνοπτικά τα ζητήματα ασφαλείας δεδομένων στο υπολογιστικό νέφος.

Στο τέταρτο κεφάλαιο, παρουσιάζονται οι διάφοροι τρόποι και τεχνικές παραβίασης της ιδιωτικότητας από κακόβουλους χρήστες. Εκτενέστερα, οι απειλές απορρήτου διαχωρίστηκαν σε δύο κατηγορίες: αυτές κατά την μεταφορά δεδομένων και αυτές που δημιουργούνται στην ίδια την υποδομή του νέφους, ενώ παρουσιάζονται και κάποιοι τρόποι άντλησης πληροφοριών.

Το πέμπτο κεφάλαιο αναφέρει τα κενά της πολιτικής των παρόχων cloud και πώς αυτά συμβάλλουν στην παραβίαση της ιδιωτικότητας τόσο από εξωτερικούς, όσο και από εσωτερικούς κακόβουλους χρήστες.

Στο έκτο κεφάλαιο, προτείνονται τεχνικές για τη διασφάλιση της ιδιωτικότητας στα υπολογιστικά νέφη. Πιο συγκεκριμένα, σκιαγραφούνται κάποια μοντέλα προστασίας υπολογιστικών νεφών, που χρησιμοποιούνται από τους διάφορους παρόχους cloud.

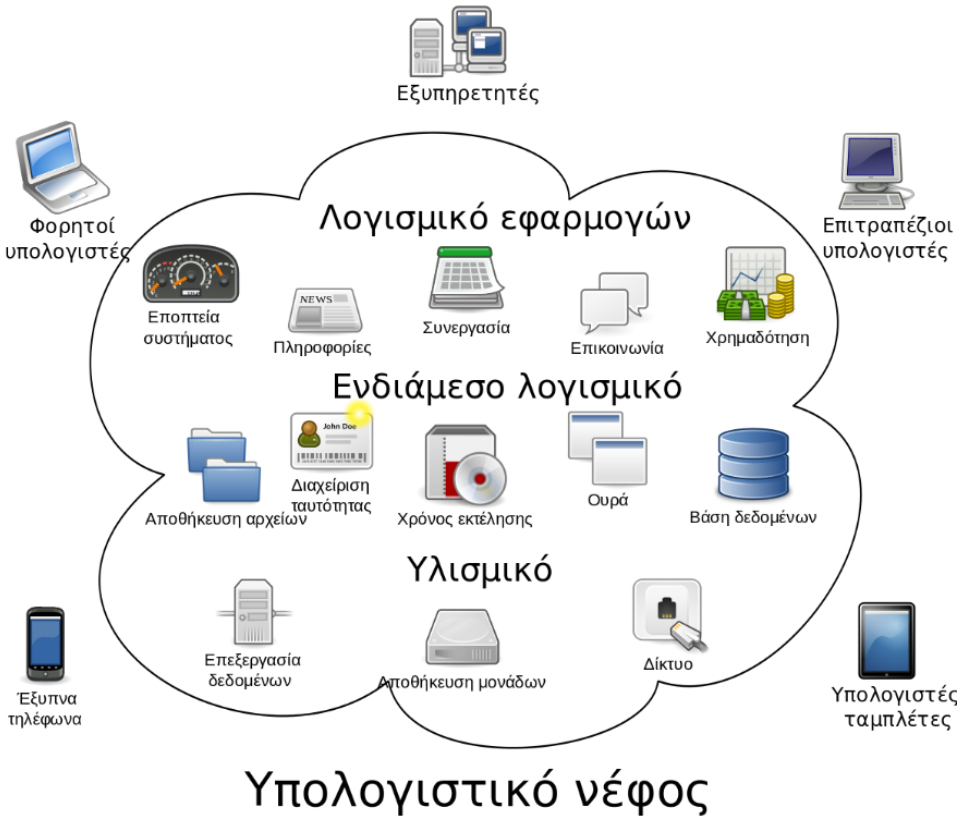
Τέλος, στο έβδομο κεφάλαιο διατυπώνονται τα συμπεράσματα που προέκυψαν από τη βιβλιογραφική μελέτη.

2. Εισαγωγή στο Cloud

Σχεδόν όλος ο χώρος της πληροφορικής αυτήν την εποχή μιλάει για το Υπολογιστικό νέφος και ειδικότερα για το τι είναι το σύννεφο, πώς μπορεί να χρησιμοποιηθεί, ποια είναι τα οφέλη του, αλλά και ποια είναι τα προβλήματα που μπορεί να επιφέρει η χρήση του. Υπηρεσίες, όπως το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα, βασίζονται πλέον στην τεχνολογία του υπολογιστικού νέφους.

2.1 Έννοια του Υπολογιστικού Νέφους

Αν ψάξει κανείς, μπορεί να βρει πληθώρα ορισμών, όμως δεν υπάρχει κάποιος



***Εικόνα 1**: Σχηματικό διάγραμμα της λειτουργίας ενός υπολογιστικού νέφους.*
Πηγή: Created by Sam Johnston using OmniGroup's OmniGraffle and Inkscape (includes Computer.svg by Sasa Stefanovic, 2009), Translation: Wikibelgiaan

ορισμός, ο οποίος να έχει καθιερωθεί και να είναι ευρέως αποδεκτός. Σύμφωνα με

την Ευρωπαϊκή επιτροπή «το υπολογιστικό νέφος είναι η αποθήκευση, η επεξεργασία και η χρήση δεδομένων από απομακρυσμένους υπολογιστές, στους οποίους εξασφαλίζεται πρόσβαση μέσω του διαδικτύου» [1]. Το υπολογιστικό νέφος, λοιπόν, είναι ένα μοντέλο που αποτελείται από υλικό (hardware), αποθηκευτικά μέσα, δίκτυα, διακομιστές (servers), εφαρμογές και υπηρεσίες, τα οποία δημιουργούν ένα κοινόχρηστο σύνολο παραμετροποιήσιμων πόρων, συνήθως με την μέθοδο της εικονικοποίησης (virtualization) , το οποίο μπορεί να παρέχεται γρήγορα και εύκολα στους χρήστες, χωρίς μεγάλη προσπάθεια διαχείρισης και αλληλεπίδρασης με τον πάροχο της υπηρεσίας. Το υπολογιστικό νέφος δεν είναι τεχνολογία από μόνο του, αλλά ο συνδυασμός πολλών προϋπαρχουσών τεχνολογιών *(εικόνα 1).* Αυτές οι τεχνολογίες έχουν ωριμάσει με διαφορετικούς ρυθμούς και σε διαφορετικά περιβάλλοντα και δε σχεδιάστηκαν ως ένα σύνολο. Ωστόσο, έχουν ενωθεί, για να δημιουργήσουν ένα τεχνικό οικοσύστημα για το cloud computing. Νέες εξελίξεις στην τεχνολογία των επεξεργαστών, της εικονικοποίησης, των αποθηκευτικών μέσων, καθώς και η συνεχώς αυξανόμενη ταχύτητα πρόσβασης στο διαδίκτυο, έχουν συνδυαστεί για να κάνουν το υπολογιστικό νέφος μια συναρπαστική λύση. Από τα παραπάνω συμπεραίνουμε ότι το υπολογιστικό νέφος προσφέρει πολλά πλεονεκτήματα στις επιχειρήσεις που το υιοθετούν. Παρακάτω αναλύουμε κάποια από αυτά:

- *Αποδοτικότητα κόστους:* Το υπολογιστικό νέφος είναι πιθανότατα η πιο οικονομική μέθοδος σε ό,τι αφορά τη χρήση, τη συντήρηση και την αναβάθμιση υλικού και λογισμικού. Τόσο το υλικό, όσο και το λογισμικό, απορροφούν μεγάλο μέρος του κεφαλαίου μίας επιχείρησης. Το νέφος, από την άλλη πλευρά, διατίθεται σε πολύ φθηνότερα ποσοστά και, ως εκ τούτου, μπορεί να μειώσει σημαντικά τα έξοδα πληροφορικής μιας εταιρείας. Άλλωστε, υπάρχουν πολλά πακέτα, όπως η εφάπαξ πληρωμή (one-time-payment), η πληρωμή για ό,τι χρησιμοποιείς (pay-as-you-go) και άλλες διαθέσιμες επεκτάσιμες επιλογές, γεγονός που καθιστά το υπολογιστικό νέφος μία πολύ ελκυστική επιλογή για τις επιχειρήσεις. Το νέφος μειώνει, επίσης, το κόστος που σχετίζεται με τον χρόνο διακοπής λειτουργίας. Δεδομένου ότι ο χρόνος διακοπής λειτουργίας είναι σπάνιος στα συστήματα cloud, αυτό σημαίνει ότι μία επιχείρηση δεν χρειάζεται να ξοδεύει χρόνο και

χρήμα για την επίλυση πιθανών προβλημάτων που σχετίζονται με τη διακοπή λειτουργίας.

- *Σχεδόν απεριόριστος χώρος αποθήκευσης:* Το cloud προσφέρει σχεδόν απεριόριστη χωρητικότητα αποθήκευσης. Ανά πάσα στιγμή, ο χρήστης μπορεί να επεκτείνει γρήγορα τη χωρητικότητα αποθήκευσης με σχετικά μικρή αύξηση της μηνιαίας χρέωσής του.

- *Δημιουργία αντιγράφων ασφαλείας και ανάκτηση:* Αφού όλα τα δεδομένα είναι αποθηκευμένα στο υπολογιστικό νέφος, η δημιουργία αντιγράφων ασφαλείας και η επαναφορά είναι σχετικά πολύ πιο εύκολη διαδικασία από ό,τι θα ήταν σε μια φυσική συσκευή μιας επιχείρησης. Επιπλέον, οι περισσότεροι πάροχοι υπηρεσιών, συνήθως, αναλαμβάνουν οι ίδιοι την δημιουργία αντιγράφων ασφαλείας, χωρίς επιπλέον κόστος.

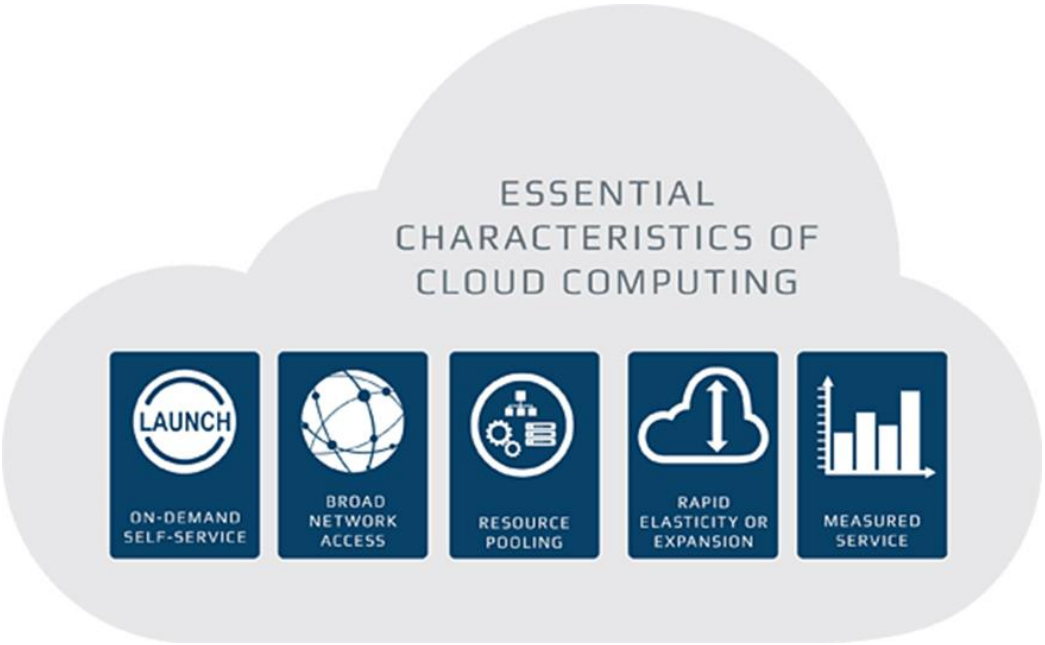
- *Γρήγορη ανάπτυξη:* Το υπολογιστικό νέφος μπορεί να παρέχει σχεδόν άμεση πρόσβαση σε πόρους υλικού και λογισμικού, χωρίς αρχικές επενδύσεις κεφαλαίου για τους χρήστες, βοηθώντας έτσι τις νέες επιχειρήσεις, που το υιοθετούν, να ξεκινήσουν πολύ γρήγορα τη λειτουργία τους. Επίσης, στο νέφος η αγορά πόρων υλικού είναι, συνήθως, ενσωματωμένη με πόρους λογισμικού. Αυτό σημαίνει ότι οι χρήστες δεν χρειάζεται να καταβάλουν επιπλέον προσπάθειες και να καταναλώσουν χρόνο, για να εγκαθιστούν τις εφαρμογές που χρειάζονται.

- *Εύκολη πρόσβαση στις πληροφορίες:* Το υπολογιστικό νέφος προσφέρει εύκολη πρόσβαση στα δεδομένα των χρηστών του. Μόλις οι χρήστες εγγραφούν σε μία υπηρεσία στο cloud, μπορούν να έχουν πρόσβαση από οπουδήποτε και από οποιαδήποτε συσκευή είναι συνδεδεμένη με το διαδίκτυο. Αυτό το βολικό χαρακτηριστικό επιτρέπει στους χρήστες να μπορούν να μετακινούνται, όπου θέλουν, ελεύθερα, χωρίς να έχουν τον περιορισμό της γεωγραφικής τοποθεσίας.

Ωστόσο, εξακολουθούν να υπάρχουν πολλά προβλήματα, που σχετίζονται με το υπολογιστικό νέφος σήμερα. Ερευνητές και επαγγελματίες επισημαίνουν ότι τόσο η ασφάλεια των δεδομένων, όσο και η ιδιωτική ζωή των φυσικών και νομικών προσώπων, κινδυνεύουν. Αυτό έχει ως αποτέλεσμα, η διασφάλιση της ιδιωτικότητας των δεδομένων να έχει γίνει η πρωταρχική μέριμνα για άτομα και επιχειρήσεις που το χρησιμοποιούν ή που θέλουν να ξεκινήσουν να το χρησιμοποιούν.

2.2 Βασικά χαρακτηριστικά υπολογιστικού νέφους

Σύμφωνα με το NIST *(National Institute of Standards and Technology)* το υπολογιστικό νέφος απαρτίζεται από πέντε βασικά χαρακτηριστικά [2] (Εικόνα 2):



Εικόνα 2: *Βασικά Χαρακτηριστικά Υπολογιστικού Νέφους*
Πηγή: http://moderncloudcomputing.blogspot.com/2016/03/the-five-essential-characteristics-of.html

1. Κατά παραγγελία αυτό-εξυπηρέτηση *(On demand self-service)*:
Οι πόροι υπολογιστικού νέφους μπορούν να χορηγηθούν, χωρίς ανθρώπινη αλληλεπίδραση, από τον πάροχο υπηρεσιών. Με άλλα λόγια, ένας οργανισμός μπορεί να επιλέγει, να αγοράζει και στη συνέχεια να χρησιμοποιεί υπηρεσίες του υπολογιστικού νέφους (όπως, για παράδειγμα, επεξεργαστική ισχύ, αποθηκευτικό χώρο), χωρίς να έρχεται σε επαφή με τον εκάστοτε πάροχο υπηρεσιών νέφους. Αυτό, συνήθως, επιτυγχάνεται με μία διαδικτυακή σελίδα αυτοεξυπηρέτησης, στην οποία οι πελάτες έχουν την δυνατότητα να αποκτούν πρόσβαση στους λογαριασμούς τους και να παρακολουθούν ή να επεξεργάζονται τις υπηρεσίες που τους παρέχονται.

2. Ευρεία πρόσβαση στο δίκτυο *(Broad network access)*:
Οι δυνατότητες που προσφέρει το υπολογιστικό νέφος χρησιμοποιούνται μέσω δικτύου και είναι προσβάσιμες από διάφορες πλατφόρμες (κινητά τηλέφωνα, ταμπλέτες, φορητούς υπολογιστές, σταθμούς εργασίας). Με άλλα λόγια, οι υπηρεσίες του υπολογιστικού νέφους είναι διαθέσιμες μέσω ενός δικτύου - ιδανικά υψηλής ευρυζωνικής σύνδεσης -, όπως το διαδίκτυο, ή στην περίπτωση ιδιωτικών σύννεφων, θα μπορούσε να είναι ένα τοπικό δίκτυο (LAN).

3. Συγκέντρωση πόρων *(Resource pooling)*:
Οι πόροι υπολογιστικού νέφους έχουν σχεδιαστεί, για να υποστηρίζουν ένα μοντέλο «πολλών ενοίκων» **(multitenancy).** Το Multitenancy επιτρέπει σε πολλούς πελάτες να μοιράζονται τις ίδιες εφαρμογές ή την ίδια φυσική υποδομή ενός παρόχου υπολογιστικού νέφους, διατηρώντας παράλληλα το απόρρητο και την ασφάλεια των πληροφοριών τους. Είναι παρόμοιο με τους ανθρώπους που ζουν σε μια πολυκατοικία, που μοιράζονται την ίδια υποδομή κτιρίου, αλλά εξακολουθούν να έχουν τα δικά τους διαμερίσματα και την ιδιωτικότητα τους εντός αυτής της υποδομής.

Η συγκέντρωση πόρων σημαίνει ότι πολλοί πελάτες εξυπηρετούνται από τους ίδιους φυσικούς πόρους. Το σύνολο πόρων των παρόχων πρέπει να είναι πολύ μεγάλο και αρκετά ευέλικτο, ώστε να εξυπηρετεί πολλαπλές απαιτήσεις πελατών και να παρέχει οικονομία κλίμακας. Όσον αφορά στη συγκέντρωση πόρων, είναι σημαντικό η κατανομή των πόρων να μην επηρεάζει τις επιδόσεις κρίσιμων εφαρμογών.

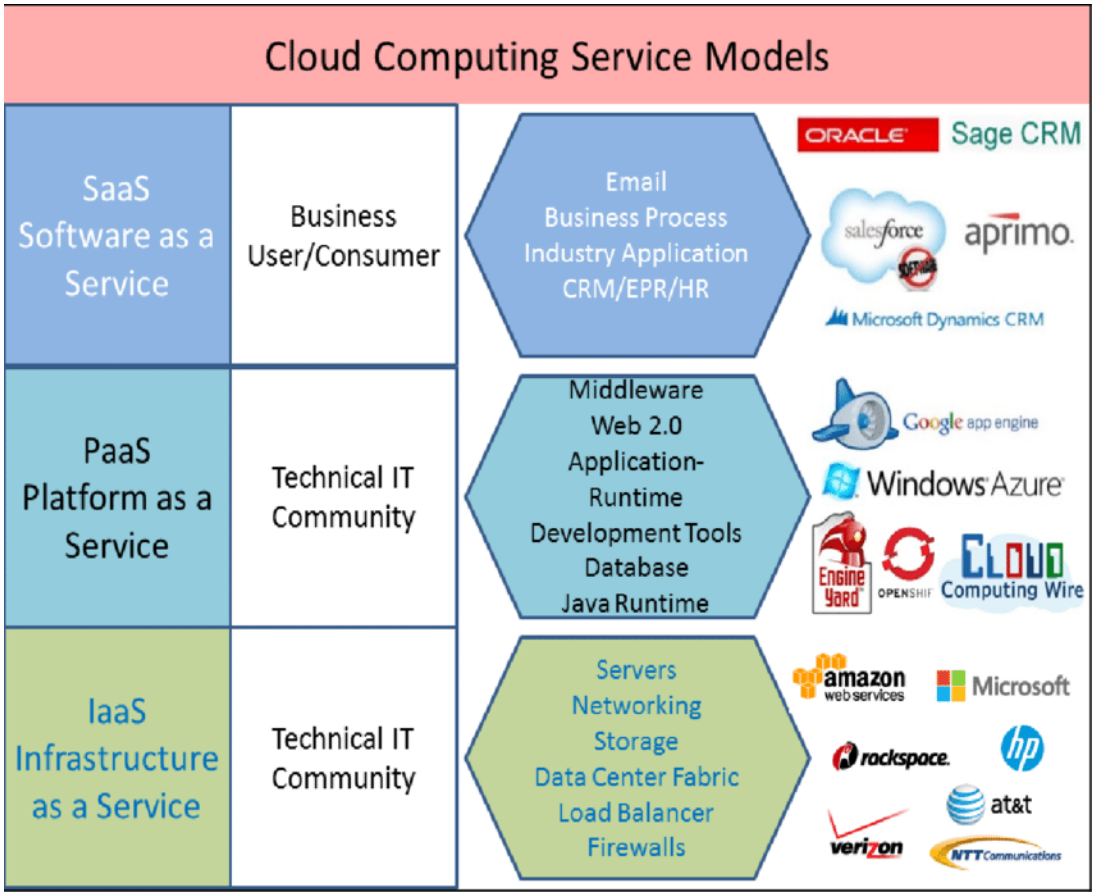
4. Γρήγορη ελαστικότητα *(Rapid elasticity)*:
Ένα από τα σπουδαιότερα χαρακτηριστικά του υπολογιστικού νέφους είναι η ελαστικότητα που προσφέρουν οι υπηρεσίες του. Δηλαδή, η δυνατότητα γρήγορης παροχής πόρων, όταν τους χρειάζονται οι πελάτες, και η αφαίρεση των επιπλέων πόρων, όταν δεν τους είναι αναγκαίοι. Οι πόροι υπολογιστικού νέφους μπορούν να αυξηθούν ή να μειωθούν γρήγορα και, σε ορισμένες περιπτώσεις, αυτόματα, ανταποκρινόμενοι στις επιχειρηματικές απαιτήσεις. Άρα, συμπεραίνουμε ότι η χρήση, η χωρητικότητα και, συνεπώς, το κόστος μπορούν να αυξηθούν ή να μειωθούν, χωρίς επιπλέον συμβόλαιο ή κυρώσεις.

5. Μετρημένη υπηρεσία *(Measured service)*:
Η χρήση των πόρων υπολογιστικού νέφους μετριέται και οι πελάτες πληρώνουν ανάλογα με αυτό που έχουν χρησιμοποιήσει. Η χρήση των πόρων μπορεί να βελτιστοποιηθεί, αξιοποιώντας τις δυνατότητες χρέωσης ανά χρήση. Αυτό σημαίνει ότι οι υπηρεσίες υπολογιστικού νέφους (π.χ. εικονικές μηχανές που εκτελούνται, αποθηκευτικός χώρος) παρακολουθούνται και μετριούνται από τον πάροχο υπηρεσιών cloud. Έτσι, η πληρωμή είναι μεταβλητή, με βάση την πραγματική κατανάλωση της υπηρεσίας νέφους από τον πελάτη.

2.3 Μοντέλα υπηρεσιών Νέφους

Οι υπηρεσίες νέφους παρέχονται σε τρία μοντέλα [2]*(Εικόνα 3)*, καθένα από τα οποία είναι προσανατολισμένο σε ειδικές κατηγορίες χρηστών.

- **Λογισμικό ως υπηρεσία (Software as a service – SaaS),** που αφορά στην παροχή εφαρμογών για τους τελικούς χρήστες και απευθύνεται σε όλους τους χρήστες.
- **Πλατφόρμα ως υπηρεσία (Platform as a service – PaaS),** που αφορά στην παροχή υπολογιστικών πλατφορμών και απευθύνεται, κυρίως, σε προγραμματιστές.
- **Υποδομή ως υπηρεσία (Infrastructure as a service – IaaS),** που αφορά στην παροχή υπολογιστικών πόρων και απευθύνεται, κυρίως, σε ειδικούς διαχείρισης δικτύων και υπολογιστικών συστημάτων.



***Εικόνα 3**: Μοντέλα υπηρεσιών νέφους*

Πηγή: Laghari, Asif Ali, Hui He, Imtiaz A. Halepoto, M. Sulleman Memon, and Sajida Parveen. "Analysis of Quality of Experience Frameworks for Cloud Computing." IJCSNS 17, no. 12 (2017): 228.

Πιο αναλυτικά:

Το **Λογισμικό ως υπηρεσία (SaaS)** είναι ένα μοντέλο διανομής λογισμικού, στο οποίο ένας τρίτος πάροχος φιλοξενεί εφαρμογές και τις καθιστά διαθέσιμες σε πελάτες μέσω του Διαδικτύου. Το συγκεκριμένο μοντέλο επιτρέπει στους χρήστες να συνδέονται και να χρησιμοποιούν εφαρμογές που βασίζονται στο νέφος μέσω του Διαδικτύου, χωρίς να απαιτείται, δηλαδή, η τοπική εγκατάσταση και συντήρηση λογισμικού, εξυπηρετητών ή άλλων συστημάτων και υποδομών. Οι εφαρμογές είναι προσβάσιμες από διάφορες συσκευές (π.χ. προσωπικοί υπολογιστές, ταμπλέτες, έξυπνα κινητά και άλλες φορητές συσκευές) μέσω ενός γραφικού περιβάλλοντος χρήστη, όπως ένα πρόγραμμα περιήγησης ιστού (π.χ.

ηλεκτρονικό ταχυδρομείο με δυνατότητα ιστού, Google Apps [3], Dropbox [4]). Ο πάροχος υπηρεσιών διαχειρίζεται το υλικό και το λογισμικό και, με την κατάλληλη συμφωνία υπηρεσίας, θα διασφαλίσει τη διαθεσιμότητα και την ασφάλεια της εφαρμογής και των δεδομένων των πελατών. Ο χρήστης δεν μπορεί να επηρεάσει τις δικτυακές υποδομές, τους διακομιστές, τα λειτουργικά συστήματα ή τους αποθηκευτικούς χώρους και, στις περισσότερες περιπτώσεις, δεν έχει καθόλου ή έχει περιορισμένο έλεγχο πάνω στην ίδια την εφαρμογή. Για παράδειγμα, ο χρήστης που αξιοποιεί τις υπηρεσίες νέφους Google Apps και Microsoft Office 365 δεν ελέγχει πού ακριβώς είναι αποθηκευμένα τα αρχεία του, πόσοι εξυπηρετητές διατίθενται για την εξυπηρέτησή του και πώς ακριβώς συνδέεται δικτυακά με τις εφαρμογές αυτές.

Το Λογισμικό ως υπηρεσία είναι από τις καλύτερες λύσεις, για να ξεκινήσει μία επιχείρηση γρήγορα την λειτουργία της με ελάχιστο αρχικό κόστος. Ένα από τα κύρια πλεονεκτήματά του είναι ότι καταργεί την ανάγκη για τους οργανισμούς να εγκαθιστούν και να εκτελούν εφαρμογές σε δικούς τους υπολογιστές ή σε δικά τους κέντρα δεδομένων. Αυτό ελαχιστοποιεί τα έξοδα απόκτησης, παροχής και συντήρησης υλικού, καθώς και τις αγορές αδειών, εγκατάστασης και υποστήριξης λογισμικού. Επίσης, ένα σημαντικό πλεονέκτημα είναι οι ευέλικτες πληρωμές, που παρουσιάζει το λογισμικό ως υπηρεσία. Αυτό σημαίνει ότι οι χρήστες πληρώνουν μόνο για ό,τι χρειάζονται, συνήθως, σε μηνιαία βάση, χρησιμοποιώντας ένα μοντέλο pay-as-you-go, το οποίο μπορούν να τερματίσουν, όποτε αυτοί θέλουν. Τέλος, οι αυτόματες ενημερώσεις, καθώς και η εύκολη προσβασιμότητα, από όποια συσκευή με δυνατότητα πρόσβασης στο διαδίκτυο θέλουν οι χρήστες, καθιστούν την υπηρεσία του νέφους πολύ ελκυστική.

Η **πλατφόρμα ως υπηρεσία (PaaS)** είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης εφαρμογών στο νέφος, με πόρους που επιτρέπουν την δημιουργία απλών εφαρμογών, που βασίζονται στο «σύννεφο», αλλά και εξελιγμένων εταιρικών εφαρμογών με δυνατότητα cloud. Αποτελεί ιδανική λύση για ομάδες προγραμματιστών που πρέπει να συνεργαστούν στην ανάπτυξη μιας εφαρμογής. Οι πάροχοι των μοντέλων PaaS παρέχουν ένα ενιαίο περιβάλλον πλατφόρμας, που, συνήθως, περιλαμβάνει λειτουργικό σύστημα, περιβάλλον εκτέλεσης γλώσσας προγραμματισμού, βάση δεδομένων και διακομιστή ιστού, στο οποίο οι

προγραμματιστές εφαρμογών μπορούν να αναπτύσσουν και να εκτελούν το λογισμικό τους, αντί να αγοράζουν και να συντηρούν το δικό τους υλικό και λογισμικό. Το PaaS έχει σχεδιαστεί, για να υποστηρίζει τον πλήρη κύκλο ζωής μιας εφαρμογής ιστού: δημιουργία, δοκιμή, ανάπτυξη, διαχείριση και ενημέρωση.

Η πλατφόρμα ως υπηρεσία προσφέρει τα ίδια πλεονεκτήματα με το SaaS, ωστόσο, οι πρόσθετες δυνατότητές του, όπως τα εργαλεία ανάπτυξης λογισμικού και άλλα επιχειρηματικά εργαλεία, προσφέρουν επιπλέον πλεονεκτήματα. Μπορεί, για παράδειγμα, να μειώσει αρκετά τον χρόνο κωδικοποίησης με προ-κωδικοποιημένα στοιχεία εφαρμογών, ενσωματωμένα στην πλατφόρμα. Το Google App Engine [5], το Windows Azure [6], το Amazon Web Services [7] αποτελούν παραδείγματα για την PaaS.

Το τρίτο και το τελευταίο μοντέλο είναι **η υποδομή ως υπηρεσία (IaaS),** το οποίο είναι μια άμεση υπολογιστική υποδομή, η οποία παρέχεται και είναι διαχειρίσιμη μέσω του Διαδικτύου. Η υπολογιστική υποδομή αυτή αποτελείται από τα παραδοσιακά στοιχεία υποδομής που υπάρχουν σε ένα κέντρο δεδομένων, όπως υπολογιστικοί πόροι, διακομιστές, υλικό αποθήκευσης και δικτύωσης, τα οποία συνήθως παρέχονται στους καταναλωτές με την μέθοδο της εικονικοποίησης (Virtualization) [8]. Οι δυνατότητες που έχει ο καταναλωτής, χρησιμοποιώντας την υποδομή ως υπηρεσία, είναι να εκτελεί και να αναπτύσσει λογισμικό (λειτουργικά συστήματα ή εφαρμογές), αλλά δεν μπορεί να διαχειριστεί ούτε να ελέγχει την υφιστάμενη υποδομή του νέφους. Ο εκάστοτε πάροχος της υποδομής ως υπηρεσία παρέχει αυτούς του πόρους από τις τεράστιες δεξαμενές εξοπλισμού, που είναι εγκατεστημένες στα κέντρα δεδομένων του. Επίσης, συνήθως, παρέχουν και μια σειρά υπηρεσιών, που συνοδεύουν τις υπολογιστικές υποδομές, όπως, για παράδειγμα, αυτόματη δημιουργία αντιγράφων ασφαλείας.

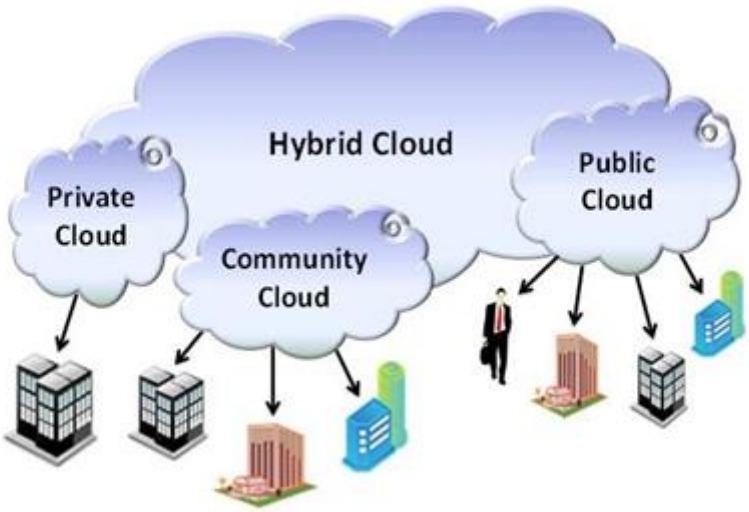
Ένα πολύ βασικό πλεονέκτημα της υποδομής ως υπηρεσία είναι ότι ο εκάστοτε καταναλωτής μπορεί να νοικιάζει τους υπολογιστικούς πόρους, ανάλογα με τις απαιτήσεις εκείνης της χρονικής στιγμής. Έτσι, ελαχιστοποιείται το κόστος σε περιπτώσεις που οι απαιτήσεις σε υπολογιστικούς πόρους της επιχείρησης ή του καταναλωτή αυξομειώνονται σημαντικά, ανάλογα την χρονική περίοδο. Πάροχοι τέτοιων υπηρεσιών είναι η Amazon(EC2) [7], Rackspace [9], Orange Business Service [10].

2.4 Μοντέλα Ανάπτυξης Νέφους

Το NIST (National Institute of Standards and Technology) ορίζει τέσσερα μοντέλα ανάπτυξης του νέφους [2]*(Εικόνα 4)*:

- **Δημόσιο νέφος (Public cloud)**
- **Ιδιωτικό νέφος (Private cloud)**
- **Νέφος κοινότητας (Community cloud)**
- **Υβριδικό νέφος (Hybrid cloud)**

Ένα μοντέλο ανάπτυξης νέφους ορίζεται, ανάλογα με το πού βρίσκεται η υποδομή για την ανάπτυξη και ποιος έχει τον έλεγχο αυτής της υποδομής. Το να αποφασίσει μία επιχείρηση ποιο μοντέλο ανάπτυξης νέφους θα ακολουθήσει είναι μια από τις πιο σημαντικές αποφάσεις, που θα λάβει. Κάθε μοντέλο καλύπτει διαφορετικές οργανωτικές ανάγκες, επομένως είναι σημαντικό να γίνει η σωστή επιλογή, αυτή, δηλαδή, που θα ικανοποιεί πλήρως τις ανάγκες του οργανισμού. Ένα ακόμη πρωτεύον κριτήριο επιλογής είναι και το κόστος αγοράς, που σχετίζεται με το



Εικόνα 4: *Μοντέλα ανάπτυξης νέφους*
Πηγή:Cloud Computing Deployment Models (Mell and Grance, 2011)

καθένα. Σε κάθε περίπτωση, όμως, για να μπορέσει ένας οργανισμός να λάβει μία σωστή απόφαση, πρέπει να γνωρίζει τα χαρακτηριστικά κάθε μοντέλου.

2.4.1 Δημόσιο νέφος

Η υποδομή του δημόσιου νέφους παρέχεται για ανοιχτή χρήση στο ευρύ κοινό, μέσω του διαδικτύου, και, πιθανότατα, η ιδιοκτησία του και η διαχείρισή του πραγματοποιούνται από μία επιχείρηση, έναν ακαδημαϊκό ή κυβερνητικό οργανισμό ή συνδυασμό όλων αυτών. Γενικά, οι πάροχοι δημόσιων υπηρεσιών νέφους, όπως η Google, η Microsoft, η Amazon Web Services (AWS) η Oracle [11], η IBM [12] και η Alibaba [13], κατέχουν και λειτουργούν όλα τα δεδομένα και τις υπηρεσίες του νέφους στις εγκαταστάσεις τους. Το μοντέλο βασίζεται σε δίκτυα πληροφοριών παγκοσμίου βεληνεκούς, προσφέροντας τις διάφορες υπηρεσίες με πληρωμή ανά χρήση, δηλαδή οι χρήστες του χρεώνονται για όσο κάνουν χρήση της υπηρεσίας νέφους. Ως αποτέλεσμα αυτού, το εν λόγω μοντέλο μπορεί να θεωρηθεί ως ένα μοντέλο πολυμίσθωσης. Τα δημόσια σύννεφα δεν απαιτούν την επένδυση αρχικού κεφαλαίου σε υποδομές, ενώ μετατοπίζουν τους κινδύνους σε παρόχους υποδομής. Σε πολλές περιπτώσεις, η παροχή των συγκεκριμένων νεφών μπορεί να διατεθεί εντελώς δωρεάν , με απώτερο σκοπό την προσέλκυση νέων χρηστών- πελατών. Το γεγονός αυτό το καθιστά το πιο οικονομικό μοντέλο. Ωστόσο, αυτό συνεπάγεται έλλειψη ελέγχου των δεδομένων, των δικτύων και των ρυθμίσεων ασφαλείας, γεγονός που εμποδίζει την αποτελεσματικότητα και την εξάπλωση αυτού του μοντέλου σε πολλά επιχειρηματικά σενάρια [14]. Αν και οι σύγχρονοι πάροχοι δημοσίου νέφους λαμβάνουν πολύ σοβαρά την ασφάλεια των δεδομένων, δεν παύει να είναι η λιγότερο ασφαλής λύση εκ των τεσσάρων μοντέλων ανάπτυξης.

2.4.2 Ιδιωτικό νέφος

Ως ιδιωτικό νέφος ορίζονται οι υπηρεσίες πληροφορικής, που προσφέρονται είτε μέσω διαδικτύου είτε από ιδιωτικό εσωτερικό δίκτυο(π.χ. Επιχείρηση, Πανεπιστήμιο), μόνο για συγκεκριμένους χρήστες και όχι για το ευρύ κοινό. Η κύρια διαφορά με το προηγούμενο είναι ότι τα δεδομένα και οι υπηρεσίες του ιδιωτικού νέφους μπορούν να φιλοξενούνται, είτε εντός είτε εκτός των εγκαταστάσεων των οργανισμών που το χρησιμοποιούν. Τα ιδιωτικά νέφη χρησιμοποιούν εικονικοποίηση, καθώς και αυτοματοποιημένες τεχνολογίες διαχείρισης για την εξασφάλιση υψηλού ελέγχου απόδοσης, αξιοπιστίας και

ασφάλειας [14]. Οι επιχειρήσεις που χρησιμοποιούν το ιδιωτικό νέφος, μπορούν να εγκαθιδρύσουν τις δικές τους πολιτικές αναφορικά με τα θέματα ασφάλειας και προστασίας της ιδιωτικότητας δεδομένων, καθώς και τους μηχανισμούς πρόσβασης τους. Ως απόρροια αυτού, το ιδιωτικό νέφος επιλέγεται από εταιρείες που δε θέλουν να εκθέσουν τα δεδομένα τους σε άλλα εικονικά περιβάλλοντα. Επιπλέον, το τοπικό κέντρο δεδομένων μειώνει τα καθήκοντα διαχείρισης και διοίκησης. Έτσι, προσφέρει μεγαλύτερη ασφάλεια στα δεδομένα από αυτήν που προσφέρει το μοντέλο του δημοσίου νέφους. Για όλα τα παραπάνω, το χτίσιμο ενός τέτοιου είδους νέφους καταλήγει να είναι η πιο δαπανηρή επιλογή νέφους, εφόσον απαιτεί μεγαλύτερους πόρους για την υλοποίηση του [15].

2.4.3 Υβριδικό νέφος

Το υβριδικό νέφος είναι μία σύνθεση δύο ή περισσοτέρων ξεχωριστών υποδομών νέφους (ιδιωτικών, δημοσίων ή κοινότητας), τα οποία, όμως, παραμένουν ξεχωριστές οντότητες. Συνεπώς, δημιουργείται ένα υπολογιστικό περιβάλλον, που συνδέει τις ιδιωτικές υπηρεσίες νέφους μιας εταιρείας και το δημόσιο νέφος τρίτων παρόχων σε μια ενιαία, ευέλικτη υποδομή για τη λειτουργία των εφαρμογών και του φόρτου εργασίας των οργανισμών. Με αυτόν τον τρόπο, έχουμε συνδυαστικά οφέλη από τα διαφορετικά μοντέλα ανάπτυξης νέφους. Παράλληλα, εμπεριέχει και τους περιορισμούς των συνδυαζόμενων νεφών [14]. Πιο συγκεκριμένα, τα *«ευαίσθητα»* δεδομένα αποθηκεύονται στο ιδιωτικό νέφος, οπότε έχουμε περισσότερη ασφάλεια, και τα υπόλοιπα στο δημόσιο, οπότε έχουμε μικρότερο κόστος. Ένα τέλειο παράδειγμα αυτού του σεναρίου είναι αυτό ενός οργανισμού που χρησιμοποιεί το ιδιωτικό σύννεφο, για να εξασφαλίσει τα δεδομένα του και να αλληλοεπιδρά με τους πελάτες του, χρησιμοποιώντας το δημόσιο σύννεφο. Αυτό το μοντέλο ανάπτυξης προσφέρει μεγαλύτερη ευελιξία, έλεγχο και ασφάλεια σε σχέση με τα δεδομένα εφαρμογής στα δημόσια νέφη, ενώ απαιτεί μία προσεκτική μελέτη για τον προσδιορισμό της καλύτερης κατανομής των στοιχείων μεταξύ δημοσίου και ιδιωτικού νέφους.

2.4.4 Νέφος κοινότητας

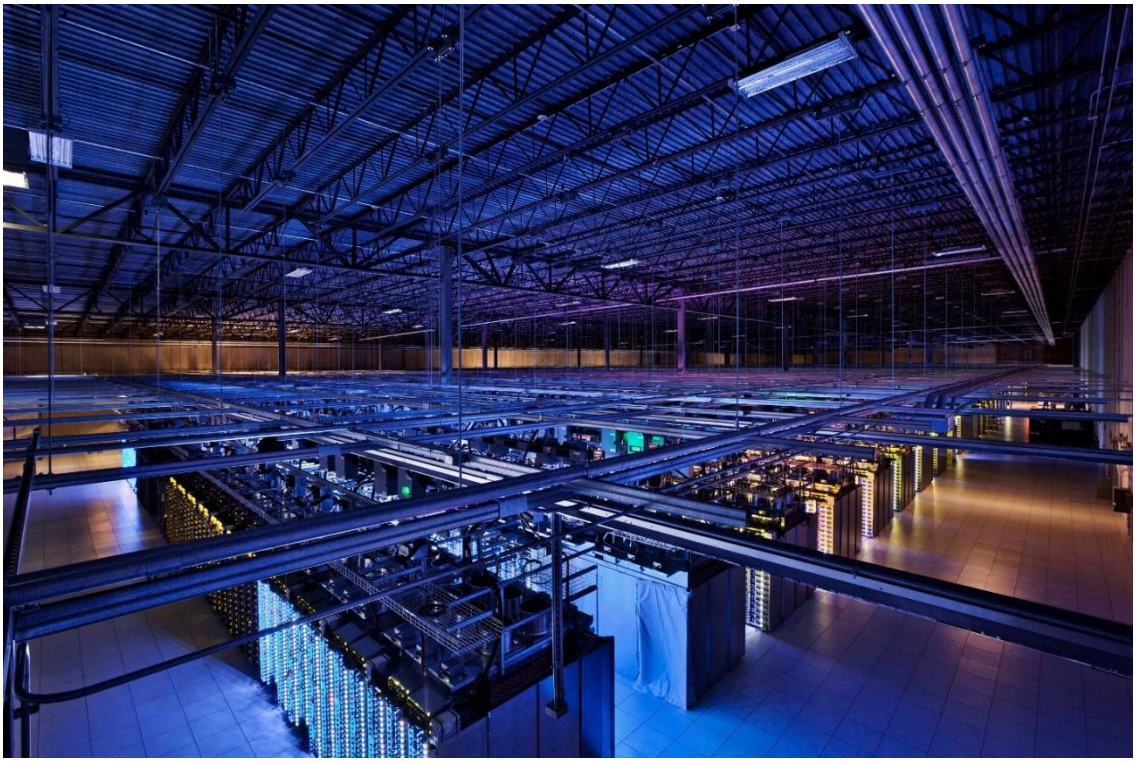
Εκτός από τα τρία βασικά μοντέλα ανάπτυξης νέφους, το NIST ορίζει και ένα τέταρτο, το Νέφος κοινότητας. Η υποδομή του νέφους κοινότητας παρέχεται για αποκλειστική χρήση από μία συγκεκριμένη κοινότητα καταναλωτών ή από οργανισμούς που έχουν κοινά συμφέροντα που έχουν κοινές απαιτήσεις, κοινή αποστολή, κοινή πολιτική, κοινούς κανόνες συμμόρφωσης ή ευρύτερα κοινά συμφέροντα (π.χ. τράπεζες, κυβερνητικές οργανώσεις, εμπορικές επιχειρήσεις). Άρα, το κοινοτικό νέφος μπορεί να διαμορφώνεται ανάλογα με τη ζήτηση των χρηστών. Μπορεί να ανήκει και να είναι αντικείμενο διαχείρισης από έναν ή περισσότερους οργανισμούς, που ανήκουν στην κοινότητα, ή και από κάποιον τρίτο πάροχο, όπως και στο ιδιωτικό νέφος. Τα δεδομένα και οι υπηρεσίες νέφους κοινότητας μπορούν να φιλοξενούνται είτε εντός είτε εκτός των εγκαταστάσεων των οργανισμών που το χρησιμοποιούν. Το νέφος κοινότητας έχει ως φιλοδοξία τη μείωση των ελλείψεων των μεμονωμένων τεχνολογιών υποδομής και τη μείωση του κόστους διοίκησης. Το αναφερόμενο νέφος θεωρείται περισσότερο έμπιστο από το δημόσιο , καθότι στηρίζεται, κυρίως, στις σχέσεις εμπιστοσύνης μεταξύ των μελών του, οι οποίες καθοδηγούνται από κοινά οφέλη που αποφέρει η χρήση αυτού του νέφους [16]. Το κόστος του παραμένει μικρότερο από αυτό του ιδιωτικού νέφους, αλλά σίγουρα υψηλότερο από τα άλλα δύο μοντέλα. Τέλος, η ασφάλεια που παρέχεται σε σχέση με την προστασία δεδομένων έχει περιθώρια βελτίωσης, διότι τα μέρη αυτού έρχονται πολλές φορές σε ρήξη απόψεων.

ΜΟΝΤΕΛΑ ΑΝΑΠΤΥΞΗΣ	ΚΑΤΟΧΟΣ	ΑΣΦΑΛΕΙΑ	ΕΠΕΚΤΑΣΙΜΟΤΗΤΑ	ΚΟΣΤΟΣ
ΔΗΜΟΣΙΟ ΝΕΦΟΣ	ΠΑΡΟΧΟΙ ΥΠΗΡΕΣΙΩΝ ΝΕΦΟΥΣ	ΧΑΜΗΛΟΤΕΡΗ ΣΕ ΣΧΕΣΗ ΜΕ ΤΑ ΥΠΟΛΟΙΠΑ ΜΟΝΤΕΛΑ	ΠΟΛΥ ΥΨΗΛΗ	ΠΛΗΡΩΜΗ/ ΧΡΗΣΗ
ΙΔΙΩΤΙΚΟ ΝΕΦΟΣ	ΜΟΝΑΔΙΚΟΣ ΙΔΙΩΤΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ	ΥΨΗΛΟΤΕΡΗ ΣΕ ΣΧΕΣΗ ΜΕ ΤΑ ΥΠΟΛΟΙΠΑ ΜΟΝΤΕΛΑ	ΠΕΡΙΟΡΙΣΜΕΝΗ	ΥΨΗΛΟ
ΥΒΡΙΔΙΚΟ ΝΕΦΟΣ	ΠΑΡΟΧΟΙ ΥΠΗΡΕΣΙΩΝ ΝΕΦΟΥΣ Ή ΙΔΙΩΤΙΚΟΙ ΟΡΓΑΝΙΣΜΟΙ	ΧΑΜΗΛΟΤΕΡΗ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟ ΙΔΙΩΤΙΚΟ ΚΑΙ ΤΟ ΝΕΦΟΣ ΚΟΙΝΟΤΗΤΑΣ – ΥΨΗΛΟΤΕΡΗ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟ ΔΗΜΟΣΙΟ	ΥΨΗΛΗ	ΠΛΗΡΩΜΗ/ ΧΡΗΣΗ
ΝΕΦΟΣ ΚΟΙΝΟΤΗΤΑΣ	ΔΥΟ Ή ΠΕΡΙΣΣΟΤΕΡΟΙ ΟΡΓΑΝΙΣΜΟΙ ΜΕ ΠΑΝΟΜΟΙΟΤΥΠΕΣ ΑΠΑΙΤΗΣΕΙΣ	ΧΑΜΗΛΟΤΕΡΗ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟ ΙΔΙΩΤΙΚΟ - ΥΨΗΛΟΤΕΡΗ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟ ΔΗΜΟΣΙΟ ΚΑΙ ΥΒΡΙΔΙΚΟ	ΠΕΡΙΟΡΙΣΜΕΝΗ	ΜΕΤΡΙΟ

Πίνακας 1 Συγκριτικός πίνακας μοντέλων ανάπτυξης νέφους

2.5 Κέντρα δεδομένων νέφους (cloud datacenters)

Το κέντρο δεδομένων είναι μια εγκατάσταση, όπου είναι συγκεντρωμένος ο εξοπλισμός υπολογιστών και δικτύων ενός οργανισμού για σκοπούς συλλογής, αποθήκευσης, επεξεργασίας, διανομής ή πρόσβασης σε μεγάλες ποσότητες δεδομένων [17] *(Εικόνα 5)*. Επειδή στεγάζουν τα πιο κρίσιμα περιουσιακά στοιχεία ενός οργανισμού, τα κέντρα δεδομένων είναι ζωτικής σημασίας για τη συνέχεια των καθημερινών εργασιών του. Κατά συνέπεια, η ασφάλεια και η αξιοπιστία των κέντρων δεδομένων και των πληροφοριών τους συγκαταλέγονται στις κορυφαίες προτεραιότητες κάθε οργανισμού.

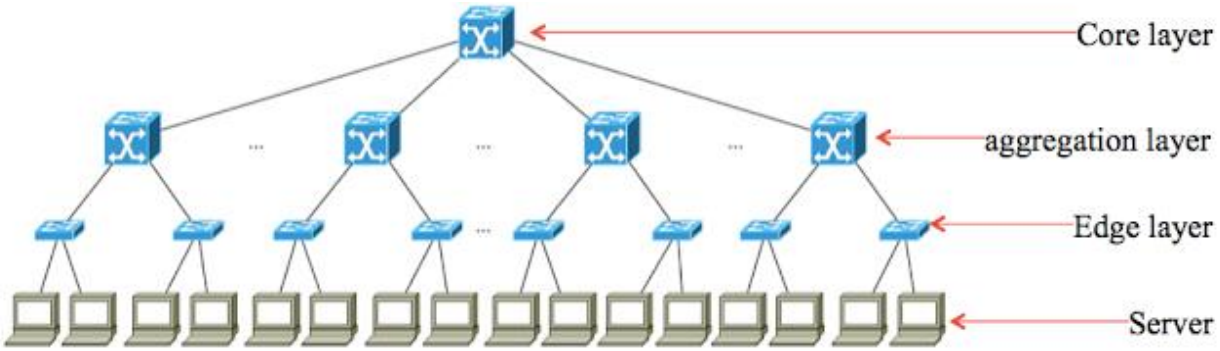


Εικόνα 5: *Κέντρο δεδομένων τις Google στην πόλη COUNCIL BLUFFS, IOWA των ΗΠΑ*
Πηγή: https://www.google.com/about/datacenters/gallery/

Στο παρελθόν, τα κέντρα δεδομένων ήταν εύκολα ελεγχόμενες φυσικές υποδομές, αλλά, σήμερα, οι πάροχοι των υπηρεσιών νέφους, που είδαμε πιο πάνω, έχουν αλλάξει ριζικά αυτό το μοντέλο. Μέρα με την μέρα οι ανάγκες επεξεργασίας δεδομένων αυξάνονται εκθετικά. Γι' αυτό, και πολλές μεγάλες εταιρείες, όπως η Google, η Amazon, η HP και η Microsoft, έχουν προνοήσει και έχουν δημιουργήσει τεράστια κέντρα δεδομένων, τα οποία έχουν πολύ πιθανόν χιλιάδες, μπορεί και εκατοντάδες διακομιστές, που λειτουργούν αδιάκοπα. Κυμαίνονται από μερικούς διακομιστές σε ένα δωμάτιο έως τεράστιες αυτόνομες δομές, που έχουν μέγεθος εκατοντάδων χιλιάδων τετραγωνικών μέτρων με δεκάδες χιλιάδες διακομιστές και άλλο συνοδευτικό υλικό *(Εικόνα 5)*. Τα μεγέθη και οι τύποι εξοπλισμού που περιέχουν ποικίλλουν ανάλογα με τις ανάγκες της οντότητας ή των οντοτήτων που υποστηρίζουν.

Η δικτύωση των κέντρων δεδομένων κατέχει σημαντικό ρόλο, καθώς διασυνδέει όλους τους πόρους τους μεταξύ τους. Πρέπει να είναι επεκτάσιμη και αποτελεσματική για την αντιμετώπιση των αυξανομένων απαιτήσεων των υπηρεσιών του υπολογιστικού νέφους. Η πιο συνηθισμένη αρχιτεκτονική δικτύωσής των μεγάλων κέντρων δεδομένων είναι η λεγόμενη **«fat-tree»** *(Εικόνα*

6), η οποία είναι βασισμένη στην τοπολογία δένδρου με πολλές ρίζες (**multi-rooted trees)** [17]. Ανάλογα με το μέγεθος του κέντρου δεδομένων, το δίκτυο αποτελείται από δύο ή τρία επίπεδα switch, που ορίζονται ως Edge layer switch, aggregation layer switch και Core layer switch.



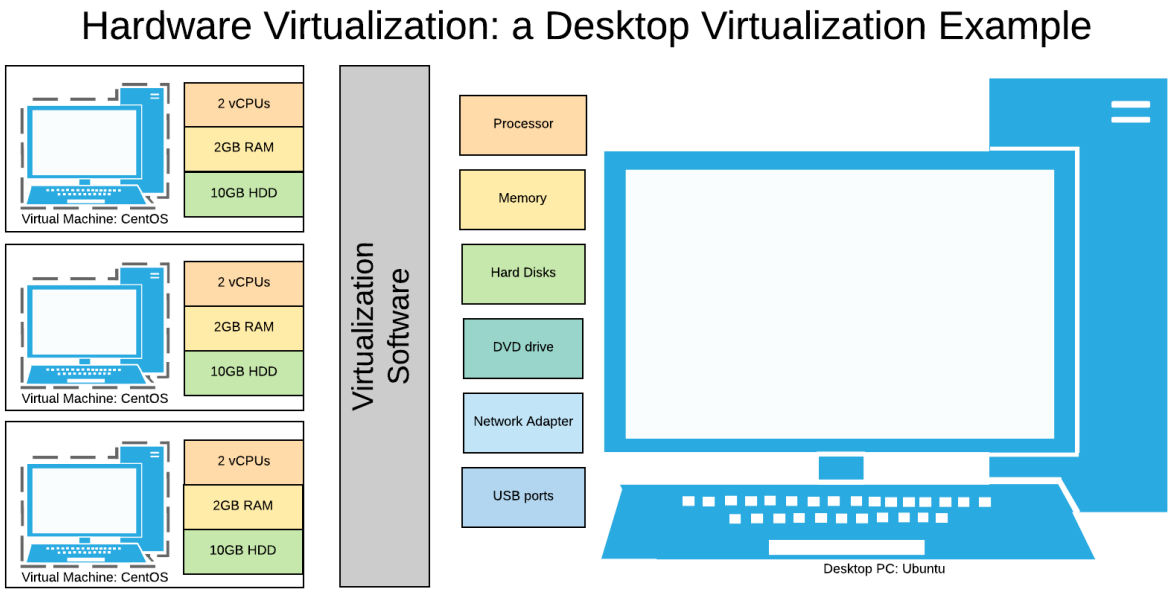
Εικόνα 6: *Παράδειγμα fat tree με τρία επίπεδα switch*

Πηγή: Yang Liu, Jogesh K. Muppala, Malathi Veeraraghavan, A Survey of Data Center Network Architectures, 2013. http://www.ece.virginia.edu/mv/pubs/recent-samples/Datacenter-Survey.pdf

2.6 Εικονικοποίηση διακομιστών (server virtualization)

Η εικονικοποίηση διακομιστών είναι μια τεχνική, που διαχωρίζει ένα φυσικό διακομιστή σε έναν αριθμό μικρότερων εικονικών διακομιστών με τη βοήθεια λογισμικού εικονικοποίησης [18] (π.χ. hypervisor). Όπως αναφέρθηκε και πιο πάνω, τα μεγάλα κέντρα δεδομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, συχνά, περιέχουν έναν μεγάλο αριθμό διακομιστών, οι οποίοι έχουν και μεγάλες δυνατότητες (πολυπύρηνοι επεξεργαστές, τεράστιος αποθηκευτικός χώρος και μνήμη RAM). Οι περισσότερες εφαρμογές και υπηρεσίες δεν απαιτούν τόσο πολλούς πόρους. Αυτό θα οδηγούσε σε σπατάλη δαπανηρών πόρων υλικού, συντήρησης και ψύξης. Έτσι, η εικονικοποίηση των διακομιστών αξιοποιεί καλύτερα τους πόρους τους, χωρίζοντάς τους σε πολλαπλούς, μικρότερων δυνατοτήτων, εικονικούς διακομιστές, με αποτέλεσμα ο καθένας να εκτελεί το δικό του λειτουργικό σύστημα και τις δικές του εφαρμογές. Με αυτόν τον τρόπο κάθε εικονικός διακομιστής μοιάζει και λειτουργεί σα φυσικός, πολλαπλασιάζοντας, έτσι, τις δυνατότητες κάθε φυσικού μηχανήματος.

Υπάρχουν πολλοί λόγοι, για τους οποίους εταιρείες και οργανισμοί επενδύουν στην εικονικοποίηση διακομιστών. Μερικοί από τους λόγους αυτούς έχουν να κάνουν με οικονομικά κίνητρα, ενώ άλλοι με τεχνικά προβλήματα των εταιριών.



Εικόνα 7: *Παράδειγμα εικονικοποίησης ενός Ηλεκτρονικού Υπολογιστή*
Πηγή: https://www.unixtutorial.org/hw-virtualization/

Αρχικά, η εικονικοποίηση διακομιστών **εξοικονομεί χώρο**. Για τους παρόχους που έχουν εκατοντάδες ή χιλιάδες διακομιστές, η ανάγκη για φυσικό χώρο μπορεί να μειωθεί σημαντικά. Επιπλέον, η εικονικοποίηση διακομιστών έχει την δυνατότητα να λειτουργήσει και ως ένα **μέτρο ασφαλείας**. Για παράδειγμα, εάν ένας εικονικός διακομιστής αποτύχει για οποιονδήποτε λόγο, μπορεί να αντικατασταθεί από έναν άλλο, που εκτελεί την ίδια εφαρμογή. Αυτό ελαχιστοποιεί κάθε διακοπή στις υπηρεσίες του παρόχου, με την προϋπόθεση, φυσικά, ότι οι εικονικοί διακομιστές βρίσκονται σε διαφορετικό φυσικό μηχάνημα. Επιπροσθέτως, προσφέρουν στους προγραμματιστές απομονωμένα και ανεξάρτητα συστήματα, στα οποία μπορούν να δοκιμάζουν νέες εφαρμογές ή αναβαθμισμένες εκδόσεις των ήδη υπαρχόντων. Επειδή κάθε εικονικός διακομιστής είναι ανεξάρτητος σε σχέση με όλους τους άλλους, οι προγραμματιστές μπορούν να εκτελούν και να τεστάρουν λογισμικό, χωρίς να ανησυχούν ότι επηρεάζουν άλλες εφαρμογές. Τέλος, ένα πολύ δυνατό

εργαλείο στην εικονικοποίηση διακομιστών είναι η **μετακίνηση (migration**) των εικονικών μηχανών από ένα φυσικό μηχάνημα σε ένα άλλο, όταν αυτά βρίσκονται στο ίδιο δίκτυο, με τη βοήθεια λογισμικού. Αυτό προσφέρει μεγάλη ελευθερία στους παρόχους και κάνει τα περισσότερα τεχνικά προβλήματα ευκόλως αντιμετωπίσιμα.

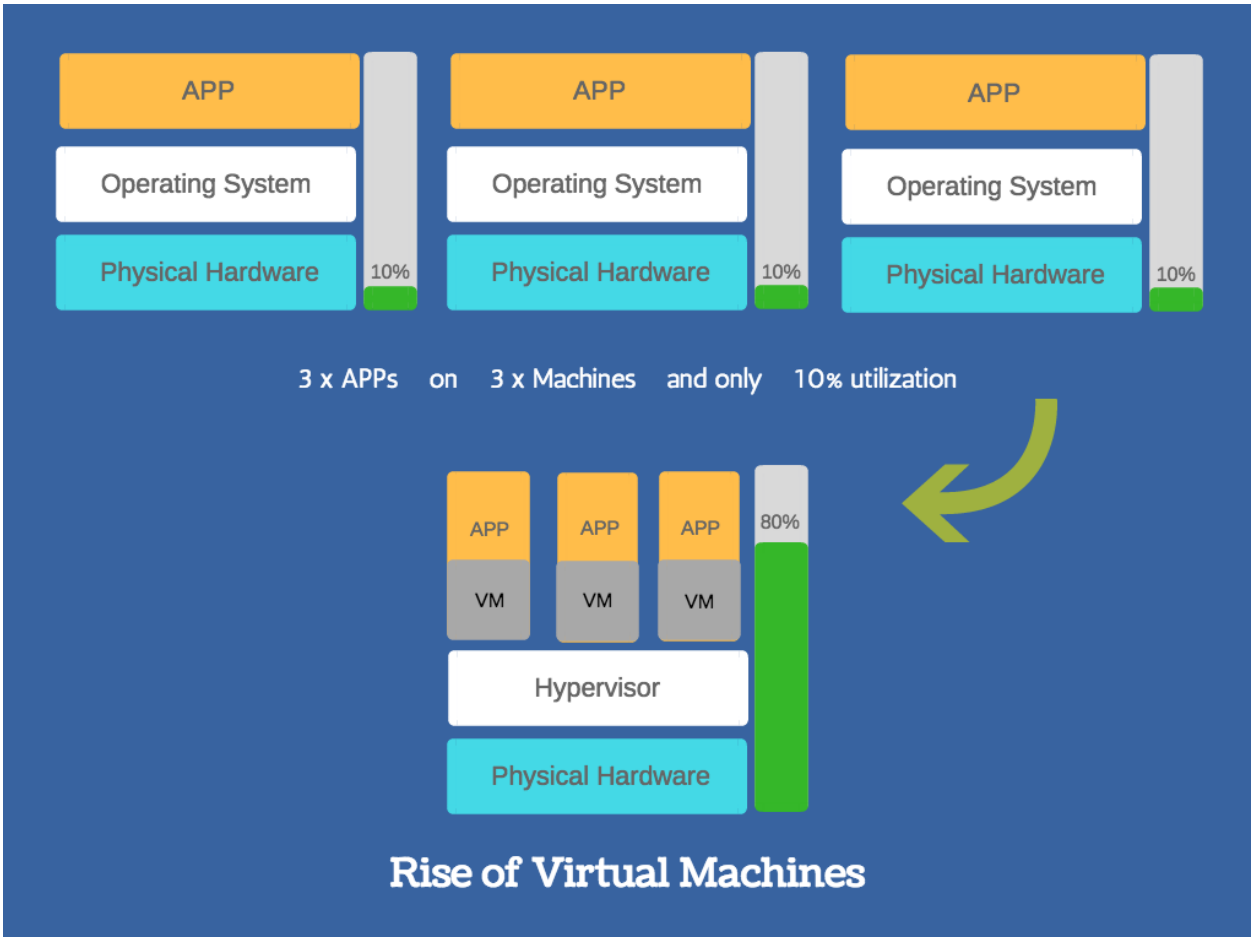
2.6.1 Τεχνικές δημιουργίας εικονικών διακομιστών

Υπάρχουν τρεις τρόποι δημιουργίας εικονικών διακομιστών: πλήρης εικονικοποίηση **(Full virtualization)**, παραεικονικοποίηση **(Paravirtualization)** και εικονικοποίηση σε επίπεδο λειτουργικού συστήματος **(OS-Level Virtualization ή Container-based virtualization)** [18]. Όλες οι παραπάνω τεχνικές επιτυγχάνονται, όπως αναφέρθηκε και πιο πάνω, με τη βοήθεια πρόσθετου λογισμικού.

Η **πλήρης εικονικοποίηση** χρησιμοποιεί ένα ειδικό είδος λογισμικού που ονομάζεται **hypervisor** (π.χ Virtual Box [19], KVM [20]). Κάθε εικονικός διακομιστής είναι εντελώς ανεξάρτητος και αγνοεί τους υπόλοιπους που εκτελούνται στο ίδιο φυσικό μηχάνημα. Επιπροσθέτως, κάθε εικονικό μηχάνημα εκτελεί το δικό του λειτουργικό σύστημα, ανεξάρτητα από τα υπόλοιπα. Μπορεί, για παράδειγμα, να υπάρχει ένας εικονικός διακομιστής με λειτουργικό σύστημα Linux και ένας άλλος με Windows. Έτσι, η πλήρης εικονικοποίηση προσφέρει υψηλότερο επίπεδο απομόνωσης ενός εικονικού διακομιστή, σε σχέση με τους υπόλοιπους τρόπους εικονικοποίησης. Από την άλλη μεριά, ο εκάστοτε χειριστής του hypervisor αλληλοεπιδρά απευθείας με τον επεξεργαστή και τον αποθηκευτικό χώρο στον δίσκο του φυσικού διακομιστή. Καθώς οι εικονικοί διακομιστές εκτελούν εφαρμογές, το hypervisor μεταδίδει πόρους από τη φυσική μηχανή στον κατάλληλο εικονικό διακομιστή. Τα hypervisors, από την μεριά τους, έχουν τις δικές τους ανάγκες για υπολογιστικούς πόρους, πράγμα που σημαίνει ότι ο φυσικός διακομιστής πρέπει να διατηρεί κάποια επεξεργαστική ισχύ για την εκτέλεση τους. Αυτό μπορεί να επηρεάσει τη συνολική απόδοση του διακομιστή και να επιβραδύνει τις εφαρμογές.

Υπάρχουν δύο μορφές πλήρους εικονικοποίησης, η εγγενής εικονικοποίηση (native - bare metal virtualization) και η φιλοξενούμενη εικονικοποίηση (Hosted

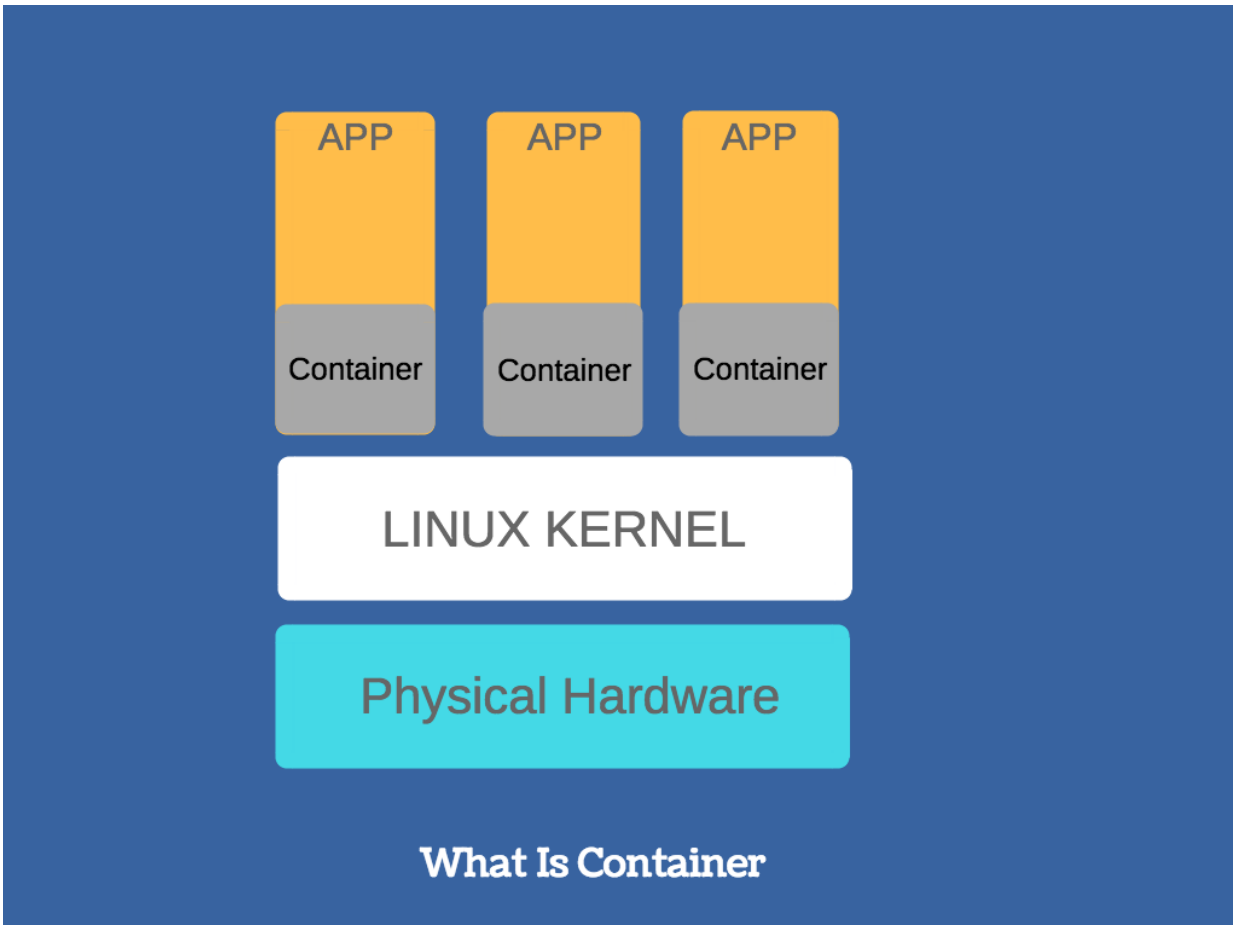
virtualization). Στην περίπτωση της εγγενούς εικονικοποίησης, το hypervisor τρέχει απευθείας στο υποκείμενο υλικό, χωρίς κεντρικό λειτουργικό σύστημα και, σε πολλές περιπτώσεις, μπορεί να είναι ενσωματωμένο στο υλικολογισμικό (firmware) του ηλεκτρονικού υπολογιστή. Στην άλλη μορφή πλήρους εικονικοποίησης, γνωστή ως φιλοξενούμενη εικονικοποίηση, το hypervisor τρέχει πάνω από το κεντρικό λειτουργικό σύστημα. Η συγκεκριμένη μορφή επιτρέπει στους χρήστες να εκτελούν εφαρμογές, όπως, για παράδειγμα, προγράμματα περιήγησης ιστού, παράλληλα με τη φιλοξενούμενη εφαρμογή εικονικοποίησης, σε αντίθεση με την εγγενή εικονικοποίηση, στην οποία η εκτέλεση εφαρμογών γίνεται μόνο σε εικονικοποιημένα συστήματα.



Εικόνα 8: *Πλήρης εικονικοποίηση με την βοήθεια hypervisor*
Πηγή:https://medium.com/@tomdeore/docking-a-docker-container-part-1-6d67d51543c3

Η τεχνική της **παραεικονικοποίησης** είναι λίγο διαφορετική. Σε αντίθεση με την πλήρη εικονικοποίηση, τα εικονικά μηχανήματα γνωρίζουν το ένα το άλλο. Αυτό επιτυγχάνεται μέσω ενός API (Application Programming Interface), μιας προγραμματιστικής διασύνδεσης δηλαδή, (π.χ. XEN) [8], η οποία διατίθεται από το φυσικό μηχάνημα σε όλα τα εικονικά. Ως εκ τούτου, τα hypervisors δε χρειάζονται πολλούς υπολογιστικούς πόρους για την διαχείριση των λειτουργιών των εικονικών μηχανών, αφού κάθε σύστημα έχει ήδη επίγνωση των απαιτήσεων που έχουν τα υπόλοιπα συστήματα. Η παραεικονικοποίηση προσπαθεί να επιλύσει το ζήτημα που εντοπίζεται στην πλήρη εικονικοποίηση, δηλαδή τείνει να εξαλείψει τους πόρους που καταναλώνονται από τα hypervisors, για να διαχειρίζονται εξ ολοκλήρου τις εικονικές μηχανές. Παρέχοντας στις εικονικές μηχανές πρόσβαση στο υποκείμενο υλικό, η τεχνική της παραεικονικοποίησης επιτρέπει την επικοινωνία μεταξύ του λειτουργικού συστήματος των εικονικών μηχανών και των hypervisors, βελτιώνοντας έτσι την απόδοση και την αποδοτικότητα ολόκληρου του συστήματος.

Η εικονικοποίηση σε επίπεδο λειτουργικού συστήματος, γνωστή και ως **Container-based virtualization** δε χρησιμοποιεί καθόλου το hypervisor. Αντί αυτού, η τεχνική αυτή δημιουργεί πολλαπλά διαμερίσματα πόρων του λειτουργικού συστήματος, που ονομάζονται containers (σημαντικά παραδείγματα Container-based virtualization είναι το Docker [21] και το LXC [22]). Επομένως, το λογισμικό που εκτελείται σε containers επικοινωνεί απευθείας με τον φυσικό διακομιστή, αλλά, ενώ περιμένει να δει ολόκληρο τον υπολογιστή, μπορεί να δει μόνο τους πόρους που έχουν διατεθεί στα containers και πιστεύει ότι μόνο οι συγκεκριμένοι πόροι είναι διαθέσιμοι. Σε κάθε λειτουργικό σύστημα μπορούν να δημιουργηθούν πολλά containers, σε καθένα από τα οποία κατανέμεται ένα υποσύνολο πόρων του υπολογιστή. Κάθε container έχει τη δυνατότητα να περιέχει οποιονδήποτε αριθμό προγραμμάτων, τα οποία μπορούν να εκτελούνται ταυτόχρονα ή ξεχωριστά, ακόμη και να αλληλοεπιδρούν μεταξύ τους.



Εικόνα 9: *Container-based Εικονικοποίηση*
Πηγή: https://medium.com/@tomdeore/docking-a-docker-container-part-1-6d67d51543c3

Ως εκ τούτου, ένα container είναι πολύ μικρότερο και ελαφρύτερο από ένα εικονικό μηχάνημα (για παράδειγμα, η εκκίνηση ενός container γίνεται σε μερικά κλάσματα δευτερολέπτου). Από την άλλη πλευρά, όμως, τα containers προσφέρουν χαμηλότερη ευελιξία και επίπεδο απομόνωσης από τα εικονικά μηχανήματα, καθώς οι χρήστες δεν έχουν πρόσβαση στον πυρήνα του λειτουργικού συστήματος.

3. Ιδιωτικότητα

3.1 Η έννοια της ιδιωτικότητας

Ο πρώτος ορισμός της ιδιωτικότητας δόθηκε το 1890 από δύο Αμερικάνους δικηγόρους, τον Samuel D. Warren και τον Louis D. Brandeis, στο άρθρο τους «Το δικαίωμα στην ιδιωτικότητα» ("The Right to Privacy") [23]. Οι συγγραφείς αυτοί όρισαν την ιδιωτικότητα ως «το δικαίωμα να μένουμε μόνοι». Ο πιο συνηθισμένος, όμως, ορισμός της ιδιωτικότητας, που χρησιμοποιείται σήμερα, είναι αυτός από τον Alan Westin (στο βιβλίο του «Privacy and freedom, 1967») [24]: «Η ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν από μόνοι τους για το πότε, πως και μέχρι ποιο σημείο οι πληροφορίες, που αφορούν αυτούς, θα διαβιβάζονται σε άλλους». Η ιδιωτικότητα έχει αναγνωριστεί ως θεμελιώδες ανθρώπινο δικαίωμα σε μία δημοκρατική κοινωνία και πρέπει να προστατεύεται. Επίσης, αποτελεί προϋπόθεση για την ανθρώπινη αξιοπρέπεια και διατηρεί την ατομικότητα του ανθρώπου.

Γενικά, η έννοια της ιδιωτικότητας μπορεί να χωριστεί σε τρεις μορφές:

1. **Εδαφική ιδιωτικότητα**, η οποία αφορά την προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο, δηλαδή οικιακά περιβάλλοντα, όπως τον εργασιακό ή τον δημόσιο χώρο.

2. **Ιδιωτικότητα του ατόμου** (ή σωματική ιδιωτικότητα), η οποία αφορά την προστασία ενός προσώπου από την αδικαιολόγητη παρέμβαση, όπως τον σωματικό έλεγχο, τη δοκιμή φαρμάκων ή τις πληροφορίες που παραβιάζουν την ηθική αίσθηση του ατόμου.

3. **Πληροφοριακή ιδιωτικότητα**, η οποία αφορά τον έλεγχο του αν και πως τα προσωπικά στοιχεία (π.χ. χρηματοπιστωτικές πληροφορίες, ιατρικά και κυβερνητικά αρχεία) μπορούν να συγκεντρωθούν, να αποθηκευτούν, να επεξεργαστούν ή να διαδοθούν επιλεκτικά.

3.2 Νομοθεσία της Ελλάδας περί προστασίας προσωπικών δεδομένων

Στην Ελλάδα το 1997, θεσπίστηκε ο νόμος 2472/1997 [25], με επίσημο τίτλο «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», αντικείμενο του οποίου ήταν η θέσπιση των προϋποθέσεων για την

Εικόνα 10: *Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR*
Πηγή: http://elitebusinessmagazine.co.uk/legal/item/gdpr-two-years-on

επεξεργασία των δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και, ιδίως, της ιδιωτικής ζωής. Ο συγκεκριμένος νόμος καταργήθηκε (με την επιφύλαξη των ορισμών του άρθρου 2, καθώς και κάποιων άλλων άρθρων και εδαφίων, όπου γίνεται ρητή παραπομπή σε αυτούς σε σχετική με τα προσωπικά δεδομένα νομοθεσία) [25] και την θέση του πήρε ο νόμος 4624/2019, με τίτλο «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», ο οποίος, μεταξύ άλλων, ενσωμάτωσε την οδηγία της Ευρωπαϊκής Ένωσης [26](2016/680 [27] και 2016/681 [28] του Ευρωπαϊκού Κοινοβουλίου) περί προστασίας προσωπικών δεδομένων. Η συγκεκριμένη οδηγία είναι κοινώς γνωστή ως Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation - **GDPR**).

Αξίζει να σημειωθεί ότι η Ελλάδα κινδυνεύει με πρόστιμο εκατομμυρίων ευρώ από το Δικαστήριο της Ευρωπαϊκής Ένωσης, λόγω καθυστέρησης στην ενσωμάτωση της οδηγίας GDPR. Συγκεκριμένα, η προθεσμία ενσωμάτωσης είχε λήξει από τις 6 Μαΐου του 2018, ενώ η οδηγία είχε ψηφιστεί από τον Απρίλιο του 2016. Συνεπώς, η χώρα μας είχε 2 χρόνια στην διάθεσή της, προκειμένου να την ενσωματώσει στο εσωτερικό της δίκαιο.
Ο Γενικός Κανονισμός Προστασίας Δεδομένων έχει ως στόχο να διευρύνει την προστασία των δεδομένων στην εποχή που αναπτύσσεται ραγδαία το υπολογιστικό νέφος, εξασφαλίζοντας ότι η προστασία των δεδομένων αποτελεί θεμελιώδες και βασικό δικαίωμα, το οποίο θα ρυθμίζεται με συνέπεια σε όλη την Ευρώπη. Στόχος του είναι να διευκολύνει τη ροή δεδομένων προσωπικού χαρακτήρα σε όλα τα μέλη της Ευρωπαϊκής Ένωσης. Κάθε εταιρεία που εξυπηρετεί ευρωπαίους πολίτες και συλλέγει τα δεδομένα τους, θα πρέπει να συμμορφώνεται με αυτή την οδηγία, ανεξάρτητα από το αν η ίδια εδρεύει σε χώρα εντός τις Ευρώπης.
Παρακάτω, θα ορίσουμε κάποιες σημαντικές έννοιες, που αφορούν την ιδιωτικότητα, έτσι όπως ορίζονται από την Ευρωπαϊκή Επιτροπή και από τον Ελληνικό νόμο 2472/1997.

3.3 Προσωπικά δεδομένα

Τα προσωπικά δεδομένα, σύμφωνα με την Ευρωπαϊκή επιτροπή, είναι οι πληροφορίες που αφορούν ένα ταυτοποιημένο άτομο ή πληροφορίες, οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου. Επιπλέον, δεδομένα προσωπικού χαρακτήρα παραμένουν τα δεδομένα, τα οποία έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα, αλλά μπορούν, ακόμα, να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου.
Ο Γενικός Κανονισμός Προστασίας Δεδομένων προστατεύει τα δεδομένα προσωπικού χαρακτήρα, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Με άλλα λόγια, είναι τεχνολογικά ουδέτερος και μπορεί να εφαρμοστεί τόσο στην αναλογική, όσο και στην ψηφιακή μορφή επεξεργασίας.

Επιπροσθέτως, δεν έχει σημασία ο τρόπος αποθήκευσης των δεδομένων (για παράδειγμα, σε έντυπη μορφή ή μέσω κλειστού κυκλώματος παρακολούθησης ή σε συστήματα τεχνολογίας πληροφοριών)

Κάποια παραδείγματα προσωπικών δεδομένων είναι:

- Όνομα και Επώνυμο
- Διεύθυνση κατοικίας
- Τηλέφωνο
- Αριθμοί χρεωστικών και πιστωτικών τραπεζικών καρτών
- Προσωπικές φωτογραφίες και βίντεο
- Ενδιαφέροντα και απόψεις
- Διεύθυνση διαδικτυακού πρωτοκόλλου IP
- Προσωπική ηλεκτρονική διεύθυνση (π.χ *όνομα.επώνυμο@εταιρεία.com*)

Κάποια προσωπικά δεδομένα χρήζουν ακόμα μεγαλύτερης προστασίας, γιατί έχουν ιδιαίτερη βαρύτητα για τον σχηματισμό της εικόνας της προσωπικότητας ενός ατόμου. Αυτά τα δεδομένα τα ονομάζουμε **Ευαίσθητα Δεδομένα** και στην ουσία αφορούν τον σκληρό πυρήνα της ιδιωτικής ζωής κάθε ατόμου.
Κάποια παραδείγματα ευαίσθητων δεδομένων είναι:

- Φυλετική ή εθνική προέλευση
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- Ερωτική ζωή
- Πολιτικά φρονήματα
- Θέματα υγείας
- Ποινικές διώξεις ή καταδίκες

3.3.1 Επεξεργασία προσωπικών δεδομένων

Σύμφωνα με τα άρθρο 2, περ. δ΄, του νόμου 2472/1997 [25], επεξεργασία προσωπικών δεδομένων είναι κάθε εργασία ή σειρά εργασιών, που

πραγματοποιείται από το Δημόσιο ή από Νομικό Πρόσωπο Δημοσίου ή Ιδιωτικού Δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο, με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων, και εφαρμόζεται σε δεδομένα προσωπικού χαρακτήρα. Οι εργασίες αυτές περιλαμβάνουν ενέργειες, όπως η συλλογή, η καταχώρηση, η χρήση, η αποθήκευση, η τροποποίηση, η διάδοση, η συσχέτιση, η διαγραφή και η καταστροφή δεδομένων.

Παραδείγματα επεξεργασίας προσωπικών δεδομένων:

- διαχείριση προσωπικού και μισθοδοσία
- προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών, που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα
- καταστροφή, διά τεμαχισμού, εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα·
- δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου στο διαδίκτυο
- αποθήκευση διευθύνσεων IP
- μαγνητοσκόπηση (κλειστό κύκλωμα βιντεοσκόπησης)

Ο συγκεκριμένος νόμος (2472/1997) [25] ορίζει, επίσης, και τα πρόσωπα, φυσικά ή νομικά, τα οποία έχουν άμεση σχέση με την επεξεργασία προσωπικών δεδομένων. Τα πρόσωπα αυτά είναι το *«Υποκείμενο των δεδομένων»*, ο *«Υπεύθυνος επεξεργασίας» , ο «Εκτελών την επεξεργασία»*, ο *«Τρίτος»* και ο *«Αποδέκτης»*.
Πιο αναλυτικά:

- **Υποκείμενο των δεδομένων**, σύμφωνα με το άρθρο 2, περ. γ΄ του νόμου 2472/1997, «είναι το φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων, που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.»

- **Υπεύθυνος επεξεργασίας**, σύμφωνα με το άρθρο 2, περ. ζ΄ του νόμου 2472/1997, «είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια, βάσει των οποίων γίνεται η επιλογή του, καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.»

- **Εκτελών της επεξεργασίας**, σύμφωνα με το άρθρο 2, περ. η΄ του νόμου 2472/1997, «είναι οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.» Η σχέση μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία έχει την μορφή σύμβασης έργου, στην οποία υπάρχει ειδικότερος όρος για επεξεργασία δεδομένων από τον εκτελούντα, βάσει καταγεγραμμένων εντολών του υπευθύνου.

- **Τρίτος,** σύμφωνα με το άρθρο 2, περ. θ΄ του νόμου 2472/1997, «είναι κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.»

- **Αποδέκτης,** σύμφωνα με το άρθρο 2, περ. ι΄ του νόμου 2472/1997, «είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξάρτητα αν πρόκειται για τρίτο ή όχι.»

Ο GDPR επιβάλλει υποχρεώσεις τόσο στους υπεύθυνους επεξεργασίας δεδομένων, όσο και στους εκτελούντες την επεξεργασία. Οι εταιρείες και οι οργανισμοί πρέπει:

- Να προστατεύουν τα προσωπικά δεδομένα λαμβάνοντας κατάλληλα μέτρα ασφαλείας
- Να γνωστοποιούν στις αρχές τις παραβιάσεις προσωπικών δεδομένων
- Να λαμβάνουν συγκατάθεση για τη συλλογή και την επεξεργασία προσωπικών δεδομένων
- Να τηρούν αρχεία, που θα παρέχουν αναλυτικές πληροφορίες για τις δραστηριότητες επεξεργασίας δεδομένων
- Να παρέχουν σαφή γνωστοποίηση για τη συλλογή δεδομένων
- Να περιγράφουν τον λόγο και τις περιπτώσεις επεξεργασίας των προσωπικών δεδομένων
- Να ορίζουν πολιτικές διατήρησης και διαγραφής δεδομένων
- Να παρέχουν σαφή γνωστοποίηση για τη συλλογή δεδομένων
- Να περιγράφουν τον λόγο και τις περιπτώσεις επεξεργασίας των προσωπικών δεδομένων
- Να ορίζουν πολιτικές διατήρησης και διαγραφής δεδομένων

3.4 Ασφάλεια των δεδομένων στο υπολογιστικό νέφος

Η τεχνολογία cloud έχει δώσει ευκαιρίες σε πολλές επιχειρήσεις να αναδείξουν τις δυνατότητές τους στον επιχειρηματικό κόσμο. Δεν έχουν, μόνο, την ευκαιρία να αναπτυχθούν, αλλά και να εξελίξουν τις επιχειρηματικές τους δραστηριότητες στο επόμενο επίπεδο. Η τεχνολογία του υπολογιστικού νέφους, δηλαδή, έχει ανοίξει μια πόρτα για τις μικρές και μεσαίες επιχειρήσεις, ώστε να αποκτήσουν ικανοποιητικό μερίδιο αγοράς.

Η τεχνολογία cloud, όπως είδαμε, παρέχει διάφορα πλεονεκτήματα. Ξεκινώντας από τη διαχείριση και αποθήκευση δεδομένων, προσφέρει σχεδόν μηδενικό χρόνο διακοπής λειτουργίας, Συστήματα Διαχείρισης Πελατειακών Σχέσεων (Customer Relationship Management - CRM), έως και ολόκληρο τον αυτοματισμό μίας επιχείρησης. Μειώνει, επίσης, ένα μεγάλο ποσό επένδυσης και εξοικονομεί πολύ χρόνο.

Ταυτόχρονα, όμως, η υιοθέτηση των υπηρεσιών του υπολογιστικού νέφους, φέρνει αντιμέτωπες τις επιχειρήσεις με μία σειρά ζητημάτων. Η ασφάλεια των δεδομένων και η ιδιωτικότητα υπήρξε, ανέκαθεν, ένα σημαντικό ζήτημα στον τομέα της πληροφορικής και, ιδιαίτερα, στην περίπτωση του υπολογιστικού νέφους, αφού τα δεδομένα των χρηστών του είναι διασκορπισμένα στους διακομιστές των παρόχων cloud υπηρεσιών. Το περιβάλλον υπολογιστικού νέφους παρέχει δύο βασικούς τύπους λειτουργιών: επεξεργασία και αποθήκευση δεδομένων. Στην ουσία, οι χρήστες δεν έχουν τον έλεγχο των αποθηκευμένων δεδομένων τους και η επεξεργασία τους γίνεται εξ αποστάσεως, με αποτέλεσμα τα δεδομένα και άλλα ιδιωτικά στοιχεία του χρήστη να πρέπει να μεταδοθούν, μέσω διαδικτύου, στην υποδομή του cloud, για να γίνουν αντικείμενα επεξεργασίας. Με άλλα λόγια, οι χρήστες δε γνωρίζουν πού είναι αποθηκευμένα τα δεδομένα τους και σε ποια μηχανήματα γίνεται η επεξεργασία τους. Ο κύριος υπεύθυνος για την ασφάλεια των δεδομένων των χρηστών του υπολογιστικού νέφους είναι ο εκάστοτε πάροχος. Από τα παραπάνω, μπορούμε να συμπεράνουμε ότι η ιδιωτικότητα των χρηστών του υπολογιστικού νέφους κινδυνεύει, κυρίως, από κακόβουλους χρήστες, αλλά και από τους ίδιους τους παρόχους τους.

Εικόνα 11: *Εμπιστευτικότητα - Ακεραιότητα - Διαθεσιμότητα των Δεδομένων (CIA triad)*

Πηγή: https://spanning.com/blog/cia-triad-best-practices-securing-your-org/

Εν ολίγοις, τα κύρια ζητήματα στην ασφάλεια δεδομένων και, κατ' επέκταση, στην ασφάλεια δεδομένων στο υπολογιστικό νέφος, περιλαμβάνουν την εμπιστευτικότητα των δεδομένων (Data Confidentiality), την ακεραιότητα των δεδομένων *(Data Integrity)* και τη διαθεσιμότητα δεδομένων *(Data Availability)* [29]. Γνωστά και ως CIA τριάδα (CIA triad), τα παραπάνω είναι ένα μοντέλο που έχει σχεδιαστεί, για να καθοδηγεί τις πολιτικές για την ασφάλεια των πληροφοριών εντός ενός οργανισμού. Το μοντέλο αυτό αναφέρεται, επίσης, μερικές φορές ως τριάδα AIC για την αποφυγή σύγχυσης με την Κεντρική Υπηρεσία Πληροφοριών των Ηνωμένων Πολιτειών Αμερικής (Central Intelligence Agency - CIA).

Σε αυτό το πλαίσιο, η εμπιστευτικότητα είναι ένα σύνολο κανόνων, που περιορίζουν την πρόσβαση σε πληροφορίες, η ακεραιότητα είναι η διασφάλιση ότι οι πληροφορίες είναι αξιόπιστες και ακριβείς και η διαθεσιμότητα αποτελεί εγγύηση αξιόπιστης πρόσβασης στις πληροφορίες από εξουσιοδοτημένα άτομα.

Εμπιστευτικότητα των δεδομένων *(Data Confidentiality)*

Η εμπιστευτικότητα των δεδομένων είναι περίπου ισοδύναμη με την ιδιωτικότητα. Η ιδιωτικότητα των δεδομένων στο υπολογιστικό νέφος αποτελεί μέρος της πληροφοριακής ιδιωτικότητας, όπως είδαμε πιο πάνω, η οποία αναφέρεται στη γενική απαίτηση των ατόμων να μην είναι διαθέσιμα τα προσωπικά τους δεδομένα σε άλλα άτομα ή οργανισμούς. Στην περίπτωση του υπολογιστικού νέφους, που ο πάροχος υπηρεσιών κατέχει τα προσωπικά δεδομένα των πελατών του, η ιδιωτικότητα αναφέρεται στην υποχρέωση που έχει ο πάροχος να τα κρατά κρυφά και να αποτρέπει πιθανούς κακόβουλους χρήστες από την κλοπή τους.

Ακεραιότητα των δεδομένων *(Data Integrity)*

Η ακεραιότητα των δεδομένων είναι ένα από τα πιο κρίσιμα στοιχεία σε οποιοδήποτε σύστημα πληροφοριών. Γενικά, η ακεραιότητα περιλαμβάνει τη διατήρηση της συνέπειας, της ακρίβειας και της αξιοπιστίας των δεδομένων, καθ' όλη τη διάρκεια του κύκλου ζωής τους. Τα δεδομένα δεν πρέπει να αλλάζουν κατά

τη μεταφορά και πρέπει να ληφθούν μέτρα, για να διασφαλιστεί ότι δεν μπορούν να τροποποιηθούν από μη εξουσιοδοτημένα άτομα. Αυτά τα μέτρα περιλαμβάνουν δικαιώματα αρχείου (file permissions) και στοιχεία ελέγχου πρόσβασης χρήστη (user access controls). Ο μηχανισμός της εξουσιοδότησης αυτής σε ένα σύστημα καθορίζει ποιο επίπεδο πρόσβασης σε δεδομένα και πόρους θα έχει ένας συγκεκριμένος πιστοποιημένος χρήστης. Λόγω της μεγάλης ποσότητας πελατών και σημείων πρόσβασης σε ένα περιβάλλον υπολογιστικού νέφους, η εξουσιοδότηση είναι ζωτικής σημασίας για την ακεραιότητα των δεδομένων.

Διαθεσιμότητα δεδομένων *(Data Availability)*

Η διαθεσιμότητα των δεδομένων είναι η διαδικασία διασφάλισης ότι τα δεδομένα είναι διαθέσιμα στους τελικούς τους χρήστες, όποτε και οπουδήποτε τα χρειάζονται. Η διαθεσιμότητα δεδομένων είναι ζωτικής σημασίας για όλες τις επιχειρήσεις. Κάθε στιγμή που περνάει και ένας οργανισμός δεν έχει διαθέσιμα τα δεδομένα του, καταναλώνεται ο χρόνος των υπαλλήλων του, με αποτέλεσμα να σπαταλούνται εργατοώρες. Όπως καταλαβαίνουμε, οι πάροχοι υπολογιστικού νέφους πρέπει να διασφαλίζουν τη διαθεσιμότητα των δεδομένων στους πελάτες τους. Αυτό το πετυχαίνουν με τη συνεχή και αυστηρή συντήρηση και αναβάθμιση όλου του υλικού, με τις απαραίτητες αναβαθμίσεις του λογισμικού, καθώς, επίσης, και κρατώντας αντίγραφα ασφαλείας των εικονικών μηχανών και, γενικά, των δεδομένων των πελατών τους σε διαφορετικές τοποθεσίες (ακόμα και σε διαφορετικά κέντρα δεδομένων). Επομένως, όταν υπάρχουν ατυχήματα, όπως βλάβες σε σκληρούς δίσκους ή αστοχίες δικτύου, οι πελάτες μπορούν να ανακτήσουν ή να χρησιμοποιήσουν τα αντίγραφα των δεδομένων τους, χωρίς χάσιμο πολύτιμου χρόνου. Ακόμα και στην χειρότερη περίπτωση καταστροφής ενός κέντρου δεδομένων (από πυρκαγιά για παράδειγμα), όλα τα δεδομένα των χρηστών του νέφους θα είναι ασφαλή σε κάποιο άλλο κέντρο δεδομένων.

4. Παραβιάσεις ιδιωτικότητας από κακόβουλους χρήστες

Λόγω της απλότητας του υπολογιστικού νέφους, οι χρήστες του και οι εφαρμογές, που φιλοξενούνται σε αυτό, αυξάνονται εκθετικά μέρα με την μέρα. Το γεγονός αυτό οδηγεί σε μεγαλύτερες απειλές για τους πελάτες των υπηρεσιών του νέφους. Εάν, δηλαδή, μία οποιαδήποτε επίθεση κακόβουλου χρήστη είναι επιτυχής στα δεδομένα που φιλοξενούνται σε έναν πάροχο, τότε θα έχουμε μη εξουσιοδοτημένη πρόσβαση και παραβίαση ιδιωτικότητας σε δεδομένα πολλών χρηστών ταυτόχρονα. Εκτός από αυτόν τον κίνδυνο, η επεξεργασία δεδομένων είναι επίσης ένα ευάλωτο σημείο του υπολογιστικού νέφους, αφού τα δεδομένα μεταδίδονται μεταξύ πολλαπλών χρηστών και των αντίστοιχων παρόχων τους.
Το γεγονός αυτό, όπως, επίσης, και ο τρόπος με τον οποίο είναι δομημένες οι εγκαταστάσεις των παρόχων υπηρεσιών υπολογιστικού νέφους, δημιουργεί απειλές και ευπάθειες. Η ευπάθεια αναφέρεται σε μια αδυναμία ή ένα ελάττωμα σε ένα σύστημα, που μπορεί να αξιοποιηθεί από μία επίθεση. Μια απειλή είναι η εκμετάλλευση οποιασδήποτε γνωστής ευπάθειας, που μπορεί να οδηγήσει σε σοβαρή απώλεια δεδομένων και πληροφοριών.

Έτσι, με βάση τα παραπάνω, το απόρρητο των δεδομένων μπορεί να τεθεί σε κίνδυνο από κακόβουλος χρήστες σε δύο βασικές περιπτώσεις:

1) Στη μετάδοση ευαίσθητων προσωπικών δεδομένων από και προς τον διακομιστή του παρόχου υπολογιστικού νέφους
2) Στην αποθήκευση των προσωπικών δεδομένων εντός της υποδομής του νέφους.

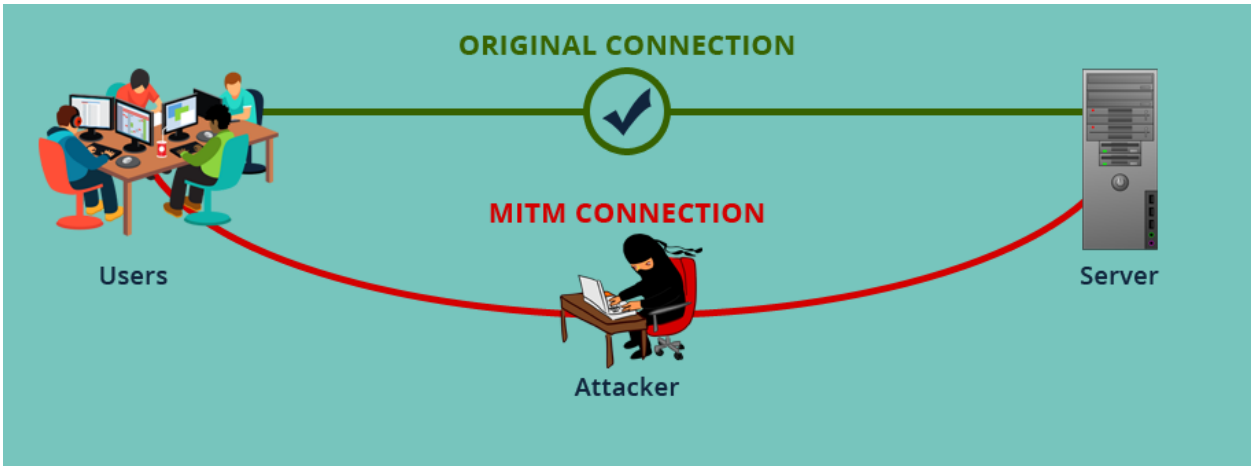
4.1 Απειλές απορρήτου κατά τη μεταφορά δεδομένων

Όπως είδαμε και παραπάνω, ένα από τα βασικά χαρακτηριστικά του υπολογιστικού νέφους είναι η απομακρυσμένη πρόσβαση του χρήστη στις διάφορες πλατφόρμες - εφαρμογές cloud μέσω διαδικτύου. Η επικοινωνία, δηλαδή, μεταξύ της συσκευής του χρήστη και του παρόχου του, πραγματοποιείται μέσω διαδρομών του διαδικτύου. Το γεγονός αυτό ανοίγει τον δρόμο σε

κακόβουλους χρήστες, να επιχειρήσουν να επιτεθούν στα συγκεκριμένα κανάλια επικοινωνίας, με αποτέλεσμα να απειλείται η ιδιωτικότητα των δεδομένων του χρήστη. Ο πιο συνηθισμένος τρόπος, με τον οποίο διεξάγονται τέτοιου είδους επιθέσεις, είναι γνωστός με το όνομα «*Man-in-the-middle attacks*».

4.1.1 Επιθέσεις Man-in-the-middle

Σε μία επίθεση «man-in-the-middle» ένας εισβολέας παρεμποδίζει ή ακούει κρυφά επικοινωνίες μεταξύ δύο μερών, είτε για να υποκλέψει πληροφορίες είτε για να τις τροποποιήσει [30]. Οι εισβολείς ενδέχεται να χρησιμοποιήσουν επιθέσεις man-in-the-middle, για να κλέψουν στοιχεία σύνδεσης ή προσωπικά στοιχεία, να κατασκοπεύσουν το θύμα ή να σαμποτάρουν επικοινωνίες και να καταστρέψουν δεδομένα. Οι επιθέσεις αυτές, οι οποίες είναι από τις παλαιότερες μορφές επίθεσης στον κυβερνοχώρο, μπορούν να εκτελεστούν με διάφορους τρόπους. Είτε παθητικά, δηλαδή με την εγκατάσταση ενός κακόβουλου προγράμματος υποκλοπής, το οποίο συλλέγει προσωπικά δεδομένα των θυμάτων, είτε ενεργητικά, δηλαδή με την ενεργή παρουσία του κακόβουλου χρήστη και την υποκλοπή πληροφοριών την ώρα που διεκπεραιώνεται επικοινωνία του χρήστη με τον πάροχο του. Εν ολίγοις, μία επίθεση man-in-the-middle βρίσκει έναν τρόπο να εισχωρήσει μεταξύ ενός χρήστη και ενός παρόχου υπολογιστικού νέφους και επιχειρεί να αποκρύψει την παραβίαση και την κλοπή πληροφοριών.



Εικόνα 12: *Man-in-the-middle Επίθεση*
Πηγή: https://www.clickssl.net/blog/how-to-stay-safe-against-the-man-in-the-middle-attack

Ακολουθούν κάποιοι συνηθισμένοι τρόποι με τους οποίους οι Man-in-the-Middle επιθέσεις επεμβαίνουν στα συστήματα επικοινωνίας.

4.1.2 Υποκλοπή (Eavesdropping)

Μια επίθεση υποκλοπής, επίσης γνωστή και ως **snifing** ή **snooping**, είναι η κλοπή πληροφοριών καθώς μεταδίδονται μέσω δικτύου από έναν υπολογιστή, ένα smartphone ή άλλη συνδεδεμένη συσκευή. Η επίθεση αυτή εκμεταλλεύεται τις μη ασφαλείς επικοινωνίες δικτύου, για να αποκτήσει πρόσβαση στα δεδομένα, καθώς αποστέλλονται ή λαμβάνονται από τον χρήστη της. Οι εισβολείς, συνήθως, παρακολουθούν ευαίσθητες οικονομικές και επιχειρηματικές πληροφορίες, τις οποίες μπορούν να πουλήσουν για εγκληματικούς σκοπούς. Μια επίθεση υποκλοπής είναι σχετικά δύσκολο να εντοπιστεί, διότι οι επικοινωνίες μεταξύ των δικτύων φαίνεται να λειτουργούν κανονικά. Για να είναι επιτυχής μια επίθεση υποκλοπής, απαιτεί μια, όχι τόσο ασφαλή, σύνδεση μεταξύ ενός πελάτη και ενός διακομιστή, την οποία ο εισβολέας μπορεί να εκμεταλλευτεί, για να παρακολουθήσει την κίνηση του δικτύου. Οι επιθέσεις αυτές είναι κυρίως παθητικές, δηλαδή, ο εισβολέας εγκαθιστά λογισμικό παρακολούθησης δικτύου (π.χ. sniffer) σε έναν υπολογιστή ή διακομιστή, το οποίο απλά «κάθεται» κάπου στην διαδρομή του δικτύου και παρακολουθεί όλα τα σχετικά πακέτα του. Έτσι, ο εισβολέας δεν χρειάζεται καν να έχει συνεχή σύνδεση με το λογισμικό παρακολούθησης. Μπορεί απλά να εγκαταστήσει το κακόβουλο λογισμικό σε μία εύκολα παραβιάσιμη συσκευή του δικτύου, και, στη συνέχεια, να επιστρέψει κάποια στιγμή στο μέλλον, για να ανακτήσει τυχόν δεδομένα που απορροφήθηκαν ή να ενεργοποιήσει το λογισμικό, για να στείλει δεδομένα σε κάποια καθορισμένη στιγμή.

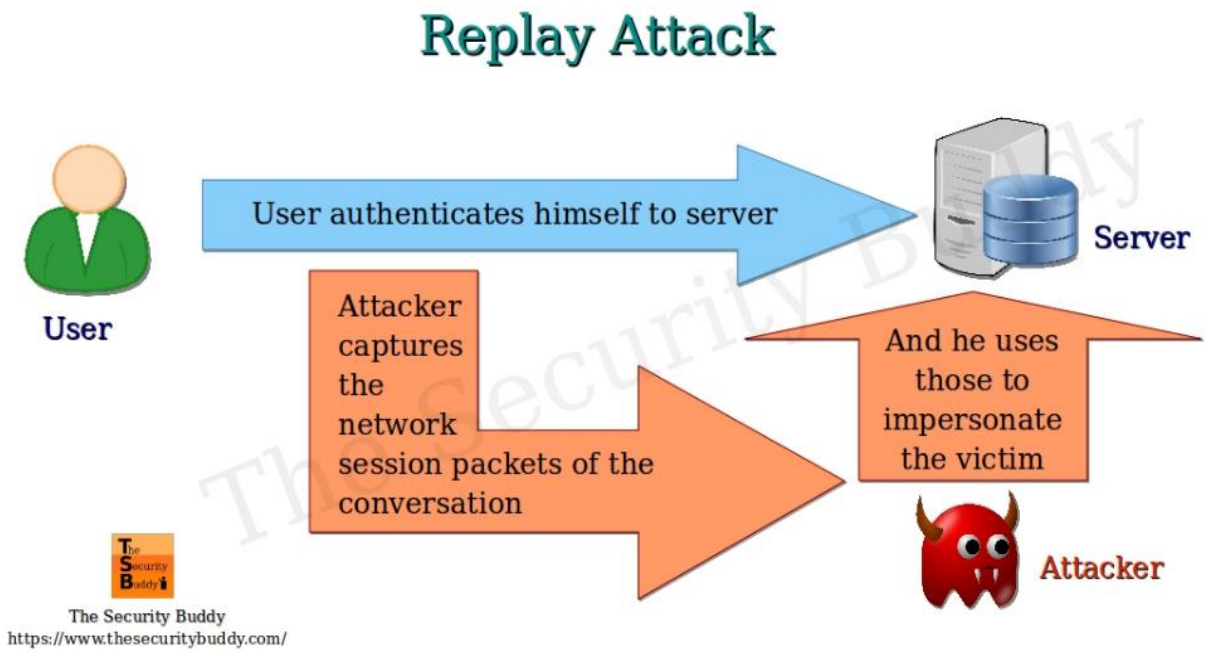
4.1.3 Επιθέσεις τροποποίησης (Message tampering)

Οι επιθέσεις τροποποίησης λειτουργούν περίπου, όπως και οι επιθέσεις υποκλοπής. Εκμεταλλεύονται, δηλαδή, μη ασφαλή δίκτυα, ώστε να υποκλέψουν δεδομένα, με τη διαφορά, όμως, ότι προσπαθούν να τα τροποποιήσουν. Έτσι, εκτός από την εισχώρηση στο δίκτυο, τέτοιου είδους επιθέσεις έχουν και την επιπρόσθετη δυσκολία του χρονικού περιορισμού. Αυτό σημαίνει ότι οι επιθέσεις αυτές πρέπει να λάβουν χώρα ακριβώς την ίδια ώρα που γίνεται η μεταφορά των δεδομένων από το ένα σημείο του δικτύου στο άλλο. Με αυτό τον τρόπο, ο

εισβολέας δεν «παρατηρεί» παθητικά τα πακέτα του δικτύου, αλλά έχει την δυνατότητα να τα λαμβάνει πρώτα αυτός, να τα τροποποιεί ή να δημιουργεί νέα δικά του, και στη συνέχεια να τα αποστέλλει στον τελικό παραλήπτη. Όπως καταλαβαίνουμε, αυτός ο τρόπος επίθεσης δεν κλέβει απλώς ιδιωτικά δεδομένα, αλλά μπορεί να τα σαμποτάρει κιόλας, δημιουργώντας μεγάλα προβλήματα σε οργανισμούς η ιδιώτες.

4.1.4 Επιθέσεις επανάληψης (Replay attacks)

Οι επιθέσεις επανάληψης είναι μία κατηγορία επίθεσης στο δίκτυο, στην οποία ένας εισβολέας παρεμποδίζει και, στη συνέχεια, επαναλαμβάνει μια έγκυρη μετάδοση δεδομένων. Λόγω της εγκυρότητας των αρχικών δεδομένων, τα οποία συνήθως προέρχονται από εξουσιοδοτημένο χρήστη, τα πρωτόκολλα ασφαλείας του δικτύου αντιμετωπίζουν την επίθεση σα να ήταν μια κανονική μετάδοση δεδομένων. Ο κίνδυνος των επιθέσεων επανάληψης είναι αρκετά μεγάλος, διότι ο εκάστοτε εισβολέας δε χρειάζεται να έχει προηγμένες δεξιότητες αποκρυπτογράφησης, δεδομένου ότι τα αρχικά μηνύματα αντιγράφονται και, στη συνέχεια, αναμεταδίδονται κατά λέξη. Με αυτόν τον τρόπο, ο εισβολέας μπορεί να ξεγελάσει τον παραλήπτη του μηνύματος, με αποτέλεσμα να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες ή ακόμα και να κλέψει χρηματικά ποσά.



Εικόνα 13: *Επίθεση Επανάληψης*
Πηγή: https://www.thesecuritybuddy.com/vulnerabilities/what-is-replay-attack/

Παρακάτω παρουσιάζεται ένα παράδειγμα μιας επίθεσης επανάληψης. Ένα μέλος του προσωπικού μιας εταιρείας ζητά οικονομική μεταφορά, στέλνοντας ένα κρυπτογραφημένο μήνυμα στον οικονομικό διαχειριστή της εταιρείας. Ένας εισβολέας παρακολουθεί αυτό το μήνυμα, το συλλαμβάνει και τώρα είναι σε θέση να το στείλει ξανά. Επειδή είναι ένα αυθεντικό μήνυμα, που απλώς έχει αποσταλεί ξανά, το μήνυμα είναι ήδη σωστά κρυπτογραφημένο και φαίνεται νόμιμο για τον οικονομικό διαχειριστή. Σε αυτό το σενάριο, ο οικονομικός διαχειριστής είναι πιθανό να ανταποκριθεί στο νέο αυτό αίτημα, με τη μεταφορά μεγάλου χρηματικού ποσού στον τραπεζικό λογαριασμό του εισβολέα. Συμπεραίνουμε, λοιπόν, ότι με τις επιθέσεις αυτές ένας κακόβουλος χρήστης μπορεί να αποκτήσει πρόσβαση σε ιδιωτικά δεδομένα, εκμεταλλευόμενος τον ανθρώπινο παράγοντα σε έναν οργανισμό.

4.2 Απειλές απορρήτου μέσα στην υποδομή του Νέφους

Μόλις τα δεδομένα των χρηστών αποθηκευτούν στις υποδομές του υπολογιστικού νέφους, ο πάροχος έχει πρόσβαση σε αυτά τα δεδομένα και ελέγχει επίσης την

πρόσβαση τους από άλλες οντότητες, συμπεριλαμβανομένων άλλων χρηστών του cloud. Οι χρήστες με πρόσβαση στα κέντρα δεδομένων των παρόχων υπηρεσιών νέφους, είτε ως νόμιμοι πελάτες, είτε με παράνομη πρόσβαση σε άλλους λογαριασμούς πελατών, αποτελούν μια από τις σημαντικότερες ανησυχίες σχετικά με το απόρρητο των δεδομένων των χρηστών του νέφους. Αποτελούν, δηλαδή, τη βασικότερη εξωτερική απειλή, από την οποία κινδυνεύει το υπολογιστικό νέφος. Οι εξωτερικές απειλές αυτές περιέχουν όλες τις επιθέσεις κακόβουλων χρηστών, οι οποίοι δε σχετίζονται άμεσα με τον πάροχο του υπολογιστικού νέφους, και αποκτούν πρόσβαση στα ιδιωτικά δεδομένα των χρηστών του νέφους με παράνομο τρόπο. Επιπροσθέτως, ο τρόπος με τον οποίο είναι οργανωμένες οι υποδομές των παρόχων υπηρεσιών υπολογιστικού νέφους, δημιουργεί μη προφανείς απειλές και τρωτά σημεία, τα οποία οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν. Για παράδειγμα, όπως είδαμε, πολλοί πάροχοι cloud επιτρέπουν το «multitenancy», την καταχώρηση, δηλαδή, διαφορετικών πελατών σε εικονικά μηχανήματα με το ίδιο φυσικό υλικό. Επομένως, είναι κατανοητό ότι το εικονικό μηχάνημα ενός πελάτη θα μπορούσε να αντιστοιχεί στον ίδιο φυσικό διακομιστή με την εικονική μηχανή ενός κακόβουλου χρήστη. Αυτό, με την σειρά του, δημιουργεί την απειλή ότι ένας κακόβουλος χρήστης μπορεί να τοποθετείται στον ίδιο φυσικό διακομιστή τρίτων πελατών και, στη συνέχεια, να διεισδύσει στα εικονικά μηχανήματα αυτών, κυρίως μέσω κάποιων τρωτών σημείων της εικονικοποίησης, παραβιάζοντας το απόρρητό τους.

4.2.1 Τοποθέτηση (Placement Locality)

Πολλοί κακόβουλοι χρήστες προσπαθούν να νοικιάσουν μία εικονική μηχανή στον ίδιο φυσικό διακομιστή με αυτό του θύματός τους. Η επίτευξη της κοινή αυτής τοποθεσίας είναι ένα ζωτικής σημασίας στάδιο. Χωρίς αυτήν, οι κακόβουλοι χρήστες δε θα μπορούσαν να περάσουν στο δεύτερο βήμα της επίθεσης, που είναι η άντληση προσωπικών δεδομένων.

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους κρατούν κρυφούς τους αλγορίθμους που χρησιμοποιούν για την τοποθέτηση των πελατών τους σε εικονικά μηχανήματα, και πολύ λογικό, αφού θέλουν να εμποδίζουν κάθε είδους επιθέσεις στα ιδιωτικά δεδομένα των πελατών τους. Αυτό, όμως, δεν αναιρεί το γεγονός ότι οι κακόβουλοι χρήστες μπορούν να παρατηρήσουν και να συλλέξουν πληροφορίες για το πως λειτουργούν αυτοί οι αλγόριθμοι τοποθέτησης. Μία εμπειρική μελέτη

που έγινε το 2009 *(Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds)* [31] παρακολούθησε πολύ σχολαστικά τον τρόπο, με τον οποίο το Amazon EC2 διαχειριζόταν την τοποθέτηση των εικονικών μηχανημάτων των πελατών της. Ο σκοπός της ήταν να καταλάβει πώς ακριβώς λειτουργούσε η τοποθέτηση εικονικών μηχανημάτων στους διακομιστές, καθώς και πώς μπορούσε πετύχει «συγκατοίκηση» μεταξύ ενός κακόβουλου χρήση και ενός τρίτου πελάτη.

Στη μελέτη αυτή [31], χρησιμοποιήθηκαν εργαλεία διερεύνησης δικτύου (**network probing**), τόσο για τον προσδιορισμό δημόσιων υπηρεσιών που φιλοξενούνται στο EC2, όσο και για τον έλεγχο ότι υπάρχει κοινή τοποθεσία μεταξύ των δύο εικονικών μηχανημάτων. Η κύρια δουλειά των εργαλείων διερεύνησης δικτύου είναι να στέλνει «ερωτήματα» σε συσκευές δικτύου και να φέρνει πίσω τις «απαντήσεις».

Πιο συγκεκριμένα, εκτελέστηκαν *TCP connect probes*, σε μία προσπάθεια να ολοκληρώσουν ένα *three-way-handshake* μεταξύ της πηγής και του στόχου. Επίσης, εκτελέστηκαν *SYN traceroutes*, για να στείλουν επαναληπτικά πακέτα TCP SYN, με αυξημένο *χρόνο ζωής (TTL)*, έως ότου δεν υπήρχε απάντηση ότι τα πακέτα έφτασαν με επιτυχία. [31]

Στη συνέχεια, έγινε χαρτογράφηση των υπηρεσιών του EC2 (π.χ πακέτα υπηρεσιών, ζώνες διαθεσιμότητας), για να προσδιορίσει πού μπορεί να είναι η τοποθεσία κάποιων εν δυνάμει στόχων, ώστε να δημιουργηθούν οι παράμετροι που χρειάζονται, για να επιτευχθεί η κοινή τοποθεσία. Θεωρητικά η χαρτογράφηση επιτρέπει σε έναν κακόβουλο χρήστη να καταλάβει ποιες διευθύνσεις IP αντιστοιχούν σε ποιες παραμέτρους δημιουργίας εικονικού μηχανήματος, οπότε και μειώνεται δραματικά ο αριθμός των εικονικών μηχανημάτων που χρειάζεται να δημιουργηθούν, μέχρι να επιτευχθεί η συγκατοίκηση του κακόβουλου χρήστη και του στόχου του. Για να επιβεβαιωθεί αυτή η θεωρία, η μελέτη συνέλλεξε δεδομένα από διαφορετικά εικονικά μηχανήματα πολλών διαφορετικών λογαριασμών και κατέληξε στα παρακάτω [31]:

- ✓ Ένας μεμονωμένος λογαριασμός είναι δύσκολο να έχει δύο εικονικά μηχανήματα στον ίδιο φυσικό διακομιστή, οπότε, ξεκινώντας δύο εικονικά μηχανήματα ταυτόχρονα από έναν λογαριασμό, θα έχει ως αποτέλεσμα την τοποθέτησή τους σε διαφορετικά φυσικά μηχανήματα.

- ✓ Ο αριθμός των εικονικών μηχανημάτων που υποστηρίζει κάθε φυσικό μηχάνημα είναι περιορισμένος και μπορεί εύκολα να υπολογιστεί. Οπότε, αν ένα φυσικό μηχάνημα είναι πλήρες σε αριθμό εικονικών μηχανημάτων, ο κακόβουλος χρήστης δεν μπορεί να τοποθετηθεί σε αυτό.
- ✓ Παρατηρείται ισχυρή διαδοχική τοποθέτηση (Sequential placement locality). Αυτό σημαίνει ότι, όταν δύο εικονικά μηχανήματα εκτελούνται διαδοχικά, δηλαδή το πρώτο τερματίζει τη λειτουργία και αμέσως μετά ξεκινάει το δεύτερο, υπάρχουν υψηλές πιθανότητες να ανατεθούν στο ίδιο φυσικό μηχάνημα.
- ✓ Παρατηρείται, επίσης, ισχυρή παράλληλη τοποθέτηση (Parallel placement locality). Δηλαδή, όταν δύο εικονικά μηχανήματα, από διαφορετικούς, όμως, λογαριασμούς, εκτελούνται την ίδια χρονική στιγμή, τότε, συνήθως, ανατίθενται στο ίδιο φυσικό μηχάνημα.
- ✓ Υπάρχει συσχέτιση μεταξύ της πυκνότητας των εικονικών μηχανημάτων, δηλαδή του αριθμού των εικονικών μηχανημάτων, που έχουν εκχωρηθεί σε μία φυσική μηχανή, και της διαθεσιμότητάς του μηχανήματος αυτού για την εκχώρηση μίας νέας εικονικής μηχανής. Με άλλα λόγια, η τοποθέτηση εικονικών μηχανημάτων τείνει να γίνεται στα φυσικά μηχανήματα με τον μικρότερο αριθμό εικονικών. Αυτό συμβαίνει, από επιχειρησιακή άποψη, για να μπορούν οι πάροχοι υπηρεσιών υπολογιστικού νέφους να εξισορροπούν τον φόρτο εργασίας μεταξύ των φυσικών μηχανημάτων τους.

Χρησιμοποιώντας όλα τα παραπάνω χαρακτηριστικά τοποθέτησης εικονικών μηχανών, η έρευνα διαχώρισε δύο βασικές στρατηγικές, που μπορεί να ακολουθήσει ένας κακόβουλος χρήστης, για να πετύχει κοινή τοποθεσία με το θύμα του.

- ***Brute-forcing placement***

Στη συγκεκριμένη στρατηγική τοποθέτησης, λαμβάνει χώρα η πιο απλή και προφανής επίθεση, που μπορεί κάποιος να επιχειρήσει. Αυτό που γίνεται στην ουσία είναι ότι ο εν δυνάμει εισβολέας εκτελεί, για σχετικά μεγάλο χρονικό διάστημα, πολλά εικονικά μηχανήματα, με την ελπίδα ότι κάποιο από αυτά θα μπορέσει να τοποθετηθεί μαζί με κάποιο μηχάνημα του στόχου του. Είναι μία τόσο απλή και μη πολύπλοκη στρατηγική, που, όμως, μπορεί να επιφέρει σχετικά καλά ποσοστά επιτυχίας για υψηλό αριθμό στόχων.

- ***Abusing placement locality***

Η δεύτερη είναι μία πιο εκλεπτυσμένη στρατηγική, στην οποία ο εισβολέας στοχεύει μόνο στα εικονικά μηχανήματα, τα οποία εκτελέστηκαν πρόσφατα. Στη συγκεκριμένη στρατηγική τοποθέτησης, ο εισβολέας εκμεταλλεύεται τη δυναμική φύση του υπολογιστικού νέφους (δηλαδή ότι οι διακομιστές ξεκινούν την λειτουργία τους, μόνο όταν χρειάζονται) και με τη βοήθεια των εργαλείων διερεύνησης δικτύου και της παράλληλης τοποθέτησης, όπως είδαμε πιο πάνω, μπορεί να εκκινήσει εικονικά μηχανήματα, σχετικά σύντομα από την έναρξη του στόχου του. Για παράδειγμα, ένας εισβολέας μπορεί να παρακολουθεί την κατάσταση ενός διακομιστή (π.χ. μέσω ανίχνευσης δικτύου) και να περιμένει, μέχρι να εξαφανιστεί η παρουσία ενός εικονικού μηχανήματος. Στη συνέχεια, αν επανεμφανιστεί μία νέα παρουσία, έχει την δυνατότητα να προβεί σε παράλληλη εκτέλεση πολλών εικονικών μηχανών από διαφορετικούς λογαριασμούς, με αποτέλεσμα να υπάρχει μεγάλη πιθανότητα ο εισβολέας να τοποθετηθεί μαζί με τον στόχο του.

4.2.2 Έλεγχοι Συγκατοίκησης (Co-location checks).

Αφού, όπως είδαμε πιο πάνω, ο κακόβουλος χρήστης έχει προσπαθήσει με κάποιες στρατηγικές να εισχωρήσει στο ίδιο φυσικό μηχάνημα με αυτό του στόχου του, στη συνέχεια μπορεί να χρησιμοποιήσει κάποιες τεχνικές, για να σιγουρευτεί ότι η συγκατοίκηση αυτή έχει επιτευχθεί. Δεδομένου ότι η κατάσταση της συγκατοίκησης δεν αναφέρεται απευθείας από τον πάροχο cloud, αυτές οι τεχνικές ανίχνευσης αναφέρονται, συνήθως, ως τεχνικές πλευρικών καναλιών (**sidechannel based techniques**), οι οποίες μπορούν να ταξινομηθούν περαιτέρω σε δύο κατηγορίες: Λογικά πλευρικά κανάλια (**logical side-channels**) και πλευρικά κανάλια απόδοσης (**performance side-channels**) [32].

- Λογικά πλευρικά κανάλια (**Logical side-channels**)

Τα λογικά πλευρικά κανάλια επιτρέπουν τη διαρροή πληροφοριών μέσω των λογικών πόρων ενός συστήματος (π.χ. διευθύνσεις IP) ,τα οποία μπορούν να παρατηρηθούν μέσω προγραμμάτων λογισμικού. Στην περίπτωση του Amazon EC2, σε κάθε εικονικό μηχάνημα ανατίθενται δύο διευθύνσεις IP, μια δημόσια

διεύθυνση IP, για επικοινωνία μέσω Διαδικτύου, και μια ιδιωτική ή εσωτερική διεύθυνση IP για επικοινωνίες μεταξύ κέντρων δεδομένων. Η υποδομή του υπολογιστικού νέφους του Amazon EC2 μπορεί να επιτρέψει την αντιστοίχιση των δημόσιων διευθύνσεων IP σε αυτές αντίστοιχων εσωτερικών. Αυτή η αντιστοίχιση μπορεί να αποκαλύψει την τοπολογία του εσωτερικού δικτύου κέντρων δεδομένων, το οποίο, με τη σειρά του, μπορεί να επιτρέψει σε έναν κακόβουλο χρήστη να χαρτογραφήσει ολόκληρη τη δημόσια υποδομή cloud του παρόχου και να προσδιορίσει, για παράδειγμα, τη ζώνη διαθεσιμότητας και τον τύπο εικονικού μηχανήματος του θύματος. Επιπλέον, στην περίπτωση του Amazon EC2, τα εικονικά μηχανήματα, που συγκατοικούν σε έναν φυσικό διακομιστή τείνουν να έχουν κοντινές εσωτερικές διευθύνσεις IP.

- Πλευρικά κανάλια απόδοσης (**Performance side-channels**)

Πλαϊνά κανάλια απόδοσης δημιουργούνται, όταν ένας κακόβουλος χρήστης μπορεί να παρατηρήσει την απόδοση (performance) των πόρων του φυσικού μηχανήματος και τις αυξομειώσεις της απόδοσης, λόγω των εργασιών που εκτελούνται στο συγκεκριμένο μηχάνημα. Τέτοιες αυξομειώσεις μπορούν να χρησιμοποιηθούν ως δείκτης συγκατοίκησης δύο εικονικών μηχανημάτων. Οι hypervisors, συχνά, μεταδίδουν πολύ γρηγορότερα πληροφορίες μεταξύ εικονικών μηχανημάτων που βρίσκονται στον ίδιο κεντρικό υπολογιστή, παρέχοντας ανιχνεύσιμα μικρότερους χρόνους επικοινωνίας από ό,τι μεταξύ εικονικών μηχανημάτων που βρίσκονται σε διαφορετικούς φυσικούς διακομιστές. Επίσης, ένας κακόβουλος χρήστης μπορεί να είναι σε θέση να εκτιμήσει τον φόρτο εργασίας της κεντρικής μονάδας επεξεργασίας του κεντρικού διακομιστή και, ως εκ τούτου, να συμπεράνει αν υπάρχουν συνυπάρχοντα εικονικά μηχανήματα.

4.3 Άντληση πληροφοριών

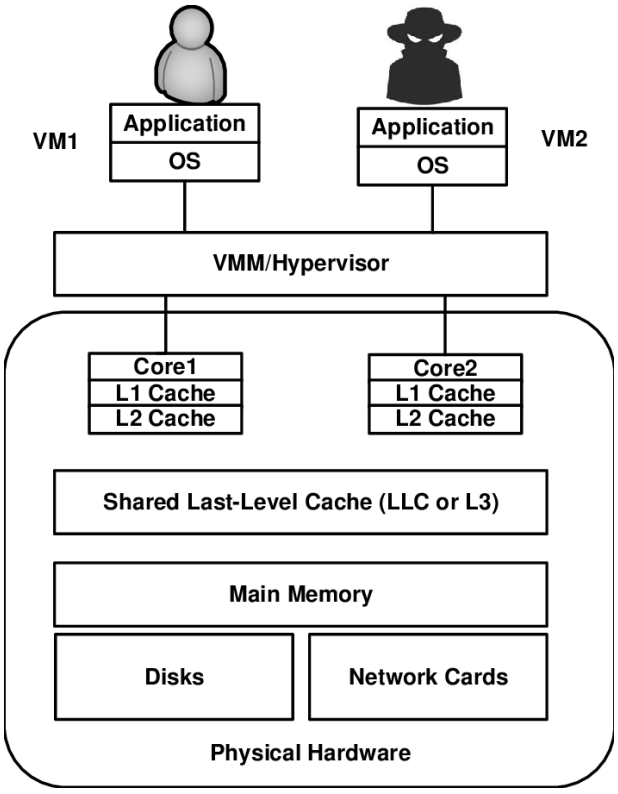
Προηγουμένως, είδαμε ότι ένας εισβολέας έχει την δυνατότητα να τοποθετηθεί στο ίδιο φυσικό μηχάνημα που βρίσκεται το εικονικό μηχάνημα του θύματός του, έτσι ώστε να μοιράζονται τους ίδιους πόρους. Μόλις το καταφέρει αυτό, μπορεί, μέσω κάποιων κακόβουλων ενεργειών, να αποκτήσει πρόσβαση στα εικονικά

μηχανήματα, με τα οποία συγκατοικεί. Κάποια παραδείγματα κακόβουλων ενεργειών είναι τα Cross-VM attacks και hypervisor attacks

4.3.1 Επιθέσεις Cross-VM

Οι επιθέσεις Cross-VM μπορούν να χρησιμοποιηθούν για την ανάκτηση εμπιστευτικών πληροφοριών (π.χ. κρυπτογραφικών κλειδιών) από γειτονικά εικονικά μηχανήματα. Ο πιο συχνός τρόπος, για να πραγματοποιηθεί μία επίθεση Cross-VM, είναι τα πλευρικά κανάλια (**Side Channel Attacks**) [33].
Όταν υπάρχουν κοινόχρηστοι πόροι υλικού, η επίθεση πλευρικού καναλιού εκμεταλλεύεται τις πληροφορίες που λαμβάνονται από την κοινή χρήση του υλικού αυτού, για παράδειγμα, της προσωρινής μνήμης της κεντρικής μονάδας επεξεργασίας (CPU cache). Μέσω της επίθεσης πλευρικού καναλιού, ένας εισβολέας που μοιράζεται την ίδια προσωρινή μνήμη με το θύμα μπορεί να παρακολουθεί τη συμπεριφορά αυτής της μνήμης και να βγάλει κάποια συμπεράσματα. Για να το καταλάβουμε αυτό, πρέπει, πρώτα, να κατανοήσουμε την αρχιτεκτονική της προσωρινής μνήμης.
Με απλά λόγια, το CPU cache είναι ένας πολύ γρήγορος τύπος μνήμης, η οποία βρίσκεται πολύ κοντά σε έναν πυρήνα τις κεντρικής μονάδας επεξεργασίας (CPU) ενός υπολογιστή. Στην ουσία, το CPU cache χρησιμοποιείται για τη μείωση του χρόνου μεταφοράς δεδομένων από την κύρια μνήμη (μνήμη RAM) στην κεντρική μονάδα επεξεργασίας. Αυτό το καταφέρνει, αποθηκεύοντας αντίγραφα των δεδομένων που χρησιμοποιούνται πιο συχνά από την κύρια μνήμη.

Οι περισσότεροι σύγχρονοι επεξεργαστές έχουν πολλαπλά επίπεδα προσωρινής μνήμης (L1, L2, L3, κ.λπ.). Σε επεξεργαστές με πολλαπλούς πυρήνες και με τρία επίπεδα προσωρινής μνήμης, κάθε πυρήνας επεξεργαστή έχει το δικό του ξεχωριστό L1, ενώ τα L2 και L3 cache μπορεί να είναι κοινόχρηστα σε όλους τους πυρήνες του επεξεργαστή. Σε ένα τυπικό σενάριο, όταν ο επεξεργαστής χρειάζεται δεδομένα, ελέγχει τις προσωρινές μνήμες L1, L2 και L3 αντίστοιχα [33]. Εάν τα ζητούμενα δεδομένα είναι παρόντα σε οποιοδήποτε επίπεδο, τότε διαβιβάζονται κατευθείαν από το αντίστοιχο επίπεδο στον επεξεργαστή. Αυτή η διαδικασία ονομάζεται cash hit. Αντίθετα, εάν τα δεδομένα δεν είναι διαθέσιμα σε κανένα



Εικόνα 14: *Επίθεση Πλευρικού Καναλιού Μέσω της Κοινής Προσωρινής Μνήμης*
Πηγή: "A Layered Graphical Model for Cloud Forensic Mission Attack Impact Analysis: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers". https://www.researchgate.net/figure/Cross-VM-side-channel-attack-using-a-shared-last-level-cache_fig2_327314423

επίπεδο προσωρινής μνήμης, τότε έχουμε cache miss και ο επεξεργαστής λαμβάνει δεδομένα από τη μνήμη RAM και το τοποθετεί στην προσωρινή μνήμη, έτσι ώστε να είναι έτοιμα για την επόμενη φορά. Ο μικρότερος όγκος δεδομένων, που μπορούν να διαβαστούν από την κύρια μνήμη στην προσωρινή μνήμη, ονομάζεται

γραμμή cache (cache line). Κάθε φορά που συμβαίνει ένα cache miss, αναγκάζει το συγκεκριμένο cache line να μεταφερθεί σε ένα ψηλότερο επίπεδο προσωρινής μνήμης.

Σε μία επίθεση πλευρικών καναλιών, ένας κακόβουλος χρήστης μπορεί μετρήσει τη χρήση της προσωρινής μνήμης του επεξεργαστή, δεδομένου ότι η προσωρινή μνήμη είναι κοινόχρηστη με το θύμα του. Αυτή η μέτρηση μπορεί να χρησιμοποιηθεί, για να εκτιμηθεί ο φόρτος εργασίας του μηχανήματος. Ένας υψηλός φόρτος εργασίας, για παράδειγμα ,υποδηλώνει ότι υπάρχει δραστηριότητα στο εικονικό μηχάνημα του συγκατοίκου – θύματός του. Για να λάβει χώρα αυτή η μέτρηση, μπορούν να χρησιμοποιηθούν κυρίως δύο τεχνικές, η τεχνική *Prime + Probe* και η τεχνική *Flush + Reload* [33].

Η τεχνική *Prime + Probe* χρησιμοποιείται από έναν εισβολέα, για να μάθει πως συμπεριφέρεται η κοινή προσωρινή μνήμη, και, πιο συγκεκριμένα, σε ποιο μέρος της έχει πρόσβαση το θύμα του. Προκειμένου να παρατηρήσει τη χρήση της προσωρινής μνήμης που χρησιμοποιεί το θύμα του, ο εισβολέας εκτελεί παράλληλα μια κατασκοπευτική υπηρεσία (spy process), για να παρατηρήσει την κατάσταση της προσωρινής μνήμης. Στην ουσία, στην τεχνική *Prime + Probe* ο εισβολέας ακολουθεί τρία βήματα:

1) Prime: Ο εισβολέας γεμίζει με δεδομένα την CPU cache.
2) Στη συνέχεια, περιμένει κάποιο χρονικό διάστημα το θύμα να εκτελέσει κάποια εργασία, έτσι ώστε να χρησιμοποιήσει την προσωρινή μνήμη.
3) Probe: Τέλος, ο εισβολέας διαβάζει τα δεδομένα με τα οποία είχε γεμίσει την προσωρινή μνήμη. Έτσι, αν παρατηρήσει ότι κάποιο μέρος των δεδομένων του αργεί να διαβαστεί (high latency), αυτό σημαίνει ότι δεν υπάρχει πλέον στην προσωρινή μνήμη (έχει δηλαδή αντικατασταθεί από τα δεδομένα του θύματος)

Σε μια επίθεση πλευρικού καναλιού με την τεχνική *Flush + Reload*, ένας εισβολέας εκτελεί μια κατασκοπευτική διεργασία, η οποία παρακολουθεί τις κοινόχρηστες σελίδες της προσωρινής μνήμης. Με αυτόν τον τρόπο, ο εισβολέας είναι σε θέση να καταλάβει σε ποιες γραμμές προσωρινής μνήμης έχει πρόσβαση

το θύμα του. Από τα παραπάνω, ο εισβολέας μπορεί να εξάγει πληροφορίες από τα δεδομένα που επεξεργάζεται το θύμα. Στην τεχνική *Flush + Reload* ακολουθούνται τα εξής τρία βήματα:

1) Flush: Ο εισβολέας αδειάζει τις κοινόχρηστες γραμμές της προσωρινής μνήμης που έχει με το θύμα.
2) Στη συνέχεια, περιμένει κάποιο χρονικό διάστημα, έτσι ώστε το θύμα να φορτώσει πάλι δεδομένα στην προσωρινή μνήμη.
3) Reload: Τέλος, ο εισβολέας φορτώνει ξανά τα δεδομένα και, αν παρατηρήσει ότι τα δεδομένα του διαβάζονται γρήγορα (low latency), τότε καταλαβαίνει ότι το θύμα του χρησιμοποίησε τις συγκεκριμένες γραμμές.

Τύποι επιθέσεων στα πλευρικά κανάλια της προσωρινής μνήμης (Cache Side Channel Attacks):

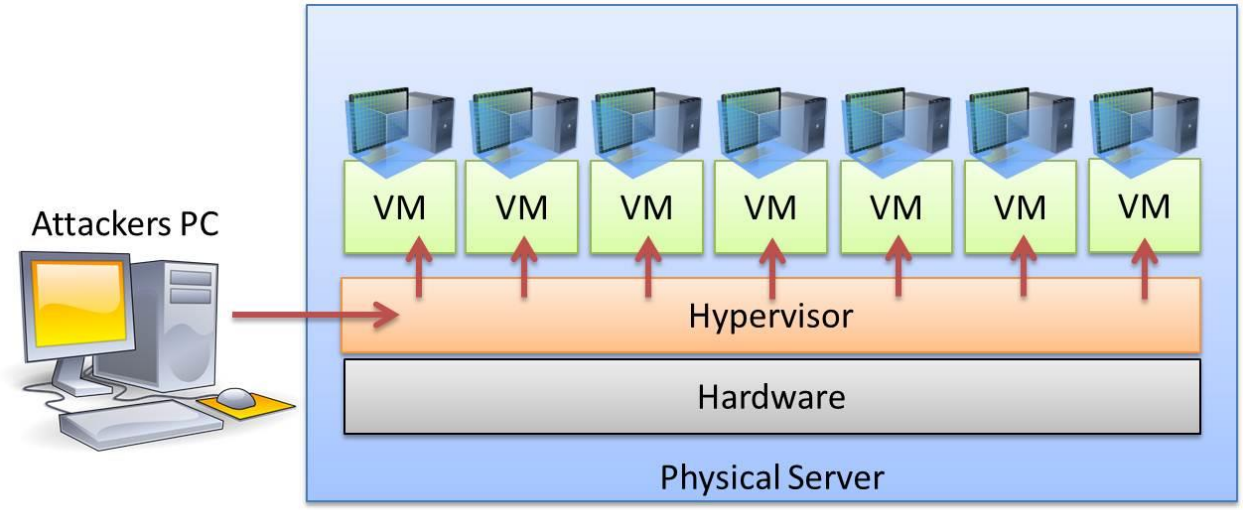
Επιθέσεις με γνώμονα τον χρόνο (Time driven attacks)
Σε αυτόν τον τύπο επίθεσης, ένας εισβολέας εκμεταλλεύεται τη συσχέτιση μεταξύ της κρυπτογραφικής λειτουργίας και των cache misses ενός θύματος. Δηλαδή, ο κακόβουλος χρήστης μετράει τον χρόνο που απαιτείται, για να ολοκληρωθεί μια κρυπτογραφική διαδικασία κατά την πρόσβαση στην κοινή προσωρινή μνήμη. Αυτό είναι εφικτό, επειδή το χρονικό διάστημα που χρειάζεται, για να αποκτήσει πρόσβαση στη μνήμη, εξαρτάται από την κατάσταση του cache. Έτσι, ο κακόβουλος χρήστης μπορεί να συγκρίνει τους διαφορετικούς χρόνους εκτέλεσης των διαδικασιών με τις αντίστοιχες εντολές που δίνει το θύμα και να αναζητά συγκεκριμένα μοτίβα. Η διαφορά στους χρονισμούς μπορεί να χρησιμοποιηθεί ως μόχλευση για την εξαγωγή πληροφοριών σχετικά με τα κλειδιά κρυπτογράφησης.

Επιθέσεις με γνώμονα την πρόσβαση (Access Driven attacks)
Αυτή η επίθεση παρέχει σε έναν αντίπαλο μια πλατφόρμα, για να εκτελέσει μια κακόβουλη διαδικασία, παράλληλα με την κρυπτογραφική διαδικασία του θύματος, προκειμένου να αντλήσει μια εικόνα της συμπεριφοράς της κρυφής μνήμης του θύματος. Ο εισβολέας μαθαίνει σε ποια σύνολα προσωρινής μνήμης

έχει προσπελαστεί η κρυπτογραφική λειτουργία του θύματος, εκδιώκοντας τις σελίδες μνήμης της προσωρινής μνήμης του θύματος. Αυτό αναγκάζει το θύμα να παρουσιάσει ένα cache miss και, έπειτα, ο εισβολέας μπορεί να παρατηρήσει τη συμπεριφορά της κρυφής μνήμης, με τη γνώση ότι η λειτουργία που εκτελείται είναι αυτή που υποκινεί το θύμα.

4.3.2 Hypervisor attacks

Μία από τις κύριες τεχνολογίες που επιτρέπουν την ανάπτυξη του υπολογιστικού νέφους είναι, όπως είδαμε, η εικονικοποίηση. Ένα βασικό μέρος του εικονικοποιημένου περιβάλλοντος είναι το hypervisor, το οποίο είναι υπεύθυνο για τη διαχείριση των φυσικών πόρων των φυσικών μηχανημάτων (CPU, μνήμη και αποθήκευση). Αυτά τα φυσικά μηχανήματα μπορούν να ομαδοποιηθούν, για να σχηματίσουν μια μεγάλη ενιαία εικονική υποδομή, επεκτείνοντας την λειτουργικότητά τους, με απώτερο σκοπό την εξισορρόπηση του φόρτου εργασίας και τη μετακίνηση εικονικών μηχανημάτων μεταξύ των φυσικών διακομιστών, χωρίς καμία διακοπή λειτουργίας.
Οι επιθέσεις στα hypervisors, γνωστές και ως hyperjacking, είναι η εκμετάλλευση κάποιον τρωτών σημείων, που μπορεί να βρεθούν στα προγράμματα αυτά [34]. Στην ουσία, αν κάποιος κακόβουλος χρήστης αποκτήσει πρόσβαση στο hypervisor, τότε όλα τα εικονικά μηχανήματα, τα οποία διαχειρίζεται, είναι εκτεθειμένα στον εισβολέα. Η επίθεση αυτή επιτυγχάνεται με την εγκατάσταση ενός κακόβουλου λογισμικού, το οποίο μπορεί να διαχειριστεί ολόκληρο το σύστημα του φυσικού διακομιστή [35]. Το λειτουργικό σύστημα ,συνήθως, δε γνωρίζει ότι το μηχάνημα έχει παραβιαστεί, διότι το κακόβουλο αυτό πρόγραμμα λειτουργεί κρυφά, κάτι το οποίο καθιστά πολύ δύσκολη την ανίχνευσή του. Επιπροσθέτως, εκτός από τα εικονικά μηχανήματα του hypervisor που δέχεται επίθεση, μπορεί να τεθεί σε κίνδυνο και το απόρρητο άλλων εικονικών μηχανημάτων, εάν βέβαια διατηρούν συνδέσεις δικτύου με το παραβιασμένο. Παρακάτω, θα αναλύσουμε κάποιους τρόπους, με τους οποίους η κακόβουλοι χρήστες μπορούν να πραγματοποιήσουν hypervisor attacks.



Εικόνα 15: *Επίθεση Στο Hypervisor*
Πηγή: Created by Anthony 27 February 2015, This file is made available under the Creative Commons CC0 1.0 Universal Public Domain Dedication, https://en.wikipedia.org/wiki/Hyperjacking#/media/File:Hyperjacking.jpg

❖ *VENOM (Virtualized Environment Neglected Operations Manipulation)*

Το VENOM είναι ένα ελάττωμα ασφάλειας εικονικών υπολογιστών, που αποκαλύφθηκε δημόσια το 2015 από τον Jason Geffner, ερευνητή της CrowdStrike (εταιρεία τεχνολογίας cybersecurity) [36]. Πιο συγκεκριμένα, το τρωτό σημείο ασφαλείας βρισκόταν στον κώδικα της μονάδας δισκέτας που χρησιμοποιείται από πολλές πλατφόρμες εικονικοποίησης υπολογιστή. Αυτή η ευπάθεια μπορούσε να επιτρέψει σε έναν εισβολέα να ξεφύγει από τα όρια ενός χρήστη εικονικής μηχανής και να αποκτήσει πρόσβαση σε εκτέλεση κώδικα στον κεντρικό υπολογιστή. Στη συνέχεια, ο εισβολέας θα μπορούσε να αποκτήσει πρόσβαση στο σύστημα του κεντρικού υπολογιστή και, επομένως, σε όλες τις άλλες εικονικές μηχανές που εκτελούνται από αυτόν, ανοίγοντας, έτσι, την πρόσβαση και στο τοπικό δίκτυο του κεντρικού υπολογιστή, οπότε και στα υπόλοιπα εικονικά μηχανήματα.

❖ *Virtual Hard Disk (VHD) Exploit*

Το VHD είναι ένα αρχείο εικόνας, που χρησιμοποιείται από το hypervisor, το οποίο περιέχει τη δομή αρχείων ενός εικονικού σκληρού δίσκου. Η δομή του μπορεί να αναπαράγει οποιοδήποτε μέρος ενός φυσικού σκληρού δίσκου. Το αρχείο αυτό μπορεί να περιέχει διαμερίσματα (partitions), στα οποία είναι αποθηκευμένα αρχεία, αλλά και διαμερίσματα με δυνατότητα εκκίνησης

λογισμικού (bootable images). Οι εικόνες VHD επιτρέπουν σε πολλά λειτουργικά συστήματα να μοιράζονται το ίδιο φυσικό μηχάνημα και έχουν εισάγει χαρακτηριστικά, όπως στιγμιότυπα (snapshots) [37] και μετακινήσεις επισκεπτών (guest migrations). Ένα στιγμιότυπό είναι ένα πλήρες αντίγραφο, μόνο για ανάγνωση, ενός εικονικού σκληρού δίσκου (VHD). Μπορεί να χρησιμοποιηθεί ως αντίγραφο ασφαλείας για την αντιμετώπιση προβλημάτων (troubleshooting) μίας εικονικής μηχανής [35]. Η μετακίνηση επισκεπτών είναι μία λειτουργία, που επιτρέπει τη μετακίνηση όλων των δεδομένων ενός εικονικού μηχανήματος, δηλαδή του εικονικού σκληρού δίσκου του, μεταξύ φυσικών διακομιστών. Οι παραπάνω δυνατότητες έχουν κάνει το αρχείο εικόνας VHD πολύ δημοφιλές, ωστόσο έχουν φέρει στο φως και τρωτά σημεία του. Στην ουσία, όποιος έχει πρόσβαση στο hypervisor, έχει τη δυνατότητα να κλέψει ένα αρχείο εικονικού σκληρού δίσκου VHD και, επομένως, ένα ολόκληρο εικονικό μηχάνημα. Αυτό θα μπορούσε να γίνει, χωρίς ο ιδιοκτήτης του εικονικού μηχανήματος να γνωρίζει ότι τα προσωπικά του δεδομένα έχουν παραβιαστεί.

- *Virtual Machine Migration Exploit*

Με την αυξανόμενη ζήτηση για μεγαλύτερη διαθεσιμότητα υπηρεσιών, η δυνατότητα μετεγκατάστασης μιας εικονικής μηχανής από έναν φυσικό διακομιστή σε έναν άλλον έχει τεράστια οφέλη. Μπορεί να βοηθήσει με τη μεταφορά μηχανών από ένα hypervisor για τη διευκόλυνση της συντήρησης σε ένα φυσικό μηχάνημα. Ένα άλλο πλεονέκτημα της μετακίνησης εικονικών μηχανών, είναι, όταν ένα τοπικό κέντρο δεδομένων αντιμετωπίζει ένα σοβαρό πρόβλημα ή μία τοπική καταστροφή. Σε αυτό το σενάριο, όλα τα VM θα μπορούσαν να μετεγκατασταθούν σε ένα δεύτερο κέντρο δεδομένων, εκτός αυτής της συγκεκριμένης πληγείσας περιοχής και μακριά από το πιθανό πρόβλημα. Στην περίπτωση μίας μετεγκατάστασης, ένας κακόβουλος χρήστης θα μπορούσε να χρησιμοποιήσει μία man-in-the-middle επίθεση, χρησιμοποιώντας εργαλεία, όπως το wireshark η το XEnsploit [37] [38] [39], στην οποία θα είναι σε θέση να «ακούσει» και να κλέψει τα δεδομένα, καθώς περνούν μεταξύ των δύο τελικών σημείων. Επιπροσθέτως, εάν ένα εικονικό μηχάνημα μετακινηθεί σε ένα διαφορετικό μέρος του δικτύου, οι πολιτικές προστασίας του θα πρέπει να εφαρμοστούν και σε εκείνη την περιοχή που μεταφέρθηκε (π.χ τείχος προστασίας), αλλιώς θα μείνει ευάλωτο [39].

5. Παραβιάσεις ιδιωτικότητας από παρόχους cloud

Στο προηγούμενο κεφάλαιο, αναλύσαμε πιθανές απειλές, που προέρχονται από χρήστες . Σε αυτό το κεφάλαιο, θα ασχοληθούμε μ' ένα ευρύτερο φάσμα απειλών , όπως αυτό των «αναξιόπιστων» παρόχων cloud ή μερών των παρόχων.

5.1 Πολιτικές παρόχων νεφών που παραβιάζουν την ιδιωτικότητα

Οι διάφοροι τρόποι, με τους οποίους μπορεί ένας πάροχος να αποκλίνει εμπιστοσύνης για τον κάθε χρήστη, παρουσιάζονται παρακάτω :

5.1.1 Αντίγραφα δεδομένων (Data copies)

Οι πάροχοι, συνήθως, ασκούν τεχνικές ανακατεύθυνσης, που απαιτούν την ανάπτυξη αντιγράφων εικονικών μηχανημάτων (δηλαδή, σε περίπτωση αποτυχίας λειτουργίας ενός εικονικού μηχανήματος, ο πελάτης μεταβαίνει στο αντίγραφο του εικονικού μηχανήματος). Ως εκ τούτου, πολλά αντίγραφα δεδομένων πελατών-χρηστών μπορούν να διατηρηθούν στην υποδομή του νέφους , γεγονός που συνεπάγεται τους ακόλουθους κινδύνους :

- Αντίγραφα δεδομένων ενδέχεται να διατηρούνται στο νέφος, ακόμα και μετά τον τερματισμό μίας υπηρεσίας cloud.
- Με τα πολλαπλά αντίγραφα ασφαλείας παραμονεύει ο κίνδυνος της υποκλοπής δεδομένων από τους διάφορους κακόβουλους χρήστες, που καραδοκούν για μία λάθος κίνηση.

Το τελευταίο είναι πιο κρίσιμο για τα εικονικά μηχανήματα που βρίσκονται σε αδρανή κατάσταση, τα οποία ενδέχεται να μην λαμβάνουν πρόσφατες ενημερώσεις ασφαλείας και, ως αποτέλεσμα, να είναι περισσότερο ευπαθή σε κακόβουλους χρήστες [40].

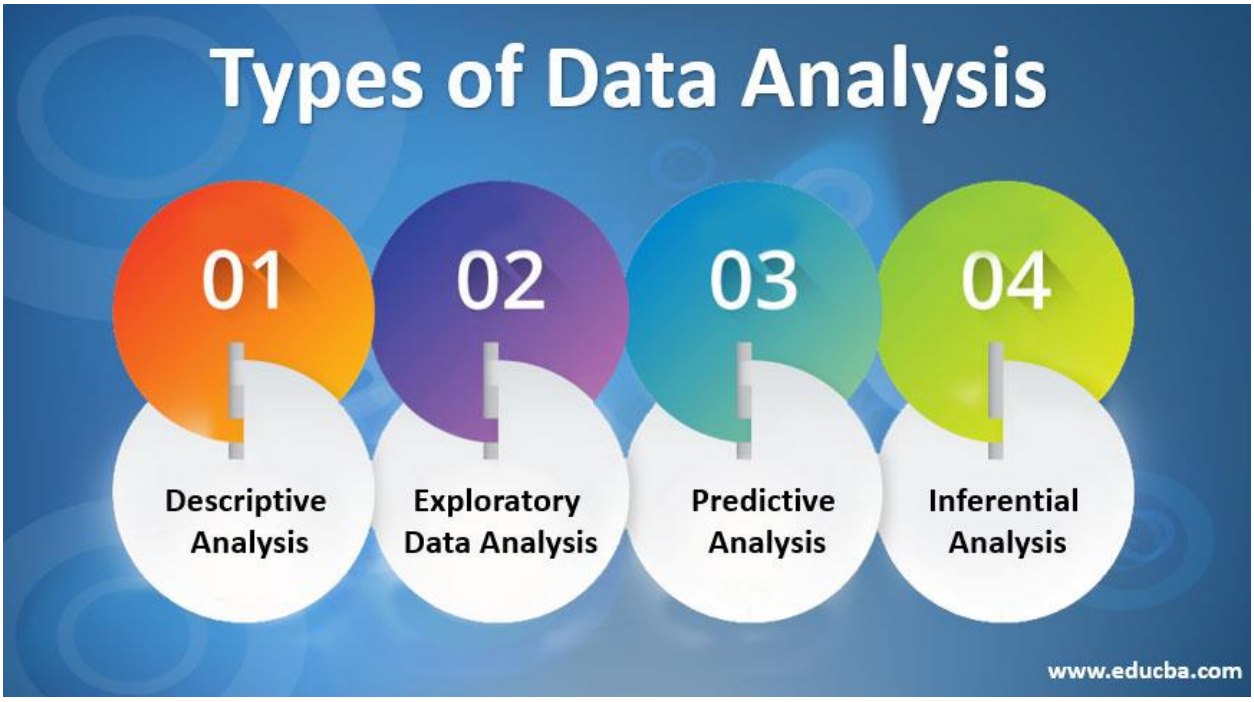
5.1.2 Καταγραφή δραστηριότητας (Activity logging)

Τα αρχεία καταγραφής δραστηριοτήτων των χρηστών νέφους μπορούν να «μαρτυρήσουν» όλες τις ενέργειες που πραγματοποίησε ένας χρήστης κατά την περίοδο χρήσης μίας πλατφόρμας cloud. Αυτή η καταγραφή δραστηριοτήτων φυλάσσεται μέσα στην υποδομή του παρόχου cloud, χωρίς αυτό να σημαίνει ότι υπάρχει η συγκατάθεση του χρήστη για τη διατήρηση τέτοιων στοιχείων. Καταγραφές τέτοιου είδους μπορεί να είναι η τοποθεσία χρήστη, η διεύθυνση IP, και, γενικότερα, ένα ηλεκτρονικό ημερολόγιο (με καταγεγραμμένη ώρα – ημερομηνία) του κάθε «click» και «keystroke», που κάνει ο χρήστης [41]. Πολλές φορές, έμπειροι εισβολείς επιτίθενται πρώτα στο σύστημα καταγραφής [42] [43]. Αξίζει να αναφερθεί ότι η καταγραφή δραστηριοτήτων μπορεί να επιφέρει σημαντικά ευρήματα σε έρευνες εγκληματολογικού περιεχομένου, ωστόσο οι εισβολείς χρησιμοποιούν ιστοσελίδες ηλεκτρονικού ψαρέματος, προκειμένου να μεταποιήσουν ή και να διαγράψουν τα αρχεία καταγραφής τους.

5.1.3 Ανάλυση δεδομένων (Data Analysis)

Η ανάλυση δεδομένων είναι μία διαδικασία «επιθεώρησης», καθαρισμού, μετατροπής και μοντελοποίησης δεδομένων, με στόχο την ανεύρεση χρήσιμων πληροφοριών και την εξαγωγή συμπερασμάτων, αναφορικά με τα δεδομένα που έχουν συλλεχθεί κατά τη διαδικασία χρήσης cloud από έναν χρήστη. Η συγκεκριμένη διαδικασία έχει πολλές πτυχές και προσεγγίσεις, που εμφανίζονται με διάφορες ονομασίες, και χρησιμοποιείται σε διάφορους τομείς επιχειρήσεων και επιστημών, καθώς παίζει πολύ σημαντικό ρόλο στη λήψη αποφάσεων, προκειμένου η λειτουργία, αφενός, των επιχειρήσεων και, αφετέρου, των επιστημονικών τομέων να είναι περισσότερο αποτελεσματική. Με απλά λόγια, η ανάλυση δεδομένων είναι μία διαδικασία συλλογής και οργάνωσης δεδομένων, με σκοπό την διεξαγωγή χρήσιμων συμπερασμάτων από αυτήν [44].

Για γίνει περισσότερο κατανοητό πώς και γιατί λειτουργεί η ανάλυση δεδομένων, ακολουθούν τέσσερις τύποι ανάλυσης δεδομένων :



Εικόνα 16: *Τύποι Ανάλυσης Δεδομένων*
Πηγή: https://www.educba.com/types-of-data-analysis/

- ✓ **Περιγραφική ανάλυση** : Η ανάλυση περιγραφικών δεδομένων εξετάζει παρελθοντικά δεδομένα και εξηγεί τι συνέβη. Αυτό χρησιμοποιείται συχνά κατά την παρακολούθηση βασικών δεικτών απόδοσης (KPI) εσόδων, δυνητικών πωλήσεων κ.ά.
- ✓ **Διαγνωστική ανάλυση** : Αυτού του είδους η ανάλυση έχει στόχο να ερευνήσει το «γιατί» συνέβη κάτι. Μόλις τελειώσει η περιγραφική ανάλυση και δώσει ένα αποτέλεσμα , θετικό ή αρνητικό, αναλαμβάνει δράση η διαγνωστική ανάλυση, για να αναζητήσει τον λόγο που το αποτέλεσμα κατέληξε να έχει αυτήν την έκβαση. Μία τέτοιου είδους ανάλυση βοηθά τα τμήματα μάρκετινγκ να διατηρήσουν ή να τροποποιήσουν τις διάφορες πολιτικές τους.
- ✓ **Ανάλυση πρόβλεψης** : Η ανάλυση πρόβλεψης προγνωστικών δεδομένων προβλέπει τι είναι πιθανό να συμβεί στο μέλλον. Σ' αυτόν τον τύπο έρευνας, οι τάσεις προέρχονται από δεδομένα, κυρίως, προηγούμενων χρόνων και χρησιμοποιούνται για τη διαμόρφωση απόψεων για το μέλλον. Συνήθως, χρησιμοποιείται για προβλέψεις ανάπτυξης και εσόδων και εφαρμόζεται σε ζητήματα εκτίμησης κινδύνου.

- ✓ **Κανονιστική ανάλυση** : Η εν λόγω ανάλυση συνδυάζει τις πληροφορίες, που βρέθηκαν από τα 3 προηγούμενα στάδια ανάλυσης, και βασικό σκοπό έχει να διαμορφώσει ένα σχέδιο δράσης για τον οργανισμό, προκειμένου να αντιμετωπίσει ένα ζήτημα ή να λάβει μία απόφαση.

Επί του θέματος, ορισμένοι πάροχοι νεφών καταχρώνται δεδομένα πελατών στο cloud, με απώτερο σκοπό την αποκόμιση επιχειρηματικών εσόδων, τόσο για τους ίδιους, όσο και για άλλες νομικές οντότητες. Αναλυτικότερα, οι πάροχοι μπορούν να ανακτούν πληροφορίες πελατών τους και, μέσω της ανωτέρω ανάλυσης τους, να τις διοχετεύουν στα τμήματά τους ή να τις μεταπωλούν σε άλλες επιχειρήσεις, συνήθως για λόγους διαφημιστικούς [40].

5.2 Τρόποι επίτευξης παραβίασης ιδιωτικότητας από παρόχους

Τα ανωτέρω, μπορούν να αξιοποιηθούν μεμονωμένα αλλά και συνδυαστικά. Οι τρόποι με τους οποίους μπορεί να πραγματοποιηθεί μία τέτοια ενέργεια είναι κατόπιν δύο περιπτώσεων :

- **Αναξιόπιστοι πάροχοι (untrusted providers)**

Σε αυτήν την περίπτωση, ο πάροχος θεωρείται αναξιόπιστος, διότι δίνει την ευκαιρία στον οποιοδήποτε κακόβουλο εξωτερικό χρήστη να εισέλθει στα συστήματα του (οι τρόποι για το πώς μπορεί να εισέλθει ένας κακόβουλος εξωτερικός χρήστης στα διάφορα cloud επεξηγούνται αναλυτικά στο κεφάλαιο 4) και να υποκλέψει την οποιαδήποτε πληροφορία, μέσω των αντιγράφων ασφαλείας, της καταγραφής δραστηριοτήτων και της ανάλυσης δεδομένων του χρήστη, καθιστώντας τον ίδιο ανεπαρκή ως προς τη διασφάλιση προστασίας δεδομένων.

- **Ημί-αναξιόπιστοι πάροχοι (semi-untrusted providers)**

Μία άλλη εκδοχή είναι αυτή του ημί- αναξιόπιστου παρόχου, όπου το cloud δεν εμφανίζει κενά ως προς την υποδομή του, αλλά ως προς τα μέρη της εταιρείας που απαρτίζουν τον πάροχο του cloud. Διευκρινίζοντας, ένα τέτοιο μέρος μιας εταιρείας, που παρέχει ένα νέφος, μπορεί να είναι ένας τρέχων ή παρελθοντικός υπάλληλος της, συνεργάτης της, εργολάβος της, επιχειρηματικός της εταίρος ή οποιοσδήποτε μπορεί να έχει πρόσβαση στα αρχεία της εταιρείας. Ο τρόπος, που ενεργεί αυτός ο κακόβουλος εσωτερικός χρήστης (malicious insider) [45], είναι με τη μη εξουσιοδοτημένη και σύμφωνη πρόσβαση στα αρχεία από τον ίδιο τον πάροχο και αποσκοπεί, συνήθως, στο χρηματικό κέρδος, μόνο προς όφελος του.

Ακολούθως, προβάλλονται μερικές έμπρακτες εφαρμογές στην καθημερινότητα των εταιριών αναφορικά με την εσωτερική παραβίαση δεδομένων :

Παραβίαση ιδιωτικού απορρήτου σε τομείς υγειονομικής περίθαλψης [46]

Όπως είναι ευρύτερα γνωστό, κάποιοι τομείς, όπως αυτοί της ιατρικής, επιβάλλουν το προσωπικό απόρρητο και την ασφάλεια των δεδομένων του πελάτη σε μεγαλύτερο βαθμό απ’ ότι κάποιων άλλων τομέων. Τι γίνεται όμως , όταν επέρχεται η ανάπτυξη της τεχνολογίας και εγκαθιδρύεται η χρήση νεφών για τη διατήρηση ιστορικού ενός ασθενή;
Τυπικές οντότητες σ’ ένα σύστημα υγείας, που βασίζεται στο cloud, είναι ασθενείς, νοσοκομειακό προσωπικό (γιατροί, νοσοκόμες, φαρμακεία, νοσοκομειακό προσωπικό, εργαστηριακό προσωπικό, ασφαλιστικές εταιρείες και πάροχοι cloud). Λόγω της κατανεμημένης αρχιτεκτονικής του cloud, το ηλεκτρονικό ιατρικό ιστορικό των ασθενών αποθηκεύεται και κοινοποιείται σε πολλούς τρίτους παρόχους. Επομένως, τα δεδομένα είναι ευαίσθητα και εκτεθειμένα σε μη εξουσιοδοτημένη πρόσβαση και επιθέσεις. Παραδείγματος χάρη, ένας γιατρός, που εργάζεται σε μία ιδιωτική κλινική, έχει πρόσβαση τόσο στα αρχεία των ασθενών του, όσο και στα αρχεία ολόκληρης της κλινικής ως προνομιούχος χρήστης. Εκείνος μπορεί να χρησιμοποιήσει τα προσωπικά

δεδομένα των ασθενών, προκειμένου να τα προωθήσει (χωρίς τη συγκατάθεση των ασθενών) σε διάφορες νομικές οντότητες, όπως φαρμακευτικές ή ασφαλιστικές εταιρείες, και σε μη νόμιμες οντότητες, για να του αποφέρουν συμπληρωματικό εισόδημα, ή, ακόμη, να κάνει χρήση των πληροφοριών για δικό του προσωπικό όφελος, λόγου χάρη να ανοίξει ένα δικό του ιατρείο, έχοντας αποκομίσει χωρίς καμία προσπάθεια ένα ευρύτερο πελατολόγιο.

Εν κατακλείδι, το πιο ανασφαλές κομμάτι για τους παρόχους είναι αυτό των αντιγράφων ασφαλείας, που εμπεριέχει τα περισσότερο ευαίσθητα τμήματα πληροφοριών ενός πελάτη και είναι το πιο εύκολα αποσπάσιμο, ακόμα και από άτομα χωρίς ιδιαίτερες γνώσεις προγραμματισμού. Εν συνεχεία, κατατάσσεται η καταγραφή δραστηριοτήτων, που εμπεριέχει εξίσου ευαίσθητα δεδομένα, αλλά χρήζει γνώσεων ανωτέρας πληροφορικής για την αποκρυπτογράφηση τους. Ενώ, τέλος, η ανάλυση δεδομένων μπορεί να καταταγεί και σε μία όχι τόσο βλαβερή παραβίαση, ανάλογα το σκοπό .

6. Τεχνικές για τη διασφάλιση της ιδιωτικότητας

Με την πάροδο των χρόνων, ολοένα και περισσότερες επιχειρήσεις χρησιμοποιούν τα υπολογιστικά νέφη στις δραστηριότητες τους, σύμφωνα με το CSA (Cloud Security Alliance). Παρόλα αυτά , ως ένα νέο τεχνολογικό μέσο η παρουσία του ελλοχεύει πολλούς κινδύνους ασφαλείας, όπως έχει προαναφερθεί σε προηγούμενα κεφάλαια. Σε αυτήν την ενότητα, θα διερευνηθούν μερικοί από τους τρόπους διασφάλισης της ιδιωτικότητας ενός δυναμικού περιβάλλοντος υπολογιστικού νέφους, τόσο από τους παρόχους, όσο και από τους καταναλωτές. Ωστόσο , οι πάροχοι υπηρεσιών υπολογιστικού νέφους πολλές φορές δε γνωρίζουν τους ακριβείς τύπους ασφαλείας που απαιτούνται, προκειμένου να προστατευθούν οι διακομιστές τους. Παρακάτω, αναλύονται μερικές προσεγγίσεις αναφορικά με το πώς μπορούν να αποφευχθούν οι διάφοροι κίνδυνοι.

6.1 Μοντέλα Προστασίας υπολογιστικών νεφών

Όπως έχει προαναφερθεί, με τη χρήση νεφών μπορούμε να συναντήσουμε διάφορες προκλήσεις. Παρακάτω συναντούμε μερικές από αυτές σε ένα ευρύτερο γενικό πλαίσιο και προτείνουμε πως μπορούν να διαχειριστούν τέτοιου είδους απειλές.

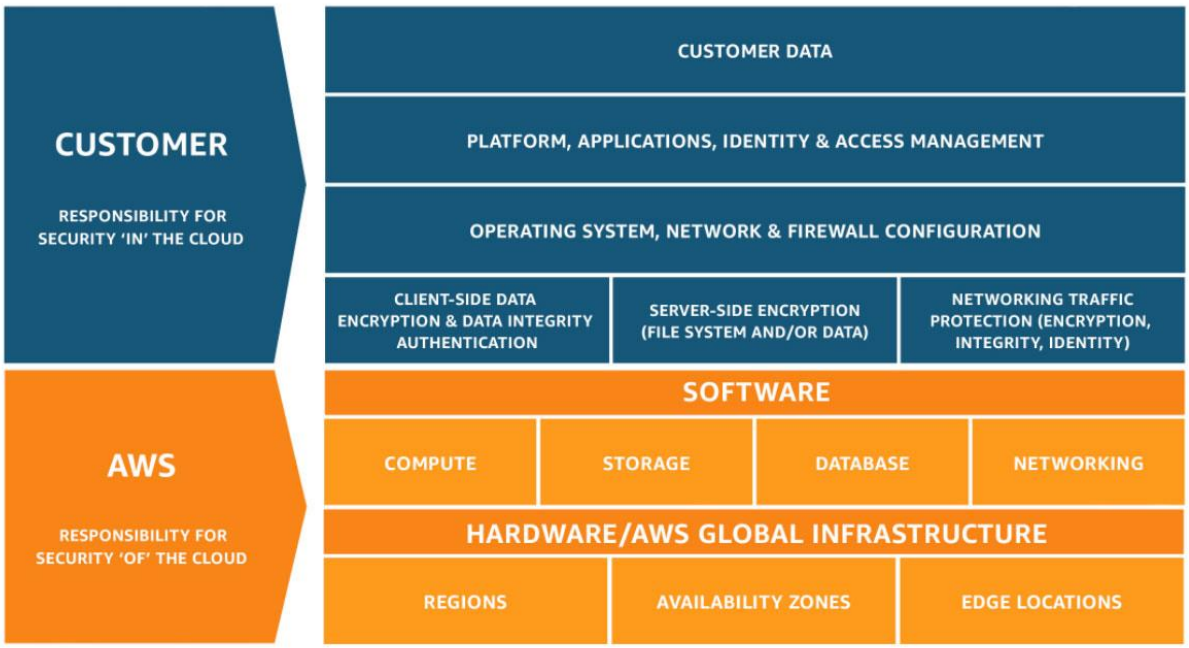
- Δυναμικό περιβάλλον : Η ελαστική φύση του περιβάλλοντος ενός υπολογιστικού νέφους, χρόνο με το χρόνο, καθιστά πιο δύσκολη την ορατότητα των διάφορων εικονικών παρουσιών. Η προστασία τέτοιων δυναμικών περιβαλλόντων απαιτεί την αδιάκοπη αναζήτηση , αξιολόγηση και προληπτική δράση σε θέματα ασφαλείας .
- Περιμετρικοί ορισμοί : Ο αυξανόμενος φόρτος εργασίας σε περιβάλλοντα cloud είναι, πολλές φορές, κατακερματισμένος σε διάφορες γεω-τοποθεσίες και περιβάλλοντα, κάτι που συνεπάγεται μία αναποτελεσματική κεντρική διαχείριση στα περιουσιακά στοιχεία.

- Απώλεια ελέγχου σε θέματα φυσικής ασφάλειας : όσο οι οργανισμοί χάνουν τον έλεγχο της φυσικής ασφάλειας λόγω του φόρτου , τόσο η ευθύνη προστασίας μετατοπίζεται στο χέρι του πελάτη.

Ακολούθως, αναπτύσσονται μερικά από τα μοντέλα ασφαλείας που ακολουθούνται από τις διάφορες εταιρείες.

6.2 Μοντέλο κοινής ευθύνης (Shared Responsibility model)

Στο μοντέλο κοινής ευθύνης είναι αναπόφευκτα αναγκαίο για τον κάθε οργανισμό, να παρακολουθεί, να αναγνωρίζει και να αποκαθιστά τυχόν εσφαλμένες διαμορφώσεις, που δημιουργήθηκαν στα επιμέρους κομμάτια του υπολογιστικού του νέφους [47] [48]. Επεξηγώντας, η ασφάλεια και η συμμόρφωση είναι κοινή ευθύνη τόσο του εκάστοτε παρόχου (π.χ. AMAZON) [47], όσο και του πελάτη-χρήστη. Αυτό έχει ως αποτέλεσμα την αμφότερη ανακούφιση του λειτουργικού φόρτου και για τα δύο μέρη. Από τη μία, ο πάροχος πρέπει να λειτουργεί, να διαχειρίζεται και να ελέγχει τα στοιχεία από το λειτουργικό σύστημα του κεντρικού υπολογιστή και το επίπεδο εικονικοποίησης, έως και τη φυσική ασφάλεια των εγκαταστάσεων στις οποίες λειτουργεί η υπηρεσία του. Επιπροσθέτως, ο πάροχος μπορεί να θεσπίζει κάποιους περιορισμούς στον εν δυνάμει πελάτη, προκειμένου να του δώσει πρόσβαση στην υπηρεσία του (π.χ. να έχει εφαρμόσει ο χρήστης συγκεκριμένα λογισμικά προστασίας στον υπολογιστή του). Ενώ, από την άλλη ο πελάτης έχει την ανάληψη ευθύνης τόσο κατά την είσοδο του στις διάφορες εικονικές υπηρεσίες, όσο και στη διαχείριση αυτών, στη διάρκεια παραμονής του σε αυτές. Αναλυτικότερα, είναι αναγκαίο από μεριάς πελατών να γίνονται οι απαραίτητες αναβαθμίσεις, αναβαθμίσεις ασφαλείας, ανάπτυξη/ εγκατάσταση τειχών προστασίας . Επιπλέον, θα πρέπει οι τελευταίοι να ενεργούν προσεκτικά ως προς τις διάφορες επιλογές τους, καθώς κάθε παρεχόμενη υπηρεσία διαφέρει. Ενώ, τέλος, και τα δύο μέρη θα πρέπει να συμμορφώνονται στους ισχύοντες νόμους και κανονισμούς.



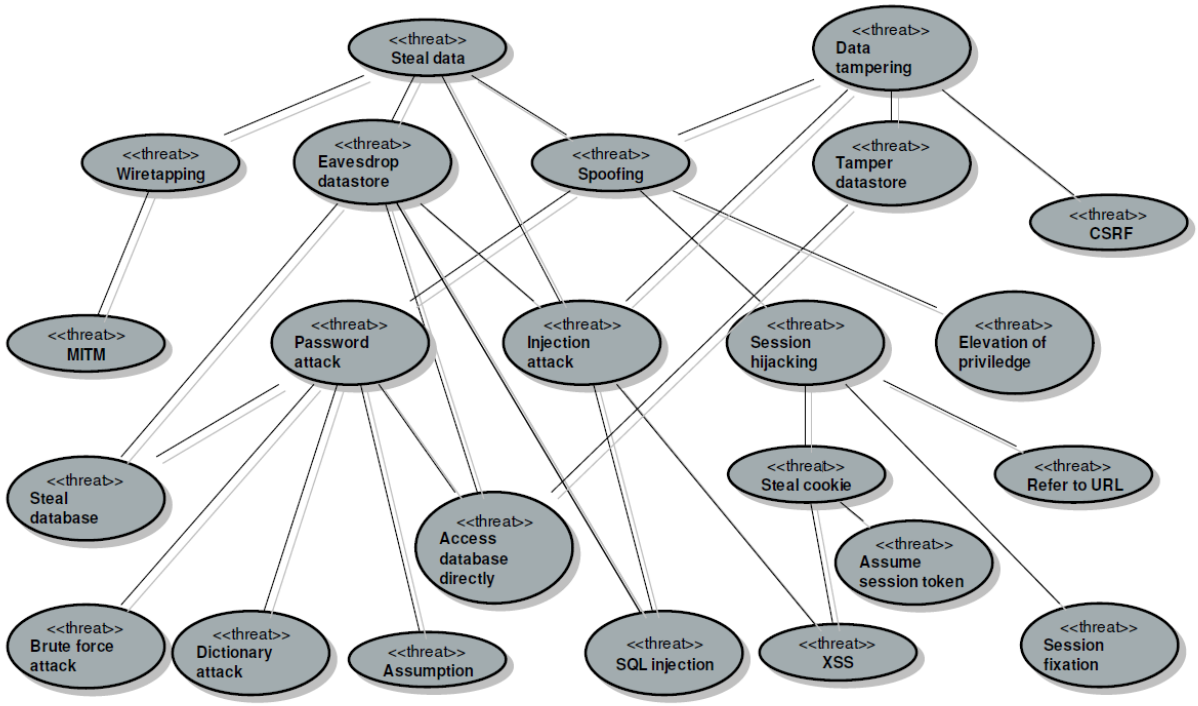
Εικόνα 17: *Μοντέλο Κοινής Ευθύνης*
Πηγή: https://aws.amazon.com/compliance/shared-responsibility-model/

6.3 Μοτίβο Απειλής Νέφους (Cloud threat pattern)

Σε αυτήν την περίπτωση τυπικές λειτουργίες ασφαλείας και ευθύνης διεξάγονται και τοποθετούνται ως ένα μοτίβο προστασίας αντιμέτρων του cloud. Αυτό συμβαίνει, διότι οι πάροχοι δε γνωρίζουν πού μπορεί να υπάρχει ακριβώς το πρόβλημα, επειδή δεν υπάρχουν καθιερωμένες σχέσεις μεταξύ των λειτουργιών και των επιμέρους στοιχείων τους, όπως επίσης υπάρχει και έλλειψη πληροφοριών σχετικά με την ασφάλεια. Τα αντίμετρα και οι τυπικές απειλές ενάντια στα συστήματα ασφαλείας του νέφους μπορούν να αποσαφηνιστούν, οι πληροφορίες σχετικά με τα επιμέρους μέρη παρόχου και χρήστη μπορούν να περιγραφούν, και, εν τέλει, μπορεί να θεσπιστεί το ανάλογο αντίμετρο ασφαλείας και να δοθεί λύση στο πρόβλημα [49].

6.3.1 Δομή λειτουργίας cloud threat pattern

Η δομή αυτού του μοτίβου είναι βασισμένη στο «Δέντρο απειλής» [50]. Η παρακάτω εικόνα *(Εικόνα 17)* παρουσιάζει τη δομή των απειλών, υπό μορφή δενδροειδούς ανάλυσης. Αν μία απειλή Απειλή-παιδί (Απ) είναι ένας θυγατρικός κόμβος μίας Απειλής-γονέα (Αγ), τότε η Απ αντιπροσωπεύει την κατάσταση ή την μέθοδο που επιτυγχάνει η Αγ. Υπάρχουν δύο τύποι σχέσης. Το «και» ή το «ή». Αυτό το μοτίβο περιέχει μόνο το «ή» στις σχέσεις του. «Ή» σημαίνει ότι μία Αγ είναι πιθανή να συμβεί, εάν μία από τις Απ είναι δυνατή. Οι περισσότερες από τις απειλές εμφανίζονται στην ταξινόμηση απειλών στην ιστοσελίδα της WASC (Web Application Security Consortium) [51].



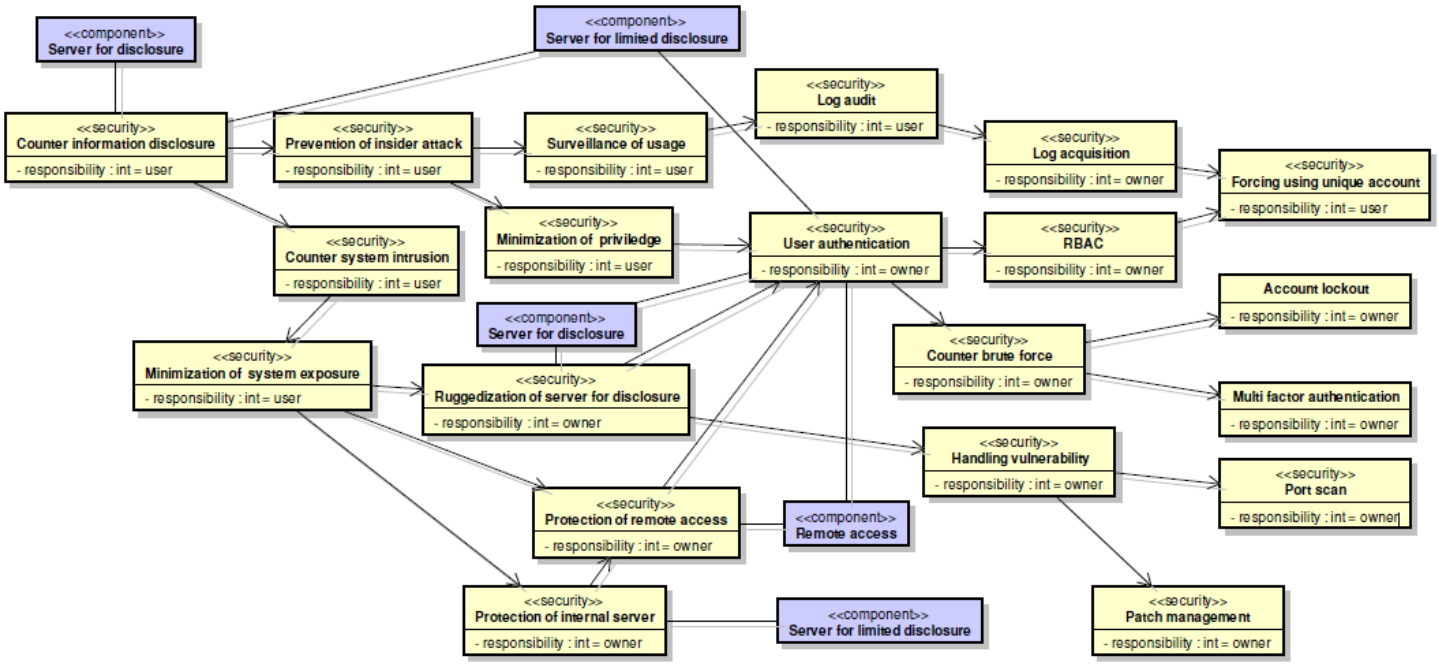
Εικόνα 18: *Μοτίβο Απειλής Υπολογιστικού Νέφους*
Πηγή: Y. W. N. K. Takao Okubo, «Threat and Countermeasure Patterns for Cloud 978-1-4799-6328-7/14,» 2014.

6.4 Μοτίβο Αντίμετρων Νέφους (Cloud Countermeasure Pattern)

Τυπικές διαδικασίες ασφαλείας και ευθύνης μπορούν να οριστούν ως μοτίβο αντιμέτρων. Όπως έχει προαναφερθεί, συνήθως, υπάρχει έλλειψη πληροφόρησης για τα πιθανά μέτρα ασφαλείας . Αν, όμως, οι απειλές είναι γνωστές, τότε μπορούν να προσδιοριστούν αντιστοίχως και τα αντίμετρα ασφαλείας. Συνδυάζοντας το Cloud threat pattern με το Countermeasure Pattern μπορεί εύκολα να αποδοθεί λύση σε κάθε πρόβλημα.

6.4.1 Δομή Cloud Countermeasure Pattern

Στο επακόλουθο σχήμα φαίνεται η δομή του Countermeasure Pattern. Κατηγορίες με την επισήμανση «security» αναπαριστούν τα αντίμετρα ασφαλείας και κατηγορίες με την επισήμανση «component» αναπαριστούν τα επιμέρους συστατικά-στοιχεία του συστήματος. Κάθε κατηγορία αντιμέτρων έχει την



Εικόνα 19: *Μοτίβο Αντίμετρων Υπολογιστικού Νέφους*

Πηγή: Y. W. N. K. Takao Okubo, «Threat and Countermeasure Patterns for Cloud 978-1-4799-6328-7/14,» 2014.

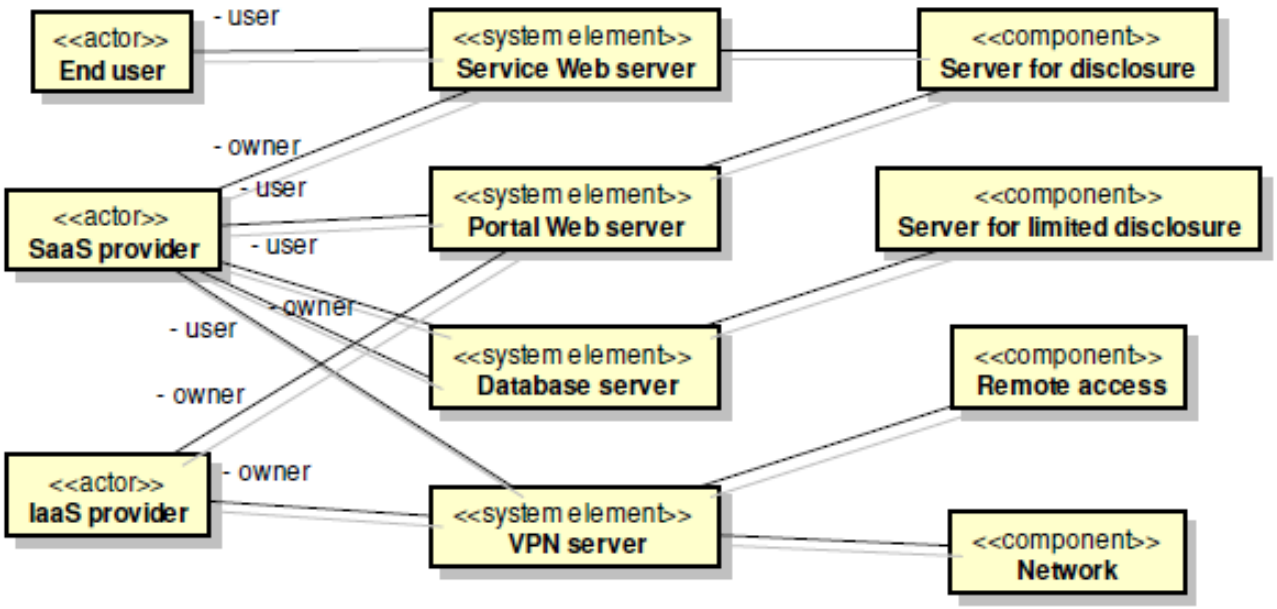
ιδιότητα να αναγνωρίζει ποιος είναι υπεύθυνος για το αντίμετρο (παρουσιάζεται ως χαρακτηριστικό με την επισήμανση «responsibility»). Αν ένα αντίμετρο είναι συνδεδεμένο απευθείας μ' ένα στοιχείο, τότε το αντίμετρο πρέπει να εφαρμοστεί σε αυτό το στοιχείο, λαμβάνοντας υπόψη τον υπεύθυνο του προβλήματος, που παρουσιάζεται στο αντίμετρο. Από την άλλη, αν ένα αντίμετρο είναι συνδεδεμένο με άλλα αντίμετρα ασφαλείας, τότε θα πρέπει να ληφθούν υπόψη και όλα τα συνδεόμενα με αυτό αντίμετρα, καθώς και τα επιμέρους στοιχεία, ώστε να βρεθούν όλοι οι υπαίτιοι και να εφαρμοστούν όλες οι απαραίτητες ενέργειες ασφαλείας στα αντίστοιχα στοιχεία. Συμπεραίνουμε ότι, πολλές φορές, τα προβλήματα είναι αλληλένδετα και δε θα πρέπει να παραλείπονται παράπλευρες διασυνδέσεις, διότι θα χάνεται η πηγή/οι πηγές ενός προβλήματος, δημιουργώντας άλλα μεγαλύτερα. Τα cloud της Fujitsu [52] ακολουθούν τέτοιου είδους μοτίβα.

6.5 Μοτίβο Ενδιαφερόμενων Μερών Νέφους (Cloud Stakeholder Pattern)

Ένα cloud stakeholder pattern μπορεί να προσδιοριστεί βασισμένο στο metamodeling. Μετά-μοντελοποίηση είναι η ανάλυση, η κατασκευή και η ανάπτυξη των πλαισίων, κανόνων, περιορισμών, μοντέλων και θεωριών που ισχύουν και είναι χρήσιμα στη μοντελοποίηση μιας προκαθορισμένης κατηγορίας προβλημάτων. Το συγκεκριμένο μοτίβο έρχεται να επιλύσει τα προβλήματα που έχουν δημιουργηθεί, λόγω της μη υπάρχουσας σχέσης των ενδιαφερομένων μερών (stakeholders) και τα στοιχεία του συστήματος (system elements) ως προς την ευθύνη ασφάλειας. Άρα, εφόσον προσδιοριστούν οι σχέσεις μεταξύ των δύο αυτών μερών, τότε θα προσδιοριστεί και το σε ποιον ανήκει η ευθύνη, και, εν τέλει, θα μπορεί να τεθεί το ανάλογο αντίμετρο, όπως αυτό έχει παρουσιαστεί ανωτέρω. Να διευκρινιστεί ότι το συγκεκριμένο μοτίβο έχει εφαρμογή σε IaaS και SaaS, αλλά όχι σε PaaS [53].

6.5.1 Δομή του Stakeholder Pattern

Το επερχόμενο σχήμα *(Εικόνα 20)* βοηθά στην κατανόηση του εν λόγω μοτίβου. Υπάρχουν τέσσερις τύποι διακομιστών, «system element», για ένα σύστημα cloud (web service, Portal web, Database και VPN). Για κάθε έναν από αυτούς τους διακομιστές, υπάρχει ένας διπλός ρόλος «actor» , αυτός του κατόχου «owner» και αυτός του χρήστη «user». Επιπλέον, κάθε διακομιστής παίζει έναν ή περισσότερους ρόλους για τα συστατικά μέρη, «components». Εν κατακλείδι, εφόσον προσδιοριστούν οι μεταξύ τους σχέσεις και με τον συνδυασμό των 2 ανωτέρω μοτίβων μπορούμε να προσδιορίσουμε τον απαιτούμενο τρόπο ασφαλείας για κάθε πάροχο ή και χρήστη cloud.



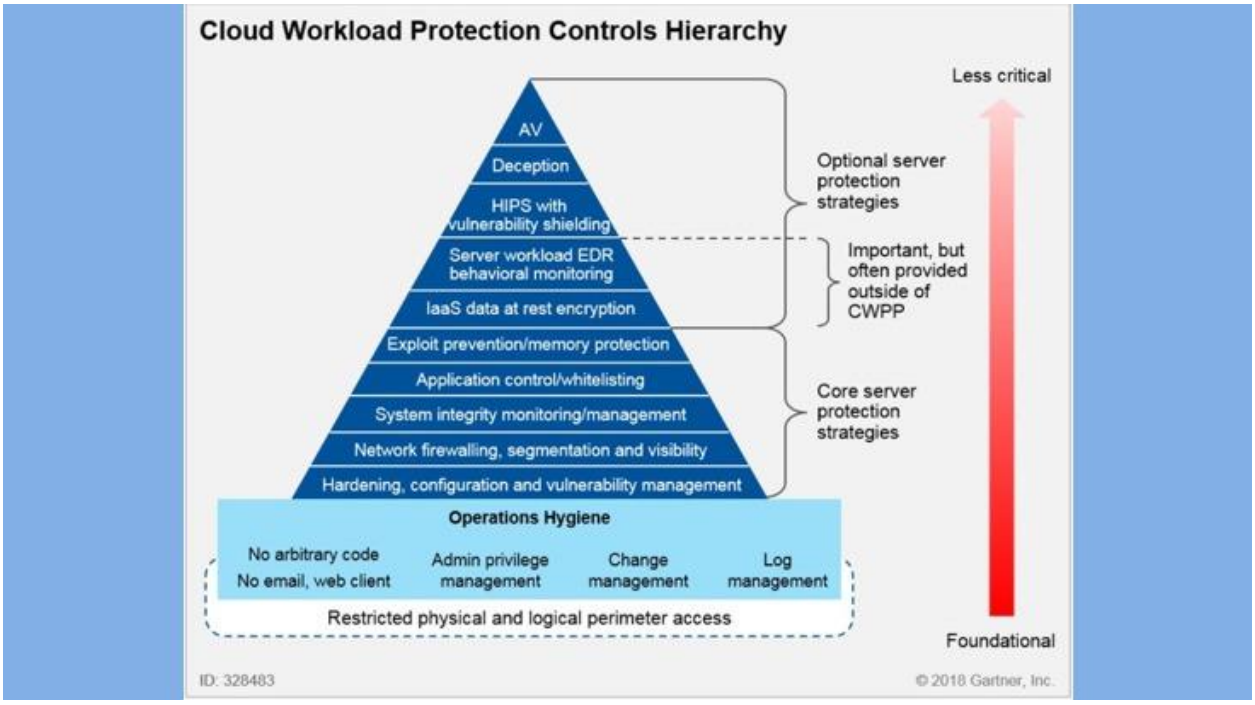
Εικόνα 20: *Μοτίβο Ενδιαφερομένων Στο Υπολογιστικό Νέφος*
Πηγή: Y. W. N. K. Takao Okubo, «Threat and Countermeasure Patterns for Cloud 978-1-4799-6328-7/14,» 2014.

6.6 Νέφος Αποφυγής της Απειλής (Cloud threat defense)

Το Cloud threat defense είναι ένα ενοποιημένο εγγενές σύννεφο ως μία επεκτάσιμη μορφή του αρχικού νέφους. Επικεντρώνεται στο τελικό σημείο και στην ασφάλεια του ίδιου του αρχικού νέφους διά μέσω των αρχείων συνεχούς καταγραφής ελέγχου, ώστε να δημιουργηθεί ένα ενοποιημένο εργαλείο ασφαλείας μέσα στο ίδιο το νέφος και να επιφέρει την κατάλληλη ορατότητα σε πιθανές απειλές, πληροφορίες σχετικά με τις απειλές και προληπτική βοήθεια αποκατάστασης. Σκοπός αυτού είναι η επιτυχής αναγνώριση των απειλών και η στοχευμένη εξόντωση αυτών μέσα από τα στοιχεία καταγραφής, που συλλέγονται από τις διάφορες πηγές [48].

6.6.1 Ιεραρχία ελέγχου άμυνας φόρτου εργασίας Cloud

Όπως σε όλους τους τομείς, έτσι και εδώ, η ιεραρχία προτεραιοτήτων παίζει σημαντικό ρόλο στη διαχείριση προστασίας φόρτου εργασίας . Με βάση τον οδηγό Gartner, το παρακάτω σχήμα *(Εικόνα 20)* βοηθά τις επιχειρήσεις να βάλουν σε μία



Εικόνα 21: *Ιεραρχία Ελέγχου Φόρτου Εργασίας υπολογιστικού Νέφους*
Πηγή: Gartner Μάρτιος 2018

τάξη τις περισσότερο αναγκαίες στρατηγικές ασφαλείας, ως προς τις λιγότερο σημαντικές για το δημόσιο σύννεφο.

6.6.2 Προσέγγιση

Οι παραδοσιακές λύσεις ασφαλείας, που χρησιμοποιούνται ακόμα και σήμερα, προβλέπουν μεγάλη κατανάλωση μνήμης. Ενώ οι διακομιστές cloud τείνουν να είναι αμετάβλητοι και η οποιαδήποτε λύση ασφαλείας έχει μεγάλο αποτύπωμα στη μνήμη και το δίσκο, η εξάρτηση των λύσεων από τον πυρήνα καταναλώνει μεγάλη επεξεργαστική ισχύ και είναι «όλεθρος» για την αξιοποίηση της μεθόδου γρήγορης ανάπτυξης (quick agile deployment workflow).
Η συγκεκριμένη λύση, ως προς την αρχιτεκτονική, προτείνει μια διαφορετική προσέγγιση στην ασφάλεια του νέφους. Αυτή επικεντρώνεται στην ανίχνευση πιθανών απειλών, παρά στην πρόληψη αυτών. Θεωρείται κατά τη συγκεκριμένη προσέγγιση ότι η αντικατάσταση ευπαθών μερών των διακομιστών είναι ευκολότερη από την επιδιόρθωση αυτών. Η λύση είναι βασισμένη στις εξής δύο μεθοδολογίες: της αμετάβλητης πολιτικής (των Immutable Servers), και της μηδενικής εμπιστοσύνης (των Zero-Trust) [48].

- ✓ **Αμετάβλητοι διακομιστές (Immutable Servers)**
  Η λύση χρησιμοποιεί το σκεπτικό των αμετάβλητων διακομιστών, ως μία από τις ενέργειες αποκατάστασης. Η βασική ιδέα είναι ότι, αντί να αντικατασταθεί ο υπάρχων διακομιστής, όταν εντοπιστεί μία απειλή , είναι προτιμότερο να δημιουργηθεί ένας νέος με όλες τις προδιαγραφές ελέγχου και ασφαλείας, καθότι αυτό αυξάνει την αξιοπιστία αναφορικά με την υποδομή και ελαχιστοποιεί τις διάφορες προκλήσεις για διαμόρφωση των επιμέρους στοιχείων.

- ✓ **Μηδενικής εμπιστοσύνης (Zero Trust)**
  Η εν λόγω μεθοδολογία αναλύει αδιάκοπα τις διαμορφώσεις, τα αρχεία καταγραφής πρόσβασης χρήστη και τα αρχεία καταγραφής τελικού σημείου,

με την ικανότητα υποβολής «μηδενικής εμπιστοσύνης» σε κάθε σημείο. Η αρχή της μεθοδολογίας είναι « never trust, always verify». Αν σε κάποιο σημείο εντοπιστεί οποιαδήποτε απόκλιση από το προκαθορισμένο και μη συμμόρφωση σε αυτό, τότε ενεργοποιούνται αυτόματα, χωρίς περαιτέρω λήψη αποφάσεων, διαμορφωμένες ενέργειες, όπως απομόνωση δικτύου, καταγγελία ή ανάκληση προνομίων κ.λπ.

6.6.3 Δομή cloud threat defense

Ο τρόπος, με τον οποίο λειτουργεί η συγκεκριμένη λύση, είναι να συγκεντρώνει, αφενός, τα πρωταρχικά αρχεία καταγραφής (τα άμεσα σχετιζόμενα με τη χρήση της υπηρεσίας που χρησιμοποιεί ο πελάτης) από διάφορες πηγές, όπως αρχεία καταγραφής πρόσβασης χρήστη (user access logs), NetFlow, τελικό σημείο(endpoint logs) auth και syslogs, αρχεία καταγραφής εφαρμογών(application logs), container ασφαλείας προμηθευτών(security vendor logs), και αφετέρου τα επιπρόσθετα συνοδευτικά αρχεία καταγραφής (backend logs), όπως γεωγραφικά, τμήματα δικτύου, αναγνωριστικά εικόνας κ.λπ., που συγκροτούν τα προσωπικά δεδομένα του χρήστη. Τα αρχεία καταγραφής που αφορούν το δεύτερο σκέλος, αναλύονται συνέχεια από το νέφος, προκειμένου να βρεθούν τυχόν ύποπτες δραστηριότητες σε αυτά και να πραγματοποιηθούν οι απαραίτητες ενέργειες αποκατάστασης [48].

6.6.4 Στάδια υλοποίησης

i. Ανίχνευση δεδομένων του cloud threat defense

Αρχικά, το cloud threat defense ανιχνεύει τον φόρτο εργασίας, τα αρχεία καταγραφής πρόσβασης, τα αρχεία καταγραφής δικτύου, μέσω των υπηρεσιών εύρεσης κακόβουλου λογισμικού. Χρησιμοποιεί, δηλαδή, υπηρεσίες εγγενών νεφών, χωρίς, όμως, να περιορίζεται σε αυτά, υπηρεσίες, όπως τα Amazon CloudWatch [54], AWS CloudTrail [55], Amazon VPC [56], AWS Lambda [57], Kinesis [58], Amazon S3 [59], Amazon Redshift [60] και τη Μηχανική Μάθηση

(Machine Learning), προκειμένου να δημιουργήσει έναν «κουβά» δεδομένων, μέσω του οποίου το Analytics και η Μηχανική Μάθηση μπορούν να συνδεθούν και να εντοπίσουν τάσεις και απειλές στο τελικό σημείο και στις υπηρεσίες του νέφους [48].

ii. Αξιολόγηση της στάσης ασφαλείας

Κατά το δεύτερο στάδιο, γίνεται η αξιολόγηση του φόρτου εργασίας, η οποία είναι μεταφρασμένη σε όρους των ελέγχων που γίνονται μέσω του τείχους προστασίας στο τμήμα δικτύου, στο οποίο βρίσκεται, γνωστά και ως τρωτά σημεία, που βασίζονται στο λειτουργικό σύστημα/ έκδοση πυρήνα και στην κατάσταση λύσεων, που έχουν αναπτυχθεί κατά το τρίτο μέρος ελέγχου από την υπηρεσία εύρεσης κακόβουλου λογισμικού.

iii. Αναγνώριση απειλών ασφαλείας

Το cloud threat defense εφαρμόζει την ανάλυση δεδομένων στα δεδομένα που συλλέχθηκαν στα παραπάνω βήματα στο μοντέλο ασφάλειας, ώστε να αποδοθεί ο βαθμός κενών ασφαλείας στο σύννεφο και να διευκρινιστεί το ποσοστό κινδύνου από τις απειλές που εντοπίστηκαν. Επίσης, στο στάδιο αυτό προτείνονται πιθανοί τρόποι επίλυσης με συγκεκριμένες ενέργειες αποκατάστασης, τόσο για τη μείωση του ίδιου φαινομένου, όσο και την αποφυγή παρόμοιων προβλημάτων ασφαλείας μελλοντικά.

iv. Επιδιόρθωση ζητημάτων ασφαλείας

Εν συνεχεία, παρέχονται διορθωτικές δράσεις για την αποκατάσταση προβλημάτων που εντοπίστηκαν με μηχανισμούς αυτόματης αποκατάστασης, όπως η απομόνωση παραβιασμένων πόρων, η ενημέρωση του τελικού σταδίου ασφαλείας, ως ανατροφοδότηση για επόμενα σφάλματα – παραβιάσεις , και, τέλος, η αυτόματη διόρθωση σε τυχόν ανασφαλείς αλλαγές στις ρυθμίσεις του τείχους προστασίας.

6.6.5 Συνοπτικός πίνακας – Δείγματα κανόνων για την ανίχνευση υπηρεσιών

ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΙΧΝΕΥΣΗΣ	ΚΑΝΟΝΕΣ
ΕΥΡΕΤΙΚΕΣ (HEURISTICS)	Αποτυχημένες προσπάθειες σύνδεσης πέρα από το προκαθορισμένο όριο
	Πολλαπλές προσπάθειες σύνδεσης απομακρυσμένης πρόσβασης από τοποθεσίες υψηλού κινδύνου
	Υψηλός όγκος εξερχόμενων συνδέσεων / ροής δεδομένων από μία καθορισμένη γραμμή βάσης
	Ασυνήθιστη σύνδεση σε μία εποχή-περίοδο, που δεν είναι καθιερωμένη για έναν χρήστη
	Προσπάθεια σύνδεσης από μία τοποθεσία, που δεν γνωστή ως συνήθης τοποθεσία σύνδεσης χρήστη
ΑΜΕΤΑΒΛΗΤΗ ΠΟΛΙΤΙΚΗ (IMMUTABLE POLICY)	Προσπάθεια για αλλαγές σε ευαίσθητα αρχεία διαμόρφωσης συστήματος/ εκκίνησης
	Προσπάθειες αλλαγής στο Τείχος Προστασίας των Windows/ Linux Iptables
	Προσπάθειες εγκατάστασης νέων εφαρμογών, που δεν είναι στη λίστα των επιτρεπόμενων
ΕΥΠΑΘΕΙΑΣ – ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ (VULNERABILITIES)	Συνεχής παρακολούθηση της χαρτογράφησης των αναφορών NIST/ CVE για ευάλωτες εφαρμογές και βιβλιοθήκες
ΔΙΑΜΟΡΦΩΣΗ ΕΛΕΓΧΟΥ (CONFIGURATION CHECKS)	Αλλαγές στους κανόνες του τείχους προστασίας του νέφους από τον προμηθευτή
	Αλλαγές στις διαμορφώσεις του νέφους που δεν εμπίπτουν στις γνωστές πολιτικές συμμόρφωσης
	Δημιουργία νέων στοιχείων τα οποία έχουν ανασφαλείς πολιτικές πρόσβασης
ΜΗΔΕΝΙΚΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ (ZERO-TRUST)	Αν ανιχνευτεί μία ύποπτη δραστηριότητα από ένα antivirus, τότε θα υπάρξει δυσπιστία σε όλους τους διακομιστές, που δημιουργούνται από το ίδιο πρότυπο μηχανήματος
	Αν εντοπιστούν ανωμαλίες στο δίκτυο ενός μηχανήματος, τότε θα υπάρξει δυσπιστία σε όλους τους διακομιστές κάτω από την ίδια πολιτική τείχους προστασίας δικτύου

Πίνακας 2 Δείγματα κανόνων για την ανίχνευση υπηρεσιών

Deepak R Bharadwaj, Anamika Bhattacharya, Manivannan Chakkaravarthy Cloud Threat Defense – a Threat Protection and Security Compliance Solution 978-1-5386-9441-1/18

7. Συμπεράσματα

Κάνοντας, λοιπόν, αυτή την εκτεταμένη επισκόπηση στο θέμα της ιδιωτικότητας στο υπολογιστικό νέφος, καταλάβαμε πως το cloud είναι ένα τεχνολογικό επίτευγμα, που έχει κάνει τις ζωές μας ακόμη πιο εύκολες. Είναι διαδεδομένο παγκοσμίως, έχει βοηθήσει και θα συνεχίσει να βοηθά πολύ στην ανάπτυξη του τομέα της πληροφορικής. Με το πέρασμα των χρόνων, έχει γίνει ένα αναπόσπαστο κομμάτι της ζωής τόσο των φυσικών, όσο και των νομικών προσώπων, και αυτό έχει σαν αποτέλεσμα οι χρήστες του να μη θέλουν να το εγκαταλείψουν.

Για την ώρα, υπάρχουν τέσσερα μοντέλα ανάπτυξης, το Δημόσιο, το Ιδιωτικό, το Υβριδικό, της Κοινότητας, με άλλα να είναι πιο οικονομικά, άλλα περισσότερο ασφαλή και άλλα να συνδυάζουν τόσο τα καλά, όσο και τα λιγότερο καλά στοιχεία αυτών. Πέρα από τα μοντέλα ανάπτυξης, υπάρχουν και τα μοντέλα υπηρεσιών, που χωρίζονται σε τρεις επιμέρους κατηγορίες: Λογισμικό ως υπηρεσία , Πλατφόρμα ως υπηρεσία και Υποδομή ως υπηρεσία. Η πρώτη κατηγορία χρησιμοποιείται, κυρίως, για οικονομική και γρήγορη έναρξη δραστηριοτήτων από μία εταιρεία, ενώ η δεύτερη θα μπορούσε να χρησιμοποιηθεί σε δεύτερο χρόνο, καθότι αφορά την ανάπτυξη περισσότερο πολύπλοκων εφαρμογών, που απαιτούν περισσότερους πόρους και γνώσεις. Τέλος, η τελευταία κατηγορία μπορούμε να πούμε ότι προσαρμόζεται αναλόγως των αναγκών τόσο του χρήστη, όσο και του παρόχου.
Η υποδομή ενός νέφους για τη σωστή λειτουργία του βασίζεται σε δύο πολύ σημαντικούς παράγοντες, στα κέντρα φιλοξενίας δεδομένων και στην εικονικοποίηση των μηχανημάτων, προκειμένου οι πάροχοι νέφους να είναι έτοιμοι να υποδεχθούν τους υπεράριθμους εν δυνάμει χρήστες τους.

Τα νέφη κρύβουν διάφορα οφέλη, όπως την αποδοτικότητα του κόστους, τον ανεξάντλητο χώρο αποθήκευσης, την ανάκτηση αντιγράφων ασφαλείας, την εύκολη πρόσβαση από οποιαδήποτε τοποθεσία και συσκευή και την ταχεία ανάπτυξή τους. Παρότι η χρήση του υπολογιστικού νέφους επιφέρει πολλά πλεονεκτήματα, δεν πρέπει να ξεχνάμε ότι η υιοθέτηση των υπηρεσιών του φέρνει αντιμέτωπες τις επιχειρήσεις και τους ιδιώτες με ένα πολύ θεμελιώδες ζήτημα, την ασφάλεια και την ιδιωτικότητα των δεδομένων τους. Το ζήτημα αυτό αποτελεί ένα

τεράστιο πρόβλημα στην σημερινή παγκοσμιοποιημένη οικονομία του διαδικτύου. Η ιδιωτικότητα, ως έννοια, διαμοιράζεται μεταξύ της εδαφικής, του ατόμου και της πληροφοριακής, κάτι το οποίο καταπατάται διαρκώς, και η Ευρωπαϊκή Ένωση έκανε μία προσπάθεια διαχείρισης του φαινομένου, θεσπίζοντας τον Γενικό Κανονισμό για την προστασία προσωπικών δεδομένων. (GDPR).

Όπως είδαμε, υπάρχουν αρκετοί τρόποι με τους οποίους μπορεί να παραβιαστεί η ιδιωτικότητα των χρηστών του υπολογιστικού νέφους, τόσο από κακόβουλους χρήστες του διαδικτύου κατά τη μετάδοση δεδομένων από και προς έναν διακομιστή ή μέσω της αποθήκευσης δεδομένων εντός της υποδομής ενός νέφους, όσο και από αναξιόπιστους παρόχους cloud, που αφήνουν ανοιχτά παραθυράκια υποκλοπής δεδομένων. Οι επιθέσεις που πραγματοποιούνται κατά τη μετάδοση δεδομένων, όπως οι επιθέσεις man-in-the-middle, υποκλοπές sniffing, τροποποίησης και επανάληψης, υπόκεινται στην έλλειψη προστασίας του δικτύου του χρήστη και του παρόχου, με συνηθέστερη αυτή του πρώτου, καθότι οι πάροχοι είναι περισσότερο υποψιασμένοι. Οι απειλές απορρήτου μέσα στην υποδομή του νέφους είναι κατά κύριο λόγο ευθύνη του παρόχου, διότι πρόκειται για υποκλοπές δεδομένων που είναι αποθηκευμένα στις υποδομές του cloud. Αυτού του είδους οι απειλές προέρχονται, συνήθως, από αδυναμίες στην εικονικοποίηση των εξυπηρετητών. Τέτοιες είναι, οι Cross-VM επιθέσεις και οι επιθέσεις στα προγράμματα εικονικοποίησης (hypervisor attacks). Επιπλέον, οι πάροχοι μπορεί να θεωρηθούν αναξιόπιστοι, όταν ένας εξωτερικός χρήστης υποκλέψει οποιαδήποτε πληροφορία μέσω των αντιγράφων ασφαλείας, της καταγραφής δραστηριοτήτων χρήστη και της ανάλυσης δεδομένων, ενώ παράλληλα έχει στην κατοχή του κάποιο άτομο από το εσωτερικό περιβάλλον της εταιρείας, που δρα κακόβουλα και αποσκοπεί σε δικό του κέρδος (malicious insider).

Ερευνώντας τους τρόπους παραβίασης της ιδιωτικότητας, αντιλαμβανόμαστε ότι το μερίδιο ευθύνης στο ζήτημα της ιδιωτικότητας στο υπολογιστικό νέφος το μοιράζονται και τα δύο μέρη, δηλαδή και ο πάροχος και ο πελάτης – χρήστης. Από τη μία, ο πάροχος, είναι ο κύριος υπεύθυνος για την ασφάλεια των δεδομένων και ως απόρροια είναι υποχρεωμένος να χρησιμοποιεί, να εξελίσσει και να αναπτύσσει μοντέλα προστασίας υπολογιστικών νεφών, όπου αυτό κρίνεται απαραίτητο. Τα διάφορα μοντέλα, που έχουν δημιουργηθεί για την αποφυγή απειλών ιδιωτικότητας από τους παρόχους, είναι το μοντέλο κοινής ευθύνης, το μοτίβο

απειλής νέφους, το μοτίβο αντίμετρων νέφους ,το μοτίβο ενδιαφερόμενων μερών νέφους και το νέφος αποφυγής της απειλής. Αυτά το μοντέλα αλλάζουν, στην ουσία, τον τρόπο αντιμετώπισης των αρχείων καταγραφής δραστηριοτήτων σε όπλο υπέρ των παρόχων, διασφαλίζοντας την προστασία του δικτύου του παρόχου των δεδομένων αυτού. Από την άλλη, ο χρήστης, εισερχόμενος στις διάφορες πλατφόρμες cloud, είναι απαραίτητο να βρίσκεται σε διαρκή επαγρύπνηση αναφορικά με τους πιθανούς κινδύνους, που μπορεί να συναντήσει, οπότε και θα πρέπει να ενημερώνεται διαρκώς για τους τρόπους που μπορούν να του επιφέρουν στο μέγιστο την προστασία των ευαίσθητων προσωπικών του δεδομένων. Τέλος, ο εκάστοτε χρήστης είναι αναγκαίο να είναι πολύ προσεκτικός ως προς την επιλογή παρόχου cloud που θα κάνει.

7.1 Μελλοντικές ερευνητικές κατευθύνσεις

Με την πάροδο των χρόνων τόσο οι κυβερνητικές μονάδες, όσο και οι επιχειρηματικές τείνουν να απλουστεύσουν και να αντικαταστήσουν διαδικασίες που χρειάζονται φυσική παρουσία πρόσωπο με πρόσωπο. Αυτό επιτυγχάνεται κυρίως με την αξιοποίηση του νέφους, ενισχύοντας την τηλεργασία και αυξάνοντας τους κινδύνους παραβίασης της ιδιωτικότητας προσωπικών δεδομένων. Εφάμιλλη της αύξησης κινδύνων είναι η αύξηση της προστασίας και διασφάλισης της ιδιωτικότητας, εφόσον λειτουργούμε σε ένα δυναμικό περιβάλλον. Άρα, όλοι οι ανωτέρω τρόποι διασφάλισης της ιδιωτικότητας που παρουσιάστηκαν χρήζουν συνεχούς εξέλιξης και βελτίωσης ανάλογα με το πως και προς ποια κατεύθυνση διευρύνονται οι τρόποι παραβίασης της ιδιωτικότητας. Αντιστοίχως, θα πρέπει το κράτος να αναδιαμορφώνει το κανονιστικό πλαίσιο μέσα στο οποίο θα κινούνται οι οργανισμοί, διαφορετικά θα υπάρχουν και θα είναι εκμεταλλεύσιμες οι πόρτες διαφυγής για τους κακόβουλους χρήστες και τους αναξιόπιστους παρόχους. Παραδείγματος χάριν, κάποιος που πλέον εργάζεται από το σπίτι του και η εργασία του απαιτεί σύνδεση σε υπολογιστικά νέφη, δεν είναι απαραίτητο ότι έχει λάβει όλα τα μέτρα ασφαλείας στο τοπικό του δίκτυο με αποτέλεσμα να εκτίθεται τόσο ο ίδιος, όσο και ο οργανισμός με τον οποίο συνεργάζεται. Επομένως, ο οργανισμός θα μπορούσε να του παρέχει εξοπλισμό

και εφαρμογές που να εξασφαλίζουν στον εργαζόμενο τις απαιτούμενες προδιαγραφές ασφαλείας.

Οι τεχνολογίες τις πληροφορικής επεκτείνονται μέρα με τη μέρα. Εκτός από το υπολογιστικό νέφος που είδαμε, το Διαδίκτυο των πραγμάτων (Internet of Things - IoT) είναι μία από αυτές. Το Διαδίκτυο των πραγμάτων είναι ένα σύστημα αλληλοσυνδεόμενων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών και αντικειμένων, που είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες με σκοπό τη σύνδεση και τη δυνατότητα ανταλλαγής δεδομένων μέσω ενός δικτύου χωρίς να απαιτείται η ανθρώπινη αλληλεπίδραση με υπολογιστή.

Το cloud computing και το IoT έχουν γίνει δύο πολύ στενά συνδεδεμένες μελλοντικές τεχνολογίες διαδικτύου, με τη μία να παρέχει στην άλλη μια πλατφόρμα επιτυχίας. Πώς όμως η μία τεχνολογία αλληλοεπιδρά στην άλλη;

Όπως προαναφέρθηκε, οι συσκευές IoT λόγω της διασύνδεσής τους παράγουν έναν πολύ μεγάλο όγκο δεδομένων με αποτέλεσμα να επιβαρύνεται το διαδίκτυο. Εδώ έρχεται να μας λύσει τα χέρια η Νεφοϋπολογιστική, η οποία παίζει καταλυτικό ρόλο στην αποθήκευση, την επεξεργασία και τη μεταφορά δεδομένων στα διάφορα νέφη. Σαν αποτέλεσμα, αυτό αποσυμφορεί την κατανάλωση υπολογιστικής ισχύος πάνω στα ίδια τα μηχανήματα, ενώ ταυτόχρονα μπορεί να αυξήσει την απόδοση τους από τα αποτελέσματα που θα προκύψουν. Η ενσωμάτωση των τεχνολογιών IoT και Cloud Computing από τις διάφορες επιχειρήσεις και οργανισμούς έχει αρχίσει να γίνεται αναπόσπαστο κομμάτι αυτών ως προς την επεκτασιμότητά τους. Παρόλα αυτά, εφόσον οι τεχνολογίες αυτές βασίζονται στο διαδίκτυο και στον τρόπο λειτουργίας των νεφών, ερχόμαστε αντιμέτωποι με το αρχικό ζήτημα, το ζήτημα της παραβίασης της ιδιωτικότητας των προσωπικών δεδομένων. Για παράδειγμα, υπάρχουν πολλές κάμερες ασφαλείας, δημόσιες ή ιδιωτικές, οι οποίες όταν υπάρχει ένα συμβάν ανίχνευσης κίνησης, στέλνουν το καταγεγραμμένο υλικό απευθείας στον αποθηκευτικό χώρο του νέφους.
Για να αποφευχθεί αυτό το φαινόμενο θα πρέπει να χρησιμοποιηθούν περισσότερες κρυπτογραφικές μέθοδοι, καθώς και να γίνει μεγαλύτερη έρευνα γύρω από το θέμα αυτό. Η κρυπτογράφηση είναι μία διέξοδος που θα βοηθήσει

στην ενίσχυση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των δεδομένων ενάντια στους πιθανούς κακόβουλους χρήστες. Επιπλέον, η εγκατάσταση νέων εφαρμογών αισθητήρων, η ενημέρωση, και ο απομακρυσμένος επαναπρογραμματισμός όλων των κόμβων στο δίκτυο, ακολουθώντας όλα τα πρωτόκολλα, θα αποτρέψει οποιαδήποτε κακόβουλη εγκατάσταση. Κλείνοντας, η αναγκαιότητα της διερεύνησης των τρόπων διασφάλισης της ιδιωτικότητας θα μπορούσε να αναδειχθεί ως ένας από τους βασικούς τομείς ενασχόλησης τα επόμενα χρόνια.

8. Βιβλιογραφία

[1] ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ, «ΕΝΗΜΕΡΩΤΙΚΟ ΣΗΜΕΙΩΜΑ,» 27 Σεπτεμβρίου 2012. [Ηλεκτρονικό]. Available: https://ec.europa.eu/commission/presscorner/detail/el/MEMO_12_713.

[2] T. G. Peter Mell, «The NIST Definition of Cloud,» Σεπτέμβριος 2011. [Ηλεκτρονικό]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final.

[3] «Google Apps,» [Ηλεκτρονικό]. Available: https://gsuite.google.com/.

[4] «Dropbox,» [Ηλεκτρονικό]. Available: https://www.dropbox.com/.

[5] «Google App Engine,» [Ηλεκτρονικό]. Available: https://cloud.google.com/appengine.

[6] «Microsoft Windows Azure,» [Ηλεκτρονικό]. Available: https://azure.microsoft.com/.

[7] «Amazon Web Services,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/.

[8] B. Paul, D. Boris, F. Keir, H. Steven, H. Tim, H. Alex, N. Rolf, P. Ian και W. Andrew, «Xen and the Art of Virtualization,» Οκτώβριος 2003.

[9] «Rackspace technology,» [Ηλεκτρονικό]. Available: https://www.rackspace.com/.

[10] «Orange Business Services,» [Ηλεκτρονικό]. Available: https://www.orange-business.com/.

[11] «Oracle Integrated Cloud Applications and Platform Services,» [Ηλεκτρονικό]. Available: https://www.oracle.com/.

[12] «IBM,» [Ηλεκτρονικό]. Available: https://www.ibm.com/.

[13] «Alibaba Cloud,» [Ηλεκτρονικό]. Available: https://eu.alibabacloud.com/.

[14] L. C. a. R. B. Q. Zhang, «“Cloud computing: state-of-theart and research challenges”, Journal of Internet Services and Applications, 1, pp. 7-18, 2010.».

[15] D. S. K. Dr Frank Alleweldt, «‘’Cloud Computing’’, 2012».

[16] G. V. S. L. T. T. T. Haselmann, «CLOSER’11, The First International Conference

on Cloud Computing and Services Science, INSTICC (2011)».

[17] A. Vahdat, M. Al-Fares και N. Farrington, «Scale-Out Networking in the Data Center,» Ιούλιος 2010. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/220290754_Scale-Out_Networking_in_the_Data_Center.

[18] S. Srinarayan, «VIRTUALIZATION: A REVIEW AND FUTURE DIRECTIONS Executive Overview,» Μάιος 2011. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/303854444_VIRTUALIZATION_A_REVIEW_AND_FUTURE_DIRECTIONS_Executive_Overview.

[19] «Virtual Box,» [Ηλεκτρονικό]. Available: https://www.virtualbox.org/.

[20] «Kernel Virtual Machine,» [Ηλεκτρονικό]. Available: https://www.linux-kvm.org/.

[21] «Docker,» [Ηλεκτρονικό]. Available: https://www.docker.com/.

[22] «Linux Containers,» [Ηλεκτρονικό]. Available: https://linuxcontainers.org/.

[23] S. D. Warren και L. D. Brandeis, «The Right to Privacy,» *Harvard Law Review, Vol. 4, No. 5.,* 1890.

[24] A. F. Westin, Privacy and freedom, New York: Atheneum, 1967, 1967.

[25] «Νόμος 2472/1997 - ΦΕΚ Α-50/10-4-1997,» 1997. [Ηλεκτρονικό]. Available: https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/n-2472-1997.html.

[26] «Νόμος 4624/2019 - ΦΕΚ 137/Α/29-8-2019,» [Ηλεκτρονικό]. Available: https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html.

[27] «ΟΔΗΓΊΑ (ΕΕ) 2016/680 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ,» 27 Απρίλιος 2016. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

[28] «ΟΔΗΓΊΑ (ΕΕ) 2016/681 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ,» 27 Απριλίου 2016. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/eli/dir/2016/681/oj.

[29] S. M. K. Q. Suhail Qadir, «Information Availability: An Insight into the Most

Important Attribute of Information Security,» 2016. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/301319816_Information_Availability_An_Insight_into_the_Most_Important_Attribute_of_Information_Security.

[30] A. R. P. Defiana Arnaldy, «Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack,» *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)* .

[31] T. Ristenpart, E. romer, H. Shacham και S. Savage, «Hey, You, Get Off of My Cloud: Exploring Information Leakage in,» Chicago, Illinois, USA., 2009.

[32] V. Varadarajan, Y. Zhang, T. Ristenpart και M. Swift, «A Placement Vulnerability Study in Multi-Tenant Public Clouds,» Ιούλιος 2015. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/280062212_A_Placement_Vulnerability_Study_in_Multi-Tenant_Public_Clouds.

[33] A. Litchfield και A. Shahzad, «Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable,» Ιούνιος 2016. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/303821673_Virtualization_Technology_Cross-VM_Cache_Side_Channel_Attacks_make_it_Vulnerable.

[34] D. Perez-Botero, J. Szefer και R. B. Lee, «Characterizing hypervisor vulnerabilities in cloud computing servers,» Μάιος 2013. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/262273414_Characterizing_hypervisor_vulnerabilities_in_cloud_computing_servers.

[35] J. P. Barrowclough και R. Asif, «Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures,» 11 Ιούνιος 2018. [Ηλεκτρονικό]. Available: https://www.hindawi.com/journals/scn/2018/1681908/.

[36] «Crowdstrike,» [Ηλεκτρονικό]. Available: https://www.crowdstrike.com/blog/venom-vulnerability-details/.

[37] A. van Cleeff, W. Pieters και R. Wieringa, «Security Implications of Virtualization: A Literature Study vol. 3, pp. 353–358,,» σε *Πroceedings of the 12th IEEE International Conference on Computational Science and Engineering*, 2009.

[38] L. Adhianto, S. Banerjee και M. M. Fagan, «HPCTOOLKIT: Tools for performance

analysis of optimized parallel programs,» αρ. Concurrency and Computation: Practice and Experience, vol. 22,, Ιανουάριος 2010.

[39] S. K. Majhi and S. K. Dhal, «Study on Security Vulnerability,» αρ. Proceedings of the 1st International Conference on Information Security and Privacy 2015pp. 55–60.

[40] P. Papadimitriou, «Privacy Aspects for Cloud Computing».

[41] A. K. D. a. R. H. Shams Zawoad, «Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service,» 2015.

[42] M. B. a. B. Yee, «"Forward-security in private-key cryptography," Topics in Cryptology, CT-RSA 2003, pp. 1–18,» 2003.

[43] «"Forward integrity for secure audit logs," Technical report, Computer Science and Engineering Department,» 1997.

[44] P. G. Belle Selene Xia, «Review of business intelligence through data analysis,» *Benchmarking An International Journal 21(2):300-311*, 2015.

[45] S. C. M. G. Adrian Duncan, «Insider Attacks in Cloud Computing 978-0-7695-4745-9/12».

[46] A. Abbas και S. U. Khan, «A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds,» 2013. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/document/6714376.

[47] Amazon, «Amazon AWS,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/.

[48] A. B. M. C. Deepak R Bharadwaj, «Cloud Threat Defense – a Threat Protection and Security Compliance Solution 978-1-5386-9441-1/18,» 2018.

[49] Y. W. N. K. Takao Okubo, «Threat and Countermeasure Patterns for Cloud 978-1-4799-6328-7/14,» 2014.

[50] F. S. a. W. Snyder, «Threat Modeling,» Microsoft Press, 2004.

[51] «WASC,» [Ηλεκτρονικό]. Available: https://www. webappsec.org/.

[52] T. S. a. T. S. M. Okuhara, «Security architectures for cloud,» *Fujitsu Science Technology Journal, vol. 46, no. 4, pp. 397–402,* 2010.

[53] E. F.-B. D. H. F. B. M. Schumacher, «Security Patterns: Integrating Security and Systems,» 2006.

[54] «Amazon CloudWatch,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/cloudwatch/.

[55] «AWS CloudTrail,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/cloudtrail/.

[56] «Amazon VPC,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/vpc/.

[57] «AWS Lambda,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/lambda/.

[58] «Amazon Kinesis,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/kinesis/.

[59] «Amazon S3,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/s3/.

[60] «Amazon Redshift,» [Ηλεκτρονικό]. Available: https://aws.amazon.com/redshift.